TUGAS AKHIR – KS141501

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO/IEC 27001:2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

EVALUATING INFORMATION SECURITY MANAGEMENT USING INDEKS KEAMANAN INFORMASI (KAMI) BASED ON ISO/IEC 27001:2013 AT DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

FIRZAH ABDULLAH BASYARAHIL
NRP 5213 100 069

Dosen Pembimbing I
Hanim Maria Astuti, S.Kom., M.Sc.

Dosen Pembimbing II
Bekti Cahyo Hidayanto, S.Si., M.Kom.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS 141501

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO/IEC 27001:2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

Firzah Abdullah Basyarahil
NRP 5213 100 069

Dosen Pembimbing 1:
Hanim Maria Astuti, S.Kom., M.Sc.

Dosen Pembimbing 2:
Bekti Cahyo Hidayanto, S.Si., M.Kom.

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 141501

EVALUATING INFORMATION SECURITY MANAGEMENT USING INDEKS KEAMANAN INFORMASI (KAMI) BASED ON ISO/IEC 27001:2013 AT DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

Firzah Abdullah Basyarahil
NRP 5213 100 069

Supervisor 1 :
Hanim Maria Astuti, S.Kom., M.Sc.

Supervisor 2 :
Bekti Cahyo Hidayanto, S.Si., M.Kom.

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institute of Technology Sepuluh Nopember
Surabaya 2017

LEMBAR PENGESAHAN

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO/IEC 27001:2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

TUGAS AKHIR

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

Oleh:

Firzah Abdullah Basyarahil
5213 100 069

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO/IEC 27001:2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

TUGAS AKHIR

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

Oleh :

Firzah Abdullah Basyarahil
5213 100 069

Disetujui Tim Penguji : Tanggal Ujian : 10 Januari 2017
Periode Wisuda: Maret 2017

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

Bekti Cahyo Hidayanto, S.Si., M.Kom. **(Pembimbing 2)**

Sholiq, S.T., M.Kom., M.SA **(Penguji 1)**

Eko Wahyu Tyas, S.Kom., MBA **(Penguji 2)**

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO/IEC 27001:2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

Nama Mahasiswa : Firzah A. Basyarahil
NRP : 5213 100 069
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing 1: Hanim Maria Astuti, S.Kom., M.Sc.
Dosen Pembimbing 2: Bekti Cahyo Hidayanto S.Si., M.Kom.

ABSTRAK

DPTSI merupakan sebuah direktorat untuk menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki oleh ITS. Semua kegiatan teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di DPTSI ITS. Menurut UU. No. 12 Tahun 12 Ttg. Perguruan Tinggi, misi mencari, menemukan, dan menyebarluaskan kebenaran ilmiah tersebut dapat diwujudkan apabila perguruan tinggi di kelola berdasarkan suatu Tata kelola perguruan tinggi yang baik (Good University Governance). Pengelolaan Informasi merupakan salah satu aspek dalam Good University Governance, termasuk kualitas dan keamanan pengelolaan informasi.

Salah satu upaya yang dapat dilakukan untuk meningkatkan kualitas dari keamanan informasi, kementrian Kominfo membuat alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Penggunaan Indeks KAMI ini juga diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif.

Hasil dari penggunaan Indeks KAMI versi 3.1 di DPTSI ITS ini adalah tingkat ketergantungan penggunaan sistem elektronik sebesar 26 dari total skor 50 dan masuk kedalam kategori Tinggi dimana sistem elektronik adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 249 dari 645 dan berada pada kategori tidak layak. Dari hasil tersebut maka dibuat rekomendasi berdasarkan kontrol ISO 27002:2013 untuk pertanyaan-pertanyaan yang mendapat nilai kurang.

Kemudian rekomendasi dari penelitian ini dapat dijadikan sebagai bahan pertimbangan dan evaluasi bagi pihak DPTSI ITS Surabaya dalam melakukan perbaikan yang berkaitan dengan mitigasi atau pencegahan kerentanan keamanan informasi, serta memastikan regulasi dapat dicapai dengan baik dan kebijakan keamanan institusi di masa yang akan datang.

Kata Kunci: Indeks KAMI, ISO 27001:2013, Keamanan Informasi, Manajemen Risiko

EVALUATION OF INFORMATION SECURITY MANAGEMENT USING INDEKS KEAMANAN INFORMASI (KAMI) BASED ON ISO/IEC 27001:2013 IN DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA

Name	**: Firzah A. Basyarahil**
NRP	**: 5213 100 069**
Department	**: Information Systems FTIF -ITS**
Supervisor 1	**: Hanim Maria Astuti, S.Kom., M.Sc.**
Supervisor 2	**: Bekti Cahyo Hidayanto S.Si., M.Kom.**

ABSTRACT

DPTSI is an institution to address the issue of information technology and information systems owned by ITS. All the activities of information technology and information systems focused and developed in DPTSI ITS. According to the Act. No. 12 of 12 about Universities, the mission of searching, finding and disseminating scientific truth can be realized if the college is managed by a governance good college (Good University Governance). Information management is one aspect of the Good University Governance, including the quality and security information management.

One effort that can be done to improve the quality of the information security, the Ministry of Communications and Information Technology makes tools for measuring the level of maturity and completeness of the information security called Information Security Index (KAMI). KAMI index usage is also followed by the implementation of ISO 27001 as an international security standards can help an organization ensure that information security is implemented have been effective.

Result of use Indeks KAMI versi 3.1 at DPTSI ITS is dependence rate an electronics system by 26 from total score

50 and its entry into high category where the electronic system is an integral part of the work process is running. The results of the five areas that assessment has been carried out amounted to 249 from 645 and is in the category is not feasible. From these results we made a recommendation based on the control ISO 27002: 2013, to the questions that scored less.

Then the recommendation from this study can be used as a material consideration and evaluation for the DPTSI ITS in the improvement associated with mitigation or prevention of a security vulnerability information, and ensure the regulation can be achieved by both institutions and security policies in the future.

Keyword: Information Security, ISO 27001:2013, KAMI Index, Risk Management

KATA PENGANTAR

Syukur Alhamdulillah dipanjatkan oleh peneliti atas segala petunjuk, pertolongan, kasih sayang, dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul **EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO/IEC 27001:2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA**

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

- Orang tua penulis yang senantiasa mendoakan dan mendukung, serta kakak-kakak tercinta yang selalu mendorong penulis untuk segera menyelesaikan tugas akhir ini.
- Pihak DPTSI ITS yaitu Ibu Hanim, Bapak Royanna, Ibu Any, Ibu Widya, Bapak Cahya, Mas Wicaq, Mas Jananta, dan Bapak Bustari yang bersedia meluangkan waktunya untuk melakukan wawancara dan mencarikan data-data yang diperlukan untuk tugas akhir ini.
- Ibu Hanim Maria Astuti, S.Kom., M.Sc. dan Bapak Bekti Cahyo Hidayanto, S.Si., M.Kom., selaku dosen pembimbing yang yang telah meluangkan waktu untuk membimbing dan mendukung dalam penyelesaian tugas akhir ini.
- Bapak Bapak Bekti Cahyo Hidayanto, S.Si., M.Kom., selaku dosen wali yang senantiasa memberikan pengarahan selama penulis menempuh masa perkuliahan dan pengerjaan tugas akhir ini.
- Bapak Hermono, selaku admin laboratoriun MSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir ini.

- Teman – teman Lab MSI dan BELTRANIS yang telah memberikan semangat dalam menyelesaikan tugas akhir
- "Keong Club" yang beranggotakan Cahya, Orie, Visha, Mahesti, Niswati, RR, Selina, Yurah, Astrid, Sarah, dan Fian serta "Sayap Kiri" yang beranggotakan Mahda, Cho, Aul, Dini, dan Chele yang selalu memberikan semangat dan menemani penulis saat mengerjakan tugas akhir ini.
- Serta pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir ini.

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

Surabaya, 10 Januari 2017

Penulis

DAFTAR ISI

"Halaman ini sengaja dikosongkan"

DAFTAR TABEL

DAFTAR GAMBAR

“Halaman ini sengaja dikosongkan”

BAB I
PENDAHULUAN

Pada bab pendahuluan ini, akan dijelaskan mengenai sekilas keadaan organisasi, masalah yang menyebabkan studi kasus ini diangkat menjadi tugas akhir, rumusan masalah dari tugas akhir ini, tujuan, dan manfaat yang dapat diambil dari *output* tugas akhir, relevansi, serta sistematika penulisan tugas akhir dengan matakuliah yang ada di Jurusan Sistem Informasi.

1.1 Latar Belakang

Menjaga keamanan informasi berarti pula perlunya usaha dalam memperhatikan faktor-faktor keamanan dari seluruh piranti pendukung, jaringan, dan fasilitas lain yang terkait secara langsung maupun tidak langsung dalam proses pengolahan informasi [1]. Instansi pendidikan di Indonesia juga perlu menerapkan keamanan informasi untuk menghindari adanya pencurian data dan hilangnya data secara sengaja maupun tidak sengaja.

Hal ini juga perlu diterapkan dan diperhatikan di Institut Teknologi Sepuluh Nopemeber Surabaya. ITS membangun sebuah direktorat yang bernama DPTSI untuk menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki. Semua kegiatan teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di DPTSI ITS [2].

Data dari DPTSI menyatakan bahwa ditemukannya beberapa celah keamanan sistem informasi dan jaringan yang cukup berbahaya [3]**.** Gangguan keamanan informasi tersebut juga dirasakan oleh pihak civitas akademika ITS, seperti pembobolan data untuk Sistem Integra ITS dimana para mahasiswa tidak dapat login pada masing-masing akun yang dimiliki. Selain gangguan pada Sistem Integra ITS, hal serupa juga pernah terjadi untuk akun email ITS yang dibobol dan harus dilakukan reset *password* untuk menangani masalah tersebut.

Salah satu upaya yang dapat dilakukan oleh kementrian Kominfo untuk meningkatkan kualitas keamanan informasi pada suatu instansi adalah dengan membuat salah satu alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Indeks KAMI mengacu pada ISO 27001 yang berisi tentang keamanan informasi [4].

ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Ada juga ISO 27002 yang berisi tentang kontrol keamanan yang dapat dijalankan oleh sebuah instansi yang telah mengimplementasikan ISO 27001. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimiliki [1].

Pada tahun 2012 pernah dilakukan penerapan penilaian keamanan informasi dengan menggunakan indeks KAMI di DPTSI ITS [5]. Namun pada penelitian sebelumnya, hanya dilakukan pada sub bagian Keamanan & Jaringan saja dan tidak menyeluruh ke instansi yang bersangkutan [5], sedangkan penerapan Indeks KAMI ini dilakukan untuk pengelolaan keamanan informasi di seluruh bagian instansi yang bersangkutan [6].

Penilaian keamanan informasi dengan menggunakan indeks KAMI hanya pernah dilakukan satu kali di DPTSI dan terbilang sudah cukup lama. Metode yang digunakan pada penilaian keamanan informasi DPTSI pada tahun 2012 juga menggunakan kuesioner penilaian (pertanyaan yang ada di Indeks KAMI) yang diisi oleh responden, sedangkan peneliti mencari temuan-temuan terkait dengan penilaian dan memastikan bahwa hasil temuan sesuai dengan nilai dari kuesioner tersebut. Setelah peneliti memastikan hasilnya, maka dilakukan pembenaran temuan sesuai dengan hasil kepatuhan [5].

Metode penilaian keamanan informasi pada penelitian kali ini akan dirubah, yaitu akan dilakukan penilaian oleh peneliti secara langsung. Peneliti akan mengumpulkan temuan-temuan pendukung untuk melakukan penilaian keamanan informasi sekaligus melakukan penilaian dengan mengisi nilai pada pertanyaan yang ada di Indeks KAMI.

Metode yang digunakan akan dirubah karena evaluasi ini dianjurkan untuk dilakukan oleh orang yang secara langsung bertanggung jawab & berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya [6]. Berhubung di DPTSI sendiri masih belum ada bagian khusus yang melakukan penilaian keamanan informasi menggunakan Indeks KAMI, maka tema ini akan diangkat menjadi sebuah penelitian dan peneliti sendiri yang akan melakukan penilain terhadap kelima area yang ada di Indeks KAMI.

Penilaian Indeks KAMI sebaiknya dilakukan secara periodik waktu tertentu sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu [7] [8]. Faktanya penilaian keamanan informasi di DPTSI terakhir kali dilakukan pada tahun 2012 dan belum dilakukan lagi sampai tahun 2016.

1.2 Perumusan Masaah

Berdasarkan uraian latar belakang diatas, maka rumusan permasalahan yang menjadi fokus utama dan akan diselesaikan dalam Tugas Akhir ini antara lain :

1. Bagaimana menentukan kategori Sistem Elektronik di DPTSI ITS?
2. Berapakah total skor dari penilaian kelima area Indeks KAMI di DPTSI ITS?

3. Bagaimana rekomendasi untuk meningkatkan manajemen keamanan informasi yang ada di DPTSI ITS?

1.3 Batasan Masalah

Dari permasalahan yang disebutkan di atas, batasan masalah dalam tugas akhir ini adalah penilaian kelengkapan & kematangan kerangka kerja keamanan informasi di DPTSI ITS dilakukan di bagian Pusat Pengelolaan & Layanan TIK, Pusat Pengembangan Sistem Informasi, Pusat Infrastruktur & Keamanan Informasi, dan Ketua Direktorat.

1.4 Tujuan Tugas Akhir

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

1. Mengetahui tingkat kategori Sistem Elektronik yang digunakan di DPTSI ITS.
2. Mengetahui nilai kematangan keamanan informasi yang ada di DPTSI ITS.
3. Memberikan rekomendasi kepada pihak DPTSI ITS untuk keamanan informasi yang harus dijlankan.

1.5 Manfaat Tugas Akhir

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

1. Bagi dunia akademis dan evaluator, sebagai referensi untuk penelitian dalam bidang evaluasi manajemen keamanan informasi khususnya di bagian instansi pemerintahan.
2. Bagi DPTSI ITS, sebagai gambaran kondisi kekinian dari manajemen keamanan informasi yang dimiliki sehingga akan selalu dilakukan perbaikan pada sistem manajemen keamanan

informasi yang ada untuk menjamin & meningkatkan kualitas keamanan informasi DPTSI ITS.

1.6 Relevansi

Tugas akhir ini berkaitan dengan mata kuliah Manajemen Risiko Teknologi Informasi, Tata Kelola Teknologi Informasi, dan Keamanan Aset Informasi.

1.7 Sistematika Penulisan

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

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

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

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

BAB IV PERANCANGAN
Bab ini menjelaskan perancangan studi kasus yang diangkat, objek penelitian, perangkat yang dilakukan oleh penulis untuk

mengumpulkan data kondisi kekinian, serta metode pengolahan data.

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

BAB VI HASIL DAN PEMBAHASAN
Bab ini berisi tentang bagaimana kesenjangan yang terjadi antara kondisi kekinian dan kondisi ideal, kemudian menjelaskan bagaimana proses penilaian perangkat keamanan informasi, hasil skor akhir dari penilaian perangkat keamanan informasi, dan rekomendasi yang diberikan untuk area yang nilainya kurang baik.

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

BAB II
TINJAUAN PUSTAKA

Bab ini akan menjelaskan mengenai penelitian sebelumnya dan dasar teori yang dijadikan acuan atau landasan dalam pengerjaan tugas akhir ini. Landasan teori akan memberikan gambaran secara umum dari landasan penjabaran tugas akhir ini.

2.1 Penelitian Sebelumnya

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

Tabel 2.1 Penelitian Terdahulu

Penelitian 1	
Judul Penelitian	Evaluasi Pengelolaan Keamanan Jarinagn di ITS dengan Menggunakan Standar Indeks KAMI Kemenkominfo RI [5]
Nama Peneliti, Tahun Penelitian	Luthfiya Ulinnuha, 2012
Metodologi	- Penelitian dilakukan di DPTSI ITS Sub Bagian Jaringan dengan menggunakan Indeks KAMI versi 2.3 untuk melakukan penilaian perangkat keamanan informasi di DPTSI ITS - Narasumber melakukan penilaian peran TIK dan kelima area Indeks KAMI yang ada di DPTSI ITS

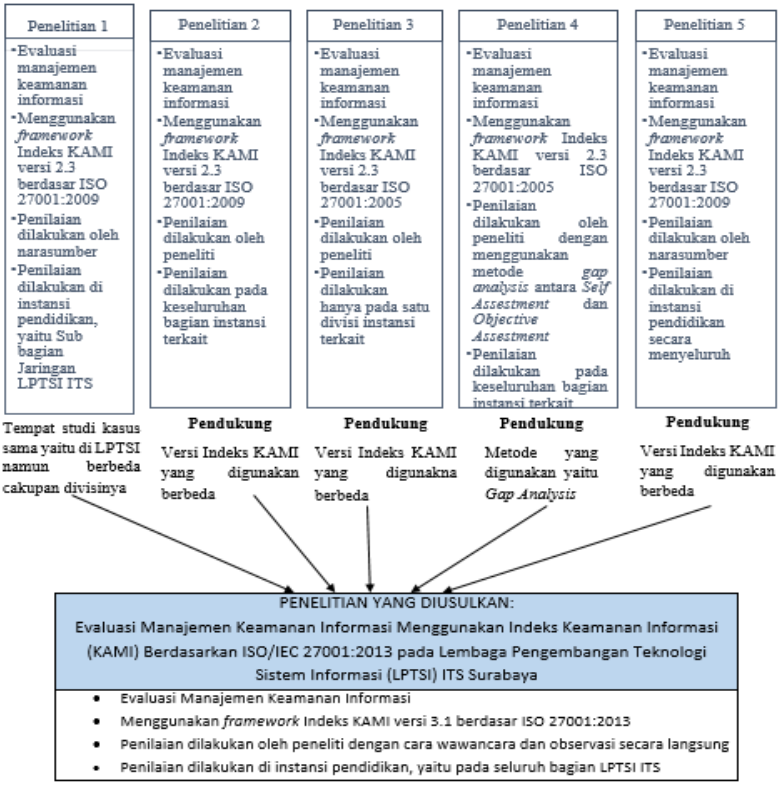
	- Standar yang diacu adalah ISO 27001:2009 - Peneliti mengumpulkan bukti-bukti berupa foto, dokumen, dan logfile
Relevansi Penelitian	Lokasi penelitian kali ini dilakukan di DPTSI ITS untuk keseluruhan bagian bukan hanya pada bagian Sub Jaringan saja. Framework yang digunakan di penelitian kali ini yaitu Indeks KAMI namun dengan versi yang terbaru dan mengacu pada ISO 27001:2013. Metode penilaian yang digunakan berbeda, dimana pada penelitian selanjutnya akan dilakukan penilaian secara langsung oleh peneliti.
Penelitian 2	
Judul Penelitian	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi dan Informatika Surabaya [9]
Nama Peneliti, Tahun Penelitian	Moch. Rashid Ridho, 2012
Metodologi	- Penelitian dilakukan dengan menggunakan Indeks KAMI versi 2.3 dan mengacu pada ISO 27001:2009 - Penilaian peran TIK dan kelima area Indeks KAMI dilakukan sendiri oleh peneliti - Peneliti mengumpulkan bukti pendukung untuk memperkuat hasil wawancara yang dilakukan
Relevansi Penelitian	Metode penelitian yang digunakan sama yaitu penilaian kelima area Indeks KAMI

	akan dilakukan oleh peneliti sendiri. Penelitian dilakukan secara menyeluruh pada instansi yang bersangkutan. Framework yang digunakan di penelitian kali ini yaitu Indeks KAMI namun dengan versi yang terbaru dan mengacu pada ISO 27001:2013.
Penelitian 3	
Judul Penelitian	Evaluasi Keamanan Informasi Pada Divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI) [10]
Nama Peneliti, Tahun Penelitian	Endi Lastyono Putra, 2014
Metodologi	- Penelitian dilakukan dengan menggunakan Indeks KAMI versi 2.3 dan mengacu pada ISO 27001:2005 - Penilaian peran TIK dan kelima area Indeks KAMI dilakukan sendiri oleh peneliti - Peneliti mengumpulkan bukti pendukung untuk memperkuat hasil wawancara yang dilakukan
Relevansi Penelitian	Metode penelitian yang digunakan sama yaitu penilaian kelima area Indeks KAMI akan dilakukan oleh peneliti sendiri. Penelitian dilakukan secara menyeluruh pada instansi yang bersangkutan bukan hanya pada satu divisi saja. Framework yang digunakan di penelitian kali ini yaitu Indeks KAMI namun dengan versi yang terbaru dan mengacu pada ISO 27001:2013.

Penelitian 4	
Judul Penelitian	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur [11]
Nama Peneliti, Tahun Penelitian	Mustaqim Siga, 2014
Metodologi	- Penelitian dilakukan dengan menggunakan Indeks KAMI versi 2.3 dan mengacu pada ISO 27001:2005 - Penilaian peran TIK dan kelima area Indeks KAMI dilakukan dengan menggunakan metode *Gap Analysis* antara *Self Assestment* dan *Objective Assestment* - Peneliti mengumpulkan bukti pendukung untuk memperkuat hasil wawancara yang dilakukan
Relevansi Penelitian	Metode penilaian yang digunakan berbeda dimana penelitian kali ini tidak menggunakan metode *Gap Analysis.* Penelitian dilakukan secara menyeluruh pada instansi yang bersangkutan bukan hanya pada satu divisi saja. Framework yang digunakan di penelitian kali ini yaitu Indeks KAMI namun dengan versi yang terbaru dan mengacu pada ISO 27001:2013.
Penelitian 5	
Judul Penelitian	Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI – SNI ISO/IEC 27001:2009 Studi Kasus Perguruan Tinggi X [12]
Nama Peneliti, Tahun Penelitian	Irawan Afrianto; Taryana Suryana; Sufa'atin, 2015

Metodologi	- Penelitian dilakukan dengan menggunakan Indeks KAMI versi 2.3 dan mengacu pada ISO 27001:2009 - Peneliti mengumpulkan data primer dan sekunder dengan cara wawancara dan penelusuran. Data-data yang diambil berupa dokumen kebijakan TIK, SK, dan buku panduan TIK - Narasumber melakukan penilaian peran TIK dan kelima area Indeks KAMI yang ada di Perguruan Tinggi X
Relevansi Penelitian	Penelitian dilakukan di instansi pendidikan secara menyeluruh bukan hanya pada divisi/ bagian tertentu. Metode penilaian yang digunakan berbeda, dimana pada penelitian selanjutnya akan dilakukan penilaian secara langsung oleh peneliti. Framework yang digunakan di penelitian kali ini yaitu Indeks KAMI namun dengan versi yang terbaru dan mengacu pada ISO 27001:2013.

Berikut ini adalah analisis kesenjangan dari kelima penelitian terdahulu yang menjadi acuan untuk penelitian selanjutnya yang ditampilkan pada Gambar 2.1:



Gambar 2.1 Keterkaitan Penelitian

2.2 Dasar Teori

Bagian ini akan membahas teori dan bahan penelitian lain yang menjadi dasar informasi untuk mengerjakan tugas akhir ini.

2.2.1 Keamanan Informasi

Menurut Sarno dan Iffano, Keamanan informasi merupakan suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin akan timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, dan

mengoptimalkan pengembalian investasi. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing-kan maka semakin besar pula risiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan (Sarno dan Iffano: 2009) [13].

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam sebuah organisasi. Jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut (Whitman & Mattord, 2013) [14]:

- Physical security: keamanan yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- Personal security: keamanan yang overlap dengan physical security dalam melindungi orang-orang dalam suatu organisasi.
- Operational security: keamanan yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- Communications security: keamanan yang bertujuan untuk mengamankan media komunikasi, teknologi komunikasi beserta isinya, dan kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan sebuah organisasi.
- Network security: keamanan yang memfokuskan pada pengamanan peralatan jaringan dan organisasi, jaringan dan isinya, beserta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi tersebut.

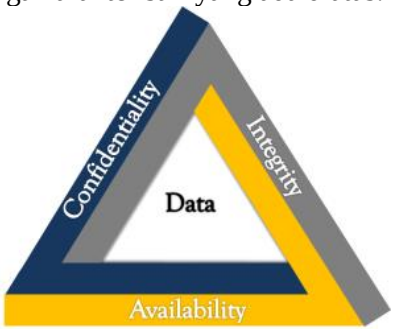
Keamanan informasi juga memiliki 3 karakteristik penting yang disebut dengan singkatan CIA dan akan dijabarkan sebagai berikut:

- Confidentiality/ kerahasiaan: karakteristik ini merupakan landasan utama dalam setiap kebijakan keamanan sistem informasi. Confidentiality ini merupakan seperangkat

aturan yang diberikan, menentukan apakah suatu subjek tertentu dapat mendapatkan akses ke objek tertentu. Karakteristik ini juga merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.

- Integrity/ kepercayaan: merupakan kepercayaan terhadap sebuah informasi yang ada. Dalam konsep ini tercakup data integrity. Keutuhan informasi dapat terwujud jika informasi belum dirubah atau masih asli. Perubahan yang dimaksud dapat berupa perubahan yang terjadi karena kesalahan secara sengaja maupun tidak.
- Availability/ ketersediaan: karakteristik ini yaitu merupakan ketersediaan sumber informasi ketika dibutuhkan. Ketersediaan ini dapat terpengaruh oleh faktor teknis, faktor alam, dan faktor manusia. Meskipun ada tiga faktor penting yang berpengaruh, tetapi umumnya manusia adalah faktor yang paling lemah.

Dari penjabaran diatas, dapat disimpulkan bahwa Confidentiality, Integrity, dan Availability adalah karakteristik yang saling berkaitan dan harus dipenuhi untuk menjaga keamanan informasi. Berikut ini adalah gambaran dari keterkaitan ketiga karakteristik yang ada diatas:



Gambar 2.2 Diagram CIA

Salah satu bentuk dukungan keamanan informasi adalah dengan adanya tata kelola keamanan informasi agar risiko keamanan

informasi dapat dikurangi atau dihindari. Keamanan informasi merupakan aspek penting dari tata kelola organisasi, kinerja TI akan terganggu jika keamanan informasi sebagai aspek penting dari keamanan informasi mengalami masalah terkait kerahasiaannya (confidentiality), keutuhannya (integrity) dan ketersediaannya (availibility).

2.2.2 Sistem Manajemen Keamanan Informasi (SMKI)

Sebuah organisasi harus menerapkan Sistem Manajemen Keamanan Informasi untuk menjamin keamanan aset teknologi informasi dan komunikasi (TIK). Sistem Manajemen Keamanan Informasi adalah kumpulan dari kebijakan dan prosedur untuk mengatur data sensitif milik organisasi secara sistematis. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan [15].

Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah ISO/IEC 27001. Standar ini telah berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat [16].

Implementasi dari SMKI ini meliputi kebijakan, proses, prosedur, struktur organisasi, serta fungsi dari software dan hardware. Pelaksanaan SMKI juga harus langsung dipengaruhi oleh tujuan organisasi, kebutuhan keamanan, dan proses yang digunakan oleh organisasi [17].

Penerapan Sistem Manajemen Keamanan Informasi pada sebuah organisasi juga harus memiliki pedoman yang ditujukan pada pimpinan organisasi. Hal ini telah dinyatakan oleh

Direktorat Sistem Informasi pada tahun 2007 bahwa telah ditetapkan 10 pedoman terbaik untuk penerapan SMKI, namun tidak menutup kemungkinan untuk terjadi perubahan pada pedoman-pedoman yang telah ada. Berikut ini adalah 10 pedoman yang disebutkan [18]:

- Pedoman 1 tentang manajemen umum
- Pedoman 2 tentang kebijakan keamanan yang memenuhi sasaran bisnis
- Pedoman 3 tentang manajemen risiko keamanan informasi yang mengidentifikasi aset kritis diantaranya sistem, jaringan, dan data
- Pedoman 4 tentang arsitektur & desain keamanan berdasar kebutuhan bisnis dan perlindungan aset informasi paling kritis
- Pedoman 5 tentang isu-isu pengguna yang meliputi akuntabilitas & pelatihan serta ekspertis yang memadai
- Pedoman 6 tentang manajemen sistem & jaringan yang meliputi kontrol akses untuk melindungi aset dalam jaringan, integritas *software*, konfigurasi aset, dan *backup* yang terjadwal
- Pedoman 7 tentang otentikasi & otorisasi bagi pengguna aset dan pihak ketiga (kontraktor & penyedia layanan)
- Pedoman 8 tentang pengawasan & audit terhadap kondisi sistem dan jaringan yang ada
- Pedoman 9 tentang keamanan fisik aset informasi dan layanan serta sumber daya TI
- Pedoman 10 tentang rencana keberlanjutan bisnis & pemulihan bencana untuk aset kritis dan dilakukannya tes secara periodik dan pastikan berfungsi secara efektif

2.2.3 Manajemen Risiko Teknologi Informasi

Manajemen risiko merupakan serangkaian aktivitas dalam menganalisis risiko. Risiko tersebut diidentifikasi, dinililai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi risiko tersebut (Stoneburner, 2002) [19].

Tujuan utama dari dilaksanakannya manajemen risiko adalah memberikan pandangan terkait kemungkinan yang bisa terjadi sehingga perusahaan dapat menyusun langkah mitigasi dan evaluasi terkait risiko. Tahapan dalam manajemen risiko berdasarkan (Spremic, 2008) diantaranya [20]:

1. Mengidentifikasi dan mengklarifikasi risiko.
2. Setiap risiko dinilai.
3. Menyusun langkah penaggulangan risiko.
4. Pendokumentasian dan pengimplementasian dari langkah menanggulangi risiko.
5. Pendekatan portfolio risiko TI.
6. Monitoring berkala terhadap tingkat risiko TI dan audit.

Berikut ini adalah diagram alur dari proses manajemen risiko secara umum.

Gambar 2.3 Alur Manajemen Risiko (Budi,2013)

Pada alur proses pelaksanaan Manajemen Risiko, ketika memasuki tahapan penanganan atau aksi apa yang harus diambil, maka terdapat 4 pilihan penanganan terhadap risiko potensial tersebut, yaitu [21]:

- **Take**

  Jika risiko yang ada dirasakan cukup besar dan tidak dapat dihindari, maka perusahaan dapat mengalami dampak yang mengganggu dan bersifat merusak secara alamiah dan seharusnya diambil tindakan take atau menerima risiko tersebut. Contoh risiko yang dapat ditangani dengan tindakan take adalah terjadinya bencana alam, yakni gempa bumi, banjir, badai, dan sebagainya. Sebab perusahaan tentunya tidak dapat melawan alam.

- **Treat**
  Jika risiko yang ada dirasakan dapat ditanggapi dengan tindakan untuk menurunkan tingkat risikonya, maka diambil tindakan Treat untuk mnegontrol risiko tersebut. Tindakan nyatanya adalah dengan menerapkan kontrol atau mitigasi terhadap risiko yang ada sehingga risiko tersebut dapat diturunkan levelnya.
- **Terminate**
  Jika risiko yang ada dirasakan terlalu besar (misalnya dalam rangka membuat suatu produk IT baru), maka dapat diambil tindakan "Terminate" terhadap risiko tersebut, artinya kita harus menghindar dan tidak mau mengambil risiko dengan membuat produk IT baru tersebut, sehingga tindakan nyatanya adalah membatalkan rencana pembuatan produk IT tersebut.
- **Transfer**
  Jika risiko yang ada dianggap akan lebih baik jika dialihkan ke pihak lain yang sesuai dengan bidang ahlinya, misalnya ke pihak asuransi, maka dapat diambil tindakan Transfer terhadap risiko tersebut.

2.2.4 ISO/IEC 27001 sebagai Standar SMKI

ISO 27001 ini merupakan sebuah standar yang dikeluarkan oleh *International Organization for Standardization*. ISO 27001 ini merupakan standar yang ditujukan dapat membantu perusahaan dalam melindungi keamanan aset perusahaan dan untuk melindungi sistem manajemen keamanan informasi (SMKI) [22].

SMKI merupakan sebuah pendekatan yang bersifat sistematis yang bertujuan untuk mengelola informasi penting maupun informasi perusahaan yang bersifat sensitif agar tetap aman. SMKI ini juga memberikan panduan untuk mengelola unsur yang termasuk dalam melakukan pengelolaan informasi penting seperti manusia, proses dan sistem Teknologi Informasi dengan menerapkan proses manajemen risiko yang telah sesuai standar.

ISO 27001 telah dirancang sedemikian rupa sehingga dapat disesuaikan dalam pengaplikasiannya pada organisasi kecil, menengah hingga organisasi besar di sektor apapun dalam rangka melindungi aset informasi penting organisasi tersebut [22].

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, review, pemeliharaan, dan peningkatan SMKI. Model *Plan Do Check Act* (PDCA) diterapkan terhadap struktur keseluruhan SMKI [23].

Pada tahap *Plan* terjadi penetapan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi. Pada tahap *Do* terjadi penerapan dan pengoperasian kebijakan SMKI, kontrol, proses dan prosedur. Pada tahap *Check* dilakukan pengkajian dan pengukuran kinerja proses terhadap kebijakan, sasaran dan praktik dalam menjalankan SMKI. Pada tahap *Act* akan dilakukan perbaikan dan pencegahan berdasar hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI untuk mencapai peningkatan yang berkelanjutan [23].

Persyaratan utama yang harus dipenuhi menyangkut [23]:
- Sistem manajemen keamanan informasi (kerangka kerja, proses, dan dokumentasi)
- Tanggung jawab manajemen
- Audit internal SMKI
- Manajemen tinjau ulang SMKI
- Peningkatan berkelanjutan

2.2.5 Indeks Keamanan Informasi (KAMI) versi 3.1 sebagai Tools SMKI

2.2.5.1 Pengertian Indeks Keamanan Informasi versi 3.1

Indeks KAMI versi 3.1 adalah sebuah tools yang digunakan untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan ISO/IEC 27001:2013 dan gambaran tata kelola keamanan informasi di sebuah organisasi. Indeks KAMI ini dibuat oleh pihak kementrian Kominfo [4]. Alat evaluasi ini tidak digunakan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat yang untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pemimpin instansi [6].

2.2.5.2 Area Penilaian Indeks Keamanan Informasi versi 3.1

Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Evaluasi yang dilakukan dengan menggunakan indeks KAMI ini mencakup 5 target area, yaitu [6]:

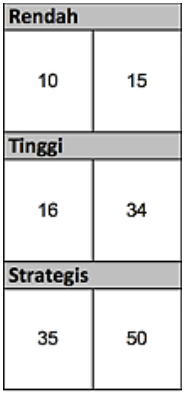
- **Area tata kelola keamanan informasi**
  Pada bagian ini dilakukan evaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi serta tugas dan tanggung jawab pengelola keamanan informasi. Kontrol yang diperlukan adalah kebijakan formal yang mendefinisikan peran, tanggung jawab, kewenangan pengelolaan keamanan informasi dari pimpinan unit kerja sampai ke pelaksana operasional. Termasuk juga adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.

- **Area pengelolaan risiko keamanan informasi**
  Pada bagian ini dilakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Kontrol yang diberlakukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji keefektivitasannya.
- **Area kerangka kerja keamanan informasi**
  Pada bagian ini dilakukan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
  Kontrol yang diperlukan adalah sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektivitas kontrol dan langkah perbaikan.
- **Area pengelolaan aset informasi**
  Pada bagian ini dilakukan evaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Kontrol yang diperlukan adalah bentuk pengamanan terkait keberadaan aset informasi serta keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.
- **Area teknologi dan keamanan informasi**
  Pada bagian ini dilakukan evaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Kontrol yang digunakan adalah strategi terkait dengan tingkatan risiko dan tidak secara eksplisit menyebutkan teknologi atau merk tertentu.

2.2.5.3 Skor Penilaian Indeks Keamanan Informasi versi 3.1

Sebelum dilakukan proses penilaian secara kuantitatif, maka dilakukan proses klasifikasi terlebih dahulu terhadap kategori

Sistem Elektronik. Responden diminta untuk mendeskripsikan Sistem Elektronik yang ada dalam satuan kerjanya secara singkat [6]. Tujuan dari penilaian kategori Sistem Elektronik ini adalah untuk mengelompokkan instansi kedalam ukuran tertentu yang akan ditampilkan dalam Gambar 2.4 [8] :



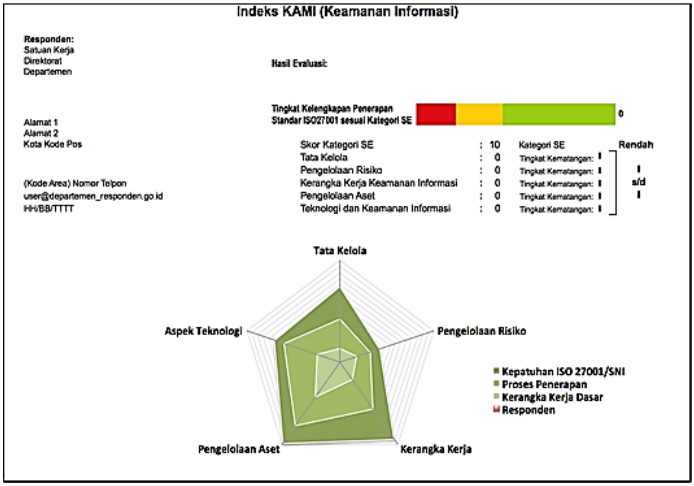
Gambar 2.4 Nilai Kategori Sistem Elektronik

Nilai dari kategori SE diklasifikasikan menjadi 3 bagian, yaitu Rendah, Tinggi, dan Strategis. Hasil pengelompokan tadi didapat dari penjumlahan semua nilai kriteria yang didapat dari setiap pertanyaan yang disuguhkan terkait kategori SE. Untuk mengetahui seberapa besar peran SE dalam instansi tersebut, maka akan diberikan 10 pertanyaan yang dapat menggambarkan hal tersebut. Setiap pertanyaan akan mempunyai 3 kriteria penilaian seperti di Tabel 2.2. Kriteria peran SE yang dimaksud akan dikategorikan pada masing-masing pertanyaan yang ada [8].

Tabel 2.2 Kriteria Pertanyaan Peran TIK

Kriteria	Nilai
A	5
B	2
C	1

Setelah menklasifikasikan Peran SE di instansi terkait, maka akan dilakukan penilaian terhadap kelima area yang ada di Indeks KAMI versi 3.1. Hasil penilaian menggunakan Indeks KAMI versi 3.1 akan digambarkan kedalam diagram yang berbentuk jaring laba-laba (*spider chart*) dengan 5 area utama. Dalam jaring laba-laba tersebut juga akan dilihat tentang nilai Indeks KAMI dengan kepatuhan terhadap ISO/IEC 27001:2013 [8]. Hasil evaluasi menggunakan indeks KAMI versi 3.1 dapat dilihat melalui Gambar 2.5 :



Gambar 2.5 Penilaian Indeks KAMI

Untuk seluruh pertanyaan yang ada dalam setiap area akan dikelompokkan menjadi tiga **kategori pengamanan** sesuai dengan tahapan dalam penerapan standar ISO/IEC 27001. Pertanyaan yang terkait dengan kerangka kerja kerja dasar keamanan informasi akan masuk dalam kategori "1", untuk efektivitas dan konsistensi penerapannya akan masuk dalam kategori "2", dan hal-hal yang merujuk pada kemampuan untuk selalu meningkatkan kinerja keamanan informasi adalah kategori "3" [6].

Ada empat jawaban untuk setiap pertanyaan yang ada di Indeks KAMI mengenai **status pengamanan** di instansi terkait, yaitu Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan/ Diterapkan Sebagian, dan Diterapkan Secara Menyeluruh [6].

Setiap jawaban dari pertanyaan akan diberikan skor yang nilainya disesuaikan dengan kategori pengamanan. Gambar 2.6 akan menunjukkan seluruh jumlah jawaban penilaian dan membentuk matriks antara status dan kategori pengamanan [6].

	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 2.6 Matriks Skor Pengamanan

Nilai yang diberikan pada kategori pengamanan yang tahapannya lebih awal yaitu lebih rendah dibandingkan dengan nilai untuk tahapan selanjutnya. Untuk keseluruhan area pengamanan, pengisian pertanyaan dengan kategori 3 hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan kategori "1" dan "2" sudah terisi dengan status minimal "Diterapkan Sebagian" [6].

Hasil dalam penjumlahan skor masing-masing area akan disajikan dalam dua instrumen di *dashboard*, yaitu dalam bentuk tabel nilai masing-masing area dan *Radar Chart* dengan lima sumbu sesuai dengan area yang dinilai.

Gambar 2.7 Radar Chart Indeks KAMI

Pada Gambar 2.7 menunjukkan bentuk *Radar Chart* yang memiliki 5 sisi untuk masing-masing area. Gradasi warna diagramnya sendiri ada tiga macam, mulai dari hijau muda sampai hijau tua. Hal ini menunjukkan ambang batas dari kategori pengamanan 1 sampai 3. Untuk nilai masing-maisng area akan digambarkan dalam area merah untuk membandingkan kondisi kesiapan dengan acuan tingkat kelengkapan yang ada.

Semakin tinggi ketergantungan sebuah instansi terhadap Peran SE, maka semakin banyak bentuk pengamanan yang diperlukan dan harus diterapkan sampai tahap tertinggi. Pada Gambar 2.8 dibawah ini akan menunjukkan skor akhir yang akan disesuaikan dengan status kesiapan instansi terkait mengenai keamanan informasinya [6].

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

Gambar 2.8 Matriks Kategori SE dan Status Kesiapan

2.2.6 Perbedaan Indeks KAMI versi 2.3 & Indeks KAMI versi 3.1

Sebagai sebuah tools untuk menilai kematangan dari keamanan informasi, Indeks KAMI pastinya akan mengalami perubahan versi untuk selalu diperbaiki dan disempurnakan oleh pihak Kominfo. Indeks KAMI memiliki beberapa versi dan versi yang

selama ini digunakan oleh pihak instansi pemerintahan adalah Indeks KAMI versi 2.3 [6]. Indeks KAMI versi 2.3 dirilis pada tahun 2012, namun pada tahun 2015 pihak Kominfo merilis Indeks KAMI versi terbaru yaitu Indeks KAMI versi 3.1.

Pada kedua versi Indeks KAMI pastinya ada perubahan yang dilakukan oleh pihak Kominfo. Berikut ini adalah Tabel 2.3 yang berisi perubahan-perubahan yang ada dari kedua versi Indeks KAMI tersebut [7] [8]:

Tabel 2.3 Perbedaan Indeks Kami v 2.3 dan Indeks KAMI v 3.1

Kategori Perubahan	Indeks KAMI versi 2.3	Indeks KAMI versi 3.1
Tahun rilis	Dirilis pada tahun 2012	Dirilis pada tahun 2015
Standar yang diacu	Standar yang digunakan yaitu SNI ISO 27001:2009 yang merupakan versi bahasa indonesia dari ISO/IEC 27001:2005	Standar yang digunakan yaitu ISO/IEC 27001:2013
Area yang dinilai	sebelum melakukan penilaian terhadap kelima area yang ada, akan dilakukan penilaian untuk **peran TIK** yang ada di instansi. Kelima area yang dinilai adalah tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, serta	sebelum melakukan penilaian terhadap kelima area yang ada, akan dilakukan penilaian untuk **kategori Sistem Elektronik** yang digunakan di instansi. Kelima area yang dinilai adalah tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, serta

Kategori Perubahan	Indeks KAMI versi 2.3	Indeks KAMI versi 3.1
	teknologi & keamanan informasi	teknologi & keamanan informasi
Nilai peran TIK / Kategori SE	Nilai peran TIK dibagi menjadi 4 kategori, yaitu rendah, sedang, tinggi, dan kritis dengan total skor 0- 48. Untuk setiap pertanyaan akan mendapat skor minimal 0 dan maksimal 4	Nilai kategori SE dibagi menjadi 3 kategori, yaitu rendah, tinggi, dan strategis dengan total skor 10-50. Untuk setiap pertanyaan akan mendapat skor minimal 1 dan maksimal 5
Status Peran TIK / Kategori SE	Disetiap pertanyaan yang dijawab akan mendapat status minim, rendah, sedang, tinggi, dan kritis	Disetiap pertanyaan yang dijawab akan mendapat status A, B, dan C
Total skor akhir	Pada versi 2.3, skor akhir yang akan dimiliki dengan menjawab semua pertanyaan yaitu maksimal 588	Pada versi 3.1, skor akhir yang akan dimiliki dengan menjawab semua pertanyaan yaitu maksimal 645
Status kesiapan	Status kesiapan dibagi menjadi 3 bagian, yaitu: - Tidak Layak - Perlu Perbaikan - Baik / Cukup	Status kesiapan dibagi menjadi 4 bagian, yaitu: - Tidak Layak - Perlu Perbaikan - Cukup - Baik
Jumlah pertanyaan	Dengan total jumlah pertanyaan sebanyak 131, berikut adalah penjabarannya:	Dengan total jumlah pertanyaan sebanyak 141, berikut adalah penjabarannya:

Kategori Perubahan	Indeks KAMI versi 2.3	Indeks KAMI versi 3.1
	- Peran TIK : 12 pertanyaan - Tata kelola : 20 pertanyaan - Risiko : 15 pertanyaan - Kerangka kerja : 26 pertanyaan - Pengelolaan aset : 34 pertanyaan - Teknologi : 24 pertanyaan	- Kategori SE : 10 pertanyaan - Tata kelola : 22 pertanyaan - Risiko : 16 pertanyaan - Kerangka kerja : 29 pertanyaan - Pengelolaan aset : 38 pertanyaan - Teknologi : 26 pertanyaan

2.2.7 Pemetaan Klausul ISO/IEC 27001:2013 dengan pertanyaan Indeks KAMI versi 3.1

Seluruh pertanyaan yang tersebar di dalam 5 area Indeks KAMI versi 3.1 berjumlah 131 pertanyaan berasal dari klausul ISO/IEC 27001:2013. Pada bagian ini akan dilakukan pemetaan pertanyaan 5 area Indeks KAMI versi 3.1 dengan klausul ISO 27001:2013 untuk mengetahui keterkaitan dari pertanyaan Indeks KAMI versi 3.1 dengan ISO 27001:2013. Berikut ini adalah Tabel 2.4 yang berisikan hasil pemetaan yang telah dilakukan:

Tabel 2.4 Pemetaan Pertanyaan Indeks KAMI versi3.1 dengan Klausul ISO 27001:2013

Pertanyaan 5 Area Indeks KAMI versi 3.1	Klausul ISO 27001:2013
Bagian Tata Kelola	
# **Fungsi/Instansi Keamanan Informasi**	

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
2,1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	A.5.1.1
2,2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	A.6.1.1 A.6.1.2
2,3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	A.6.1.2
2,4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	A.7.1.1 A.7.1.2 A.12.1.3
2,5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	A.6.1.2 A.6.1.4
2,6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	A.7.2.2
2,7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	A.7.2.3

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
2,8	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	A.5.1.2
2,9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	A.7.2.2
2.10	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	A.7.3.1
2.11	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	A.6.1.1 A.18.1.4
2.12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	A.6.1.3
2.13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan	A.6.1.3 A.18.1.3

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
	informasi terkait proses kerja yang melibatkan berbagai pihak?	
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	A.5.1.2
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	A.7.3.1
2.16	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	A.7.2.1
2.17	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	A.6.1.5
2.18	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	A.6.1.5

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
2.19	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	A.7.2.3
2.20	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	A.7.3.1
2.21	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	A.8.2.1 A.18.1.1
2.22	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	A.8.2.1
Bagian Risiko		
#	**Kajian Risiko Keamanan Informasi**	
3,1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	A.16.1.1 A.16.1.4
3,2	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	A.16.1.3

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
3,3	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	A.16.1.6
3,4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	A.8.2.1
3,5	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	A.8.2.3
3,6	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?	A.8.1.2
3,7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	A.8.1.3 A.8.2.3
3,8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	A.16.1.6
3,9	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)?	A.16.1.1

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
3.10	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	A.16.1.5
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	A.16.1.2
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	A.16.1.7
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	A.16.1.7
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	A.16.1.7
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	A.16.1.6
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	A.16.1.1
Bagian Kerangka Kerja		

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
#	**Penyusunan dan Pengolahan Kebijakan & Prosedur Keamanan Informasi**	
4,1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	A.9.1.1 A.10.1.1 A.12.3.1 A.14.2.1
4,2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	A.5.1.1
4,3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	A.18.2.1 A.18.2.2 A.18.2.3
4,4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	A.5.1.1 A.15.2.2
4,5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?	A.16.1.5

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
4,6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	A.16.1.6
4,7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	A.15.1.1 A.15.1.2 A.15.2.2
4,8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	A.18.1.5
4,9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	A.18.2.3
4.10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	A.14.1.1 A.12.1.1
4,11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	A.6.1.5

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
4,12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	A.14.1.1
4,13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	A.12.1.4 A.14.2.1 A.14.2.2
4,14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	A.14.2.7
4,15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	A.17.1.3
4,16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	A.17.1.1
4.17	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	A.17.1.2

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	A.17.1.3
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	A.5.1.2
#	**Pengelolaan Strategi dan Program Keamanan Informasi**	
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	A.16.1.6
4,21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	A.17.1.2
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	A.16.1.5
4,23	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)?	A.12.7.1
4,24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan,	A.12.7.1

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
	konsistensi dan efektifitas penerapan keamanan informasi?	
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	A.12.7.1
4,26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	A.12.7.1
4,27	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?	A.17.1.3
4,28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	A.17.2.1
4,29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	A.17.2.1

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
Bagian Pengelolaan Aset		
#	**Pengelolaan Aset Informasi**	
5,1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	A.8.1.1 A.8.1.2 A.8.2.2
5,2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	A.8.1.3 A.8.2.1
5,3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	A.8.2.1
5,4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	A.8.2.3
5,5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	A.12.1.2
5,6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	A.9.4.4
5,7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	A.14.2.6
	Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
5,8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	A.8.1.3
5,9	Tata tertib penggunaan komputer, email, internet dan intranet	A.14.1.1 A.14.1.2
5.10	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	A.8.1.4
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	A.12.6.2
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	A.18.1.4
5.13	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	A.9.4.1 A.9.3.1
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	A.9.1.1
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	A.11.2.5 A.8.3.1
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	A.15.2.1
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	A.13.2.4 A.14.3.1
5.18	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	A.12.3.1
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	A.8.3.3
5.20	Proses pengecekan latar belakang SDM	A.7.1.1

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	A.15.1.3
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan	A.8.3.2 A.11.2.7
5.23	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku	A.9.2.3
5.24	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	A.9.2.6
5.25	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	A.12.3.1
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	A.12.4.1
5.27	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	A.15.1.2 A.18.1.2 A.18.1.4
#	**Pengamanan Fisik**	
5.28	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?	A.11.1.6 A.11.1.2

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	A.11.1.3
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	A.11.1.4 A.11.2.1
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	A.11.1.4 A.11.2.2 A.11.2.3
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	A.11.1.5 A.11.2.6
5.33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	A.11.1.6 A.11.2.9 A.13.2.1
5.34	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?	A.11.1.4
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	A.11.2.4

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	A.11.2.6 A.11.2.8 A.13.2.2
5.37	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)	A.11.1.3 A.11.1.6
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	A.11.1.2
Bagian Teknologi & Keamanan Informasi		
#	**Pengamanan Teknologi**	
6,1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	
6,2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	A.9.1.2 A.13.1.3
6,3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	A.13.1.1 A.13.1.2

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
6,4	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	A.13.1.1
6,5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	A.14.1.2
6,6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	A.17.2.1
6,7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	A.14.1.1 A.14.1.3
6,8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	A.12.4.1
6,9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	A.9.2.1 A.12.4.1
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	A.12.4.2 A.12.4.3
6.11	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	A.10.1.2
6.12	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	A.10.1.1

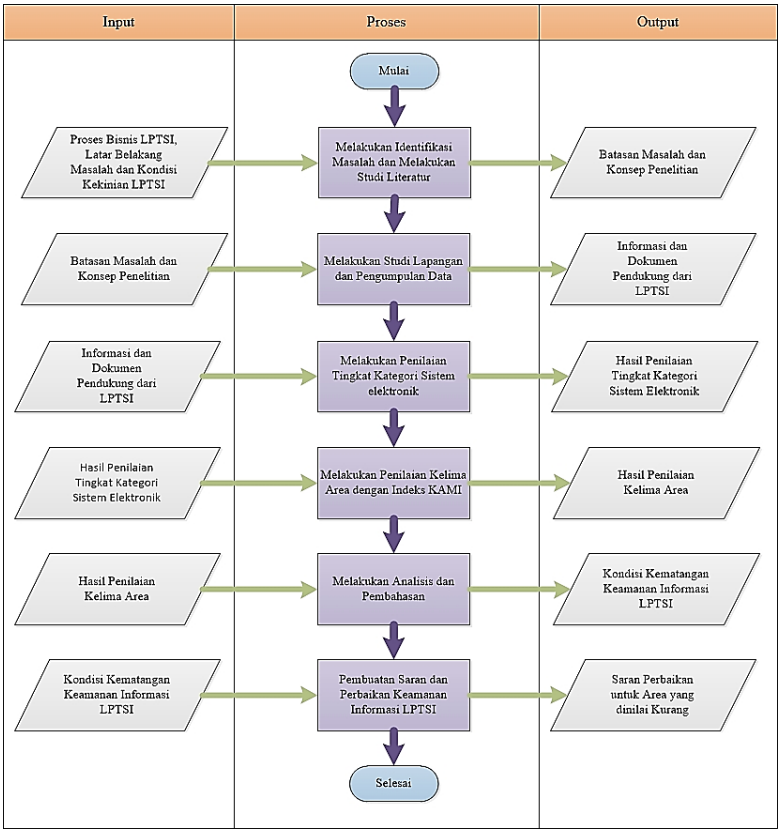
Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
6.13	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	A.10.1.2 A.13.2.3
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	A.9.4.3
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	A.9.4.2 A.9.4.5
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	A.9.2.3 A.9.2.4 A.9.2.5
6.17	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	A.9.4.2
6.18	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	A.9.2.6
6.19	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	A.12.5.1
6.20	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	A.12.6.1 A.12.2.1

Pertanyaan 5 Area Indeks KAMI versi 3.1		Klausul ISO 27001:2013
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	A.12.2.1
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	A.12.2.1
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	A.12.4.4
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?	A.14.2.8 A.14.2.5 A.14.2.9
6.25	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	A.14.2.6 A.11.1.1 A.14.2.4
6.26	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	A.15.2.2 A.18.2.1

“Halaman ini sengaja dikosongkan”

BAB III
METODOLOGI PENELITIAN

Pada bagian ini akan dijelaskan mengenai metodologi dalam melakukan pengerjaan Tugas Akhir, sehingga langkah-langkah pengerjaan menjadi lebih sistematis dan terorganisir lebih rapi. Berikut ini merupakan tahapan metodologi pengerjaan tugas akhir :



3.1 Melakukan Identifikasi Masalah & Studi Literatur

Tahapan ini adalah tahap awal yang akan dilakukan untuk mengerjakan Tugas Akhir. Dalam tahap ini, akan dilakukan identifikasi masalah yang akan dijadikan topik tugas akhir. Setelah menemukan masalah yang akan diangkat, maka akan dilakukan studi literatur dengan mengumpulkan referensi dari buku, narasumber, jurnal, penelitian sebelumnya, dan dokumen terkait. Pada tahap ini akan diakukan berbagai kajian tentang konsep serta metode yang dapat digunakan untuk menyelesaikan permasalahan pada tugas akhir ini.

3.2 Melakukan Studi Lapangan & Pengumpulan Data

Pada tahap ini akan dilakukan pengumpulan data-data terkait dengan tugas akhir yang akan dikerjakan. Data yang didapat ini berasal dari DPTSI ITS. Data akan didapatkan selama melakukan wawancara dan observasi secara langsung oleh peneliti. Data yang akan diperoleh adalah bukti pendukung berupa dokumen-dokumen yang dapat memperkuat pernyataan dari pihak yang diwawancara. Peneliti dapat melakukan wawancara dengan pihak kasubbag umum, koordinator pusat pengelolaan & layanan TIK, dan koordinator pusat infrastruktur & keamanan jaringan.

Tabel 3.1 Daftar Narasumber

Area Indeks KAMI	Narasumber
Area Tata Kelola Keamanan Informasi	Ketua Direktorat
Area Pengelolaan Risiko Keamanan Informasi	Pusat Pengelolaan & Layanan TIK
Area Kerangka Kerja Pengelolaan Keamanan Informasi	Pusat Pengembangan Sistem Informasi, Ketua Direktorat
Area Pengelolaan Aset Informasi	Pusat Infrastruktur & Keamanan Informasi

Area Indeks KAMI	Narasumber
Area Teknologi dan Keamanan Informasi	Pusat Infrastruktur & Keamanan Informasi

3.3 Melakukan Penilaian Tingkat Kategori Sistem Elektronik

Setelah melakukan studi lapangan dan mendapat data, akan dilakukan penilaian terhadap tingkat kategori SE di DPTSI. Kategori SE akan dibagi menjadi tiga tingkat mulai dari rendah sampai strategis. Penilaian ini dapat diperoleh dari responden yang diwawancara dan dengan cara observasi secara langsung. Pada tahap ini juga perlu didapatkannya data pendukung sebagai bukti dari penilaian kategori SE di DPTSI.

3.4 Melakukan Penilaian Kelima Area dengan Indeks KAMI

Setelah dilakukan penilaian tingkat kategori SE di DPTSI, maka akan dilanjutkan dengan penilaian kelima area yang ada di Indeks KAMI untuk menentukan nilai kematangan dari keamanan informasi yang ada di DPTSI. Penilaian ini juga diperoleh dari responden yang diwawancara serta dengan cara observasi secara langsung.

3.5 Melakukan Analisis dan Pemabahasan

Pada tahap ini akan dilakukan analisis dan pembahasan dari hasil nilai yang didapatkan. Penarikan kesimpulan tentang kesiapan DPTSI untuk keamanan informasi yang ada juga akan dilakukan pada tahap ini. Pengambilan keputusan juga belum berhenti pada tahap ini, karena masih ada tahap selanjutnya untuk memberikan saran perbaikan yang dapat dilakukan oleh pihak DPTSI.

3.6 Pembuatan Saran dan Perbaikan

Setelah melakukan pembahasan dari hasil penilaian keamanan informasi di DPTSI, maka akan diberikan saran perbaikan yang sesuai untuk DPTSI. Saran perbaikan dapat berupa saran yang sebelumnya sudah ada pada penelitian tahun 2012 atau saran baru yang dirasa lebih cocok untuk meningkatkan nilai di semua area keamanan informasi di DPTSI.

BAB IV
PERANCANGAN

Pada bab ini akan dijelaskan mengenai proses perancangan penelitian tugas akhir. Perancangan perlu dilakukan sebagai panduan dalam pengerjaan tugas akhir ini.

4.1 Perancangan Studi Kasus

Pada bagian perancangan studi kasus ini akan dijelaskan mengenai tujuan dari studi kasus yang diangkat dan *unit of analysis* yang diangkat.

4.1.1 Tujuan Studi Kasus

Tujuan dari tugas akhir ini adalah untuk mengetahui tingkat kategori Sistem Elektronik yang digunakan di DPTSI ITS, untuk mengetahui nilai kematangan keamanan informasi yang ada di DPTSI ITS, dan untuk memberikan rekomendasi kepada pihak DPTSI ITS untuk keamanan informasi yang harus dijlankan. Ketiga tujuan tugas akhir tersebut akan dijawab dengan menggunakan tujuan dari adanya studi kasus yang diangkat pada tugas akhir kali ini.

Menurut Stake studi kasus adalah dimana peneliti melakukan eksplorasi secara mendalam terhadap program, acara, aktivitas, proses, dan individu. Kasus tersebut juga dibatasi oleh waktu dan aktivitas. Peneliti melakukan pengumpulan informasi rinci menggunakan berbagai macam prosedur pengumpulan data selama periode waktu yang berkelanjutan . Menurut Creswell studi kasus adalah suatu proses mengeksplorasi dan deskriptif dari suatu kasus maupun beragam kasus dari waktu ke waktu melalui pengumpulan data yang mendalam serta melibatkan berbagai macam sumber informasi dalam sebuah konteks [24].

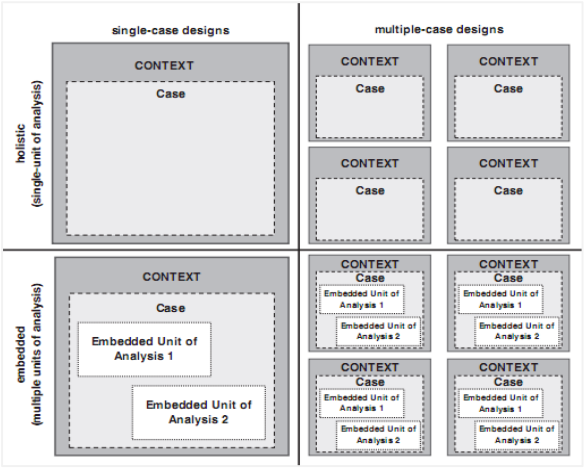
Yin juga mendefinisikan studi kasus sebagai penyelidikan empiris yang menyelidiki fenomena kontemporer dengan

menggunakan cara-cara yang sistematis dalam pengumpulan data, seperti observasi dan wawancara [25]. Menurut Yin, terdapat tiga kategori studi kasus, antara lain [25]:

- Eksplorasi: melakukan penggalian fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk peneliti.
- Deskriptif: menggambarkan fenomena ilmiah yang terjadi di dalam data yang dimaksud dengan tujuan untuk menggambarkan data yang terjadi dalam bentuk narasi.
- *Explanatory*: menjelaskan fenomena dalam data secara jelas dan detail dari dasar sampai dalam.

Pada pengerjaan tugas akhir ini menggunakan kategori studi kasus eksplorasi dan deskriptif. Kategori eksplorasi digunakan karena pada tugas akhir ini akan dilakukan penggalian kondisi kekinian dari instansi terkait dan kategori deskriptif digunakan karena akan ada penggalian data untuk memperkuat kondisi kekinian dari instansi terkait.

Perancangan studi kasus dibagi menjadi dua yaitu *single-case design* dan *multiple-case design. Single-case design* menggunakan satu kasus untuk diuji sedangkan multiple case design menggunakan dua atau lebih kasus yang diuji. Dari kedua perancagan tersebut dibagi menjadi empat tipe yang diseuaikan dengan banyaknya *unit of analysis* yang digambarkan pada Gambar 4.1:



Gambar 4.1 ***Unit of Analysis***

Single-case design dibagi menjadi dua bagian, yaitu *single unit of analysis* dan *multiple unit of analysis*. *Single unit of analysis* dapat digunakan pada penelitian dengan kasus kritis atau unik, menguji teori yang telah dirumuskan dan melakukan eksplorasi. Sedangkan *multiple unit of analysis* digunakan pada penelitian eksplorasi perbedaan di dalam dan diantara kasus serta bertujuan untuk melakukan replikasi temuan di seluruh kasus dengan cara membandingkan sub-unit. Yin menyatakan bahwa *Single unit of analysis* akan logis jika digunakan ketika tidak mungkin untuk dilakukan identifikasi sub-unit [25].

Pada penelitian tugas akhir ini menggunakan perancangan *single-case design* dengan *multiple unit of analysis*. Tugas akhir ini menggunakan *single-case design* karena studi kasus yang diangkat adalah satu kasus mengenai sistem manajemen keamanan informasi dan menggunakan *multiple unit of analysis* karena studi kasus yang diambil akan menganalisis sampai ke sub-unit dari organisasi terkait.

Untuk menjawab tujuan tugas akhir yang telah dijabarkan sebelumnya, tujuan dari adanya studi kasus ini adalah untuk melakukan penggalian data dari kondisi kekinian serta menggambarkan data yang ada dari sistem manajemen keamanan informasi di DPTSI ITS untuk melakukan evaluasi terhadap sistem manajemen keamanan informasi yang ada di DPTSI ITS .

4.1.2 *Unit* of *Analysis*

Unit of Analysis adalah alat konseptual untuk membimbing investigator terlibat dalam pengamatan bermakna serta observasi dan analisis yang sistematis. *Unit of analysis* dapat berupa individu, group, artifact, interaksi antar individu, atau dibatasi dengan sistem yang didefinisikan oleh investigator (Merriam,2009; Patton,2002; Stake,1995) [26].

Unit of analysis yang digunakan pada tugas akhir kali ini adalah bagian pengelola keamanan informasi DPTSI ITS yang akan dijadikan gambaran nilai sistem manajemen keamanan informasi di DPTSI ITS kedepannya.

4.2 Subjek dan Objek Penelitian

Penelitian ini dilakukan pada Direktorat Pengembangan Teknologi Sistem Informasi (DPTSI) yang merupakan salah badan layanan teknologi informasi dan komunikasi di Institut Teknologi Sepuluh Nopember (ITS). Subjek penelitian kali ini adalah Ketua DPTSI, Kepala Pusat Pengelolaan & Layanan TIK, Kepala Pusat Pengembangan Sistem Informasi, Kepala Pusat dan Staff Infrastruktur & Keamanan Informasi.

Objek yang akan diteliti pada penelitian kali ini adalah sistem manajemen keamanan informasi (SMKI) yang ada di DPTSI ITS yang nantinya keamanan informasi tersebut akan disempurnakan dengan rekomendasi yang telah disesuaikan dengan ISO/IEC 27002:2013 sehingga SMKI pada DPTSI dapat meningkat menjadi lebih baik lagi.

4.3 Data yang Diperlukan

Pada bagian ini akan dijelaskan mengenai data yang diperlukan dalam penelitian tugas akhir. Dalam melakukan penelitian dibutuhkan data yang dapat mendukung tahapan pengalian data dan informasi sesuai dengan studi kasus penelitian. Poin-poin mengenai data yang diperlukan antara lain sebagai berikut:

1. Tugas pokok dan fungsi dari Direktorat Pengembangan Teknologi Sistem Informasi ITS Surabaya.
2. Gambaran kondisi Tata Kelola Keamanan Informasi saat ini seperti apakah terdapat kontrol yang diperlukan (kebijakan formal yang mendefinisikan peran, tanggung-jawab, kewenangan pengelolaan keamanan informasi, dari pimpinan unit kerja sampai ke pelaksana operasional). Dalam area ini termasuk juga gambaran apakah ada program kerja yang berkesinambungan, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.
3. Gambaran kondisi Pengelolaan Risiko Keamanan Informasi seperti bagaimana bentuk tata kelola yang diperlukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji efektifitasnya.
4. Gambaran kondisi Kerangka Kerja Keamanan Informasi yang digunakan seperti apakah ada sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikannya.
5. Gambaran kondisi Pengelolaan Aset Informasi seperti kontrol dalam bentuk pengamanan terkait keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.
6. Gambaran kondisi Teknologi dan Keamanan Informasi seperti aspek pengamanan di area teknologi mensyaratkan adanya strategi yang terkait dengan pengamanan informasi

secara rutin, pengamanan seluruh infrastruktur jaringan, dan penggunaan antivirus.

4.4 Persiapan Pengumpulan Data

Pada bagian ini akan menjelaskan mengenai persiapan pengumpulan data pada penelitian tugas akhir ini. Dalam penelitian tugas akhir ini, metode pengumpulan data yang digunakan adalah wawancara, observasi, dan *review* dokumen.

4.4.1 Instrumen Wawancara

Instrumen wawancara merupakan daftar pertanyaan yang akan diajukan pada saat wawancara dengan narasumber. Pada tugas akhir ini, instrumen wawancara yang digunakan berdasarkan kriteria yang ada di dalam Indeks KAMI versi 3.1 yang mencakup kategori sistem elektonik yang digunakan dan kelengkapan pengamanan kelima area keamanan informasi.

Wawancara akan dilakukan kepada narasumber yang paham mengenai kondisi kekinian dari DPTSI ITS Surabaya. Narasumber dipilih dengan memperhatikan kapasitas serta kewenangannya untuk memberikan informasi yang valid sesuai dengan pertanyaan yang diajukan untuk menghindari terjadinya kesalahan informasi yang didapat. Instrumen wawancara yang akan digunakan untuk pengumpulan data disertakan dalam LAMPIRAN A, sedangkan untuk pemetaan pertanyaan yang ditanyakan akan dikelompokkan pada Tabel 4.1 dibawah ini:

Tabel 4.1 Pemetaan Pertanyaan Indeks KAMI dengan Narasumber

Narasumber	Pertanyaan Indeks KAMI
Ketua DPTSI (Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom.)	2.1; 2.2; 2.3; 2.5; 2.6; 2.7; 2.8; 2.9; 2.10; 2.14; 2.16; 2.17; 2.18; 2.19; 2.20; 2.21; 2.22 4.10; 4.11;4.16; 4.17; 4.18; 4.19; 4.20; 4.21; 4.22; 4.27; 4.28; 4.29
Koordinator pusat pengelolaan dan layanan TIK (Hanim Maria Astuti, S.Kom., M.Sc.)	1-SE; 2-SE; 3-SE; 4-SE; 5-SE; 6-SE; 7-SE; 8-SE; 9-SE; 10-SE
Koordinator pusat infrastruktur dan keamanan informasi (Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D.)	2.4; 2.7; 2.11; 2.12; 2.13; 2.15; 2.17; 2.22 3.1; 3.2; 3.3; 3.4; 3.5; 3.6; 3.7; 3.8; 3.9; 3.10; 3.11; 3.12; 3.13; 3.14; 3.15; 3.16 4.1; 4.2; 4.3; 4.4; 4.5; 4.6; 4.7; 4.8; 4.9; 4.15; 4.19; 4.20; 4.21; 4.22; 4.28; 4.29 5.2; 5.3; 5.4; 5.8; 5.9; 5.10; 5.11; 5.14; 5.19; 5.20; 5.21; 5.22; 5.23; 5.24; 5.27; 5.28; 5.29; 5.30; 5.32; 5.34; 5.35; 5.36; 5.37; 5.38 6.12; 6.13; 6.14; 6.15; 6.16; 6.17; 6.21; 6.22; 6.23; 6.26

Narasumber	Pertanyaan Indeks KAMI
Admin pusat infrastruktur dan keamanan informasi (Satriyo Wicaksono, S.Kom, Achmad Bustari, A.Md., Cahya Purnama Dani, A.Md., Jananta Permata Putra, S.ST)	5.1; 5,5; 5.6; 5.7; 5.12; 5.13; 5.15; 5.16; 5.17; 5.18; 5.25; 5.26; 5,31; 5,33 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 6.7; 6.8; 6.9; 6.10; 6.11; 6.17; 6.18; 6.19; 6.20; 6.21; 6.22; 6.23
Koordinator pusat pengembangan sistem informasi (Anny Yuniarti, S.Kom., M.Comp.Sc.)	4.12; 4.13; 4.14; 4.23; 4.24; 4.25; 4.26; 6.24; 6.25

4.4.2 Observasi

Selain melakukan wawancara, juga akan dilakukan observasi untuk mengamati keadaan yang sebenarnya dari DPTSI ITS secara langsung. Observasi juga dilakukan untuk memperkuat dan mendukung hasil dari wawancara itu sendiri. Hasil yang diharapkan dari observasi ini adalah foto-foto bukti dari penerapan sistem manajemen keamanan informasi di DPTSI ITS.

4.4.3 Review Dokumen

Review dokumen adalah metode yang digunakan untuk mendukung berbagai informasi yang belum didapatkan dan memiliki kaitan dengan hasil wawancara. Dalam penelitian ini, berbagai informasi yang didapatkan dari *review* dokumen terkait kondisi kekinian DPTSI ITS adalah informasi struktur organisasi, fungsi, tupoksi, log aktivitas, serta kebijakan-kebijakan terkait keamanan informasi yang terlampir dalam dokumen fisik maupun digital yang berhubungan dengan hasil

wawancara. *Review* dokumen juga dilakukan untuk mendukung hasil wawancara yang dilakukan dan dapat dijadikan bukti secara nyata.

Selain dokumen yang diatas, juga akan dilakukan *review* dokumen hasil penilaian Indeks KAMI yang pernah dilakukan tahun 2012 untuk mengetahui apakah kondisi SMKI yang ada di DPTSI sudah semakin baik atau bahkan menurun di beberapa bagian tertentu.

Dari ketiga metode pengumpulan data diatas akan dijabarkan tujuan, sasaran, dan sumber dari masing-masing metode pada Tabel 4.2 dibawah ini:

Tabel 4.2 Tujuan, Sasaran, dan Sumber Metode Pengumpulan Data

Tujuan	Sasaran	Sumber
Metode Wawancara		
Mengetahui jumlah anggaran dan jumlah pengguna sistem elektronik	Jumlah investasi yang terpasang untuk sistem elektronik Jumlah anggaran untuk sistem elektronik Jumlah pengguna sistem elektronik	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui standar dan algoritma keamanan informasi pada sistem elektronik	Standar keamanan informasi pada sistem elektronik Jenis algoritma khusus pada sistem elektronik	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui jenis data yang dikelola, tingkat kekritisan data, dan tingkat kekritisan proses	Data pribadi yang dikelola sistem elektronik Tingkat klasifikasi data dalam sistem elektronik Tingkat kekritisan proses dalam sistem elektronik	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
pada ancaman yang ada di sistem elektronik		
Mengetahui dampak dan kerugian dari kegagalan sistem elektrinok	Dampak dari kegagalan sistem elektronik Kerugian dari insiden keamanan sistem elektronik	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui alokasi SDM, kompetensi SDM, pembagian tanggung jawab, standar, perangkat hukum, serta kebijakan yang diterapkan terkait tata kelola keamanan informasi yang ada	Struktur Organisasi Tupoksi Jumlah SDM di bagian Keamanan Standar pengelola keamanan informasi Kompetensi dan keahlian SDM dalam mengelola keamanan informasi Penerapan program sosialisasi & program peningkatan kompetensi bagi SDM Data pribadi sesuai UU yang berlaku Koordinasi dengan pihak tertentu untuk pengamanan informasi Alokasi keberlanjutan bisnis Pelaporan kondisi & kepatuhan program keamanan informasi secara rutin Keputusan strategis dari permasalahan keamanan	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
	informasi Program khusus untuk pengamanan informasi Parameter pengukuran kinerja & program penilaian kinerja pengelolaan keamanan informasi Target sasaran, evaluasi capaian, dan langkah perbaikan keamanan informasi Perangkat hukum serta kebijakan terkait pelanggaran hukum keamanan informasi	
Mengetahui penanggung jawab risiko, framework yang digunakan, risiko yang menyangkut aset informasi, dan dampak risiko terkait pengelolaan risiko keamanan informasi yang ada	Program Kerja pengelolaan risiko keamanan informasi Tupoksi pengelolaan risiko keamanan informasi Framework risiko keamanan informasi Ambang batas risiko dan dampak kerugian akibat risiko keamanan informasi Ancaman terkait aset informasi Kajian, langkah mitigasi, tingkat prioritas risiko keamanan infomasi Evaluasi penanganan risiko dan framework pengelolaan risiko keamanan informasi	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui rencana, penerapan, dan evaluasi dari	Kebijakan & prosedur keamanan informasi Mekanisme pengelolaan dokumen kebijakan &	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
pengelolaan kebijakan & prosedur keamanan informasi	prosedur keamanan informasi Proses identifikasi ancaman keamanan informasi sesuai prosedur Kontrak dengan pihak ketiga terkait keamanan informasi Kebijakan & prosedur pengelolaan security patch Evaluasi risiko penerapan sistem baru SDLC yang digunakan beserta prosedur Framework keberlanjutan bisnis/ layanan TIK Rencana, uji coba, dan evaluasi pemulihan bencana terhadap layanan TIK evaluasi kebijakan & prosedur keamanan informasi	
Mengetahui rencana, penerapan, dan evaluasi dari pengelolaan kebijakan & prosedur keamanan informasi	Kebijakan & prosedur keamanan informasi Mekanisme pengelolaan dokumen kebijakan & prosedur keamanan informasi Proses identifikasi ancaman keamanan informasi sesuai prosedur Kontrak dengan pihak ketiga terkait keamanan informasi Kebijakan & prosedur pengelolaan security patch Evaluasi risiko penerapan sistem baru SDLC yang digunakan beserta prosedur Framework keberlanjutan	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
	bisnis/ layanan TIK Rencana, uji coba, dan evaluasi pemulihan bencana terhadap layanan TIK evaluasi kebijakan & prosedur keamanan informasi	
Mengetahui strategi dan program keamanan informasi	Strategi penerapan & penggunanaan teknologi keamanan informasi Pelaksanaan audit internal dan evaluasinya Revisi kebijakan & prosedur Analisa aspek finansial Evaluasi status kepatuhan program keamanan informasi Rencana dan program peningkatan keamanan informasi jangka panjang	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui proses dan prosedur pengelolaan aset informasi	Daftar aset informasi dan kepemilikannya Klasifikasi & tingkat kepentingan aset informasi sesuai peraturan yang berlaku Tingkatan akses dari setiap klasifikasi aset informasi Proses pengelolaan sistem, proses bisnis, dan proses TI Proses pengelolaan konfigurasi Proses perilisan aset baru Tata tertib penggunaan komputer, email, internet, pengamanan aset, instalasi software, dan penggunaan data pribadi	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
	Pengelolaan username & password Prosedur pemberian akses penggunaan aset informasi Ketepatan penghancuran data dan pertukaran data dengan pihak eksternal Daftar data yang harus dibackup dan restore data latar belakang SDM Prosedur penggunaan akses dan hak akses Prosedur untuk mutasi user Prosedur penggunaan perangkat pengolah informasi miliki pihak ketiga	
Mengetahui peraturan pengamanan fisik beserta proses-proses pengelolaan aset informasi	Pengamanan lokasi kerja sesuai klasifikasi aset informasi Proses mengelola alokasi kunci masuk ke lokasi kerja Perlindungan infrastruktur dari bencana dan gangguan listrik Peraturan pengamanan perangkat komputasi Proses pemindahan aset TIK ke lokasi lain Proses pemeriksaan dan perawatan perangkat komputer Mekanisme pengamanan dan pengiriman aset infomasi terkait pihak ketiga	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
Mengetahui kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengamanan aset teknologi	Perlindungan saat mengunakan internet Segmentasi jaringan komunikasi Standar keamanan aset jaringan, sistem, dan aplikasi Pemindaian jaringan, sistem, dan aplikasi Kapasitas yang dipenuhi dengan adanya jaringan, sistem, dan aplikasi Analisa log perubahan sistem informasi dan upaya akses Standar dan pengamanan penggunaan enkripsi untuk perlindungan aset informasi Waktu akses yang otomatis Versi dari sistem operasi yang digunakan Perlindungan dari virus & malware serta rekamanan dan hasil analisa pembaruan dari antivirus yang digunakan Penindaklanjutab dari adanya virus & malware sinkronisasi waktu jaringan, sistem, dan aplikasi sesuai standar Verifikasi/ validasi saat proses pengembangan setiap aplikasi Pengamanan lingkungan pengembangan sesuai standar yang digunakan untuk sikus hidup sistem	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
	Pihak independan untuk mengkaji keamanan informasi	
Metode Observasi		
Mengetahui proses dan prosedur pengelolaan aset informasi	Pengelolaan username & password waktu penyimpanan data & penghancuran data Backup dan restore data Proses pelaporan insiden keamanan informasi ke pihak eksternal Hak akses yang sesuai	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui peraturan pengamanan fisik beserta proses-proses pengelolaan aset informasi	Pengamanan lokasi kerja Pengelolaan alokasi kunci masuk secara fisik dan elektronik Perlindungan infrastruktur komputasi dari bencana dan gangguan listrik Pengamanan infrastruktur komputasi diluar lokasi kerja Konstruksi ruang penyimpanan peragkat pengolah informasi dan fasilitas pendukung Fasilitas perawatan perangkat komputer Pengamanan ruang server dan ruang arsip serta larangan yang ada Pengamanan lokasi dari kehadiran pihak ketiga	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
Mengetahui kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengamanan aset teknologi	Perlindungan pada internet Jalur akses Pemindaian aset jaringan, sistem, dan aplikasi kapasitas yang dipenuhi dengan jaringan, sistem, dan aplikasi Enkripsi untuk melindungi aset informasi Penggantian password secara otomatis Pembatasan waktu akses Pengamanan akses jaringan Pengamanan akses dari luar Versi dekstop dan server Antivirus yang digunakan Sinkronisasi waktu untuk jaringan, sistem, dan aplikasi	Indeks KAMI versi 3.1 ISO 27001:2013
Metode Review Dokumen		
Mengetahui bukti dari penggunaan anggaran dan standar sistem elektronik serta dampak dari kegagalan sistem elektronik	Dokumen anggaran sistem elektronik Dokumen dampak dan kerugian kegagalan sistem elektronik	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
Mengetahui bukti dari dokumen terkait pentata kelolaan keamanan informasi, mulai dari standar, perangkat hukum, dan data SDM yang ada	Dokumen tupoksi dan struktur organisasi bagian keamanan informasi Dokumen standar kompetensi bagi SDM keamanan informasi Dokumen undang-undang tentang identifikasi data pribadi Dokumen keberlanjutan bisnis mengenai layanan TIK Dokumen hasil laporan kondisi keamanan informasi Dokumen standar dan perangkat hukum terkait keamanan informasi	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui bukti dari dokumen terkait pengelolaan risiko, klasifikasi aset, dan evaluasi framework pengelolaan risiko	Dokumen program kerja pengelolaan risiko keamanan informasi Dokumen struktur organisasi dan tupoksi mengenai manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi Dokumen framework pengelolaan risiko keamanan informasi Dokumen klasifikasi aset, tingkat ancaman, dan dampak kerugian keamanan informasi Dokumen ambang batas risiko Dokumen analisa/kajian risiko keamanan informasi	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
	Dokumen mitigasi risiko beserta prioritas penyelesaiannya Dokumen evaluasi langkah mitigasi secara berkala Dokumen evaluasi framework pengelolaan risiko	
Mengetahui bukti dokumen pendukung terkait standar, prosedur, dan tata tertib terkait pengelolaan aset keamanan informasi	Dokumen daftar inventaris aset informasi dan aset TI Dokumen pengelolaan konfigurasi Dokumen struktur dan tupoksi secara individu Tata tertib penggunaan komputer, email, inetrnet, dan intranet Tata tertib penggunaan dan pengaman aset Dokumen peraturan instalasi software dan penggunaan data pribadi Dokumen syarat serta prosedur penghancuran data dan pertukaran data dengan pihak eksternal Dokumen prosedur backup dan restore Dokumen pelaporan insiden keamanan informasi pada pihak internal dan eksternal	Indeks KAMI versi 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
Mengetahui bukti dokumen peraturan pengamanan fisik beserta proses-proses pengelolaan aset informasi	Dokumen pengelolaan fasilitas fisik/ lokasi kerja Dokumen peraturan pengamanan lokasi ruang server dan ruang arsip	Indeks KAMI versi 3.1 ISO 27001:2013
Mengetahui tindakan pengamanan dan pengamatan keamanan informasi yang diterapkan	Dokumen log perubahan sistem informasi dan upaya akses yang tidak pantas Dokumen standar penggunaan enkripsi Dokumen verifikasi & validasi pengembangan aplikasi	Indeks KAMI versi 3.1 ISO 27001:2013

4.5 Metode Pengol ahan Data

Setelah didapatkan hasil dari pengumpulan data melalui wawancara, observasi, dan *review* dokumen akan dilakukan pengolahan data dengan cara menulis ulang rekaman wawancara yang tersimpan pada media *recorder* dan penulisan akan dilakukan menggunakan aplikasi pengolah kata (*word processing*).

Berdasarkan data yang diperoleh akan dilakukan pembobotan terhadap area Indeks KAMI versi 3.1 yang kemudian semua skor pembobotan akan dijumlahkan dan menghasilkan skor total pada *dashboard* yang ada di Indeks KAMI versi 3.1. Total skor tersebut akan menggambarkan kondisi keamanan informasi yang ada di DPTSI ITS Suarabaya.

Berdasarkan hasil gambaran kondisi keamanan informasi yang ada akan dibuatkan rekomendasi berdasarakan area yang dinilai masih kurang baik. Keseluruhan data yang tekait dengan operasi matematis diolah menggunakan perantara *Dashboard* Indeks KAMI yang dikembangkan dari *software* Microsoft Office Excel.

4.6 Penentuan Pendekatan Analisis

Analisis terhadap data perlu dilakukan setelah melakukan pengumpulan data. Hal ini dilakukan untuk mengetahui hubungan antara data dengan objek yang diinginkan. Beberapa pendekatan yang akan dilakukan adalah:

- **Pendekatan Penggunaan Kategori Sistem Elektronik Indeks KAMI**
  Pendekatan ini adalah merupakan tahap awal dari Indeks KAMI yang digunakan untuk mengetahui tingkat

klasifikasi terhadap kategori sistem elekatronik yang digunakan di DPTSI ITS Surabaya.

- **Pendekatan 5 Area Keamanan Informasi Indeks KAMI**
  Pendekatan ini digunakan untuk membantu proses identifikasi kesiapan dan kelengkapan keamanan informasi di DPTSI ITS yang nantinya akan dilakukan penilaian terhadap 5 area tersebut.
- **Pemberian Rekomendasi Perbaikan**
  Rekomendasi yang diberikan mengacu pada standar kontrol keamanan informasi ISO/IEC 27002:2013 dimana standar ini memberikan panduan serta rekomendasi dalam perencanaan dan implementasi suatu program untuk melindungi aset informasi ukuran pemetaan sasaran kontrol keamanan informasi yang meliputi berbagai aspek berikut ini:

  - Kebijakan Keamanan Informasi (*Information Security Policies*)
  - Organisasi Keamanan Informasi (*Organization of Information Security*)
  - Keamanan Sumber Daya Manusia (*Human Resources Security*)
  - Manajemen Aset (*Asset Management*)
  - Akses Kontrol (*Access Control*)
  - Kriptografi (*Cryptography)*
  - Keamanan Fisik dan Lingkungan (*Physical and Environtmental Security*)
  - Keamanan Operasi (*Operations Security)*
  - Keamanan Komunikasi (*Communications Security*)
  - Pengadaan/akuisisi, Pengembangan dan Pemeliharaan Sistem (*Systems Acquisitions, Development, and Maintenance*)
  - Hubungan Pemasok (*Supplier Relationships)*
  - Pengelolaan Insiden Keamanan Informasi (*Information Security Incident Management*)

- Aspek Keamanan Informasi Manajemen Kelangsungan Usaha (*Information Security Aspects of Business Continuity Management*)
- Kesesuaian (*Compliance*)

"Halaman ini sengaja dikosongkan"

BAB V
IMPLEMENTASI

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

5.1 Profil Organisasi

Pada bagian ini dibahas mengenai profil dari Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya.

5.1.1 Sejarah Singkat DPTSI ITS Surabaya

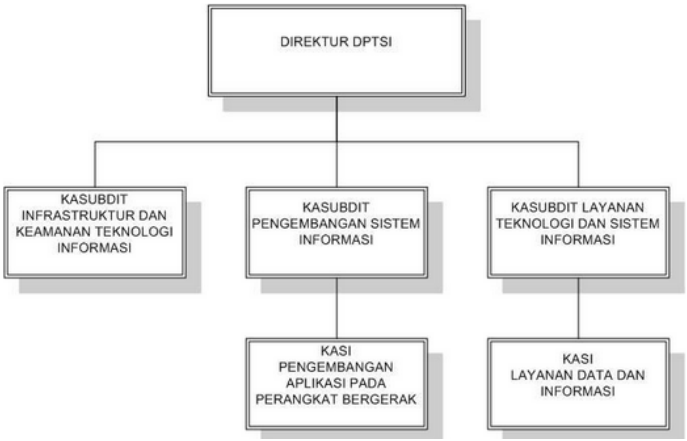
Institut Teknologi Sepuluh Nopember memiliki UPT Pusat Komputer yang telah lama berdiri. UPT Pusat Komputer ini berkembang menjadi Badan Teknologi Sistem Informasi (BTSI) pada tahun 2012 berdasarkan SK Rektor ITS. Kemudian dengan OTK Permendikbud nomor 86 tahun 2013, BTSI berubah nama lagi menjadi Direktorat Pengembangan Teknologi Sistem Informasi (DPTSI) [2]. Pada bulan Oktober 2016 ini DPTSI ITS berubah nama lagi menjadi Direktorat Pengembangan Teknologi dan Sistem Informasi atau DPTSI.

Direktorat ini mempunyai beberapa ranah tugas yang berkaitan dengan melaksanakan penyiapan perumusan kebijakan pengembangan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan di bidang teknologi dan sistem informasi.

5.1.2 Struktur Organisasi dan Tugas Pokok DPTSI ITS Surabaya

DPTSI memiliki beberapa fungsi dalam menjalankan tugasnya yang akan dijabarkan seperti dibawah ini [27]:

- Penyusunan rencana, program, dan anggaran lembaga.
- Pelaksanaan penelitian dan pengembangan teknologi dan sistem informasi.
- Pelaksanaan penjaminan keamanan sistem informasi.
- Pelaksanaan peningkatan kemampuan dan kompetensi tenaga pendidikan di bidang teknologi dan sistem informasi.
- Pengelolaan sistem informasi berbasis web.
- Pelaksanaan pemberian layanan jasa dibidang teknologi dan sistem informasi.
- Pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi.
- Pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi.
- Pelaksanaan urusan administrasi Lembaga.



Gambar 5.1 Struktur Organisasi DPTSI ITS

Direktorat Pengembangan Teknologi Sistem Informasi juga menjalankan beberapa tugas pokok yang harus dikerjakan dan menjadi tanggung jawab semua anggota yang ada di DPTSI. Berikut adalah beberapa tugas pokok yang dijalankan di DPTSI

yang dikoordinasikan bersama oleh pusat-pusat tersebut dalam Tabel 5.1 berikut [3]:

Tabel 5.1 Tugas Pokok di DPTSI ITS Surabaya

NO	TUGAS POKOK DAN FUNGSI (TUPOKSI) DPTSI	PUS YAN	PUS NET	PUSB ANG
1	Menyusun dan melaksanakan Rencana Induk Pengembangan Teknologi dan Sistem Informasi;	V	V	V
2	Menetapkan Standar teknologi dan sistem informasi yang dibutuhkan;	V	V	V
3	Mengembangkan standar data dan informasi;	V		
4	Melakukan audit sistem informasi;			V
5	Mengelola database ITS;	V	V	V
6	Menyediakan dan mengelola infrastruktur;		V	
7	Menyediakan dan mengelola situs dan portal ITS yang berkualitas;	V		
8	Menyediakan dan mengelola aplikasi sistem informasi berbasis web untuk mengoptimalkan e-layanan;			V
9	Menyediakan dan mengelola paket program lisensi tunggal;	V		

NO	TUGAS POKOK DAN FUNGSI (TUPOKSI) DPTSI	PUS YAN	PUS NET	PUSB ANG
10	Menjamin keamanan sistem informasi;		V	
11	Menyediakan layanan komunikasi suara dan video berbasis teknologi dan sistem informasi;		V	
12	Mendukung peningkatan kemampuan dan kompetensi tenaga kependidikan di bidang teknologi dan sistem informasi	V	V	V
13	Menyediakan dan mengelola knowledge management system	V		
14	Mengelola ICT Center, E-learning dan pembelajaran jarak jauh;		V	
15	Mengkoordinasikan jaringan kerjasama antar institusi berbasis teknologi dan sistem informasi;		V	
16	Menyediakan jasa di bidang teknologi dan sistem informasi dengan berbagai pihak	V	V	V

5.1.3 Peran Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi

Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi dipimpin oleh seorang Kasubdit. Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan

pemantauan, evaluasi, pemeliharaan, dan pelaporan untuk pengembangan dan pengkajian infrastruktur dan keamanan teknologi informasi [28].

Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi DPTSI juga menyelenggarakan fungsinya sebagai berikut ini [28]:

- penyiapan bahan perumusan kebijakan dan standar mutu pengembangan infrastruktur dan keamanan teknologi informasi
- pelaksanaan pengembangan infrastruktur dan keamanan teknologi informasi
- pelaksanaan pengawasan dan pemantauan pengembangan infrastruktur dan keamanan teknologi informasi
- pelaksanaan pemeliharaan infrastruktur dan keamanan teknologi informasi
- pelaksanaan evaluasi dan pelaporan infrastruktur dan keamanan teknologi informasi

5.1.4 Peran Subdirektorat Pengembangan Sistem Informasi

Subdirektorat Pengembangan Sistem Informasi dipimpin oleh seorang Kasubdit dan dibantu oleh Seksi Pengembangan Aplikasi pada Perangkat Bergerak. Subdirektorat Pengembangan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan pengembangan sistem informasi [28].

Subdirektorat Pengembangan Sistem Informasi DPTSI juga menyelenggarakan fungsinya sebagai berikut ini [28]:

- penyiapan bahan perumusan kebijakan dan standar mutu pengembangan sistem informasi
- pelaksanaan pengembangan sistem informasi

- pelaksanaan pengawasan dan pemantauan pengembangan sistem informasi
- pelaksanaan pemeliharaan data dan sistem informasi
- pelaksanaan evaluasi dan pelaporan pengembangan sistem informasi

5.2 Hasil Wawancara dan Observasi

Berdasarkan perancangan studi kasus yang telah dilakukan sebelumnya mengenai Indeks Keamanan Informasi, yaitu melakukan wawancara dengan:

- Bapak Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D selaku Kepala SubDirektorat Infrastruktur dan Keamanan Teknologi pada tanggal 28 November 2016, 29 November 2016, dan 30 November 2016
- Ibu Hanim Maria Astuti, S.Kom., M.Sc. selaku Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi pada tanggal 6 Desember 2016
- Ibu Anny Yuniarti, S.Kom., M.Comp.Sc. selaku Kepala SubDirektorat Pengembangan Sistem Informasi pada tanggal 24 November 2016 dan 9 Desember 2016
- Bapak Satriyo Wicaksono, S.Kom, Bapak Achmad Bustari, A.Md., Bapak Cahya Purnama Dani, A.Md., dan Bapak Jananta Permata Putra, S.ST selaku staff dari SubDirektorat Infrastruktur & Keamanan Teknologi Informasi pada tanggal 24 November 2016, 28 November 2016, dan 5 Desember 2016

Wawancara dan observasi secara langsung dilakukan di DPTSI ITS dan perpustakaan ITS lantai 6 dimana merupakan kantor utama staff SubDirektorat Infrastruktur & Keamanan Teknologi Informasi. Hasil wawancara dapat dilihat secara detail pada **LAMPIRAN B.** Dari hasil wawancara dan observasi tersebut didapatkan beberapa fakta atau temuan yang menggambarkan secara umum kondisi kekinian keamanan informasi yang secara singkat diuraikan dalam beberapa poin berikut.

5.2.1 Kategori Penggunaan Sistem Elektronik di DPTSI ITS Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi DPTSI ITS Surabaya dengan penggunaan Sistem Elektronik pada Indeks KAMI.

Untuk kondisi kekinian dari penggunaan sistem elektronik terbilang sangat penting karena data yang disimpan mengandung data yang rahasia dan terbatas, data pribadi yang berhubungan juga dengan data pribadi lainnya. Dampak dari kegagalan penggunaan sistem elektronik di DPTSI juga dapat berpengaruh terhadap tidak tersedianya layanan publik berskala nasional/ dapat membahayakan pertahanan negara. Pengguna dari sistem elektronik di DPTSI ITS juga terdiri dari seluruh civitas akademik yang berjumlah ± 5.000 pengguna. Kriteria Hasil wawancara secara lengkap dapat dilihat pada **LAMPIRAN B**.

5.2.2 Tata Kelola Keamanan Informasi di DPTSI ITS Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi DPTSI ITS Surabaya dengan kriteria Tata Kelola Keamanan Informasi pada Indeks KAMI.

Untuk kondisi kekinian dari tata kelola keamanan informasi sudah diberikan tanggung jawab kepada bagian-bagian tertentu dengan keahlian tertentu dan memadai kebutuhan DPTSI untuk menjaga keamanan informasi yang ada. Untuk kebijakan terkait keamanan informasi juga sudah dimiliki oleh pihak DPTSI dan akan dilakukan pelaporan kondisi keamanan informasi kepada kepala instansi.

Kekurangan dari pelaksanaan pentata kelolaan keamanan informasi yang ada di DPTSI ITS adalah masih belum lengkapnya dokumen-dokumen yang menjelaskan pembagian kewenangan dan tanggung jawab dari masing-masing individu, belum adanya dokumen yang membahas tentang BCP dan DRP, serta belum adanya penggunaan standar tertentu terkait kompetensi dan keahlian pelaksana pengelolaan keamanan informasi. Kriteria Hasil wawancara secara lengkap dapat dilihat pada **LAMPIRAN B**.

5.2.3 Pengelolaan Risiko Keamanan Informasi di DPTSI ITS Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi DPTSI ITS Surabaya dengan kriteria Pengelolaan Risiko Keamanan Informasi pada Indeks KAMI.

Untuk kondisi kekinian dari pengelolaan risiko keamanan informasi yaitu sudah ditentukan batas ambang risiko yang dapat diterima, ada pencatatan mengenai kepemilikan aset, dilakukan kajian risiko terkait dampak dan mitigasi risiko.

Kekurangan dari pelaksanaan pengelolaan risiko ini yaitu masih belum adanya bagian-bagian tertentu yang bertanggung jawab langsung dalam mengelola risiko keamanan informasi, belum adanya kerangka kerja risiko yang digunakan, tidak ada pencatatan terkait penyelesaian risiko, dan tidak ada dokumen yang mendaftar semua ancaman terkait aset informasi. Kriteria Hasil wawancara secara lengkap dapat dilihat pada **LAMPIRAN B**.

5.2.4 Kerangka Kerja Pengelolaan Keamanan Informasi di DPTSI ITS Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi DPTSI

ITS Surabaya dengan kriteria Kerangka Kerja Pengelolaan Keamanan Informasi pada Indeks KAMI.

Untuk kondisi kekinian dari kerangka kerja keamanan informasi yang ada yaitu untuk prosedur kebijakan terkait keamanan sudah ada namun tidak tidak terlalu lengkap, dilakukan publikasi prosedur kebijakan kepada semua karyawan, dilakukan identifikasi kondisi yang berbahaya dengan menggunakan log ids, ada kontrak dengan pihak lain yang menyangkut HAKI, dilakukan keterkaitan keamanan informasi dengan manajemen proyek, dibuatnya dokumen pengembangan aplikasi (SDLC), ada strategi dalam menangani keamanan informasi.

Kekurangan dari pelaksanaan kerangka kerja keamanan informasi yaitu masih belum diterapkan program audit internal, belum ada penilaian aspek finansial dalam kebijakan prosedur, program keaman informasi jangka panjang juga masih dalam proses perancangan, belum ada dokumen kebijakan terkait penggunaan daftar induk, belum adanya dokumen resmi terkait konsekuensi khusu bagi para pelanggan aturan di ITS, belum ada kebijakan terkait *security patch*, dan belum dilakukannya evaluasi terhadap prosedur kebijakan keamanan informasi. Kriteria Hasil wawancara secara lengkap dapat dilihat pada **LAMPIRAN B**.

5.2.5 Pengelolaan Aset Informasi di DPTSI ITS Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi DPTSI ITS Surabaya dengan kriteria Pengelolaan Aset Informasi pada Indeks KAMI.

Untuk kondisi kekinian dari pengelolaan aset informasi yang ada yaitu sudah ada daftar inventaris aset, dilakukan pencatatan insiden, dilakukan backup data secara berkala, ada ketentuan

pengamanan fisik sesuai dengan kepentingan aset informasi, ada proses mengelola kunci fisik dan elektronik untuk fasilitas fisik, infrastruktur TI juga sudah dilindungi dari bencana dan listrik, dan untuk ruang server yang berada di DPTSI sudah sesuai dengan standar ruang server yang seharusnya.

Kekurangan dari pelaksanaan pengelolaan aset informasi yaitu belum adanya undang-undang yang digunakan untuk klasifikasi aset, tanggung jawab per individu belum dijabarkan secara keseluruhan, tidak ada tata tertib terkait penggunaan email dan komputer, tidak ada kebijakan tertulis untuk pengelolaan passord dan username, prosedur untuk mutasi user masih dalam perencanaan, dan masih belum adanya mekanisme pengamanan fisik dalam pengiriman aset. Kriteria Hasil wawancara secara lengkap dapat dilihat pada **LAMPIRAN B.**

5.2.6 Teknologi dan Keamanan Informasi di DPTSI ITS Surabaya

Hasil dari wawancara ini nantinya akan digunakan pada tahap penilaian atau dengan kata lain untuk memetakan posisi DPTSI ITS Surabaya dengan kriteria Teknologi dan Keamanan Informasi pada Indeks KAMI.

Untuk kondisi kekinian dari teknologi dan keamanan informasi yang ada yaitu sudah dilakukan pengamanan secara berlapis, dilakukan segmentasi jaringan sesuai kebutuhan, dilakukan monitor terhadap jaringan dan sistem aplikasi, dilakukan perlindungan aset dari virus, dilakukan sinkronisasi waktu yang akurat, ada monitor terhadap upaya masuk oleh oknum tertentu, dan pembuatan aplikasi sudah sesuai dengan standar.

Kekurangan dari kondisi teknologi dan keamanan informasi yaitu tidak adanya standar keamanan yang digunakan secara tertulis, belum dilakukan scan pada celah keamanan secara rutin, tidak ada dokumen untuk penerapan keamanan berlapis, tidak ada dokumen daftar penyerangan virus, dan tidak ada standar tertentu yang digunakan untuk pengembangan aplikasi.

Kriteria Hasil wawancara secara lengkap dapat dilihat pada **LAMPIRAN B**.

5.3 Hasil Review Dokumen

Seperti yang telah disebutkan di BAB IV sebelumnya tentang dokumen-dokumen yang dibutuhkan untuk menjadi bukti bahwa pelaksaaan sistem manajemen keamanan informasi yang dilakukan oleh DPTSI ITS Surabaya sudah memnuhi standar yang ada, maka dibawah ini akan dijabarkan kembali data apa saja yang sudah dimiliki oleh DPTSI ITS Surabaya dan data apa saja yang belum ada:

Tabel 5.2 Ketersediaan Dokumen Pendukung DPTSI ITS Surabaya

No	Dokumen yang Diperlukan	Ketersediaan Dokumen
1.	Dokumen anggaran sistem elektronik	Tersedia
2.	Dokumen dampak dan kerugian kegagalan sistem elektronik	Tidak tersedia
3.	Dokumen tupoksi dan struktur organisasi bagian keamanan informasi	Tersedia
4.	Dokumen standar kompetensi bagi SDM keamanan informasi	Tidak tersedia
5.	Dokumen undang-undang tentang identifikasi data pribadi	Tidak tersedia
6.	Dokumen keberlanjutan bisnis mengenai layanan TIK	Tidak tersedia
7.	Dokumen hasil laporan kondisi keamanan informasi	Tidak tersedia
8.	Dokumen standar dan perangkat hukum terkait keamanan informasi	Tidak tersedia

No	Dokumen yang Diperlukan	Ketersediaan Dokumen
9.	Dokumen program kerja pengelolaan risiko keamanan informasi	Tidak tersedia
10.	Dokumen struktur organisasi dan tupoksi mengenai manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi	Tidak tersedia
11.	Dokumen framework pengelolaan risiko keamanan informasi	Tidak tersedia
12.	Dokumen klasifikasi aset, tingkat ancaman, dan dampak kerugian keamanan informasi	Tersedia beberapa
13.	- Dokumen analisa/kajian risiko keamanan informasi - Dokumen mitigasi risiko beserta prioritas penyelesaiannya - Dokumen evaluasi langkah mitigasi secara berkala - Dokumen evaluasi framework pengelolaan risiko	Tidak tersedia
14.	Dokumen daftar inventaris aset informasi dan aset TI	Tersedia
15.	Dokumen pengelolaan konfigurasi	Tersedia
17.	Tata tertib penggunaan komputer, email, inetrnet, dan intranet Tata tertib penggunaan dan pengaman aset	Tidak tersedia

No	Dokumen yang Diperlukan	Ketersediaan Dokumen
18.	Dokumen peraturan instalasi software dan penggunaan data pribadi	Tidak tersedia
19.	Dokumen syarat serta prosedur penghancuran data dan pertukaran data dengan pihak eksternal	Tidak tersedia
20.	Dokumen prosedur backup dan restore	Tidak tersedia
21.	Dokumen pelaporan insiden keamanan informasi pada pihak internal dan eksternal	Tidak tersedia
22.	Dokumen pengelolaan fasilitas fisik/ lokasi kerja	Tidak tersedia
23.	Dokumen peraturan pengamanan lokasi ruang server dan ruang arsip	Tersedia
24.	Dokumen log perubahan sistem informasi dan upaya akses yang tidak pantas	Tersedia
25.	Dokumen standar penggunaan enkripsi	Tidak tersedia
26.	Dokumen verifikasi & validasi pengembangan aplikasi	Tersedia

5.4 Hambatan

Dalam melakukan wawancara dan observasi penulis terbantu dengan tanggapan pihak DPTSI ITS yang bersedia ditemui di DPTSI ITS apabila diperlukan komunikasi secara langsung. Namun ada beberapa hambatan yang perlu dilalui oleh penulis, diantaranya :

- Untuk pembalasan pesan melalui email dari pihak DPTSI ITS masih terlalu lama karena membutuhkan beberapa hari untuk mendapatkan data yang dikirim melalui email.
- Penulis kesulitan untuk mendapatkan data seperti dokumen dan foto karena harus menemui pihak-pihak tertentu diluar rencana sebelumnya dari penulis.
- Jawaban yang diberikan oleh narasumber terkadang berbeda satu dengan yang lainnya.
- Saat pengambilan data di Ruang IKTI lantai 6 agak kesulitasn karena pihak narasumber sibuk untuk pindahan ruang ke gedung baru yang telah disediakan pihak ITS.

BAB VI
HASIL DAN PEMBAHASAN

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

6.1 Hasil Analisis Kesenjangan Pengelolaan Keamanan Informasi

Berikut ini adalah analisis kesenjangan yang didapatkan antara kondisi kekinian yang ada di Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya dengan kondisi ideal yang tertera didalam Indeks KAMI yang mengacu pada standar ISO 27002:2013. Analisis kesenjangan ini akan dilakukan untuk masing-masing area keamanan informasi yang ada pada Tabel 6.1- Tabel 6.5:

Tabel 6.1 Analisis Kesenjangan Kategori Tata Kelola Keamanan Informasi

Kondisi Kekinian	Kondisi Ideal
- Dibentuk Sub Direktorat Infrastruktur dan Keamanan Informasi yang bertugas khusus menangani keamanan informasi di ITS - Sumber daya keamanan informasi yang disediakan masih kurang dan belum dipetakan secara lengkap/ belum ada segregasi kewenangan yang paten - Belum ada standar untuk patokan minimum kompetensi dan keahlian dari staff pengelolaan keamanan informasi	- Dibentuk bagian khusus untuk menangani infrastruktur dan keamanan informasi dalam sebuah instansi dengan sumber daya yang memadai dan pembagian kewenangan yang baik dan tertulis - Digunakan standar untuk menentukan kompetensi minimum dari staff keamanan informasi - Dilakukan program peningkatan kompetensi

Kondisi Kekinian	Kondisi Ideal
- Sudah diterapkan program peningkatan kompetensi untuk staff pengelolaan keamanan informasi, seperti pelatihan terkait keamanan. Pelatihan tidak diikuti oleh semua staff bagian keamanan informasi karena sistem yang digunakan yaitu akan ada *sharing* pengetahuan dari staff yang mengikuti pelatihan ke staff yang tidak mengikuti pelatihan - Pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengguna internal dan eksternal untuk menyelesaikan masalah yang ada, namun untuk dokumen dengan pihak terkait masih belum ada - Pelaporan kondisi keamanan informasi dilakukan secara rutin kepada pimpinan instansi, namun tidak ada dokumen pelaporan yang dibuat - Pertanggung jawaban pada dokumen BCP dan DRP masih belum terpusat dan belum ada secara formal - Belum ada program penilaian kinerja pengelolaan keamanan informasi untuk masing-masing staff terkait	untuk seluruh staff keamanan informasi - Dilakukan dokumentasi terhadap adanya koordinasi dengan pihak internal maupun eksternal untuk menyelesaikan permasalahan terkait keamanan informasi - Dilakukan dokumentasi terhadap laporan kondisi keamanan informasi secara ruti yang akan diberikan kepada pimpinan instansi - Dibuat dokumen BCP dan DRP secara formal dan terpusat - Dibuat program untuk melakukan penilaian terhadap kinerja staff pengelolaan keamanan informasi terkait - Mengacu pada standar tertentu untuk pengelolaan keamanan informasi - Dibuat kebijakan dan langkah-langkah penanggulangan insiden keamanan informasi yang juga terkait hukum pidana dan perdata

Kondisi Kekinian	Kondisi Ideal
- Belum ada standar terkait pengamanan informasi yang harus dipatuhi - Belum diterapkan kebijakan dan langkah penanggulangan insiden keamanan informasi terkait hukum pidana dan perdata	
Kesenjangan: - Kurangnya jumlah SDM yang menangani pengelolaan keamanan informasi dan belum ada pembagian wewenang yang tertulis secara baik - Tidak adanya standar untuk patokan minimum kompetensi dan keahlian dari staff pengelolaan keamanan informasi - Program peningkatan kompetensi yang dilakukan untuk staff pengelolaan keamanan informasi masih belum merata dan tidak dapat dipastikan bahwa seluruh staff terkait bisa mendapatkan ilmu yang sepadan - Tidak adanya dokumen koordinasi dengan pihak pengguna internal dan eksternal - Tidak adanya dokumen BCP dan DRP yang formal dan terpusat - Tidak adanya program penilaian kinerja pengelolaan keamanan informasi untuk masing-masing staff - Tidak adanya standar terkait pengamanan informasi yang harus dipatuhi - Tidak adanya kebijakan dan langkah penanggulangan insiden keamanan informasi terkait hukum pidana dan perdata	

Tabel 6.2 Analisis Kesenjangan Kategori Pengelolaan Risiko Keamanan Informasi

Kondisi Kekinian	Kondisi Ideal
- Belum ada proker terkait pengelolaan risiko keamanan	- Terdapat proker beserta dokumentasi yang

Kondisi Kekinian	Kondisi Ideal
informasi yang didokumentasikan - Belum ada bagian yang bertanggung jawab terhadap manajemen risiko keamanan informasi - Belum ada kerangka kerja yang digunakan terkait pengelolaan risiko keamanan informasi beserta dokumentasinya - Belum dilakukan dokumentasi keterhubungan klasifikasi aset informasi, tingkat ancaman, dan dampak yang dihasilkan dari terjadinya risiko keamanan informasi - Ambang batas risiko sudah dipantau melalui log sensor yang ditangani bagian Sub Direktorat Infrastruktur dan Keamanan Informasi - Terdapat dokumen yang berisi kepemilikan aset dan pihak pengelolanya - Dilakukan kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada termasuk langkah mitigasinya sesuai tingkat prioritas penyelesaian namun tidak terdapat dokumentasi yang resmi - Status dari langkah mitigasi dipantau secara berkala	mengarah pada pengelolaan risiko keamanan informasi - Dibentuk bagian khusus yang bertanggung jawab terhadap pengelolaan manajemen risiko keamanan informasi - Menggunakan kerangka kerja khusus terkait pengelolaan risiko keamanan informasi dan dilakukan dokumentasi pengelolaan risiko keamanan informasi - Dilakukan dokumentasi/ pencatatan terkait klasifikasi aset informasi, tingkat ancaman, dan dampak yang yang dihasilkan dari risiko keamanan informasi - Dilakukan penetapan ambang batas risiko yang dapat diterima oleh instansi - Memiliki pencatatan terkait kepemilikan aset dan custodian yang bertanggung jawab sebagai pengelola aset - Dilakukan kajian terkait risiko keamanan informasi terhadap aset informasi, langkah mitigasi risiko, dan

Kondisi Kekinian	Kondisi Ideal
namun tidak secara resmi melainkan hanya melalui grup chat oleh pihak DPTSI	tingkat prioritasi penyelesaian risiko yang ada dan dilakukan pencatatan - Dilakukan pemantauan terhadap langkah mitigasi yang dilakukan secara berkala dan resmi dengan adanya pencatatan bahwa insiden telah selesai ditangani dengan baik - Kerangka kerja pengelolaan risiko harus dikaji secara berulang untuk memastikan keefektivitasannya
Kesenjangan: - Tidak adanya proker terkait pengelolaan risiko keamanan informasi - Tidak adanya bagian khusus yang bertanggung jawa menangani pengelolaan risiko keamanan informasi - Tidak adanya kerangka kerja yang digunakan terkait pengelolaan risiko keamanan informasi, seperti standar ISO 27001:2013 - Tidak adanya dokumentasi keterhubungan klasifikasi aset informasi, tingkat ancaman, dan dampak yang dihasilkan dari terjadinya risiko keamanan informasi - Tidak adanya dokumentasi secara resmi terkait dengan kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada termasuk langkah mitigasinya sesuai tingkat prioritas penyelesaian - Tidak adanya pemantauan langkah mitigasi secara resmi dan berkala (dalam bentuk pencatatan dokumen) dengan status yang selalu diperbarui	

Kondisi Kekinian	Kondisi Ideal
- Tidak dilakukan pengkajian ulang terhadap kerangka kerja pengelolaan risiko karena pihak DPTSI masih belum menerapkan penggunaan kerangka kerja pengelolaan risiko keamanan informasi	

Tabel 6.0.3 Analisis Kesenjangan Kategori Kerangka Kerja Pengelolaan Keamanan Informasi

Kondisi Kekinian	Kondisi Ideal
- Terdapat beberapa kebijakan dan prosedur terkait keamanan informasi yang mencantumkan peran dan tanggung jawab masing-masing pihak - Dilakukan publikasi terhadap adanya kebijakan dan prosedur kepada seluruh staff DPTSI - Tidak dilakukan mekanisme dalam pengelolaan distribusi, penyimpanan, dan penarikan dari peredaran terkait kebijakan dan prosedur keamanan informasi - Tidak dilakukan proses pengkomunikasian kebijakan keamanan informasi serta perubahannya pada pihak ketiga - Dilakukan identifikasi dan pemantauan secara rutin terkait kondisi yang membahayakan keamanan informasi dengan menggunakan log sensor ids. Namun untuk dokumentasi	- Terdapat kebijakan dan prosedur yang dibuat untuk semua bahasan keamanan informasi beserta peran dan tanggung jawab masing-masing pihak - Dilakukan publikasi terkait adanya kebijakan dan prosedur kepada seluruh staff instansi - Terdapat mekanisme pengelolaan distribusi, penyimpanan, dan penarikan dari peredaran kebijakan dan prosedur keamanan informasi - Selalu dilakukan komunikasi terkait perubahan kebijakan keamanan informasi dengan pihak ketiga - Harus dilakukan pemantauan dan pencatatan secara rutin terkait kondisi yang membahayakan keamanan informasi

Kondisi Kekinian	Kondisi Ideal
pencatatan masih belum dilakukan - Kontrak dengan pihak ketiga juga mendefinisikan tentang pelaporan insiden, HAKI, tata tertib penggunaan dan pengamanan aset - Konsekuensi atas pelanggaran kebijakan keamanan informasi sudah didefinisikan namun ada pada peraturan kemahasiswaan yang dikelola oleh Bagian Hukum ITS - Dilakukan implementasi *security patch*, alokasi tanggung jawab untuk melakukan monitor adanya *security patch* baru, dan memastikan pemasangannya. Namun belum ada kebijakan dan prosedur yang dibuat terkait *security patch* - Dilakukan pembahasan terkait keamanan informasi dalam pelaksanaan manajemen proyek - Dilakukan penerapan SDLC dengan aman. Penggunaan SDLC tidak selalu sama untuk masing-masing aplikasi yang dikembangkan dan tidak semua	- Kontrak dengan pihak ketiga harus lengkap berisi tentang HAKI, pelaporan adanya insiden, dan tata tertib penggunaan aset - Pihak instansi harus menerapkan kebijakan yang berisi konsekuensi bagi pelanggar keamanan informasi - Penerapan kebijakan dan prosedur terhadap implementasi *security patch*, alokasi tanggung jawab untuk melakukan monitor adanya *security patch* baru, dan memastikan pemasangannya - Pembahasan terkait keamanan informasi harus dilakukan saat melakukan proses manajemen proyek - Pembuatan dokumentasi SDLC untuk setiap pembangunan aplikasi baru - Dilalukan pengelolaan BCP yang disesuaikan dengan standar yang ada dan dilakukan evaluasi secara berkala - Dilakukan evaluasi secara berkala dan secara

Kondisi Kekinian	Kondisi Ideal
pembangunan aplikasi memiliki dokumentasi - Belum adanya kerangka kerja yang digunakan terkait pengelolaan BCP - Belum dilakukan evaluasi terhadap keseluruhan kebijakan dan prosedur keamanan informasi - Sudah dilakukan strategi penerapan keamanan informasi sesuai dengan hasil analisis risiko. Integrasi biasanya dilakukan dengan Sub Direktorat Pengembangan - Dilakukan realisasi strategi penerapan keamanan informasi sebagai bagian dari pelaksanaan proker DPTSI - Belum pernah dilakukan audit internal dan evaluasinya - Tidak ada penilaian terkait aspek finansial untuk merevisi kebijakan dan prosedur yang berlaku - DPTSI mempunyai rencana untuk meningkatkan keamanan informasi untuk jangka menengah/ panjang dengan menerapkan standar ISO 270001: 2013	keseluruhan pada kebijakan dan prosedur keamanan informasi yang digunakan - Menentukan strategi dalam melakukan penerapan keamanan informasi sesuai dengan hasil analisis risiko yang dilakukan sebelumnya. Strategi juga diperbarui sesuai dengan kebutuhan dan perubahan profil risiko - Dilakukan audit internal untuk melakukan evaluasi tingkat kepatuhan, konsistensi, dna efektivitas penerapan keamanan informasi - Dilakukan evaluasi hasil audit internal untuk identifikasi langkah pembenahan dan pencegahan atau peningkatan kinerja keamanan informasi. Dilakukan juga pelaporan hasil audit internal kepada pihak pimpinan instansi - Dilakukan revisi terhadap kebijakan dan prosedur yang berlaku dan dilakukan analisis untuk menilai aspek finansial

Kondisi Kekinian	Kondisi Ideal
Kesenjangan: - Tidak adanya mekanisme dalam pengelolaan distribusi, penyimpanan, dan penarikan dari peredaran terkait kebijakan dan prosedur keamanan informasi - Tidak adanya proses pengkomunikasian kebijakan keamanan informasi serta perubahannya pada pihak ketiga - Tidak adanya dokumentasi dan pencatatan terkait identifikasi dan pemantauan secara rutin tentang kondisi yang membahayakan keamanan informasi - Tidak adanya kebijakan dan prosedur implementasi *security patch*, alokasi tanggung jawab untuk melakukan monitor adanya *security patch* baru, dan memastikan pemasangannya - Penerapan SDLC tidak dilakukan untuk semua pembangunan aplikasi yang dilakukan di DPTSI - Tidak adanya kerangka kerja yang digunakan terkait pengelolaan BCP - Tidak dilakukan evaluasi terhadap keseluruhan kebijakan dan prosedur keamanan informasi - Tidak adanya kegiatan audit internal yang terdiri dari rencana audit, audit program, evaluasi hasil, dan pelaporan hasil audit pada pimpinan instansi yang diterapkan di DPTSI ITS	

Tabel 6.4 Analisis Kesenjangan Kategori Pengelolaan Aset Informasi

Kondisi Kekinian	Kondisi Ideal
- Tersedia daftar inventaris aset informasi dan kepemilikan dari aset tersebut - Klasifikasi aset informasi dan evaluasi klasifikasi aset tidak disesuaikan dengan peraturan perundangan karena memang	- Dibuat daftar inventaris aset informasi secara lengkap berisi kode dan kepemilikan inventaris tersebut - Dilakukan klasifikasi aset informasi yang disesuaikan dengan peraturan perundang-

Kondisi Kekinian	Kondisi Ideal
belum ada penerapan undang-undang di DPTSI - Tingkatan akses sudah tidak dibedakan dengan proxy lagi melalainkan menggunakan *single sign on* dengan akun integra masing-masing user - Dilakukan proses pengolahan perubahan terhadap konfigurasi teknologi informasi - Dilakukan pemrosesan dalam merilis aset baru kedalam lingkungan operasional dan memperbarui inventaris aset informasi - Terdapat pendefinisian tanggung jawab pengamanan informasi untuk masing-masing individu bagian Infrastruktur & Keamanan Informasi - Tidak ada tata tertib terkait penggunaan komputer, email, internet, intranet, dan pengamanan aset terkait HAKI - Peraturan terhadap instalasi *software* sudah dicantumkan beberapa dalam website khusus, yaitu https//unduh.its.ac.id - Tidak ada peraturan terhadap penggunaan data pribadi yang bersyaratkan harus	undangan terkait dan dilakukan evaluasi secara berkala untuk memantau klasifikasi aset informasi yang dimiliki - Tingkatan akses dapat dibedakan dengan menggunakan beberapa cara yang berbeda - Adanya penerapan terkait pengolahan perubahan untuk konfigurasi teknologi informasi yang dimiliki instansi - Ada proses untuk merilis aset baru dalam lingkungan operasional dan memperbarui inventaris aset informasi - Tanggung jawab individu harus dibagi secara jelas untuk melakukan tindakan pengamanan informasi - Dibuat tata tertib terkait penggunaan komputer, email, internet, intranet, dan pengamanan aset instansi terkait HAKI - Dibuat peraturan mengenai instalasi *software* secara lengkap - Dibuat peraturan terkait penggunaan data pribadi dimana harus ada ijin tertulis oleh pemilik data

Kondisi Kekinian	Kondisi Ideal
adanya ijin tertulis oleh pemilik data pribadi - Tidak ada kebijakan terhadap pelanggaran dari pengelolaan identitas serta proses otentikasi (username & password) - Tidak ada prosedur dan syarat terkait pemberian akses, otentikasi, dan otorisasi untuk penggunaan aset informasi - Tidak ada prosedur terkait tindakan backup dan restore namun dilakukan secara rutin untuk semua data-data yang ada didalam database - Dilakukan pendefinisian zona untuk pengamanan fisik aset informasi yang ada - Dilakukan pengecekan latar belakang SDM saat masa perekrutan karyawan, namun tidak ada bentuk tertulisnya - Dilakukan koordinasi pelaporan insiden keamanan informasi dengan pihak eksternal - Terdapat prosedur penghancuran dokumen yang sudah tidak diperlukan lagi - Prosedur untuk mutasi user atau tenaga kontrak yang habis masa kerjanya masih dalam proses pembuatan	pribadi jika ingin ada penggunaan data tersebut oleh pihak lain - Diterapkan kebijakan dan prosedur pelanggaran dari pengelolaan identitas serta proses otentikasi (username & password) dan pemberian akses, otentikasi, dan otorisasi untuk penggunaan aset informasi - Dibuat beberapa lapis zona yang berbeda untuk pengamanan fisik aset informasi yang ada - Harus dilakukan koordinasi pelaporan insiden keamanan informasi dengan pihak eksternal - Memiliki dan menerapkan prosedur penghancuran dokumen dan dat yang sudah tidak diperlukan lagi - Dibuat prosedur dan kebijakan terkait mutasi user atau tenaga kontrak yang habis masa kerjanya - Dibuat daftar data apa saja yang harus di backup, dilakukan pemantauan secara berkala untuk pembaruan data tersebut,

Kondisi Kekinian	Kondisi Ideal
- Tidak tersedianya daftar data yang harus di backup dan laporan hasil analisa kepatuhan terhadap prosedur backup - Tidak ada prosedur penggunaan perangkat pengolah informasi milik pihak ketiga - Dilakukan penerapan pengamanan fasilitas fisik yang sesuai dengan klasifikasi aset informasi secara berlapis yaitu dengan adanya fingerprint, kunci otomatis, dan penggunaan buku tamu di ruang server - Dilakukan proses pengelolaan alokasi kunci masuk secara fisik dan elektronik ke fasilitas fisik - Terdapat perlindungan infrastruktur dari dampak lingkungan (api, suhu, dan kelembaban) dengan adanya gas pemadam, pengaturan suhu dan kelembaban - Terdapat perlindungan dari gangguan listrik dan petir untuk infrastruktur yang ada - Terdapat surat terima yang dibuat untuk peraturan pengamanan perangkat komputasi jika digunakan diluar lokasi kerja resmi	dan dilakukan pelaporan dari hasil analisa kepatuhan terhadap prosedur backup - Dibuat prosedur terkait penggunaan perangkat informasi yang dimiliki oleh pihak ketiga - Harus adanya penerapan terkait pengamanan fasilitas fisik yang telah disesuaikan dengan klasifikasi aset informasi secara berlapis. Klasifikasi aset dapat dibedakan dari tingkat kepentingan aset informasi yang dimiliki - Diterapkan perlindungan infrastruktur dari bencana alam dan gangguan manusia yang dilengkapi dengan beberapa peralatan pendukung seperti alat pemadam kebakaran, cctv, penangkal petir, pendeteksi suhu dan kelembaban - Diterapkan perlindungan listrik dari gangguan-gangguan yang dapat terjadi untuk infrastruktur yang ada - Dibuat bukti untuk pengamanan perangkat

Kondisi Kekinian	Kondisi Ideal
- Konstruksi ruang penyimpanan perangkat sudah menggunakan material yang baik untuk menghindari risiko yang disesuaikan dengan standar dari pihak pengadaan - Mekanisme pengamanan dalam pengiriman aset informasi dengan pihak ketiga hanya sebatas penggunaan password saja, untuk perlindungan fisik masih tidak dilakukan - Tidak ada peraturan resmi untuk pengamanan ruang server dan ruang arsip dari ancaman aset informasi, seperti larangan penggunaan handphone, larangan penggunaan kamera dan lain-lain	komputasi jika digunakan diluar lokasi kerja resmi - Konstruksi ruang penyimpanan perangkat harus menggunakan material yang baik untuk menghindari risiko yang disesuaikan dengan standar ruang server - Dilakukan pengamanan secara virtual dan fisik untuk melakukan pengiriman aset informasi dengan pihak ketiga - Dibuat peraturan yang resmi untuk pengamanan ruang server dan ruang arsip dari ancaman aset informasi, seperti larangan penggunaan alat elektronik lainnya yang tidak perlu
Kesenjangan: - Tidak adanya peraturan perundang-undangan yang digunakan DPTSI terkait klasifikasi aset informasi dan evaluasinya - Tidak adanya tata tertib terkait penggunaan komputer, email, internet, intranet, dan pengamanan aset terkait HAKI - Tidak lengkapnya peraturan penginstalan *software* yang ada di DPTSI - Tidak adanya peraturan terhadap penggunaan data pribadi yang bersyaratkan harus adanya ijin tertulis oleh pemilik data pribadi	

Kondisi Kekinian	Kondisi Ideal
- Tidak adanya kebijakan terhadap pelanggaran dari pengelolaan identitas serta proses otentikasi (username & password) - Tidak adanya prosedur dan syarat terkait pemberian akses, otentikasi, dan otorisasi untuk penggunaan aset informasi - Tidak adanya prosedur terkait tindakan backup dan restore namun dilakukan secara rutin untuk semua data-data yang ada didalam database - Tidak adanya prosedur untuk mutasi user atau tenaga kontrak yang habis masa kerjanya - Tidak adanya daftar data yang harus di backup dan laporan hasil analisa kepatuhan terhadap prosedur backup - Tidak adanya prosedur penggunaan perangkat pengolah informasi milik pihak ketiga - Tidak adanya mekanisme pengamanan fisik dalam pengiriman aset informasi dengan pihak ketiga - Tidak adanya peraturan resmi untuk pengamanan ruang server dan ruang arsip dari ancaman aset informasi, seperti larangan penggunaan handphone, larangan penggunaan kamera dan lain-lain	

Tabel 6.5 Analisis Kesenjangan Kategori Teknologi dan Keamanan Informasi

Kondisi Kekinian	Kondisi Ideal
- Dilakukan pembagian zona/ pengamanan berlapis untuk layanan TIK yang menggunakan internet - Dilakukan segmentasi terhadap jaringan komunikasi sesuai dengan kepentingan, dan jalur akses - Belum dilakukan pemindaian jaringan, sistem, dan aplikasi secara rutin. Jaringan, sistem, dan aplikasi akan dipindai	- Harus ada pembagian zona/ pengamanan yang berlapis untuk seluruh layanan TIK yang dilakukan menggunakan internet - Harus adanya segmentasi jaringan komunikasi sesuai dengan kepentingan dan jalur akses - Dilakukan pemindaian jaringan, sistem, dan

Kondisi Kekinian	Kondisi Ideal
hanya jika ada insiden yang terjadi - Seluruh infrastruktur jaringan dan sistem telah dirancang untuk memastikan ketersediaan sesuai kebutuhan yang ada dengan menggunakan fungsi *single sign on* - Setiap perubahan dalam sistem informasi secara otomatis akan terekam dalam *log* - *Log* sensor yang ada akan dianalisa secara berkala. DPTSI menggunakan sistem *alliance fault* sebagai log sensor yang dapat memantau serangan dari pihak luar - Diterapkan enkripsi untuk perlindungan aset informasi yang ada - Untuk penerapan enkripsi masih belum ada standar yang digunakan - Sudah terdapat penerapan sertifikat enkripsi yang dimiliki DPTSI, yaitu dari Digisearch tentang sertifikasi enkripsi - Sistem aplikasi tidak menerapkan pergantian password secara otomatis untuk para user	aplikasi yang dilakukan secara rutin dan dilakukan jejak rekam terhadap hasil pemindaian yang dilakukan - Infrastruktur jaringan dan sistem dirancang untuk memastikan ketersediaan/ aturan redundansi sesuai kebutuhan yang ada - Digunakan *log* yang berjalan secara otomatis utuk merekam semua perubahan dalam sistem informasi dan dilakukan analisis secara berkala untuk pemantauan serangan dari pihak luar instansi - Dilakukan penerapan enkripsi untuk perlindungan aset informasi sesuai dengan standar yang ada - Dilakukan sertifikasi terkait penggunaan enkripsi yang baik dan sesuai dengan standar - Dilakukan penerapan/ pengaturan terhadap sistem aplikasi yang digunakan untuk pergantian password secara otomatis di masing-masing akun

Kondisi Kekinian	Kondisi Ideal
- Semua sistem aplikasi dan jaringan yang dimiliki DPTSI sudah menerapkan pembatasan waktu akses misal jumlah kegagalan *login*, *timeouts* dan *lockout* - Penerapan pengamanan untuk mencegah penggunaan akses jaringan yang tidak resmi dilakukan dengan menggunakan *firewall* - Versi desktop dan server akan diupdate sesuai dengan versi yang terbaru terkecuali ada fungsi-fungsi tertentu yang tidak dapat dijalankan pada versi yang baru maka akan tetap menggunakan versi yang lama - Desktop dan server sudah dilengkapi dengan antivirus agar terhindar dari virus dan malware - Tidak ada rekaman hasil analisa yang berisi bahwa antivirus telah diupdate secara berkala dan tidak ada laporan tentang penyerangan virus yang berhasil ditindaklanjuti dan diselesaikan - Seluruh jaringan, sistem, dan aplikasi telah menggunakan mekanisme sinkronisasi waktu yang akurat. Untuk	- Diterapkan pembatasan waktu akses misal jumlah kegagalan *login*, *timeouts* dan *lockout* pada semua sistem aplikasi dan jaringan yang ada di instansi - Penggunaan *firewall* sebagai tameng pertama untuk mencegah penggunaan akses jaringan yang tidak resmi - Dilakukan update terhadap versi desktop dan server yang digunakan dalam instansi - Ditanamkan antivirus pada desktop dan server yang memang membutuhkan untuk menghindari serangan virus dan malware - Dilakukan perekapan dan dokumentasi pada rekaman hasil analisa yang berisi bahwa antivirus telah diupdate secara berkala dan laporan tentang penyerangan virus yang berhasil ditindaklanjuti - Diterapkan mekanisme sinkronisasi waktu yang akurat terhadap jaringan, sistem, dan aplikasi yang digunakan di instansi

Kondisi Kekinian	Kondisi Ideal
server telah tersinkronisasi secara otomatis - Tidak ada pihak independen yang ditugaskan untuk mengkaji kehandalan keamanan informasi secara rutin	- Menerapkan pengkajian yang dilakukan oleh pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin
Kesenjangan: - Tidak dilakukannya pemindaian jaringan, sistem, dan aplikasi secara rutin. Jaringan, sistem, dan aplikasi akan dipindai hanya jika ada insiden yang terjadi - Tidak digunakannya standar untuk penerapan enkripsi - Tidak adanya pemberitahuan secara otomatis pada sistem sistem aplikasi yang digunakan untuk mengganti password oleh user secara berkala - Tidak adanya rekaman hasil analisa yang berisi bahwa antivirus telah diupdate secara berkala dan tidak ada laporan tentang penyerangan virus yang berhasil ditindaklanjuti - Tidak adanya pihak independen yang ditugaskan untuk mengkaji kehandalan keamanan informasi secara rutin	

6.2 Hasil Penilaian Kepentingan Penggunaan Sistem Elektroik di DPTSI ITS Surabaya

Sebelum proses penilaian terhadap 5 (lima) area dilakukan secara kuantitatif, akan dilakukan proses klasifikasi terlebih dahulu terhadap penggunaan Sistem Elektronik dalam instansi atau cakupan evaluasinya. Tujuan dari proses ini adalah untuk mengelompokkan instansi kedalam "ukuran" tertentu: Rendah, Tinggi, dan Strategis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik penggunaan Sistem Elektronik yang spesifik.

Hasil pengelompokan tadi didapat dari penjumlahan semua nilai kriteria yang didapat dari setiap pertanyaan yang

disuguhkan terkait kategori SE. Untuk mengetahui seberapa besar peran penggunaan SE dalam instansi tersebut, maka akan diberikan 10 pertanyaan yang dapat menggambarkan hal tersebut. Setiap pertanyaan akan mempunyai 3 kriteria penilaian, yaitu A B dan C.

Gambar 6.1 berikut menjelaskan tingkat kesiapan keamanan informasi yang dibagi menjadi tiga tingkat.

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

Gambar 6.1 Tingkat Kematangan Indeks KAMI versi 3.1

Berikut ini adalah hasil dari penilaian tingkat kepentingan penggunaan Sistem Elektronik di Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya:

Tabel 6.6 Hasil Penilaian Penggunaan Sistem Elektronik DPTSI ITS Surabaya

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	**Status**	Skor

#	**Karakteristik Instansi**		
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C	1
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	B	2
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	B	2
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus	C	1
1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	A	5

#	**Karakteristik Instansi**		
1,6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A	5
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	B	2
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak	B	2

#	**Karakteristik Instansi**		
1,9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih [C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih	A	5
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)	C	1
	Skor penetapan Kategori Sistem Elektronik	**26**	

Dari hasil penilaian tingkat kepentingan penggunaan Sistem Elektronik di Direktorat Pengembangan Teknologi dan Sistem Informasi ITS telah didapatkan skor sebesar 26, sehingga dapat masuk kedalam kategori Tinggi sesuai dengan tabel tingkat kematangan Indeks KAMI dimana kategori **Tinggi** berkisar antara skor 16 sampai dengan 34.

Maksud dari kategori Tinggi disini yaitu kepentingan penggunaan sistem elektronik di DPTSI merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan. Penggunaan sistem elektronik ini mendapat nilai ynag lumayan

tinggi karena kewajiban kepatuhan terhadap Peraturan atau Standar Nasional, pengguna sistem elektronik juga lebih dari 5000 pengguna, keterhubungan data pribadi yang diolah terkait dengan data pribadi lainnya, dan dampak dari kegeglannya juga dapat berdampak pada tidak tersedianya layanan publik berskala nasional.
Menurut kepentingan penggunaan Sistem Elektronik di DPTSI ITS, maka hasil dari penilaian kelima area Indeks KAMI selanjutnya harus mendapatkan nilai diatas 583 untuk mendapatkan status Baik.

6.3 Penilaian Kesiapan 5 Area Keamanan Informasi di DPTSI ITS Surabaya

Penilaian kelima area ini bertujuan untuk menilai kondisi kemaatangan keamanan informasi sesuai dengan standar ISO 27001:2013. Lima area keamanan informasi ini adalah sebagai berikut:

I: Tata Kelola Keamanan Informasi
II: Pengelolaan Risiko Keamanan Informasi
III: Kerangka Kerja Keamanan Informasi
IV: Pengelolaan Aset Informasi
V: Teknologi dan Keamanan Informasi

Dalam penilaian kelima area tersebut akan terdapat beberapa warna yang berbeda dalam tabel penilaian. Warna tersebut menunjukkan tingkatan yang berbeda. Tabel 6.7 berikut akan berisikan keterangan dari tingkatan warna yang terdapat dalam penilaian lima area Indeks KAMI:

Tabel 6.7 Penjelasan Tingkatan Warna dalam Penilaian Indeks KAMI

Tingkat Keamanan		Tingkat Kematangan Keamanan II
		Tingkat Kematangan Keamanan III
		Tingkat Kematangan Keamanan IV

		Tingkat Kematangan Keamanan V
Kategori Pengamanan		Kategori Kematangan Pengamanan I
		Kategori Kematangan Pengamanan II
		Kategori Kematangan Pengamanan III
Status Pengamanan		Tidak Dilakukan
		Dalam Perenanaan
		Dalam Penerapan/ Diterapkan Sebagian
		Diterapkan Secara Menyeluruh

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

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

Gambar 6.2 Hasil Pemetaan Skor Indeks KAMI

Berikut ini adalah Tabel 6.8 yang berisikan identitas responeden yang terkait dengan pengumpulan data penilaian Indeks KAMI di DPTSI ITS Surabaya:

Tabel 6. 8 Identitas Responden Terkait Penilaian Indeks KAMI

Indeks Keamanan Informasi (Indeks KAMI)	
Identitas Instansi Pemerintah	Direktorat Pengembangan Teknologi dan Sistem Informasi
Alamat	Jl. Raya ITS, Keputih, Sukolilo, Keputih, Sukolilo, Kota SBY, Jawa Timur 60111, Indonesia

Nomor Telepon	(031) 5994251
Email	lptsi@its.ac.id
Pengisi Lembar Evaluasi	Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D. Hanim Maria Astuti, S.Kom., M.Sc. Satriyo Wicaksono, S.Kom. Achmad Bustari, A.Md. Cahya Purnama Dani, A.Md. Jananta Permata Putra, S.ST Anny Yuniarti, S.Kom., M.Comp.Sc.
NIP	197708242006041001 198410292010122003 198110112007101001 196412202001121001 197011062007011001 905014001 198106222005012002
Jabatan	KaSubDit Infrastruktur & Keamanan Teknologi Informasi KaSubDit Layanan Teknologi & Sistem Informasi Staff Bagian Jaringan Staff Bagian Listrik Staff Bagian Inventaris & Sistem Staff Bagian Sistem KaSubDit Pengembangan Sistem Informasi

6.3.1 Hasil Penilaian Tata Kelola Keamanan Informasi

Tabel 6.9 dibawah ini merupakan hasil penilaian yang berkaitan penilaian Tata Kelola Keamanan Informasi yang ada pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya yang mana didapatkan total nilai untuk evaluasi tata

kelola sebesar 45. Hasil lengkapnya dapat dilihat pada **LAMPIRAN C-2**.

Tabel 6.9 Hasil Penilaian Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#	**Fungsi/Instansi Keamanan Informasi**				
2,1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	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?	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
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	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			pengelolaan keamanan informasi?		
2,7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan	0
2,8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan	0
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			keamanan informasi dalam proses kerja yang ada?		
2.1 1	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
2.1 2	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
2.1 3	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Diterapkan Secara Menyeluruh	6
2.1 4	II I	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?	Tidak Dilakukan	0
2.1 5	II I	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?		
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Diterapkan Secara Menyeluruh	6
2.17	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak Dilakukan	0
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?		
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0
2.20	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	Tidak Dilakukan	0
2.21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?		
2.2.2	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
			Total Nilai Evaluasi Tata Kelola	**45**	

Pada Tabel 6.10 di bawah ini akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 8 bernilai 9. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 8 bernilai 36. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan 1 dan 2 berjumlah 45.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Tata Kelola yaitu 48. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 45 sehingga dapat disimpulkan skor tidak melebihi Tahapan Penerapan 3. Maka dari itu bagian Tata Kelola disimpulkan masih menduduki Tingkat Kematangan I+.

Tabel 6.10 Tingkat Kelengkapan Tata Kelola Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Tata Kelola	Nilai
1	8	9
2	8	36
3	6	0
Total	22	45

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

Tabel 6.11 Tingkat Kematangan Tata Kelola Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Tata Kelola	Nilai	Tingkat Validitas Kematangan
II	13	33	I+
III	3	12	No
IV	6	0	No
Total	22	45	

Area Tata Kelola Keamanan Informasi hanya valid ditingkat kematangan I+ yang artinya dalam kondi awal (Reaktif):

- Sudah adanya pemahaman mengenai perlunya pengelolaan keamanan informasi
- Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan
- Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik

- Pihak yang terlibat belum semuanya menyadari tanggung jawab mereka

Area Tata Kelola Keamanan Informasi ini medapat poin 45 dari 126 dimana poin ini terbilang sangat rendah karena pihak DPTSI hanya menerapkan:

- pembagian tanggung jawab terkait program keamanan informasi
- menerapkan fungsi secara spesifik terkait tugas dan tanggung jawan dalam pengelolaan keamanan informasi
- menerapkan program peningkatan kompetensi sesuai standar yang berlaku
- melakukan integrasi terhadap keperluan keamanan informasi dalam proses kerja
  dilakukan koordinasi dengan pihak terkait (internal dan eksternal) untuk menerapkan dan menjamin kepatuhan pengamanan informasi
- Menjadikan kondisi dan permasalahan keamanan informasi di Instansi anda sebagai konsideran atau bagian dari proses pengambilan keputusan strategis

6.3.2 Hasil Penilaian Pengelolaan Risiko Keamanan Informasi

Tabel 6.12 dibawah ini merupakan hasil penilaian yang berkaitan penilaian Pengelolaan Risiko Keamanan Informasi yang ada pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya yang mana didapatkan total nilai untuk evaluasi pengelolaan risiko sebesar 21. Hasil lengkapnya dapat dilihat pada **LAMPIRAN C-3.**

Tabel 6.12 Hasil Penilaian Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi	
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.	

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#	**Kajian Risiko Keamanan Informasi**				
3,1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
3,2	II	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Tidak Dilakukan	0
3,3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
3,4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?		
3,5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Diterapkan Secara Menyeluruh	3
3,6	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Diterapkan Secara Menyeluruh	3
3,7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Tidak Dilakukan	0
3,8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terangguny a fungsi aset utama sudah ditetapkan sesuai	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			dengan definisi yang ada?		
3,9	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Tidak Dilakukan	0
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Diterapkan Secara Menyeluruh	3
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?		
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Diterapkan Secara Menyeluruh	6
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan	0
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			atau keperluan penerapan bentuk pengamanan baru?		
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan	0
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan	0
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**21**	

Pada Tabel 6.13 di bawah ini akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 10 bernilai 9. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 4 bernilai 12. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan 1 dan 2 berjumlah 21.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Pengelolaan Risiko

yaitu 36. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 21 sehingga dapat disimpulkan skor tidak melebihi Tahapan Penerapan 3. Maka dari itu bagian Pengelolaan Risiko disimpulkan masih menduduki Tingkat Kematangan I.

Tabel 6.13 Tingkat Kelengkapan Pengelolaan Risiko Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Risiko	Nilai
1	10	9
2	4	12
3	2	0
Total	16	21

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

Tabel 6.14 Tingkat Kematangan Pengelolaan Risiko Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Risiko	Nilai	Tingkat Validitas Kematangan
II	10	9	No
III	2	12	No
IV	2	0	No
V	2	0	No
Total	16	21	

Area Pengelolaan Risiko Keamanan Informasi hanya valid ditingkat kematangan I yang artinya dalam kondi awal (Reaktif):

- Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi

- Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan
- Kelemahan tekis dan non-teknis tidak teridentifikasi dengan baik
- Pihak yang terlibat tidak semuanya menyadari tanggung jawab mereka

Area Pengelolaan Risiko Keamanan Informasi ini medapat poin 21 dari total 72 dimana poin ini terbilang sangat rendah karena pihak DPTSI hanya menerapkan:

- Ambang batas risiko yang diterima
- Mendefinisikan kepemilikan dan pihak pengelola aset informasi
- Dilakukan penyusunan langkah mitigasi untuk risiko yang ada
- Langkah mitigasi dilakukan sesuai tingkat prioritas dan target penyelesaiannya
- Dilakukan pemantauan terhadap langkah mitigasi risiko yang dilakukan

6.3.3 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Tabel 6.15 dibawah ini merupakan hasil penilaian yang berkaitan penilaian Kerangka Kerja Pengelolaan Keamanan Informasi yang ada pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya yang mana didapatkan total nilai untuk evaluasi kerangka kerja sebesar 35. Hasil lengkapnya dapat dilihat pada **LAMPIRAN C-4 .**

Tabel 6.15 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
4,1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian	2
4,2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			yang membutuhkannya?		
4,3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Tidak Dilakukan	0
4,4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Tidak Dilakukan	0
4,5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?		
4,6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh	3
4,7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan	0
4,8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?		
4,9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	Tidak Dilakukan	0
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan	0
4,11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			manajemen proyek yang terkait dengan ruang lingkup?		
4,12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Tidak Dilakukan	0
4,13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Diterapkan Secara Menyeluruh	6
4,14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya?		
4,15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Tidak Dilakukan	0
4,16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.17	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	Tidak Dilakukan	0
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Tidak Dilakukan	0
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan	0
#	**Pengelolaan Strategi dan Program Keamanan Informasi**				
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?		
4,21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Diterapkan Secara Menyeluruh	3
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh	3
4,23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?		
4,24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Tidak Dilakukan	0
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
4,26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4,27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan	0
4,28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			diterapkan secara efektif?		
4,29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan	0
			Total Nilai Evaluasi Kerangka Kerja	**35**	

Pada Tabel 6.16 di bawah ini akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 12 bernilai 17. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 10 bernilai 18. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan 1 dan 2 berjumlah 35.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Pengelolaan Kerangka Kerja yaitu 64. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 35 sehingga dapat disimpulkan skor tidak melebihi Tahapan Penerapan 3. Maka dari itu bagian Pengelolaan Kerangka Kerja disimpulkan masih menduduki Tingkat Kematangan I+.

Tabel 6.16 Tingkat Kelengkapan Pengelolaan Kerangka Kerja Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Kerangka Kerja	Nilai
1	12	17
2	10	18
3	7	0
Total	29	35

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

Tabel 6.17 Tingkat Kematangan Pengelolaan Kerangka Kerja Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Kerangka Kerja	Nilai	Tingkat Validitas Kematangan
II	11	20	I+
III	13	15	No
IV	3	0	No
V	2	0	No
Total	29	35	

Area Kerangka Kerja Pengelolaan Keamanan Informasi hanya valid ditingkat kematangan I+ yang artinya dalam kondi awal (Reaktif):

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

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

Area Kerangka Kerja Pengelolaan Keamanan Informasi ini medapat poin 35 dari total 159 dimana poin ini terbilang sangat rendah karena pihak DPTSI hanya menerapkan:
- Kebijakan keamanan informasi secara formal dan dipublikasikan ke seluruh staff instansi
- Dilakukan identifikasi kondisi yang membahayakan keamanan informasi dan ditetapkan sebagai insiden keamanan informasi
- Pendefinisian konsekuensi dari pelanggaran kebijakan keamanan informasi dan dikomunikasikan
- Pembahasan aspek keamanan informasi dalam manajemen proyek yang dilakukan
- SDLC yang aman dalam pengembangan sistem dengan menggunakan prinsip/ metode sesuai dengan standar yang digunakan
- Dilakukan strategi pengamanan informasi sesuai dengan hasil analisis risiko dan dijadikan bagian dari rencana kerja organisasi
- Realisasi penerapan keamanan informasi sebagai bagian dari pelaksanaan program kerja organisasi

6.3.4 Hasil Penilaian Pengelolaan Aset Informasi

Tabel 6.18 dibawah ini merupakan hasil penilaian yang berkaitan penilaian Pengelolaan Aset Informasi yang ada pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya yang mana didapatkan total nilai untuk evaluasi pengelolaan aset sebesar 73. Hasil lengkapnya dapat dilihat pada **LAMPIRAN C-5.**

Tabel 6.18 Hasil Penilaian Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5,1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	3
5,2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
5,3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Tidak Dilakukan	0
5,4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut		
5,5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
5,6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
5,7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
5,8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Diterapkan Secara Menyeluruh	3
5,9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak Dilakukan	0
5.10	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak Dilakukan	0
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	Diterapkan Secara Menyeluruh	3
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak Dilakukan	0
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Tidak Dilakukan	0
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			akses, otentikasi dan otorisasi untuk menggunakan aset informasi		
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak Dilakukan	0
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan	0
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Tidak Dilakukan	0
5.18	II	1	Prosedur back-up dan ujicoba pengembalian data (restore) secara berkala	Tidak Dilakukan	0
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Diterapkan Secara Menyeluruh	6
5.20	III	2	Proses pengecekan latar belakang SDM	Tidak Dilakukan	0
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			eksternal ataupun pihak yang berwajib.		
5.2.2	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Diterapkan Secara Menyeluruh	6
5.2.3	III	2	Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku	Tidak Dilakukan	0
5.2.4	III	2	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.	Dalam Perencanaan	2
5.2.5	III	3	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?	Tidak Dilakukan	0
5.2.6	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			pengamanan yang sesuai dengan klasifikasinya?		
5.27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan	0
#	**Pengamanan Fisik**				
5.28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Diterapkan Secara Menyeluruh	3
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	3
5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?		
5.3 1	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
5.3 2	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Diterapkan Secara Menyeluruh	3
5.3 3	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	Diterapkan Secara Menyeluruh	3
5.3 4	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?		
5.3 5	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian	4
5.3 6	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	4
5.3 7	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)		
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Tidak Dilakukan	0
			Total Nilai Evaluasi Pengelolaan Aset	**73**	

Pada Tabel 6.19 di bawah ini akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 24 bernilai 39. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 10 bernilai 34. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan 1 dan 2 berjumlah 73.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Pengelolaan Aset yaitu 88. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 73 sehingga dapat disimpulkan skor tidak melebihi

Tahapan Penerapan 3. Maka dari itu bagian Pengelolaan Aset disimpulkan masih menduduki Tingkat Kematangan I+.

Tabel 6.19 Tingkat Kelengkapan Pengelolaan Aset Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Aset	Nilai
1	24	39
2	10	34
3	4	0
Total	38	73

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan terkait dengan aset informasi akan menentukan tingkat kematangan pada bagian ini. Semakin tinggi nilai tingkat kelengkapan maka semakin tinggi pula tingkat kematangan keseluruhan pada tiap bagian. Berikut merupakan hasil tingkat kematangan pada bagian Pengelolaan Aset Informasi:

Tabel 6.20 Tingkat Kematangan Pengelolaan Aset Informasi

Kategori Tingkat Kematangan	Pertanyaan Pengelolaan Aset	Nilai	Tingkat Validitas Kematangan
II	29	59	I+
III	9	14	No
Total	38	73	

Area Pengelolaan Aset Informasi hanya valid ditingkat kematangan I+ yang artinya dalam kondi awal (Reaktif):

- Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi
- Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan
- Kelemahan tekis dan non-teknis tidak teridentifikasi dengan baik

- Pihak yang terlibat tidak semuanya menyadari tanggung jawab mereka

Area Pengelolaan Aset Informasi ini medapat poin 73 dari total 168 dimana poin ini terbilang lumayan bagus karena pihak DPTSI sudah menerapkan:

- Tersedianya daftar inventaris aset informasi
- Mendefinisikan tingkatan akses yang berbeda dari setiap klasifikasi aset
- Dilakukan proses pengelolaan konfigurasi secara konsisten
- Terdapat tanggung jawab pengamanan informasi secara individu untuk semua personil instansi
- Dilakukan peraturan terkait instalasi perangkat lunak milik instansi
- Dilakukan pengamanan fisik sesuai dengan definisi zona dan klasifikasi aset
- Terdapat prosedur penghancuran dokumen yang sudah tidak diperlukan
- Diterapkan pengamanan fasilitas fisik sesuai klasifikasi aset informasi
- Ada proses pengelolaan alokasi kunci masuk secara fisik dan elektronik ke fasilitas fisik
- Komputasi dilindungi dari dampak lingkungan, kondisi suhu, dan kelembaban sesuai dengan syarat yang ada
- Komputasi dilindungi dari gangguan pasokan listrik dan petir
- Tersedia proses pemindahan aset informasi dari lokasi yang sudah ditetapkan

6.3.5 Hasil Penilaian Teknologi dan Keamanan Informasi

Tabel 6.21 dibawah ini merupakan hasil penilaian yang berkaitan penilaian Teknologi dan Keamanan Informasi yang ada pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya yang mana didapatkan total nilai untuk

evaluasi teknologi dan keamanan informasi sebesar 75. Hasil lengkapnya dapat dilihat pada **LAMPIRAN C-6.**

Tabel 6.21 Hasil Penilaian Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Teknologi**		
6,1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
6,2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6,3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			perkembangan (standar industri yang berlaku) dan kebutuhan?		
6,4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Diterapkan Secara Menyeluruh	3
6,5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2
6,6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Diterapkan Secara Menyeluruh	3
6,7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?		
6,8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6,9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
6.11	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
6.12	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan	0

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.13	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh	6
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?	Tidak Dilakukan	0
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh	6
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah	Dalam Penerapan /	4

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses?	Diterapkan Sebagian	
6.17	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh	6
6.18	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Diterapkan Secara Menyeluruh	3
6.19	II	1	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Diterapkan Secara Menyeluruh	3
6.20	II	1	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	Diterapkan Secara Menyeluruh	3

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.2.1	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak Dilakukan	0
6.2.2	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan	0
6.2.3	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
6.2.4	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?	Diterapkan Secara Menyeluruh	6

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.25	III	3	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Tidak Dilakukan	0
6.26	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**75**	

Pada Tabel 6.22 di bawah ini akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 14 bernilai 41. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 10 bernilai 34. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan 1 dan 2 berjumlah 75.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Pengelolaan Aset yaitu 68. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2

adalah 75 sehingga dapat disimpulkan skor melebihi Tahapan Penerapan 3 dan tahapan ini dinilai valid. Maka dari itu bagian Teknologi & Keamanan Informasi disimpulkan telah menduduki Tingkat Kematangan II.

Tabel 6.22 Tingkat Kelengkapan Teknologi & Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Aset	Nilai
1	14	41
2	10	34
3	2	0
Total	26	75

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

Tabel 6.23 Tingkat Kematangan Teknologi & Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Pengelolaan Aset	Nilai	Tingkat Validitas Kematangan
II	14	41	II
III	11	34	Yes
IV	1	0	No
Total	26	75	

Area Teknologi dan Keamanan Informasi hanya valid ditingkat kematangan II yang artinya dalam penerapan kerangka kerja dasar (Aktif):

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya

keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi
- Langkah pengamanan operasional yang diterapkan bergantung pada pengetahuan dan motivasi individu pelaksana
- Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten
- Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka

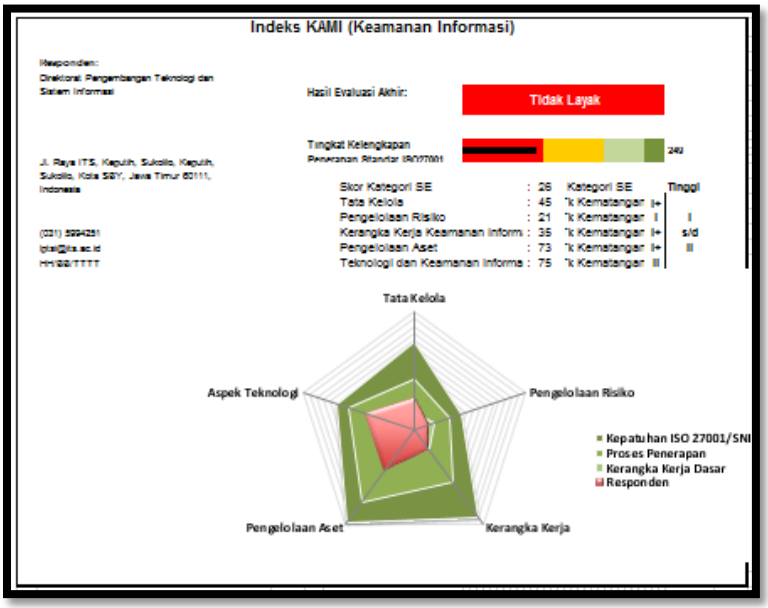
Area Pengelolaan Aset Informasi ini medapat poin 75 dari total 120 dimana poin ini terbilang lumayan baik karena pihak DPTSI hanya belum menerapkan:
- Standar terkait penggunaan enkripsi
- Belum adanya penerapan pergantian password secara otomatis pada sistem dan aplikasi yang digunakan
- Tidak adanya rekam jejak hasil analisa yang mengkonfirmasi pembaruan anti virus secara rutin
- Belum ada laporan terkait penyerangan virus yang telah ditindaklanjuti
- Belum dilakukan pengkajian terkait kehandalan keamanan informasi secara rutin yang dilakukan pihak independen

6.4 Pembahasan

6.4.1 Analisis Hasil Akhir Penilaian Indeks KAMI

Bagian ini akan menjelaskan hasil dari penilaian indeks KAMI pada Direktorat Pengembangan Teknologi dan Sistem

Informasi ITS Surabaya. Berikut ini adalah tampilan dari *dashboard* indeks KAMI yang dihasilkan:



Gambar 6.3 Hasil Dashboard Indeks KAMI DPTSI ITS

Dashboard diatas merupakan gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan indeks KAMI versi 3.1. Dari *dashboard* diatas, dapat dilihat bahwa tingkat kematangan keamanan informasi di DPTSI ITS Surabaya masih sangat kurang, yaitu tingkat II dengan nilai sebesar 249. Dapat dilihat pada *radar chart dashboard* tersebut bahwa hampir seluruh area yang dinilai dalam indeks KAMI belum terpenuhi dan sesuai dengan ISO 27001. Jika dilihat dibagian *radar chart dashboard*, hasil yang didapat hanya sebatas sampai kategori kerangka kerja dasar dan sebagian pada proses penerapan.

Gambar 6.4 Hasil Evaluasi Indeks KAMI di DPTSI ITS Surabaya

Dari Gambar 6.4 diatas dapat terlihat jika nilai indeks KAMI yang telah dicapai tergolong tidak layak, yaitu hanya mencapai tingkat II. Nilai yang didapatkan masih dikatakan tidak layak karena nilai yang dicapai tidak sesuai dengan kepentingan penggunaan sistem elektronik yang digunakan pada DPTSI ITS Surabaya, yaitu mencapai tingkat **Tinggi**.
Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI versi 3.1 masih sangat kurang. Berikut ini adalah uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

Tabel 6.24 Tingkat Kematangan Kelima Area

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Tingkat Kematangan II					
Status	I+	No	I+	I+	II
Tingkat Kematangan III					
Status	No	No	No	No	II
Validitas	No	No	No	No	Yes
Tingkat Kematangan IV					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Tingkat Kematangan V					
Status	No	No	No	No	No

Validitas	No	No	No	No	No
Status Akhir	I+	I	I+	I+	II

Urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III+, sedangkan untuk saat ini tingkat kematangan dari DPTSI ITS Surabaya hanya dibatas I-II. Tingkat kematangan ini menunjukkan posisi DPTSI ITS Surabaya sebagai berikut ini:

Tabel 6.25 Tingkatan Kondisi DPTSI ITS

Tingkatan	Kondisi
I	Kondisi Awal
II	Penerapan Kerangka Kerja Dasar
III	Terdefinisi dan Konsisten
IV	Terkelola dan Terukur
V	Optimal

Hasil penilaian kelima area Indeks KAMI ini dibatasi sampai penilaian kualitas tanpa adanya penilaian kuantitas pada pertanyaan-pertanyaan tertentu. Ada beberapa pertanyaan dimasing-masing area yang juga membutuhkan penilaian terhadap kuantitas dan hal ini dapat mempengaruhi hasil penilaian pada instansi terkait.

Validasi terkait penilaian manajemen keamanan informasi yang ada di DPTSI ITS telah dilakukan guna memastikan bahwa penilaian yang dilakukan sudah benar dan sesuai dengan kondisi sesungguhnya yang ada di instansi terkait. Validasi dilakukan peneliti dengan Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi sebagai wakil dari Direktur DPTSI ITS Surabaya.
Validasi dilakukan dengan pengecekan terhadap nilai-nilai yang masih kurang di masing-masing area dan disesuaikan

dengan kondisi sesungguhnya di DPTSI ITS. Selain itu juga dilakukan pengecekan apakah pihak yang dipilih sebagai narasumber sudah tepat atau belum dengan menandai pertanyaan-pertanyaan yang telah disesuaikan dengan keahlian dari masing-masing narasumber.

6.4.2 Saran Perbaikan 5 Area Keamanan Informasi

Setelah melakukan penilaian dengan indeks KAMI versi 3.1 dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI versi 3.1, maka tahap selanjutnya adalah membuat saran perbaikan pada setiap bagian yang masih kurang baik. Berikut ini adalah saran perbaikan yang dibuat per masing-masing area yang ada dengan tabel berisikan pertanyaan, status, nilai, dan saran perbaikan.

6.4.2.1 Saran Perbaikan Area Tata Kelola Keamanan Informasi

Saran perbaikan untuk area Tata Kelola Keamanan Informasi ini berisikan saran perbaikan untuk 13 pertanyaan yang mendapat nilai kurang/ tidak dilakukan oleh DPTSI ITS. Saran perbaikan ini mengacu pada ISO/IEC 27002:2013.

Tabel 6.26 Saran Perbaikan Area Tata Kelola KI

No	Pertanyaan	Status	Nilai
2,4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
Saran Perbaikan **Control 12.1.3 Capacity management** Alokasi sumber daya harus dipantau dan diproyeksikan untuk menyesuaikan dengan kebutuhan dimasa mendatang. Kebutuhan kapasitas harus diidentifikasi dengan			

No	Pertanyaan	Status	Nilai
mempertimbangkan kekritisan bisnis dari sistem yang bersangkutan. Untuk proyeksi kebutuhan kapasitas dimasa mendatang juga dapat mempertimbangkan persyaratan sistem baru dan tren saat ini dan diproyeksikan dalam kemampuan pemrosesan informasi organisasi. Menyediakan kapasitas yang cukup juga dapat dicapai dengan meningkatkan kapasitas atau dengan mengurangi permintaan dengan cara: - Menghapus data yang sudah usang (*disk space*) - Dekomisioning aplikasi, sistem, dan database - Mengoptimalkan proses pengelompokan dan penjadwalan - Mengoptimalkan penggunaan logika aplikasi dan *query* database - Membatasi bandwidth untuk layanan yang tidak penting terkait bisnis (misal *streaming* film dan video) Dibuat dokumen terkait rencana pengelolaan kapasitas yang harus mempertimbangkan sistem yang penting/ kritis.			
2,5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.2 Reporting information security events** Untuk segregasi kewenangan harus diurus agar tidak ada satu orang yang dapat mengakses, memodifikasi, atau menggunakan aset tanpa adanya otorisasi. Jika sulit untuk memisahkan kewenangan, maka dapat menerapkan kontrol lain seperti melakukan monitoring kegiatan, melakukan audit			

No	Pertanyaan	Status	Nilai
dan pengawasan manajemen. Segregasi kewenangan ini merupakan sebuah cara untuk mengurangi risiko penyalahgunaan terhadap aset organisasi. Dapat dibuat dokumen yang berisikan peran dari para pelaksana pengamanan informasi dan persyaratan terkait kewenangan masing-masing pihak.			
2,6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
Saran Perbaikan **Control 7.2.1 Management responsibilities** Dibuat dokumen yang berisikan standar kompetensi dan keahlian yang harus dimiliki oleh para pelaksana pengelolaan keamanan informasi dengan spesifikasi sebagai berikut: - Memiliki keterampilan dan kualifikasi yang sesuai dan dididik secara teratur - Karyawan menerima pendidikan dan pelatihan kesadaran yang tepat dan terupdate dijalankan sesuai dengan kebijakan dan prosedur keamanan informasi yang ada - Menerapkan tingkat kesadaran keamanan informasi yang relevan dengan peran dan tanggung jawab dalam organisasi			
2,7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan	0
Saran Perbaikan **Control 7.2.1 Management responsibilities**			

No	Pertanyaan	Status	Nilai
Control 7.2.2 Information security awareness, education and training Dilakukan penilaian terhadap kompetensi dan keahlian karyawan sesuai dengan kewaspadaan mereka terhadap keamanan informasi, motivasi para karyawan untuk meningkatkan kehandalan dan mengurangi kegiatan yang dapat menyebabkan insiden keamanan informasi. Penilaian terhadap kompetensi dan keahlian karyawan dapat dilakukan dengan menilai: - Pernyataan komitmen manajemen untuk keamanan informasi - Tanggung jawab masing-masing individu terkait aktivitas yang dilakukan dalam mengamankan dan melindungi informasi milik instansi - Pendidikan keamanan informasi dan materi pelatihan lebih lanjut			
2,8	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan	0
Saran Perbaikan **Control 7.2.2 Information security awareness, education and training** Semua stakeholder instansi harus menerima pendidikan terkait kewaspadaan terhadap informasi dan pelatihan terhadap pemahaman prosedur dan kebijakan terkait keamanan informasi, dimana pendidikan dan pelatihan keamanan informasi mencakup aspek-aspek sebagai berikut: - Komitmen manajemen untuk keamanan informasi di seluruh organisasi			

No	Pertanyaan	Status	Nilai
- Tanggung jawab masing-masing individu atas tindakan terhadap pengamanan dan perlindungan informasi milik organisasi dan milik eksternal - Prosedur dasar keamanan informasi, seperti pelaporan insiden keamanan informasi			
2,11	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
Saran Perbaikan **Control 18.1.4 Privacy and protection of personally identifiable information** Privasi dan perlindungan informasi terkait data pribadi harus dipastikan sebagaimana disyaratkan dalam undang-undang dan peraturan yang berlaku dengan relevan. Instansi terkait juga harus membuat kebijakan terkait perlindungan data pribadi serta mengkomunikasikannya dengan semua orang yang terlibat dalam pengelolaan data pribadi. Selain penerapan undang-undang, peraturan, dan kebijakan juga dapat diperlukan struktur manajemen yang tepat beserta kontrol-kontrolnya seperti menunjuk orang-orang yang bertanggung jawab (petugas privasi yang memberi bimbingan pada manajer, pengguna dan penyedia layanan yang bertanggung jawab pada masing-masing prosedur)			
2,14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
Saran Perbaikan **Control 17.1.1 Planning information security continuity** **Control 17.1.2 Implementing information security continuity** Instansi harus menentukan bahwa keberlangsungan keamanan informasi menjadi bagian dari proses manajemen keberlangsungan bisnis dan pemulihan bencana. Syarat keamanan informasi harus ditentukan ketika merencanakan keberlangsungan bisnis dan pemulihan bencana. Instansi juga harus melakukan analisis dampak bisnis terkait aspek keamanan informasi untuk menentukan syarat keamanan informasi yang berlaku pada situasi yang merugikan. Informasi lebih detail mengenai manajemen keberlangsungan bisnis dapat ditemukan pada ISO/IEC 27031, ISO/IEC 22313, dan ISO/IEC 22301 DPTSI juga harus memastikan: - Adanya struktur manajemen yang berwenang, berpengalaman, dan berkompetensi untuk mempersiapkan, memitigasi, dan menanggapi suatu peristiwa yang mengganggu - Pihak terkait harus memiliki kewenangan, tanggung jawab, dan kompetensi dalam mengelola insiden dan menjaga keamanan informasi - Mengembangkan dan menyetujui dokumentasi rencana, respon, dan pemulihan prosedur secara rinci sebagaimana organisasi akan mengelola suatu peristiwa yang mengganggu dan akan menjaga keamanan informasi untuk tingkat yang telah ditentukan, berdasarkan pada tujuan kelangsungan keamanan informasi manajemen yang disetujui			
2,17	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi	Tidak Dilakukan	0

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

<table>
<tr><th>No</th><th>Pertanyaan</th><th>Status</th><th>Nilai</th></tr>
<tr><td colspan="4">Penerapan program untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi dapat diterapkan/ diintegrasikan pada manajemen proyek agar dapat memastikan bahwa risiko etrkait keamanan informasi telah diidentifikasi dan ditangani sebagai bagian dari proyek. Metode manajemen proyek ini harus mensyaratkan:
- Tujuan keamanan informasi termasuk dalam tujuan proyek
- penilaian risiko keamanan informasi dilakukan pada tahap awal dari proyek untuk mengidentifikasi kendali yang diperlukan
- keamanan informasi adalah bagian dari semua tahapan metodologi proyek yang diterapkan
Keamanan informasi harus ditangani dan ditinjau secara teratur dalam semua proyek. Tanggung jawabnya juga harus dialokasikan secara spesifik dalam manajemen proyek.</td></tr>
<tr><td>2,19</td><td>Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?</td><td>Tidak Dilakukan</td><td>0</td></tr>
<tr><td colspan="4">Saran Perbaikan
Control 7.2.1 Management responsibilities
Control 7.2.3 Disciplinary process
Diterapkan program penilaian kinerja pengelolaan keamanan informasi bagi masing-masing individu terkait. Penilaian kinerja terhadap masing-masing individu dapat dilihat dari beberapa hal antara lain:
- Kedisiplinan dalam menjalankan keamanan informasi sesuai dengan prosedur dimana instansi harus terlebih dahulu menerapkan proses kedisiplinan secara formal
- Pelanggaran yang pernah dilakukan terkait keamanan informasi organisasi</td></tr>
</table>

No	Pertanyaan	Status	Nilai
	- Motivasi dalam memenuhi kebijakan keamanan informasi yang ada - Kepatuhan terhadap syarat dan kondisi kerja, termasuk kebijakan keamanan informasi organisasi - Memiliki keterampilan dan kualifikasi yang sesuai dengan persyaratan yang telah ditentukan sebelumnya		
2,20	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	Tidak Dilakukan	0
Saran Perbaikan **Control 5.1.2 Review of the policies for information security** Target dan sasaran keamanan informasi terdapat dalam kebijakan keamanan informasi yang mana harus dilakukan peninjauan secara rutin untuk memastikan kesesuaian, kecukupan, dan efektivitasnya secara terus menerus. Tinjauan tersebut harus mencakup penilaian peluang perbaikan kebijakan organisasi dan pendekatan untuk mengelola keamanan informasi dalam menanggapi perubahan lingkungan organisasi, situasi bisnis, kondisi hukum atau lingkungan teknis. Jika terjadi revisi saat melakukan review kebijakan ini maka harus mendapatkan persetujuan dari manajemen terkait.			
2,21	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?		
Saran Perbaikan **Control 18.1.1 Identification of applicable legislation and contractual requirements** Semua aturan legislatif yang relevan, peraturan, dan syarat kontrak untuk memenuhi persyaratan ini harus secara diidentifikasi secara eksplisit, didokumentasikan dan terus diperbarui. Terkait kontrol spesifik dan tanggung jawab masing-masing individu juga harus diidentifikasikan dan didokumentasikan. Pimpinan DPTSI harus mengidentifikasi semua undang-undang yang berlaku untuk instansi dalam rangka memenuhi persyaratan untuk jenis bisnis yang dijalankan.			
2,22	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.1 Responsibilities and Procedures** DPTSI harus menerapkan tanggung jawab dan prosedur untuk memastikan respon yang cepat, efektif dan tertib terkait insiden keamanan informasi. Berikut ini adalah pedoman untuk tanggung jawab dan prosedur yang berkaitan dengan manajemen insiden keamanan informasi: - Mempersiapkan prosedur untuk persiapan dan perencanaan respon terhadap insiden			

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

6.4.2.2 Saran Perbaikan Area Pengelolaan Risiko Keamanan Informasi

Saran perbaikan untuk area Pengelolaan Risiko Keamanan Informasi ini berisikan saran perbaikan untuk 11 pertanyaan yang mendapat nilai kurang/ tidak dilakukan oleh DPTSI ITS. Saran perbaikan ini mengacu pada ISO/IEC 27002:2013.

Tabel 6.27 Saran Perbaikan Area Pengelolaan Risiko KI

No	Pertanyaan	Status	Nilai
3,1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.1 Responsibilities and Procedures** **Control 16.1.2 Reporting information security events**			

No	Pertanyaan	Status	Nilai
Control 16.1.3 Reporting information security weaknesses **Control 16.1.4 Assessment of and decision on information security events** DPTSI harus menerapkan tanggung jawab dan prosedur untuk memastikan respon yang cepat, efektif dan tertib terkait insiden keamanan informasi. Berikut ini adalah pedoman untuk tanggung jawab dan prosedur yang berkaitan dengan manajemen insiden keamanan informasi: - Mempersiapkan prosedur untuk persiapan dan perencanaan respon terhadap insiden - Prosedur terkait pemantauan, pendeteksian, analisis, dan pelaporan insiden keamanan informasi - Prosedur terkait insiden *logging* - Prosedur penanganan bukti forensik - Prosedur respon termasuk untuk eskalasi, pemulihan kendali dari insiden, dan komunikasi untuk pihak internal dan eksternal instansi Dalam prosedur juga harus memastikan bahwa pelaksana harus berkompeten dalam menangani masalah terkait insiden keamanan informasi. Tujuan dari pengelolaan insiden keamanan informasi harus disepakati dengan manajemen, dan harus dipastikan bahwa mereka yang bertanggung jawab untuk manajemen insiden keamanan informasi memahami prioritas organisasi untuk menangani insiden keamanan informasi. Detail panduan tentang pengelolaan insiden keamanan informasi disediakan dalam ISO/IEC 27035. Harus dilakukan juga pelaporan terhadap kejadian yang menyangkut keamanan informasi. Kejadian yang dapat dilaporkan sebagai insiden adalah kontrol keamanan yang tidak efektif, pelanggaran integritas informasi, kesalahan manusia, ketidaksesuaian dengan kebijakan/ pedoman, pelanggaran keamanan fisik, perubahan sistem yang tidak		

No	Pertanyaan	Status	Nilai
terkendali, pelanggaran aset, dan melfungsi perangkat lunak/ perangkat keras. Selanjutnya harus dilakukan dokumentasi terkait dengan penilaian terhadap setiap kejadian keamanan informasi apakah dapat diklasifikasikan sebagai insiden keamanan informasi. Klasifikasi dan prioritas insiden dapat membantu untuk mengidentifikasi dampak dan tingkat insiden yang terjadi.			
3,2	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.5 Response to information security incidents** Dilakukan penentuan bagian khusus dalam menangani insiden keamanan informasi. Bagian penanganan insiden keamanan informasi bisa dari orang bagian dalam DPTSI yang relevan atau dari pihak luar DPTSI. Bagian yang bertanggung jawab ini harus memberikan tanggapan yang mencakup: - Pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi - Melakukan informasi forensik keamanan analisis - Melakukan eskalasi jika diperlukan - Memastikan bahwa respon yang dilakukan sudah sesuai dengan prosedur - Setelah insiden itu telah berhasil ditangani, maka harus secara resmi ditutup dan dicatat			
3,3	Apakah Instansi anda mempunyai kerangka kerja	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?		
Saran Perbaikan **Control 16.1.6 Learning from information security incidents** Menerapkan kerangka kerja pengelolaan risiko keamanan informasi seperti ISO/IEC 27001 dan dilakukan dokumentasi secara rutin dan benar. Harus ada mekanisme yang dilakukan DPTSI untuk mengukur dan memonitor biaya dan tipe insiden keamanan informasi. Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk mengidentifikasi dampak dari insiden yang terjadi.			
3,4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Tidak Dilakukan	0
Saran Perbaikan **Control 8.2.1 Classification of information** Dilakukan penerapan kerangka kerja pengelolaan risiko terlebih dahulu di DPTSI dan dilakukan pembuatan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum. Untuk mengurangi/ menghindari pelanggran tersebut, maka dapat dilakukan klasifikasi aset informasi. Selain itu juga harus diidentifikasikan terkait kepemilikan aset informasi terkait masing-masing klasifikasi.			

No	Pertanyaan	Status	Nilai
Dibuat skema klasifikasi aset dengan tingkatan tertentu dan nama yang masuk akal. Skema ini harus diterapkan secara konsisten di seluruh organisasi sehingga setiap orang akan mengklasifikasikan informasi dan aset terkait dengan cara yang sama dan menerapkan perlindungan yang tepat. Hasil klasifikasi harus menunjukkan sensitivitas dan kekritisan nilai aset untuk organisasi. Contoh skema klasifikasi kerahasiaan aset informasi dapat didasarkan pada 4 tingkatan sebagai berikut: - Tidak menyebabkan kerugian - Menyebabkan kerugian ringan dan gangguan kecil pada operasional - Dampak jangka pendek yang signifikan pada operasional dan tujuan taktis - Dampak serius pada tujuan strategis jangka panjang atau berisiko pada kelangsungan hidup organisasi			
3,7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Tidak Dilakukan	0
Saran Perbaikan **Control 8.2.3 Handling of assets** Diilakukan pencatatan terkait dengan kelemahan dan ancaman terhadap aset informasi. Penyusunan prosedur dalam menangani, mengelola, menyimpan, dan mengkomunikasikan informasi harus mencakup: - Pembatasan akses yang mendukung persyaratan perlindungan untuk setiap tingkat klasifikasi aset - Perlindungan terhadap salinan informasi ke tingkat yang konsisten - Penyimpanan aset TI sesuai dengan spesifikasi			
3,8	Apakah dampak kerugian yang terkait dengan	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?		
Saran Perbaikan **Control 16.1.6 Learning from information security incidents** Harus ada mekanisme yang dilakukan DPTSI untuk mengukur dan memonitor biaya dan tipe insiden keamanan informasi. Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk mengidentifikasi dampak dari insiden yang terjadi. Evaluasi insiden keamanan informasi dapat mengindikasikan peningkatan kebutuhan kontrol untuk membatasi kerusakan yang terjadi dimasa mendatang dan agar diperhitungkan dalam proses peninjauan kebijakan keamanan informasi.			
3,9	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.1 Responsibilities and procedures** DPTSI harus menerapkan tanggung jawab dan prosedur untuk memastikan respon yang cepat, efektif dan tertib terkait insiden keamanan informasi.			

<table>
<tr><th>No</th><th>Pertanyaan</th><th>Status</th><th>Nilai</th></tr>
<tr><td colspan="4">Berikut ini adalah pedoman untuk tanggung jawab dan prosedur yang berkaitan dengan manajemen insiden keamanan informasi:
- Mempersiapkan prosedur untuk persiapan dan perencanaan respon terhadap insiden
- Prosedur terkait pemantauan, pendeteksian, analisis, dan pelaporan insiden keamanan informasi
- Prosedur terkait insiden logging
- Prosedur penanganan bukti forensik
- Prosedur respon termasuk untuk eskalasi, pemulihan kendali dari insiden, dan komunikasi untuk pihak internal dan eksternal instansi
Dalam prosedur juga harus memastikan bahwa pelaksana harus berkompeten dalam menangani masalah terkait insiden keamanan informasi. Tujuan dari pengelolaan insiden keamanan informasi harus disepakati dengan manajemen, dan harus dipastikan bahwa mereka yang bertanggung jawab untuk manajemen insiden keamanan informasi memahami prioritas organisasi untuk menangani insiden keamanan informasi.</td></tr>
<tr><td>3,13</td><td>Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?</td><td>Tidak Dilakukan</td><td>0</td></tr>
<tr><td colspan="4">Saran Perbaikan
Control 16.1.7 Collection of evidence
Dilakukan penentuan dan penetapan prosedur untuk identifikasi, pengumpulan, dan akuisisi informasi yang dapat berfungsi sebagai bukti. Setelah melakukan mitigasi terhadap insiden yang terjadi maka dapat diukur apakah langkah tersebut berjalan dengan baik dan efektif untuk menanggulangi insiden yang terjadi.</td></tr>
</table>

No	Pertanyaan	Status	Nilai
Ketika insiden keamanan informasi terdeteksi pertama kali, mungkin sulit untuk menentukan tindakan penyelesaiannya. Oleh karena itu setiap bukti yang diperlukan harus dijaga/ tidak boleh dihancurkan sebelum langkah mitigasi insiden direalisasikan.			
3,14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.7 Collection of evidence** Dilakukan penentuan dan penetapan prosedur untuk identifikasi, pengumpulan, dan akuisisi informasi yang dapat berfungsi sebagai bukti. Setelah melakukan mitigasi terhadap insiden yang terjadi maka dapat diukur apakah langkah tersebut berjalan dengan baik dan efektif untuk menanggulangi insiden yang terjadi. Ketika insiden keamanan informasi terdeteksi pertama kali, mungkin sulit untuk menentukan tindakan penyelesaiannya. Oleh karena itu setiap bukti yang diperlukan harus dijaga/ tidak boleh dihancurkan sebelum langkah mitigasi insiden direalisasikan.			
3,15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan	0
Saran Perbaikan			

No	Pertanyaan	Status	Nilai
Control 16.1.6 Learning from information security incidents Harus ada mekanisme yang dilakukan DPTSI untuk memastikan dan meningkatkan efektifitas dari kerangka kerja risiko yang digunakan. Hal ini dapat dilihat dari seberapa besar pengaruh kerangka kerja tersebut dalam menangani insiden keamanan informasi yang terjadi di instansi. Jika efek yang diberikan masih belum terlalu signifikan maka kerangka kerja tersebut dapat dikaji ulang.			
3,16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan	0
Saran Perbaikan **Control 16.1.1 Responsibilities and Procedures** DPTSI harus menerapkan tanggung jawab dan prosedur untuk memastikan respon yang cepat, efektif dan tertib terkait insiden keamanan informasi. Berikut ini adalah pedoman untuk tanggung jawab dan prosedur yang berkaitan dengan manajemen insiden keamanan informasi: - Mempersiapkan prosedur untuk persiapan dan perencanaan respon terhadap insiden - Prosedur terkait pemantauan, pendeteksian, analisis, dan pelaporan insiden keamanan informasi - Prosedur terkait insiden *logging* - Prosedur penanganan bukti forensik - Prosedur respon termasuk untuk eskalasi, pemulihan kendali dari insiden, dan komunikasi untuk pihak internal dan eksternal instansi Dalam prosedur juga harus memastikan bahwa pelaksana harus berkompeten dalam menangani masalah terkait insiden keamanan informasi. Tujuan dari pengelolaan insiden keamanan informasi harus disepakati dengan manajemen, dan harus dipastikan bahwa mereka yang			

No	Pertanyaan	Status	Nilai
bertanggung jawab untuk manajemen insiden keamanan informasi memahami prioritas organisasi untuk menangani insiden keamanan informasi.			

6.4.2.3 Saran Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi

Saran perbaikan untuk area Kerangka Kerja Pengelolaan Keamanan Informasi ini berisikan saran perbaikan untuk 21 pertanyaan yang mendapat nilai kurang/ tidak dilakukan oleh DPTSI ITS. Saran perbaikan ini mengacu pada ISO/IEC 27002:2013.

No	Pertanyaan	Status	Nilai
4,1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian	2
Saran Perbaikan **Control 5.1.1 Policies for information security** Pembuatan kebijakan dan prosedur terkait keamanan informasi di DPTSI ITS hanya dilakukan pada beberapa prosedur saja, tidak keseluruhan ada. Maka dari itu DPTSI harus memenuhi semua prosedur terkait keamanan informasi yang belum dibuat dimana kebijakan keamanan informasinya harus memperhatikan syarat sebagai berikut: - Berisi strategi bisnis			

No	Pertanyaan	Status	Nilai
- Peraturan, perundang-undangan, dan kontrak - Lingkungan ancaman keamanan informasi saat ini dan dimasa mendatang - Definisi keamanan informasi, tujuan dan prinsip-prinsip untuk memandu semua kegiatan yang berkaitan dengan keamanan informasi - Tanggung jawab untuk manajemen keamanan informasi untuk peran didefinisikan - Proses untuk menangani penyimpangan dan pengecualian			
4,3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Tidak Dilakukan	0
Saran Perbaikan **Control 18.2.1 Independent review of information security** **Control 18.2.2 Compliance with security policies and standards** Harus dilakukan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi yang ditinjau secara independen pada jangka waktu yang telah ditentukan atau saat terjadi perubahan yang signifikan pada prosedur. Pimpinan instansi juga harus melakukan peninjauan kepatuhan pengolahan informasi dan prosedur dalam area tanggung jawab mereka dengan kebijakan keamanan yang sesuai, standar dan persyaratan keamanan lainnya secara teratur. Jika ada ketidakpatuhan maka harus dilakukan: - Identifikasi penyebab ketidakpatuhan - Evaluasi kebutuhan tindakan untuk mencapai kepatuhan - Menerapkan tindakan koreksi yang tepat			

No	Pertanyaan	Status	Nilai
-	Meninjau tindakan korektif yang dilakukan untuk verifikasi efektivitas dari setiap kekurangan dan kelemahan yang ada		
4,4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Tidak Dilakukan	0
Saran Perbaikan **Control 5.1.1 Policies for information security** Pihak DPTSI seharusnya mengkomunikasikan kebijakan terkait keamanan informasi kepada seluruh karyawan dan pihak eksternal dalam bentuk yang relevan, mudah diakses dan dipahami pembaca yang dituju.			
4,5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?	Tidak Dilakukan	0
Saran Perbaikan **Cotrol 16.1.5 Response to information security incidents** Dilakukan identifikasi mitigasi terhadap insiden keamanan informasi yang dicantumkan dalam kebijakan dan prosedur			

No	Pertanyaan	Status	Nilai
terkait keamanan informasi. Bagian yang bertanggung jawab ini harus memberikan tanggapan yang mencakup: - Pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi - Melakukan informasi forensik keamanan analisis - Melakukan eskalasi jika diperlukan - Memastikan bahwa respon yang dilakukan sudah sesuai dengan prosedur Setelah insiden itu telah berhasil ditangani, maka harus secara resmi ditutup dan dicatat			
4,7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan	0
Saran Perbaikan **Control 15.1.1 Information security policy for supplier relationships** DPTSI harus melakukan identifikasi terhadap kontrol keamanan informasi yang menangani akses supplier terhadap kebijakan informasi organisasi. Prosedur terkait kontrak dengan pihak ketiga dapat berisi: - Identifikasi jenis pemasok - Proses standar dan siklus hidup untuk mengelola hubungan dengan pemasok - Identifikasi jenis akses informasi yang diijinkan untuk pemasok - Persyaratan keamanan informasi minimum untuk setiap jenis informasi dan jenis akses untuk melayani pemasok berdasarkan kebutuhan bisnis organisasi dan persyaratan dan profil risiko			

No	Pertanyaan	Status	Nilai
- Proses dan prosedur untuk memantau kepatuhan untuk menetapkan persyaratan keamanan informasi untuk setiap jenis pemasok dan jenis akses, termasuk Ulasan pihak ketiga dan validasi produk - Jenis kewajiban yang berlaku kepada pemasok untuk melindungi informasi organisasi			
4,9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	Tidak Dilakukan	0
Saran Perbaikan **Control 18.2.3 Technical compliance review** DPTSI harus menerapkan prosedur resmi untuk meninjau kepatuhan teknis dan tindak lanjut dalam pengecualian penerapan keamanan informasi. Setiap tinjauan kepatuhan teknis seharusnya hanya dilakukan oleh orang yang kompeten atau oleh orang yang berwenang dan berada di bawah pengawasan orang tersebut.			
4,10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
Saran Perbaikan **Control 14.1.1 Information security requirements analysis and specification** DPTSI harus membuat kebijakan dan prosedur terkait dengan persyaratan adanya keamanan informasi untuk sistem baru atau tambahan keamanan informasi untuk sistem yang sudah ada. Hal ini harus dilakukan untuk mempermudah pihak keamanan informasi dalam melakukan *security patch* secara konsisten dan terstruktur.			
4,12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Tidak Dilakukan	0
Saran Perbaikan **Control 14.1.1 Information security requirements analysis and specification** Pihak DPTSI harus mengidentifikasikan persyaratan keamanan informasi pada sistem informasi baru dengan menggunakan berbagai macam metode seperti persyaratan kepatuhan dari kebijakan dan peraturan terkait, jenis ancaman yang mungkin terjadi, atau penggunaan ambang batas kerentanan. Hasil identifikasi ini harus didokumentasikan dan ditinjau oleh semua pemangku kepentingan.			
4,14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?		
Saran Perbaikan **Control 14.2.1 Secure development policy** Pihak DPTSI dapat membuat rencana penanggulangan risiko baru saat menerapkan sistem informasi baru dengan cara menerapkan pengamanan-pengamanan yang lebih baik. pengembangan yang aman merupakan syarat untuk membangun layanan, arsitektur, perangkat lunak dan sistem yang aman juga. Dalam kebijakan pembangunan sistem yang aman, aspek-aspek berikut harus dipertimbangkan: - Keamanan lingkungan pengembangan - Pedoman keamanan dalam siklus pengembangan perangkat lunak - Keamanan dalam metodologi pengembangan perangkat lunak - Pedoman pengkodean aman untuk setiap bahasa pemrograman yang digunakan - Persyaratan keamanan dalam tahap desain - Penggunaan repositori yang aman - Diperlukan pengetahuan terkait keamanan aplikasi - Kemampuan pengembang dalam menghindari, menemukan, dan memperbaiki kerentanan.		
4,15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi,	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	termasuk penjadwalan uji-cobanya?		
Saran Perbaikan **Control 17.1.1 Planning information security continuity** DPTSI harus menentukan bahwa keberlangsungan keamanan informasi menjadi bagian dari proses manajemen keberlangsungan bisnis dan pemulihan bencana. Syarat keamanan informasi harus ditentukan ketika merencanakan keberlangsungan bisnis dan pemulihan bencana. Instansi juga harus melakukan analisis dampak bisnis terkait aspek keamanan informasi untuk menentukan syarat keamanan informasi yang berlaku pada situasi yang merugikan. Informasi lebih detail mengenai manajemen keberlangsungan bisnis dapat ditemukan pada ISO/IEC 27031, ISO/IEC 22313, dan ISO/IEC 22301			
4,16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan	0
Saran Perbaikan **Control 17.1.2 Implementing information security continuity** Pihak DPTSI harus mendefinisikan peran tanggung jawab dan harus memastikan: - Adanya struktur manajemen yang berwenang, berpengalaman, dan berkompetensi untuk mempersiapkan, memitigasi, dan menanggapi suatu peristiwa yang mengganggu			

No	Pertanyaan	Status	Nilai
	- Pihak terkait harus memiliki kewenangan, tanggung jawab, dan kompetensi dalam mengelola insiden dan menjaga keamanan informasi - Mengembangkan dan menyetujui dokumentasi rencana, respon, dan pemulihan prosedur secara rinci sebagaimana organisasi akan mengelola suatu peristiwa yang mengganggu dan akan menjaga keamanan informasi untuk tingkat yang telah ditentukan, berdasarkan pada tujuan kelangsungan keamanan informasi manajemen yang disetujui		
4,17	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak Dilakukan	0
Saran Perbaikan **Control 17.1.2 Implementing information security continuity** Setelah menentukan kebijakan dan prosedur terkait BCP dan DRP, pihak DPTSI harus melakukan uji coba terhadap dokumen tersebut yang dilakukan sesuai dengan tanggung jawab dan jadwal yang sudah direncanakan.			
4,18	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	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	bisa (gagal) memenuhi persyaratan yang ada?		
Saran Perbaikan **Control 17.1.3 Verify, review and evaluate information security continuity** Setelah melakukan uji coba terhadap dokumen, pihak DPTSI juga dapat melakukan evaluasi langkah perbaikan. DPTSI harus memverifikasi keberlangsungan manajemen keamanan informasinya dengan cara: - Menguji fungsi dari proses kesinambungan keamanan informasi, prosedur dan kontrol untuk memastikan bahwa mereka sudah konsisten dengan tujuan kelangsungan keamanan informasi - Meninjau validitas dan efektivitas informasi terkait langkah-langkah penilaian keberlangsungan keamanan informasi, proses keamanan informasi, prosedur dan kontrol manajemen kelangsungan bisnis/ manajemen pemulihan bencana			
4,19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan	0
Saran Perbaikan **Control 5.1.2 Review of the policies for information security** Target dan sasaran keamanan informasi terdapat dalam kebijakan keamanan informasi yang mana harus dilakukan peninjauan secara rutin untuk memastikan kesesuaian, kecukupan, dan efektivitasnya secara terus menerus. Tinjauan tersebut harus mencakup penilaian peluang perbaikan kebijakan organisasi dan pendekatan untuk mengelola keamanan informasi dalam menanggapi perubahan lingkungan organisasi, situasi bisnis, kondisi hukum atau lingkungan teknis. Jika terjadi revisi saat			

No	Pertanyaan	Status	Nilai
melakukan review kebijakan ini maka harus mendapatkan persetujuan dari manajemen terkait.			
4,23	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Tidak Dilakukan	0
Saran Perbaikan **Control 12.7.1 Information systems audit controls** Pihak DPTSI sebaiknya melakukan kegiatan audit internal yng dilakukan oleh pihak independen. Persyaratan audit harus direncanakan secara hati-hati untuk meminimalkan gangguan proses bisnis. Pedoman yang harus dipatuhi adalah sebagai berikut: - Persyaratan audit untuk akses ke sistem dan data harus disepakati dengan manajemen - Lingkup penilaian audit harus disepakati dan dikendalikan - Pengujian audit harus dibatasi untuk akses *read-only* ke perangkat lunak dan data yang ada - Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati - Tes pemeriksaan yang dapat mempengaruhi ketersediaan sistem harus berjalan diluar jam kerja - Semua akses harus dipantau dan dicatat untuk menghasilkan jejak referensi			
4,24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan,	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	konsistensi dan efektifitas penerapan keamanan informasi?		
Saran Perbaikan **Control 12.7.1 Information systems audit controls** Pihak DPTSI sebaiknya melakukan kegiatan audit internal yng dilakukan oleh pihak independen. Audit internal tersebut juga dapat dilakukan terkait keamanan informasi di DPTSI dengan menggunakan kerangka kerja yang sesuai.			
4,25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
Saran Perbaikan **Control 12.7.1 Information systems audit controls** Pihak DPTSI sebaiknya melakukan kegiatan audit internal yng dilakukan oleh pihak independen. Persyaratan audit harus direncanakan secara hati-hati untuk meminimalkan gangguan proses bisnis. Pedoman yang harus dipatuhi adalah dimana semua akses harus dipantau dan dicatat untuk menghasilkan jejak referensi. Setelah proses audit selesai dan muncul rekomendasi atas kekurangan penerapan keamanan informasi yang ada maka pihak DPTSI harus melakukan inisiatif peningkatan kinerja keamanan informasi sesuai dengan kontrol pada kerangka kerja keamanan informasi.			
4,26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	perbaikan atau program peningkatan kinerja keamanan informasi?		
Saran Perbaikan **Control 12.7.1 Information systems audit controls** Untuk menetapkan langkah perbaikan untuk keamanan informasi atas hasil audit yang didapat maka hasil audit internal yang diperoleh harus dilaporkan pada pimpinan DPTSI.			
4,27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan	0
Saran Perbaikan **Control 5.1.2 Review of the policies for information security** Dalam melakukan review kebijakan dan prosedur terkait keamanan informasi, pihak DPTSI juga harus memperhitungkan aspek finansial terkait perubahan infrastruktur dan proses perubahannya.			
4,28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?		
Saran Perbaikan **Control 17.2.1 Availability of information processing facilities** DPTSI harus melakukan identifikasi kebutuhan bisnis untuk ketersediaan sistem informasi dimana ketersediaan tidak bisa dijamin dengan menggunakan arsitektur sistem yang ada.			
4,29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan	0
Saran Perbaikan **Control 17.2.1 Availability of information processing facilities** Untuk rencana kedepannya terkait peningkatan keamanan informasi harus direncanakan dalam membentuk strategi organisasi yang memperhatikan pentingnya keamanan informasi didalam instansi.			

6.4.2.4 Saran Perbaikan Area Pengelolaan Aset Informasi

Saran perbaikan untuk area Pengelolaan Aset Informasi ini berisikan saran perbaikan untuk 21 pertanyaan yang mendapat

nilai kurang/ tidak dilakukan oleh DPTSI ITS. Saran perbaikan ini mengacu pada ISO/IEC 27002:2013.

Tabel 6.28 Saran Perbaikan Area Pengelolaan Aset Informasi

No	Pertanyaan	Status	Nilai
5,2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0

Saran Perbaikan

Control 8.2.1 Classification of information

Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan, dan kepekaan terhadap penggunaan/ modifikasi yang tidak sah. Untuk mengurangi/ menghindari pelanggran tersebut, maka dapat dilakukan klasifikasi aset informasi. Selain itu juga harus diidentifikasikan terkait kepemilikan aset informasi terkait masing-masing klasifikasi.

Dibuat skema klasifikasi aset dengan tingkatan tertentu dan nama yang masuk akal. Skema ini harus diterapkan secara konsisten di seluruh organisasi sehingga setiap orang akan mengklasifikasikan informasi dan aset terkait dengan cara yang sama dan menerapkan perlindungan yang tepat.

Hasil klasifikasi harus menunjukkan sensitivitas dan kekritisan nilai aset untuk organisasi.

Contoh skema klasifikasi kerahasiaan aset informasi dapat didasarkan pada 4 tingkatan sebagai berikut:

- Tidak menyebabkan kerugian
- Menyebabkan kerugian ringan dan gangguan kecil pada operasional
- Dampak jangka pendek yang signifikan pada operasional dan tujuan taktis

Dampak serius pada tujuan strategis jangka panjang atau berisiko pada kelangsungan hidup organisasi

No	Pertanyaan	Status	Nilai
5,3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Tidak Dilakukan	0
Saran Perbaikan **Control 8.2.1 Classification of information** Setelah dilakukan klasifikasi aset informasi yang ada di DPTSI maka perlu juga dilakukan evaluasi terkait apakah tingkat kepentingan aset sudah sesuai dengan kebutuhan instansi dan apakah keperluan pengamanannya sudah sesuai dengan masing-masing tingkatannya.			
5,9	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak Dilakukan	0
Saran Perbaikan Seharusnya diterapkan tata tertib dalam penggunaan komputer, email, internet, dan intranet yang ada di DPTSI. Dimana tidak boleh ada pencabutan perangkat-perangkat yang melekat pada komputer, peraturan kedisiplinan terkait penggunaan kabel LAN, peraturan terkait poisoning jaringan DPTSI yang digunakan oleh user, dan lain sebagainya.			
5,10	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak Dilakukan	0
Saran Perbaikan **Control 8.1.3 Acceptable use of assets** Dibuat standar terkait kebutuhan keamanan informasi dalam penggunaan akses ke aset DPTSI. Pengguna harus bertanggung jawab untuk penggunaan sumber daya pengolahan informasi yang ada.			
5,12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	ijin tertulis oleh pemilik data pribadi		
Saran Perbaikan **Control 18.1.4 Privacy and protection of personally identifiable information** DPTSI harus mengembangkan kebijakan terkait privasi data pribadi. Kebijakan ini harus dikomunikasikan kepada semua orang yang terlibat dalam pengolahan informasi pribadi. Tanggung jawab untuk menangani data pribadi dan menjamin kesadaran prinsip-prinsip privasi harus ditangani sesuai dengan undang-undang dan peraturan yang relevan. DPTSI dapat menggunakan ISO/IEC 29100 sebagai peraturan yang terkait perlindungan data pribadi dalam teknologi informasi dan komunikasi sistem.			
5,13	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Tidak Dilakukan	0
Saran Perbaikan **Control 9.4.1 Information access restriction** **Control 9.3.1 Use of secret authentication information** DPTSI harus menerapkan kebijakan terkait pembatasan akses yang didasarkan pada kebutuhan aplikasi bisnis dan sesuai dengan kebijakan kontrol akses yang diterapkan. Hal yang harus dipertimbangkan dalam rangka mendukung kebutuhan pembatasan akses adalah: - Menyediakan menu untuk mengontrol akses ke fungsi sistem aplikasi - Menyediakan data yang dapat diakses oleh pengguna tertentu - Mengontrol hak akses pengguna (membaca, menulis, menghapus, dan mengeksekusi) - Mengontrol hak akses dari aplikasi lain			

No	Pertanyaan	Status	Nilai
Pengguna juga diminta untuk mengikuti praktek-praktek organisasi dalam penggunaan informasi otentikasi rahasia. Semua pengguna disarankan untuk: - Menyimpan informasi otentikasi rahasia dan memastikan bahwa itu tidak dibocorkan kepada pihak lain - Mengubah informasi otentikasi rahasia setiap ada indikasi upaya masuk oleh pihak lain - Pilih password yang berkualitas dengan panjang minimum yang cukup - Tidak menggunakan informasi otentikasi yang sama untuk aplikasi yang berbeda			
5,14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak Dilakukan	0
Saran Perbaikan **Control 9.1.1 Access control policy** DPTSI harus menerapkan prosedur kebijakan terkait dengan pengelolaan akses kontrol yang tepat, hak akses, dan pembatasan untuk pengguna aset. Kebijakan tersebut harus memperhatikan hal berikut: - Persyaratan keamanan dari aplikasi bisnis - Konsistensi antara hak akses dan kebijakan klasifikasi informasi dari sistem dan jaringan - Peraturan yang relevan mengenai pembatasan akses ke data atau layanan - Pemisahan peran kontrol akses, misalnya meminta akses, akses otorisasi, administrasi akses - Penghapusan hak akses - Pengarsipan catatan semua peristiwa penting mengenai penggunaan dan pengelolaan identitas pengguna dan informasi otentikasi rahasia			
5,15	Ketetapan terkait waktu penyimpanan untuk	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	klasifikasi data yang ada dan syarat penghancuran data		
Saran Perbaikan **Control 8.3.1 Management of removable media** DPTSI dapat mendefinisikan keterkaitan waktu penyimpanan yang konsisten untuk klasifikasi data yang diterapkan organisasi dan dilakukan penyesuaian terhadap pengelolaan penghancuran data.			
5,16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan	0
Saran Perbaikan **Control 15.2.1 Monitoring and review of supplier services** Pemantauan dan Peninjauan layanan pemasok harus memastikan bahwa syarat dan kondisi keamanan informasi dari perjanjian sudah dipatuhi. DPTSI harus mempertahankan kontrol secara keseluruhan kedalam semua aspek keamanan informasi termasuk pengelolaan/ pertukaran data.			
5,17	Proses penyidikan/ investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Tidak Dilakukan	0
Saran Perbaikan **Control 13.2.4 Confidentiality or non-disclosure agreements** DPTSI dapat melakukan pencatatan terhadap penyelesaian insiden yang dilakukan terkait kegagalan keamanan informasi yang terjadi. Hal ini dapat membantu DPTSI untuk melakukan investigasi lebih lanjut terkait kesesuaian tindakan penyelesaian insiden yang dilakukan.			

No	Pertanyaan	Status	Nilai
5,18	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	Tidak Dilakukan	0

Saran Perbaikan
Control 12.3.1 Information backup
DPTSI harus membuat sebuah kebijakan yang menentukan persyaratan organisasi dalam melakukan backup informasi, perangkat lunak, dan sistem. Kebijakan backup harus menentukan retensi dan perlindungan persyaratan. Fasilitas backup yang memadai harus disediakan untuk memastikan bahwa semua informasi penting dan software dapat dipulihkan setelah kegagalan bencana atau media. Ketika merancang rencana backup, berikut ini adalah hal yang perlu dipertimbangkan:

- Catatan yang akurat dan lengkap dari salinan backup dan dokumentasi dari prosedur pemulihan
- Frekuensi backup harus mencerminkan kebutuhan bisnis
- Backup harus disimpan dilokasi terpencil dengan jarak yang cukup jauh untuk menghindari bencana yang terjadi dipusat utama
- Data backup harus diberi tingkat perlindungan secara fisik sesuai dengan standar yang diterapkan
- Data backup yang sangat rahasia harus dilindungi secara enkripsi

5,20	Proses pengecekan latar belakang SDM	Tidak Dilakukan	0

Saran Perbaikan
Control 7.1.1 Screening
DPTSI seharusnya melakukan proses verifikasi latar belakang SDM sesuai dengan undang-undang yang berlaku terkait:

- Karakter yang memuaskan
- Kelengkapan dan verifikasi dari riwayat hidup pemohon
- Konfirmasi kualifikasi akademik dan keprofesionalan

No	Pertanyaan	Status	Nilai
- Verifikasi identitas independen seperti paspor dan dokumen sejenis - Verifikasi catatan kriminal			
5,23	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Tidak Dilakukan	0
Saran Perbaikan **Control 9.2.3 Management of privileged access rights** Pembuatan prosedur yang membahas alokasi hak akses yang dikontrol melalui proses otorisasi resmi. Hal yang harus dipertimbangkan adalah: - Identifikasi hak akses istimewa yang terkait dengan setiap sistem operasi, database, dan aplikasi - Keistimewaan hak akses tidak boleh diberikan sampai proses otorisasi selesai - Persyaratan untuk berakhirnya hak akses istimewa harus didefinisikan - Kompetensi pengguna dengan hak akses istimewa harus ditinjau secara teratur untuk memverifikasi apakah mereka sejalan dengan tugas mereka			
5,24	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Perencanaan	2
Saran Perbaikan **Control 9.2.6 Removal or adjustment of access rights**			

No	Pertanyaan	Status	Nilai
DPTSI membuat prosedur dan kebijakan terkait dengan hak akses user untuk informasi dan aset yang terkait dengan fasilitas dan layanan pengolahan informasi harus dihapus atau ditangguhkan setelah mereka keluar dari instansi. Penghapusan atau penyesuaian dapat dilakukan dengan penghapusan, pencabutan atau penggantian kunci, kartu identifikasi, fasilitas pengolahan informasi atau langganan.			
5,25	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan	0
Saran Perbaikan **Control 12.3.1 Information backup** DPTSI harus membuat sebuah kebijakan yang menentukan persyaratan organisasi dalam melakukan backup informasi, perangkat lunak, dan sistem. Kebijakan backup harus menentukan retensi dan perlindungan persyaratan. Fasilitas backup yang memadai harus disediakan untuk memastikan bahwa semua informasi penting dan software dapat dipulihkan setelah kegagalan bencana atau media. Ketika merancang rencana backup, berikut ini adalah hal yang perlu dipertimbangkan: - Catatan yang akurat dan lengkap dari salinan backup dan dokumentasi dari prosedur pemulihan - Frekuensi backup harus mencerminkan kebutuhan bisnis - Backup harus disimpan dilokasi terpencil dengan jarak yang cukup jauh untuk menghindari bencana yang terjadi dipusat utama - Data backup harus diberi tingkat perlindungan secara fisik sesuai dengan standar yang diterapkan - Data backup yang sangat rahasia harus dilindungi secara enkripsi			
5,26	Apakah tersedia daftar rekaman pelaksanaan	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?		
Saran Perbaikan **Control 12.4.1 Event logging** DTSI harus menerapkan pembuatan daftar log aktivitas pengguna, kesalahan, dan kejadian terkait keamanan informasi dan disimpan secara berkala. Yang dapat dicatat dalam log adalah: - ID pengguna - Kegiatan sistem - Tanggal, waktu dan rincian peristiwa penting - Identitas perangkat atau lokasi jika mungkin - Perubahan konfigurasi sistem - Penggunaan hak akses istimewa - Penggunaan utilitas sistem dan aplikasi - File yang diakses dan jenis akses - Alamat jaringan dan protokol - Catatan transaksi yang dieksekusi oleh pengguna dalam aplikasi			
5,27	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan	0
Saran Perbaikan Control **18.1.2 Intellectual property rights** DPTSI harus membuat prosedur untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak terkait dengan HAKI dan penggunaan produk			

No	Pertanyaan	Status	Nilai
perangkat lunak. Pedoman berikut harus dipertimbangkan untuk melindungi materi yang dapat dianggap kekayaan intelektual: - Mendefinisikan penggunaan hukum terkait perangkat lunak dan produk informasi - Menggunakan perangkat lunak hanya dari sumber terkemuka untuk memastikan tidak adanya pelanggaran hak cipta - Memelihara bukti lisensi terhadap perangkat yang digunakan			
5,35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian	4
Saran Perbaikan **Control 11.2.4 Equipment maintenance** Untuk proses pemeriksaan dan perawatan perangkat komputer dan fasilitas pendukung harus diterapkan secara keseluruhan dengan cara membuat panduan pemeliharaan dengan mempertimbangkan hal: - Peralatan harus dipelihara sesuai dengan interval servis yang direkomendasikan pemasok dan spesifikasi - Hanya personil pemeliharaan yang berwenang yang harus melakukan perbaikan dan peralatan layanan - Semua catatan terkait kegiatan pemeliharaan harus disimpan dengan baik - Semua persyaratan perawatan yang dikenakan oleh kebijakan asuransi harus dipenuhi - Sebelum meletakkan peralatan kembali ke dalam operasi setelah pemeliharaan, itu harus diperiksa untuk			

No	Pertanyaan	Status	Nilai
	memastikan bahwa peralatan tersebut belum dirusak dan tidak berfungsi		
5,36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	4
Saran Perbaikan **Control 13.2.2 Agreements on information transfer** DPTSI harus menetapkan kebijakan, prosedur, dan standar untuk melindungi pengiriman informasi dan media fisik dan harus dirujuk pada perjanjian transfer tersebut. Isi keamanan informasi dari setiap kesepakatan harus mencerminkan sensitivitas informasi yang terlibat.			
5,37	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Tidak Dilakukan	0
Saran Perbaikan **Control 11.1.5 Working in secure areas** DPTSI harus menerapkan pedoman untuk mengamankan kantor, ruangan, dan fasilitas dengan mempertimbangkan:			

No	Pertanyaan	Status	Nilai
- Pihak terkait harus menyadari keberadaan dan kegiatan yang dilakukan dalam ruangan tersebut - Dilakukan pengawasan kerja didaerah aman untuk alasan keamanan dan untunk mencegah peluang dari kegiatan yang berbahaya - Dilakukan pengamanan fisik untuk daerah aman yang sedang kosong - Fotografi, video, audio atau peralatan rekaman lainnya, seperti kamera di perangkat mobile, seharusnya tidak diperbolehkan, kecuali jika diizinkan Peraturan untuk bekerja di daerah aman termasuk kontrol untuk karyawan dan pengguna pihak eksternal yang bekerja di daerah aman dan mereka mencakup semua kegiatan yang terjadi di daerah aman.			
5,38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Tidak Dilakukan	0
Saran Perbaikan **Control 11.1.2 Physical entry controls** Harus dilakukan pengamanan terkait kontrol masuk untuk menghindari akses oleh orang yang tidak berhak. Dibuat pedoman yang mempertimbangkan: - Tanggal dan waktu masuk dari pengunjung harus dicatat, dan semua pengunjung harus diawasi kecuali akses mereka telah disetujui sebelumnya - Akses ke daerah-daerah di mana informasi rahasia diproses atau disimpan harus dibatasi untuk individu yang berwenang hanya dengan menerapkan kontrol akses yang sesuai, misalnya dengan menerapkan mekanisme otentikasi dua faktor seperti kartu akses dan PIN rahasia			

No	Pertanyaan	Status	Nilai
- Sebuah buku log fisik atau jejak audit elektronik dari semua akses harus dipelihara secara aman dan harus dipantau - Pihak eksternal harus diberikan akses terbatas untuk mengamankan daerah atau fasilitas pengolahan informasi rahasia hanya ketika diperlukan			

6.4.2.5 Saran Perbaikan Area Teknologi dan Keamanan Informasi

Saran perbaikan untuk area Teknologi dan Keamanan Informasi ini berisikan saran perbaikan untuk 8 pertanyaan yang mendapat nilai kurang/ tidak dilakukan oleh DPTSI ITS. Saran perbaikan ini mengacu pada ISO/IEC 27002:2013.

Tabel 6.29 Saran Perbaikan Area Teknologi & KI

No	Pertanyaan	Status	Nilai
6,5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2
Saran Perbaikan **Control 14.1.2 Securing application services on public networks** Pihak DPTSI harus melakukan penerapa n pemindaai jaringan, sistem, dan aplikasi secara rutin untuk menghindari risiko insiden keamanan informasi. Pemindaian tidak boleh dilakukan jika hanya sudah terjadi insiden keamanan informasi karena hal ini dapat membahayakan organisasi.			

No	Pertanyaan	Status	Nilai
6,12	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan	0
Saran Perbaikan **Control 10.1.1 Policy on the use of cryptographic controls** DPTSI harus mengembangkan standar terkait penggunaan enkripsi dengan mempertimbangkan hal sebagai berikut: - Dilakukan pendekatan manajemen kebijakan kriptografi di seluruh organisasi - Diidentifikasi jenis, kekuatan, dan kualitas algoritma enkripsi yang digunakan berdasar penilaian risiko - Penggunaan enkripsi untuk perlindungan informasi - Dampak penggunaan informasi terenkripsi pada kontrol yang bergantung pada pemeriksaan konten, seperti *malware detection*			
6,14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Tidak Dilakukan	0
Saran Perbaikan **Control 9.4.3 Password management system** DPTSI harus menerapkan syarat pergantian password yang berkualitas secara otomatis pada semua aplikasi dan sistem yang dimiliki.			
6,16	Apakah sistem dan aplikasi yang digunakan	Dalam Penerapan/	4

No	Pertanyaan	Status	Nilai
	sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Diterapkan Sebagian	
Saran Perbaikan **Control 9.2.3 Management of privileged access rights** Semua sistem aplikasi yang dimiliki DPTSI harus menerapkan pembatasan waktu akses secara otomatis dengan tujuan untuk menjaga pengamanan pada sistem dan aplikasi yang tidak dipakai lama dalam kondisi login.			
6,21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak Dilakukan	0
Saran Perbaikan **Control 12.2.1 Controls against malware** DPTSI harus melakukan pencatatan jejak rekam untuk pendeteksian malware dan perbaikan perangkat lunak. Jejak rekam juga berisi lapoan pembaharuan anti virus yang dilakukan secara rutin.			
6,22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan	0
Saran Perbaikan **Control 12.2.1 Controls against malware**			

No	Pertanyaan	Status	Nilai
DPTSI harus melakukan pencatatan jejak rekam untuk pendeteksian malware dan perbaikan perangkat lunak. Jejak rekam juga berisi lapoan pembaharuan anti virus yang dilakukan secara rutin. Selain itu juga dapat ditetapkan kebijakan formal yang melarang penggunaan perangkat lunak yang tidak sah dan pendeteksian penggunaan sistus yang berbahaya.			
6,25	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Tidak Dilakukan	0
Saran Perbaikan **Control 14.2.6 Secure development environment** DPTSI harus menerapkan penggunaan standar platform untuk teknologi dan yang mangtur keseluruhan siklus hidup pengembangan sistem. Lingkungan uji coba harus dijamin keamanannya termasuk orang-orang, proses, dan teknologi yang terkait dengan pengembangan sistem. DPTSI harus menilai risiko yang terkait dengan upaya pengembangan sistem dan membangun lingkungan pengembangan yang aman bagi upaya pengembangan sistem tertentu.			
6,26	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
Saran Perbaikan **Control 18.2.1 Independent review of information security**			

No	Pertanyaan	Status	Nilai
Control 18.2.2 Compliance with security policies and standards Harus dilakukan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi yang ditinjau secara independen pada jangka waktu yang telah ditentukan atau saat terjadi perubahan yang signifikan pada prosedur. Pimpinan instansi juga harus melakukan peninjauan kepatuhan pengolahan informasi dan prosedur dalam area tanggung jawab mereka dengan kebijakan keamanan yang sesuai, standar dan persyaratan keamanan lainnya secara teratur. Jika ada ketidakpatuhan maka harus dilakukan: - Identifikasi penyebab ketidakpatuhan - Evaluasi kebutuhan tindakan untuk mencapai kepatuhan - Menerapkan tindakan koreksi yang tepat - Meninjau tindakan korektif yang dilakukan untuk verifikasi efektivitas dari setiap kekurangan dan kelemahan yang ada			

“Halaman ini sengaja dikosongkan”

BAB VII
KESIMPULAN DAN SARAN

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

7.1 Kesimpulan

Kesimpulan yang dapat diperoleh dari penelitian tugas akhir ini terkait penilaian manajemenen keamanan informasi di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya dnegan menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

- Hasil dari penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 26 dari jumlah total keseluruhan sebesar 50. Hal ini menunjukkan bahwa DPTSI ITS Surabaya sudah tinggi dalam kebutuhan penggunaan sistem elektronik yang artinya penggunaan sistem elektronik adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan
- Hasil keseluruhan dari penilaian kelima area dalam Indeks KAMI adalah sebesar 249 dari jumlah total keseluruhan sebesar 645 dan berada pada level I-II dimana level ini masih berada pada kondisi awal penerpan keamanan informasi dan kondisi penerapan kerangka kerja dasar penerapan keamanan informasi
- Tingkat kematangan per-area akan dijabarkan sebagai berikut: Area Tata Kelola Keamanan Informasi berada pada tingkat I+, area Pengelolaan Risiko Keamanan Informasi pada tingkat I, area Kerangka kerja Pengelolaan Keamanan Informasi pada tingkat I+, area Pengelolaan Aset Informasi pada tingkat I+, dan area Teknologi & Keamanan Informasi pada tingkat II.

- Poin nilai paling tinggi yang diperoleh dari kelima area tersebut adalah pada area Teknologi & Keamanan Informasi dengan nilai 75 poin. Poin ini diperoleh karena dari 26 pertanyaan, terdapat 6 pertanyaan yang tidak dilakukan dan 2 pertanyaan yang diterapkan sebagian. Untuk 18 pertanyaan yang lain sudah diterapkan secara keseluruhan oleh pihak DPTSI ITS Surabaya
- Poin nilai paling rendah yang diperoleh dari kelima area tersebut adalah pada area Pengelolaan Risiko Keamanan Informasi dengan nilai 24 poin. Poin ini diperoleh karena dari 16 pertanyaan, terdapat 10 pertanyaan yang tidak dilakukan dan 6 pertanyaan yang lain sudah diterapkan secara keseluruhan oleh pihak DPTSI ITS Surabaya
- Hasil penilaian kelima area yang menunjukkan nilai sebesar 252, dengan hasil nilai tingkat penggunaan sistem elektronik sebesar 26 maka DPTSI ITS Surabaya belum dapat dikatakan matang dan sesuai dengan standar ISO 27001:2013 karena belum mencapai level III+ dimana penerapan keamanan informasi telah terdefinisi dan konsisten

7.2 Saran

Saran yang dapat diberikan untuk penelitian selanjutnya dari hasil pengerjaan tugas akhir dengan studi kasus Evaluasi Keamanan Informasi Pada Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya dengan Menggunakan Indeks Keamanan Informasi (KAMI) ini adalah sebagai berikut:

- Alangkah lebih baikya jika mengikuti petunjuk teknis secara detail dengan megikuti acara Bimbingan Teknis yang diadakan oleh pihak Kominfo mengenai proses penilaian pada Indeks KAMI guna memahami perolehan skor yang didapat maupun untuk perbaikan

serta pengembangan proses penilaian untuk kedepannya

- Perhatikan cara pengujian pada pertanyaan yang membutuhkan jenis penilaian lebih dari satu, maka lakukan pengujian terhadap kualitas dan juga kuantitas pada item yang dinilai agar nilai yang diberikan pada pertanyaan tersebut benar-benar valid

“Halaman ini sengaja dikosongkan”

DAFTAR PUSTAKA

[1] "Keamanan Informasi," 04 09 2012. [Online]. Available: https://keamananinformasi.wordpress.com/2012/09/04/definis-keamanan-informasi/. [Diakses 10 09 2016].

[2] "LPTSI," ITS, 2016. [Online]. Available: http://lptsi.its.ac.id/?page_id=150. [Diakses 11 09 2016].

[3] A. Affandi, "Memorandum Akhir Jabatan Ketua LPTSI ITS," LPTSI ITS, Surabaya, 2016.

[4] "Indeks Keamanan Informasi (KAMI)," Kementerian Komunikasi dan Informatika RI, 23 10 2013. [Online]. Available: https://kominfo.go.id/index.php/content/detail/3326/Indeks-Keamanan-Informasi--KAMI-/0/kemanan_informasi. [Diakses 10 09 2016].

[5] L. Ulinnuha, Evaluasi Pengelolaan Keamanan Jaringan di ITS Dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI, Surabaya: Sistem Informasi ITS, 2013.

[6] T. D. K. Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik," Jakarta, Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, 2012, pp. 34 - 58.

[7] K. K. d. Informasi, Penulis, *Indeks KAMI versi 2.3*. [Performance]. 2012.

[8] K. K. d. Informasi, Penulis, *Indeks KAMI versi 3.1*. [Performance]. 2015.

[9] M. R. Ridho, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI)

Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi dan Informatika Surabaya," *TEKNIK POMITS* , vol. 1, pp. 1-6, 2012.

[10 E. L. Putra, Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI), Surabaya: Sistem Informasi ITS, 2014.

[11 M. Siga, Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur, Surabaya: Sistem Informasi ITS, 2014.

[12 I. Afrianto, "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009 Studi Kasus Perguruan Tinggi X," *ULTIMA InfoSys,* vol. VI, pp. 1-7, 2015.

[13 R. Sarno dan I. Iffano, "Sistem Manajemen Keamanan Informasi," 2009.

[14 M. Whitman dan H. Mattord, Principles of Information Security Fifth Edition, Boston: Cengage Learning, 2014.

[15 M. Rouse, "Information Security Management System (ISMS)," 2011. [Online]. Available: http://whatis.techtarget.com/definition/information-security-management-system-ISMS. [Diakses 05 10 2016].

[16 "Mengenal Sistem Manajemen Keamanan Informasi," Lembaga Sandi Negara, 10 12 2015. [Online]. Available: http://www.lemsaneg.go.id/index.php/2015/12/10/mengenal-sistem-manajemen-keamanan-informasi/. [Diakses 5 10 2016].

[17 "Information Security Management System (ISMS)," CNNI Portal, [Online]. Available:

http://cnii.cybersecurity.my/main/isms-home.html. [Diakses 5 10 2016].

[18 Direktorat Sistem Informasi, Perangkat Lunak dan Konten Direktorat Jenderal Aplikasi Telematika Departemen Komunikasi dan Informatika, "Pedoman Praktis Manajemen Keamanan Informasi untuk Pimpinan Organisasi," vol. 2, 2007.

[19 G. Stoneburner, Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce, National Institute of Standards and Technology, 2002.

[20 M. Spremic, IT Governance and IT Risk Management Principles and Methods for Supporting 'Always-On'Enterprise Information Systems, 2010.

[21 T. Merna dan F. Al-Thani, Corporate Risk Management 2nd Edition, 2008.

[22 "ISO/IEC 27001- Information Security Management," ISO , 2013. [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Diakses 11 09 2016].

[23 T. D. K. Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik," Jakarta, Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, 2012, pp. 10-12.

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

[25 C. Schell, "The Value of the Case Study as a Research Strategy," 1992.

[26 L. Yamagata Lynch, "Unit of Analysis in Cultural Historical Activity Theoretical Research," 23 6

2013. [Online]. Available: http://www.slideshare.net/lisayamagatalynch/unit-of-analysis-in-cultural-historical-activity-theoretical-research-can-we-talk-about-the-methodological-dilemmas. [Diakses 20 10 2016].

[27 "LPTSI," ITS, 2016. [Online]. Available: lptsi.its.ac.id/?page_id=154. [Diakses 11 09 2016].

[28 Institut Teknologi Sepuluh Nopember , "Peraturan Rektor Institut Teknologi Sepuluh Nopember Nomor 10 Tahun 2016," Surabaya, 2016.

BIODATA PENULIS

FIRZAH A BASYARAHIL, lahir 2 Juni 1995 di kota Surabaya. Penulis merupakan anak keempat dari lima bersaudara. Penulis pernah menempuh pendidikan formal di SDN Simomulyo VIII Surabaya, SMPN 2 Surabaya, SMAN 2 Surabaya, dan akhirnya masuk menjadi mahasiswa program sarjana jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) angkatan 2013 dan terdaftar dengan NRP 5213100069. Pada akhir masa perkuliahan di jurusan Sistem Informasi ITS, penulis memilih untuk mengerjakan tugas akhir di Laboratorium Manajemen Sistem Informasi (MSI). Penulis mengambil topik mengenai evaluasi manajemen keamanan informasi dibawah bimbingan Hanim Maria Astuti, S.Kom., M.Sc dan Bekti Cahyo Hidayanto, S.Si., M.Kom. Selama menjadi mahasiswa di jurusan Sistem Informasi, penulis aktif dalam mengikuti kegiatan organisasi jurusan yaitu HMSI dan menjabat sebagai staff departemen sosial masyarakat. Tidak hanya itu, penulis juga aktif menjadi panitia diberbagai kegiatan kampus dan salah satunya pernah menjadi staff dan koordinator tim soal acara ISE 2014 dan ISE 2015. Untuk kepentingan penelitian penulis dapat dihubungi melalui e-mail: firzahab@gmail.com

"*Halaman ini sengaja dikosongkan"*

LAMPIRAN A

Interview Protocol Penggunaan Kategori Sistem Elektronik & 5 Area Indeks KAMI Pada DPTSI ITS

A-1 Form wawancara mengenai Kategori Sistem Elektronik

Hari/Tanggal :
Pukul :
Lokasi :
Narasumber :
Jabatan :

No	Pertanyaan Kategori Sistem Elektronik
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus

No	Pertanyaan Kategori Sistem Elektronik
1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna
1,6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak

No	Pertanyaan Kategori Sistem Elektronik
1,9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih [C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)

A-2 Form wawancara mengenai Tata Kelola Keamanan Informasi

Hari/Tanggal :
Pukul :
Lokasi :
Narasumber :
Jabatan :

No.	Kategori	Pertanyaan Tata Kelola Keamanan Informasi
2,1	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi

No.	Kategori	Pertanyaan Tata Kelola Keamanan Informasi
		(misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?
2,2	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?
2,3	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?
2,4	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?
2,5	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?
2,6	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?
2,7	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?
2,8	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?

No.	Kategori	Pertanyaan Tata Kelola Keamanan Informasi
2,9	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?
2.10	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?
2.11	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?
2.12	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?
2.13	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?
2.14	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business*

No.	Kategori	Pertanyaan Tata Kelola Keamanan Informasi
		continuity dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?
2.15	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?
2.16	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?
2.17	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?
2.18	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?
2.19	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?
2.20	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?

No.	Kategori	Pertanyaan Tata Kelola Keamanan Informasi
2.21	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?
2.22	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?

A-3 Form wawancara mengenai Pengelolaan Risiko Keamanan Informasi

Hari/Tanggal :
Pukul :
Lokasi :
Narasumber :
Jabatan :

No.	Kategori	Pertanyaan Pengelolaan Risiko Keamanan Informasi
3,1	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
3,2	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?
3,3	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi

No.	Kategori	Pertanyaan Pengelolaan Risiko Keamanan Informasi
		yang terdokumentasi dan secara resmi digunakan?
3,4	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?
3,5	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?
3,6	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?
3,7	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?
3,8	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?
3,9	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?
3.10	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?

No.	Kategori	Pertanyaan Pengelolaan Risiko Keamanan Informasi
3.11	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?
3.12	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?
3.13	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?
3.14	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?
3.15	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?
3.16	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?

A-4 Form wawancara mengenai Kerangka Kerja Pengelolaan Keamanan Informasi

Hari/Tanggal :
Pukul :
Lokasi :
Narasumber :
Jabatan :

No.	Kategori	Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi
4,1	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?
4,2	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?
4,3	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?
4,4	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?
4,5	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko

No.	Kategori	Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi
		keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?
4,6	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?
4,7	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?
4,8	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?
4,9	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?
4.10	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?

No.	Kategori	Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi
4,11	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?
4,12	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?
4,13	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?
4,14	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?
4,15	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?
4,16	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?
4.17	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?

No.	Kategori	Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi
4.18	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?
4.19	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?
4.20	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?
4,21	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?
4.22	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?
4,23	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?
4,24	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?

No.	Kategori	Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi
4.25	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?
4,26	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?
4,27	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?
4,28	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?
4,29	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?

A-5 Form wawancara mengenai Pengelolaan Aset Informasi

Hari/Tanggal :
Pukul :
Lokasi :
Narasumber :
Jabatan :

No.	Kategori	Pertanyaan Pengelolaan Aset Informasi
5,1	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)
5,2	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?
5,3	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?
5,4	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut
5,5	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?
5,6	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?
5,7	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?

No.	Kategori	Pertanyaan Pengelolaan Aset Informasi
		Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?
5,8	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda
5,9	1	Tata tertib penggunaan komputer, email, internet dan intranet
5.10	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI
5.11	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi
5.12	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
5.13	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya
5.14	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
5.15	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
5.16	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
5.17	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
5.18	1	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala
5.19	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya

No.	Kategori	Pertanyaan Pengelolaan Aset Informasi
5.20	2	Proses pengecekan latar belakang SDM
5.21	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
5.22	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan
5.23	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku
5.24	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.
5.25	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?
5.26	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?
5.27	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?
5.28	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?

No.	Kategori	Pertanyaan Pengelolaan Aset Informasi
5.29	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?
5.30	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?
5.31	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?
5.32	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?
5.33	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)
5.34	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?
5.35	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?
5.36	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?

No.	Kategori	Pertanyaan Pengelolaan Aset Informasi
5.37	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)
5.38	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?

A-6 Form wawancara mengenai Teknologi dan Keamanan Informasi

Hari/Tanggal :
Pukul :
Lokasi :
Narasumber :
Jabatan :

No.	Kategori	Pertanyaan Teknologi dan Keamanan Informasi
6,1	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?
6,2	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?

No.	Kategori	Pertanyaan Teknologi dan Keamanan Informasi
6,3	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?
6,4	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?
6,5	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?
6,6	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?
6,7	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?
6,8	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?
6,9	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?
6.10	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?
6.11	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?

No.	Kategori	Pertanyaan Teknologi dan Keamanan Informasi
6.12	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?
6.13	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?
6.14	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?
6.15	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?
6.16	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts, lockout* setelah kegagalan *login,*dan penarikan akses?
6.17	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?
6.18	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?
6.19	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?
6.20	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?

No.	Kategori	Pertanyaan Teknologi dan Keamanan Informasi
6.2 1	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?
6.2 2	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?
6.2 3	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?
6.2 4	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?
6.2 5	3	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?
6.2 6	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?

LAMPIRAN B

Hasil Wawancara Penggunaan Kategori Sistem Elektronik & 5 Area Indeks KAMI Pada DPTSI ITS

B-1 Hasil wawancara mengenai Kategori Sistem Elektronik

Hari/Tanggal : Jumat/ 6 Desember 2016
Pukul : 10.00 WIB
Lokasi : DPTSI ITS
Narasumber : Ibu Hanim Maria Astuti & Ibu Nuli
Jabatan : Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi & Bendahara DPTSI

No	Pertanyaan Kategori Sistem Elektronik
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus

1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna
1,6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak
1,9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih

	[C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)

B-2 Hasil wawancara mengenai Tata Kelola Keamanan Informasi

Hari/Tanggal **:** Senin/ 28 November 2016
Pukul **:** 13.00 WIB
Lokasi **:** DPTSI ITS Surabaya
Narasumber **:** Bapak Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D & Ibu Hanim Maria Astuti, S.Kom., M.Sc.
Jabatan **:** Kepala SubDirektorat Infrastruktur & Keamanan Teknologi Informasi, Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi

No.	Pertanyaan Tata Kelola Keamanan Informasi	Jawaban Wawancara
2,1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP),	Sudah dijalankan

	termasuk penetapan kebijakan terkait?	
2,2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Sudah ada bagian khusus yang menangani yaitu bagian infrastruktur & keamanan, namun tidak terlalu dispesifikkan untuk perorangan
2,3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Wewenang dibagi kedalam bagian listrik, jaringan, dan sistem namun tidak ada tugas khusus dan tidak dilakukan pengkotakan bagian secara tertulis dan paten
2,4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Ada PIC dari masing-masing tugas namun tidak secara tertulis. Untuk jumlah anggota masih sangat kurang kaerena hanya terdiri dari 8 orang saja
2,5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Belum ada pemetaan secara tertulis dan tidak dilakukan audit internal
2,6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar	Untuk staff ada standar kompetensi khusus

	kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	namun tidak ada secara tertulis
2,7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Kompetensi yang dimiliki sudah cukup baik namun kembali lagi bahwa tidak ada persyaratan secara tertulis
2,8	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Belum pernah ada sosialisasi secara resmi namun untuk semua pihak sudah paham dan sadar akan keamanan informasi di instansi
2,9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dilakukan beberapa pelatihan yang dirasa penting dan terkait keamanan. Tahun 2016 ini dilakukan pelatihan tentang *honeypot* yang diadakan oleh Kominfo bagi beberapa staff infrastruktur
2.10	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Integrasi dilakukan di bagian internet dan intranet. Namun tidak ada pengamanan khusus pda intranet
2.11	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan	Belum ada identifikasi data pribadi sesuai undang-undang. Belum

	menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	ada penerapan perundang-undangan
2.12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Ada koordinasi dengan pihak lain yang terkait namun masih belum ada dokumen yang resmi untuk hal tersebut
2.13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Proaktif dilakukan. Biasanya dengan pihak ISP dan ke bagian developer jika ada masalah di aplikasi yang dibuat
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah	Belum ada dokumen BCP dan DRP secara formal namun tetap dilakukan per masing-

	kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	masing bagian di DPTSI ITS (Bu Hanim)
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Dilakukan pelaporan ke kepala instansi secara rutin. Bisa setiap hari, mingguan, dan bulanan namun untuk dokumen pelaporan secara tertulis masih belum ada
2.16	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dibahas sebelum mengambil keputusan karena memang kamanan informasi sangat penting. Seperti misalnya mengeluarkan kebijakan terkait email untuk menghindari risiko-risiko (Bu Hanim)
2.17	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak dilakukan penerapan program khusus
2.18	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja	Tidak ada parameter dan pengukuran untuk kinerja pengelolaan keamanan

	pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	
2.19	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak ada program untuk melakukan penilaian kinerja pengelolaan keamanan
2.20	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	Tidak ada target dan sasaran khusus
2.21	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak ada perangkat hukum yang digunakan untuk keamanan informasinya
2.22	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden	Tidak ada kebijakan khusus yang diterapkan

	keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	

B-3 Hasil wawancara mengenai Pengelolaan Risiko Keamanan Informasi

Hari/Tanggal **:** 29 November 2016 dan 30 November 2016
Pukul **:** 13.00 WIB, 11.00 WIB
Lokasi **:** DPTSI ITS Surabaya
Narasumber **:** Bapak Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D
Jabatan **:** Kepala SubDirektorat Infrastruktur & Keamanan Teknologi Informasi

No.	Pertanyaan Pengelolaan Risiko Keamanan Informasi	Jawaban Wawancara
3,1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Belum ada pengelolaan risiko secara tertulis dan resmi
3,2	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Masih belum penanggung jawab risiko yang ditugaskan khusus
3,3	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang	Belum ada, masih perencanaan untuk menggunakan ISO 27001

	terdokumentasi dan secara resmi digunakan?	
3,4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Masih belum ada karena kerangka kerjanya masih belum diterapkan
3,5	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Ada catatan risiko yang diterima, dicatat di dalam log sensor ids terkait upaya masuk dari pihak yang tidak berhak
3,6	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?	Untuk kepemilikan aset sudah ada dokumen tertulisnya
3,7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Sudah pernah dilakukan identifikasi namun tidak ada dokumen tertulisnya
3,8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah	Sudah ada dampak yang dipikirkan dan juga langkah-langkah mitigasinya

	ditetapkan sesuai dengan definisi yang ada?	
3,9	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)?	Sudah ada kajian risiko saat rapat dibahas biasanya, seperti saat rilis layanan baru itu harus diketahui *performance* keamanannya dan akhirnya dilakukan balancing dan penerapan firewall. Namun untuk dokumennya memang masih belum ada
3.10	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Saat memikirkan risiko yang akan terjadi otomatis juga langsung dipikirkan langkah mitigasinya
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Untuk dokumentasi masih belum ada namun tingkat prioritasnya berdasarkan *urgency*nya. Biasanya yang harus dipulihkan cepat itu terkait data user dan infrastruktur

3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak dilakukan secara resmi, biasanya dibahas melalui grup chat
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Masih belum dilakukan evaluasi secara terukur
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Tidak dilakukan pengkajian ulang terhadap profil risiko dan bentuk mitigasinya , karena mitigasi yang biasanya dilakukan sudah dianggap baik dan membantu menyelesaikan masalah
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak, karena belum ada kerangka kerja
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak dimasukkan sebagai kriteria penilaian kinerja pengamanan

B-4 Hasil wawancara mengenai Kerangka Kerja Pengelolaan Keamanan Informasi

Hari/Tanggal **:** Kamis/24 November 2016 dan Rabu/30 November 2016
Pukul **:** 09.0 WIB dan 13.00 WIB
Lokasi **:** DPTSI ITS
Narasumber **:** Ibu Anny, Bapak Royyana, Mas Wicaq
Jabatan **:** Kepala SubDirektorat Pengembangan TI, Kepala SubDirektorat Infrastruktur & Keamanan Teknologi Informasi, Staff Jaringan

No.	Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi	Jawaban Wawancara
4,1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Sudah ada kebijakan terkait keamanan informasi namun belum lengkap untuk peran masing-masing pihak
4,2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Sudah pernah dipublikasikan, namun semua dokumen kebijakan disimpan oleh 1 orang di bagian helpdesk/ layanan dan dalam bentuk hardcopy

4,3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Masih belum ada
4,4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Masih belum dilakukan
4,5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?	Untuk mitigasi dan risiko seperti yang sudah dijelaskan sebelumnya bahwa masih belum ada penerapannya
4,6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak	Untuk dokumentasinya masih belum ada, namun sudah dilakukan. Untuk semua identifikasinya dilakukan dengan menggunakan log ids dan log file

	lanjuti sesuai prosedur yang diberlakukan?	
4,7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Sudah ada. Kontrak yang terkait itu dengan bagian pengadaan & perawatan server dan dengan bagian penyambungan kabel
4,8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Untuk konsekuensi yang secara tertulis mungkin ada namun bukan kewenangan dari DPTSI melainkan di bagian hukum ITS. Untuk kejadian pelanggaran keamanan pernah terjadi tahun 2007 dan dilakukan oleh mahasiswa, konsekuensinya di skors
4,9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	Tidak ada secara resmi
4.10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur	Untuk *security patch* sudah dilakukan namun

	operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	tidak ada kebijakan khusus yang diterapkan
4,11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Dibahas saat membahas proyek yang dikerjakan. Misal saat ada pengembangan proyek itu juga dibatasi penggunaan servernya, tidak boleh langsung ke server live karena kalau langsung ke server live itu bisa diakses semuanya
4,12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Belum ada secara tertulis
4,13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	SDLC pasti diterapkan dan berbeda-beda dari setiap proyeknya dan tidak semua ada dokumentasinya.

4,14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Untuk penerapan pengamanan sudah dilakukan, namun untuk dokumentasi risikonya masih belum ada. Untuk jangka waktu penyelesaiannya sudah ditetapkan
4,15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Masih belum punya untuk dokumen BCP
4,16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Untuk DRP sendiri DPTSI maish belum punya namun untuk rencana pemulihan sudah diterapkan dan DPTSI memiliki DRC dibeberapa tempat yang terpisah
4.17	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Belum pernah dilakukan

4.18	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?	Belum dilakukan evaluasi
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak ada evaluasi secara berkala terkait kebijakan dan prosedur keamanan informasi
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Sudah ada strateginya dan biasanya dilakukan integrasi dengan bagian pengemabangan
4,21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Lebih ke mencegah dengan cara mengencourage dan menenkripsi dengan menggunakan https. Namun tidak ada secara tertulis dalam dokumen

4.2 2	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Direalisasikan untuk penerapan strategi keamanan informasinya
4,2 3	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)?	Belum pernah dilakukan audit internal
4,2 4	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Belum ada
4.2 5	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Belum ada
4,2 6	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Belum dilakukan

4,27	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?	Belum ada penilaian aspek finansial untuk perubahan infrastruktur dan pengelolaan perubahannya
4,28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak dilakukan pengujian secara rutin dan efektif terhadap kepatuhan program keamanan informasi
4,29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Belum diterapkan, masih mau disesuaikan dengan ISO

B-5 Hasil wawancara mengenai Pengelolaan Aset Informasi

Hari/Tanggal **:** Kamis/24 November 2016 dan Senin/28 November 2016
Pukul **:** 10.00 WIB dan 08.00 WIB
Lokasi **:** DPTSI ITS Surabaya dan Lantai 6 Perpustakaan ITS
Narasumber **:** Bapak Royanna, Mas Wicaq, Bapak Cahya, Mas Anta
Jabatan **:** Kepala SubDirektorat Infrastruktur & Keamanan Teknologi Informasi, Staff Infrastruktur & Keamanan Teknologi Informasi

No.	Pertanyaan Pengelolaan Aset Informasi	Jawaban Wawancara
5,1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Ada daftar inventaris aset milik ITS
5,2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak ada undang-undang yang digunakan untuk klasifikasi aset
5,3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Belum dilakukan juga karena masih belum ada undang-undang yang dipakai

5,4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	Tingkatan akses dulu dibedakan dengan menggunakan proxy, namun sekarang sudah tidak lagi
5,5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Ada pengelolaan perubahan sistem dan konfigurasi
5,6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Sudah dilakukan untuk pengelolaan konfigurasi
5,7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Ada dengan cara menambahkan aset baru ke daftar inventaris yang dimiliki
	Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5,8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Untuk secara individu adanya hanya dibagian sistem bukan untuk smeua bagian

5,9	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak ada tata taertib
5.10	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak ada secara tertulis
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	Hanya ada beberapa di website namun tidak semuanya
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Masih belum diterapkan
5.13	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Untuk kebijakannya masih belum ada secara tertulis. Untuk pelanggaran yang dilakukan user, misalkan spam ke email maka dapat diberi sanksi yaitu diblokir akunnya
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak ada prosedur secara tertulis
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak pernah dilakukan penghancuran data sebelumnya
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak pernah dilakukan pertukaran data dengan pihak eksternal

5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dilakukan secara keseluruhan dan ada pencatatan insiden
5.18	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	Dilakukan backup secara berkala dan ada prosedur yang mengaturnya
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	ada pembagian zona dan klasifikasi aset
5.20	Proses pengecekan latar belakang SDM	Dilakukan saat diawal perekrutan karyawan, dilakukan penilaian terhadap bidang terkait
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Ada koordinasi dengan pihak lain, biasanya dengan pihak ISP terkait
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Sudah ada prosedur penghancuran dokumen
5.23	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Sudah dimiliki. Sekarang akses menggunakan integra
5.24	Prosedur untuk *user* yang mutasi/keluar atau tenaga	Belum ada prosedur, namun sekarang sedang dalam tahap pembuatan

	kontrak/*outsource* yang habis masa kerjanya.	
5.25	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak ada daftar khusus untuk di*backup*.
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak ada
5.27	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?	Belum ada prosedur khusus yang mengatur
5.28	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?	Sudah ada pengamanan berlapis, misalnya dengan menggunakan firewall dengan tingkatan yang berbeda
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan	Sudah ada dengan menggunakan *finger print*

	elektronik) ke fasilitas fisik?	
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Sudah ada alarm kebakaran dan tabung gas pemadam kebakaran. Untuk suhu dan kelembaban sendiri sudah ada notifikasi khusus yang dikirimkan ke orang terkait jika tidka sesuai dengan batas minimal yang ditentukan
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Sudah ada didalam ruang server
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Ada surat terima, biasanya dilakukan dengan jurusan-jurusan yang ada di ITS
5.33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	Untuk pemindahannya menggunakan berita acara lalu didaftar inventaris akan diperbaharui
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan	Sangat penting dan sudah ada semua standarnya untuk ruang server yang di DPTSI,

	dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	namun untuk yang ruang server di lantai 6 masih belum mengikuti standar
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Tidak dilakukan perawatan komputer secara khusus jika ada kerusakan. Biasanya dilakukan pada jaringan
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Untuk pengamanan khusus fisik tidak ada, namun hanya dilengkapi dengan pengamanan password
5.37	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Tidak ada peraturan resmi dan tanda larangan. Untuk orang yang masuk juga tidak diperingatkan ataupun diingatkan dan tidak diperiksa

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

B-6 Hasil wawancara mengenai Teknologi dan Keamanan Informasi

Hari/Tanggal **:** Senin/ 5 Desember 2016
Pukul **:** 08.00 WIB
Lokasi **:** Lantai 6 Perpustakaan ITS
Narasumber **:** Bapak Cahya, bapak Bustari, Mas Anta
Jabatan **:** Staff Infrastruktur & Keamanan Informasi

No.	Pertanyaan Teknologi dan Keamanan Informasi	Jawaban Wawancara
6,1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Ada beberapa zona untuk pembagian akses. Zona server dibedakan dengan IP, zona untuk internet juga dibedakan dengan tingkatan firewall
6,2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Sudah ada segmentasinya
6,3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang	Ada yang sudah ada dan ada yang tidak ada. Yang ada itu untuk server jaringan dan aplikasi

	dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	
6,4	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dilakukan analisa
6,5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dilakukan tetapi tidak secara rutin, hanya dilakukan jika ada insiden saja
6,6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Iya, dan sekarang sudah disamakan semua dengan menggunakan *single sign-on*
6,7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Ada monitoring kapasitas

6,8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Terekam dalam log yang dipegang oleh staff infrastruktur
6,9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Ada notifikasi yang masuk ke bagian admin
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dilakukan analisa berkala dari dashboard sensor yang dikumpulkan setiap hari. Menggunakan aplikasi alliance fault
6.11	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Pasti ada enkripsi
6.12	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Untuk standar tertentu tidak ada, namun sudah diterapkan enkripsi dari password dan penggunaan https
6.13	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Ada sertifikasi enkripsi yang diambil dari digisearch
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan	Ada peraturan tetapi tidak tertulis. Untuk ganti password juga kembali lagi ke orangnya masing-masing

	password, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Ada sebagian saja, namun untuk dokumen tertulisnya masih belum ada
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Sudah diterapkan kesemuanya. Jika untuk jaringan biasanya akan diputus kalau sudah lama tidak dipakai
6.17	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Ada dengan menggunakan firewall
6.18	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Sudah diterapkan
6.19	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Diperbarui untuk versi dekstop dab server namun jug adilihat apakah fungsinya dapat berjalan dengan sempurna jika pakai versi yang terbaru, jika

		ada fungsi yang terganggu maka tetap memakai versi yang lama
6.20	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Sudah ada. Jika windows ya pakai *default* anti virus dan anti virus tamabahan, untuk linux sudah aman
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak ada
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak ada laporan khusus
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Sudah diterapkan secara keseluruhan. Untuk server sendiri bisa otomatis
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?	Sudah dilakukan verifikasi dan validasi namun untuk dokumentasi masih belum diterapkan
6.25	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-	Ada pengamanan untuk tempat pengembangan namun tidak

	coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	menggunakan standar tertentu
6.26	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak dilakukan secara rutin, namun dahulu pernah dilakukan

“Halaman ini sengaja dikosongkan”

LAMPIRAN C

Hasil Penilaian Indeks KAMI Versi 3.1 – DPTSI ITS Surabaya

C-1 Hasil Penilaian Aspek Kepatuhan Penggunaan Sistem Elektronik

No	Pertanyaan	Status	Skor
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C	1
	Temuan Nilai investasi yang keluarkan oleh pihak DPTSI untuk keperluan sistem elektronik adalah kurang dari 3 miliar		
	Bukti Daftar anggaran tahun 2016 yang dialokasikan untuk sistem elektronik sebanyak ± 1,2 miliar Bukti disertakan di **LAMPIRAN D (Foto D.1)**		
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik	B	2

No	Pertanyaan	Status	Skor
	[A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar		
	Temuan Untuk anggaran operasional terkait pengelolaan sistem elektronik DPTSI ITS tahun 2016 mencapai lebih dari 3 miliar		
	Bukti Daftar anggraan operasinal sistem elektronik sebanyak ± 3 miliar Bukti disertakan di **LAMPIRAN D (Foto D.2)**		
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	B	2
	Temuan DPTSI menggunakan standar nasional yang bernama LPSE (Layananan Pengadaan Sistem Elektronik) yang merupakan sistem pengadaan barang/ jasa pemerintah yang dilaksanakan secara elektronik. Dasar hukum pembentukan LPSE adalah Pasal 111 Nomor 54 Tahun		

No	Pertanyaan	Status	Skor
	2010 tentang pengadaan barang/jasa pemerintah yang ketentuan teknis operasionalnya diatur oleh Peraturan Kepala LKPP Nomor 2 Tahun 2010 tentang Layanan pengadaan Secara Elektronik		
	Bukti Website LPSE yang sudah bekerja sama dengan ITS dapat diakses pada alamat http://www.lpse.its.ac.id/eproc4 Penjelasan tentang LPSE sendiri dapat diakses pada website yang beralamatkan di https://lpse.lkpp.go.id/eproc/tentangkami Bukti disertakan di **LAMPIRAN D (Foto D.3 dan Foto D.4)**		
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus	C	1
	Temuan Tidak digunakan algoritma khusus untuk keamanan informasi dalam sistem elektronik yang digunakan		
	Bukti Tidak Ada		

No	Pertanyaan	Status	Skor
1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	A	5
	Temuan Jumlah pengguna dapat dilihat dari daftar username pengguna sitem elektronik. Pengguna terdiri dari seluruh civitas akademik ITS. Untuk jumlah mahasiswa sudah diperkirakan hingga mencapai ±18.000 orang dan jumlah dosen mencapai ±900 orang termasuk yang sedang *study* ke luar negeri		
	Bukti Penjelasan ini disampaikan didalam website ITS yang dapat diakses pada alamat https://www.its.ac.id/berita/12827/en. Jumlah tersebut belum termasuk jumlah karyawan pengguna sistem elektronik di ITS. Bukti pendukung lainnya yaitu database jumlah pengguna e-mail mahasiswa dan non mahasiswa di ITS Bukti disertakan di **LAMPIRAN D (Foto D.5, Foto D.6, Foto D.7 dan Foto D.8)**		
1,6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya	A	5

No	Pertanyaan	Status	Skor
	[B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi		
	Temuan Data pribadi yang dikelola memiliki keterkaitan dengan data pribadi lainnya. Seperti halnya data pribadi kepegawaian yang bersifat umum yang terhubung dengan data pribadi gaji yang dimiliki oleh pegawai DPTSI,		
	Bukti Data yang ada di akun Integra memiliki keterhubungan satu sama lain, misalnya data yang ada SIM Akademik terdapat data nilai mahasiswa setiap semester, hasil ekivalensi, dan biaya pendidikan. Untuk yang ada di SIM Beasiswa dapat menampilkan data diri mahasiswa, gaji orang tua, hingga biaya kuliah yang dikeluarkan Bukti disertakan di **LAMPIRAN D (Foto D.9)**		
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	B	2

No	Pertanyaan	Status	Skor
	[A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa		
	Temuan Data yang dikelola tidak semuanya rahasia namun juga ada data yang dapat diakses oleh publik/ untuk umum. Ada beberapa website its yang dapat diakses oleh umum dimana data yang disimpan bukan termasuk data rahasia, namun ada beberapa website its yang harus diakses dengan menggunakan akun ITS yang dimiliki oleh user.		
	Bukti Data rahasia harus diakses dengan menggunakan masing-masing akun ITS yang dimiliki oleh user. Data yang tidak rahasia dapat diakses dimanapun dan oleh siapapun juga walaupun tidak memasukkan akun ITS. Contoh data yang tidak rahasia dapat diakses pada website publikasi ilmiah online mahasiswa ITS Contoh data yang rahasia dapat diakses pada website integra, share its, unduh aplikasi berlisensi, dan webmail Bukti disertakan di **LAMPIRAN D (Foto D.10, Foto D.11, Foto D.12, Foto D.13, dan Foto D.14)**		

No	Pertanyaan	Status	Skor
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak	B	2
	Temuan Proses Sistem Elektronik di DPTSI menyangkut data-data milik banyak orang yang berstatus menjadi user di ITS, jika error atau serangan keamanan informasi terjadi maka akan mengganggu atau bahkan menghentikan sementara proses bisnis. Serangan keamanan informasi ini tidak menyangkut pada layanan publik di luar instansi yang terkait dengan DPTSI ITS secara langsung		
	Bukti Jika terjadi penyerangan keamanan informasi seperti pembobolan akun integra dimana user tidak bisa login dengan menggunakan masing-masing akun yang dimiliki, maka hal ini mengganggu hajat hidup orang banyak tetapi tidak memberikan dampak secara		

No	Pertanyaan	Status	Skor
	langsung pada layanan publik yang diberikan ITS. Akibat dari tidak bisa login integra maka tidak bisa juga login ke akun lainnya dan tidak bis atersambung ke internet yang ada dilokasi ITS karena akun integra digunakan sebagai portal *single sign-on* Bukti integra sebagai akun *single sign-on* disertakan di **LAMPIRAN D (Foto D.16 dan Foto D.17)**		
1,9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih [C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih	A	5
	Temuan ITS merupakan instansi milik negara dan berskala nasional. Jika terjadi kebobolan data/ kegagalan sistem elektronik maka dapat membahayakan negara karena data yang dikelola merupakan data penting		
	Bukti		

No	Pertanyaan	Status	Skor
	Peraturan Rektor No. 10 Tahun 2016 yang menjabarkan pengesahan ITS sebagai Perguruan Tinggi Negeri Badan Hukum (PTNBH) yang didukung dengan berbagai macam Undang-Undang milik Negara Republik Indonesia Bukti disertakan di **LAMPIRAN D (Foto D.19)**		
1,10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)	C	1
	Temuan Dampaknya hanya mengganggu proses bisnis organisasi dan tidak sampai membahayakan jiwa. Dampak mengenai finansial masih belum dipengaruhi hingga saat ini.		
	Bukti Saat kegagalan sistem elektronik terjadi maka kegiatan operasional di ITS yang terkait penggunaan sistem, aplikasi, dan jaringan akan terganggu sementara hingga sistem elektronik terkait dapat dikembalikan seperti sedia kala/ normal		

No	Pertanyaan	Status	Skor
	Total Skor Kategori Sistem Elektronik	26	

C-2 Hasil Penilaian Aspek Kepatuhan Area I – Tata Kelola Keamanan Informasi

No			Pertanyaan	Status	Skor
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
			Temuan Direktur DPTSI memiliki peran dan tanggung jawab dalam melaksanakan program keamanan informasi yang telah tercantum dalam Peraturan Rektor ITS No.10 Tahun 2016		
			Bukti Dijelaskan bahwa Direktur DPTSI bertanggung jawab pada Wakil Rektor III yang bertugas untuk menyelenggarakan perumusan dan pelaksanaan kebijakan dalam bidang teknologi dan sistem informasi		

No			Pertanyaan	Status	Skor
			Bukti disertakan di **LAMPIRAN D (Foto D.19)**		
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
			Temuan DPTSI sudah memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya		
			Bukti Struktur organisasi DPTSI dan tupoksi Sub Direktorat Infrastruktur dan Keamanan Informasi Bukti disertakan di **LAMPIRAN D (Foto D.15 dan Foto D.20)**		
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

No			Pertanyaan	Status	Skor
			Temuan Pelaksana pengamanan informasi mempunyai hak untuk melakukan penerapan dan penjaminan terhadap kepatuhan program keamanan informasi		
			Bukti Dijabarkan pada tupoksi bagian Sub Direktorat Infrastruktur dan Keamanan Informasi Bukti disertakan di **LAMPIRAN D (Foto D.20)**		
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
			Temuan Alokasi jumlah sumber daya masih kurang dibandingkan dengan pekerjaan yang dilakukan		
			Bukti Jumlah anggota Sub Direktorat Infrastruktur dan Keamanan Informasi ada 8 orang yang telah terdaftar sebagai karyawan DPTSI		

No			Pertanyaan	Status	Skor
			Bukti disertakan di **LAMPIRAN D (Foto D.18)**		
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
			Temuan Tidak dilakukan segregasi kewenangan dan rencana kebutuhan audit internal		
			Bukti Tidak ada		
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
			Temuan Belum ada standar kompetnesi yang harus dimiliki staff Sub Direktorat Infrastruktur dan Keamanan Informasi		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
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
			Temuan Untuk kompetensi/ keahlian yang dimiliki sudah memadai namun belum ada standar yang dijadikan patokan minimal kompetensi/ keahlian staff Sub Direktorat Infrastruktur dan Keamanan Informasi		
			Bukti Tidak ada		
2,8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan	0
			Temuan Sosialisasi tidak dilakukan secara resmi karena dianggap semua SDM di DPTSI ITS sudah paham tentang keamanan informasi		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
			Temuan Dilakukan pelatihan terkait materi keamanan/ teknologi terbaru namun hanya untuk beberapa staff yang dijadikan perwakilan.		
			Bukti Pelatihan dan workshop pemasangan honeynet terakhir dilakukan tahun 2016 yang diadakan oleh komunitas dan dibantu pihak Kominfo Bukti disertakan di **LAMPIRAN D (Foto D.21)**		
2,10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Diterapkan Secara Menyeluruh	6
			Temuan Integrasi pengamanan informasi dilakukan pada bagian internet dan intranet yang ada di ITS		

No			Pertanyaan	Status	Skor
			Bukti Tidak ada		
2,11	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
			Temuan Tidak ada undang-undang yang digunakan terkait pendefinisian data pribadi		
			Bukti Tidak ada		
2,12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi	Diterapkan Secara Menyeluruh	6

No			Pertanyaan	Status	Skor
			penting) dan menyelesaikan permasalahan yang ada?		
			Temuan Dilakukan koordinasi dengan pihak pengguna aset yang berkepentingan. Koordinasi dapat dilakukan melalui email untuk pihak eksternal dan melalui chat untuk pihak internal ITS		
			Bukti Selalu dilakukan koordinasi dengan pihak eksternal malalui email untuk dilakukan pertukaran informasi dan penyelesaian masalah mulai dari awal hingga akhir Bukti disertakan di **LAMPIRAN D (Foto D.22)**		
2,13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Diterapkan Secara Menyeluruh	6

No			Pertanyaan	Status	Skor
			Temuan Dilakukan koordinasi dengan pihak eksternal melalui email dengan staff bagian Infrastruktur & keamanan Informasi guna menjamin kepatuhan pengamanan informasi yang ada		
			Bukti Selalu dilakukan koordinasi dengan pihak eksternal malalui email untuk dilakukan pertukaran informasi dan penyelesaian masalah mulai dari awal hingga akhir masalah ditutup Bukti disertakan di **LAMPIRAN D (Foto D.22)**		
2,14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Tidak Dilakukan	0
			Temuan Rancangan dan pelaksanaan BCP dan DRP dilakukan permasing-masing bagian namun tidak secara formal dilakukan pendokumenan		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
2,15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Diterapkan Secara Menyeluruh	6
			Temuan Dilakukan pelaporan secara rutin dalam kurun waktu harian dan bulanan namun tidak ada dokumentasi secara resmi. Hal yang dapat dilaporkan yaitu tentang keadaan jaringan, berjalannya sistem atau tidak, dan permasalahan-permasalahan lain terkait jaringan, sistem, dan aplikasi		
			Bukti Ada pencatatan log harian, dan topologi jaringan yang dapat dilaporkan keadaannya kepada Direktur DPTSI Bukti disertakan di **LAMPIRAN D (Foto D.23, Foto D.24, Foto D.25, dan Foto D.26)**		
2,16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses	Diterapkan Secara Menyeluruh	6

No			Pertanyaan	Status	Skor
			pengambilan keputusan strategis di Instansi anda?		
			Temuan Diutamakan tentang keamanan informasi saat dilakukan rapat. Untuk saat ini telah ditetapkan kebijakan tentang email dan masih akan dilakukan pembaruan terus-menerus		
			Bukti Hasil dari keputusan strategis pihak DPTSI ITS yang dapat menghasilkan berbagai macam prosedur yang didalamnya mengutamakan keamanan informasi, seperti prosedur pembuatan e-mail ITS Bukti disertakan di **LAMPIRAN D (Foto D.27)**		
2,17	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak Dilakukan	0
			Temuan		

No			Pertanyaan	Status	Skor
			Belum ada program khusus untuk keamanan informasi		
			Bukti Tidak ada		
2,18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan	0
			Temuan Belum dilakukan pendefinisian parameter dan pengukuran kinerja pengelolaan keamanan informasi		
			Bukti Tidak ada		
2,19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0
			Temuan		

No			Pertanyaan	Status	Skor
			Belum dilakukan penilaian kinerja staff keamanan informasi secara individu		
			Bukti Tidak ada		
2,20	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	Tidak Dilakukan	0
			Temuan Belum dilakukan penerapan target dan sasaran keamanan informasi diberbagai area lain yang relevan dan belum dilakukan langkah perbaikannya		
			Bukti Tidak ada		
2,21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?		
			Temuan Tidak ada perangkat hukum yang dijadikan patokan untuk keamanan informasi		
			Bukti Tidak ada		
2,22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
			Temuan Belum ada kebijakan terkait penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum		
			Bukti Tidak ada		
			Total Skor Kategori Tata Kelola Keamanan Informasi	45	

C-3 Hasil Penilaian Aspek Kepatuhan Area II –Pengelolaan Risiko Keamanan Informasi

No			Pertanyaan	Status	Skor
3,1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
			Temuan Belum ada proker terkait pengelolaan risiko apalagi pendokumentasiannya		
			Bukti Tidak ada		
3,2	II	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Tidak Dilakukan	0
			Temuan Belum ada bagian yang bertugas khusus menangani manajemen risiko dan pengelolaannya		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
3,3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
			Temuan Belum digunakan *framework* khusus terkait pengelolaan risiko keamanan informasi		
			Bukti Tidak ada		
3,4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Tidak Dilakukan	0
			Temuan Belum digunakan *framework* khusus terkait pengelolaan risiko keamanan informasi		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
3,5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Diterapkan Secara Menyeluruh	3
			Temuan Sudah ada ambang batas tingkat risiko yang direkap dalam *log* sensor, yaitu log proxy dan log ids dimana ITS menggunakan AlienVault sebagai aplikasi untuk keperluan melakukan monitoring jaringan, HIDS, dan NIDS untuk memantau serangan dari luar instansi		
			Bukti *Log* proxy dan *log* ids yang selalu dipantau setiap harinya dan jika ada ada yang aktivitas yang mencurigakan maka akan dilakukan blok oleh admin Bukti disertakan di **LAMPIRAN D (Foto D.26, Foto D.28, dan Foto D.29)**		
3,6	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Diterapkan Secara Menyeluruh	3
			Temuan		

No			Pertanyaan	Status	Skor
			Dalam daftar aset informasi yang dimiliki oleh DPTSI ITS terdaftar seluruh aset informasi yang dimiliki beserta pihak-pihak yang bertanggung jawab		
			Bukti Dalam daftar aset terdapat kolom kepemilikan dimana semua berisi milik DPTSI dan ada bagian pengelola aset informasi yang bertanggung jawab Bukti disertakan di **LAMPIRAN D (Foto D.30, Foto D.31, dan Foto D.32)**		
3,7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Tidak Dilakukan	0
			Temuan Untuk ancaman dan kelemahan yang terkait dengan aset informasi belum diidentifikasi dan dicatat dalam dokumen risiko keamanan informasi		
			Bukti Tidak ada		
3,8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			Temuan Dampak dari kerugian terkait terganggunya fungsi aset utama tidak diidentifikasikan dan tidak ada pendokumentasian		
			Bukti Tidak ada		
3,9	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Tidak Dilakukan	0
			Temuan Dilakukan kajian risiko namun tidak secara terstruktur untuk dan tidak ada penentuan langkah mitigasi yang harus dilakukan dalam pengamanan aset informasi secara tertulis		
			Bukti Tidak ada dokumen kajian risiko		

No			Pertanyaan	Status	Skor
3,10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Diterapkan Secara Menyeluruh	3
			Temuan Langkah mitigasi sudah dilakukan untuk menangani risiko yang mungkin terjadi. Diterapkan pengamanan-pengamanan terkait listrik, penerapan enkripsi, penerapan password untuk sistem aplikasi penting, dan pengamanan di ruang server		
			Bukti Ruang server dilengkapi dengan alat pendukung untuk menanggulangi risiko Bukti disertakan di **LAMPIRAN D (Foto D.33, Foto D.34, dan Foto D.35)**		
3,11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Diterapkan Secara Menyeluruh	6

No			Pertanyaan	Status	Skor
			Temuan Penyelesaian risiko diprioritaskan berdasarkan tingkat kepentingannya. Hal yang diprioritaskan adalah risiko terkait dengan data user dan infrastruktur penting, seperti server		
			Bukti Tidak ada		
3,12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Diterapkan Secara Menyeluruh	6
			Temuan Status penyelesaian risiko keamanan informasi selalu dipantau mulai dari awal terjadi hingga masalah sudah terselesaikan. Pemantauan ini dilakukan secara tidak formal yaitu melalui email dan chat WA dengan pihak terkait		
			Bukti Pelaporan risiko keamanan informasi yang dilakukan lewat email dan chat WA Bukti disertakan di **LAMPIRAN D (Foto D.22)**		
3,13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?		
			Temuan Tidak dilakukan evaluasi terhadap mitigasi yang telah dijalankan sebelumnya		
			Bukti Tidak ada		
3,14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Tidak Dilakukan	0
			Temuan Tidak dilakukan pengkajian ulang terhadap profil risiko dan bentuk mitigasinya , karena mitigasi yang biasanya dilakukan sudah dianggap baik dan membantu menyelesaikan masalah		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
3,15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan	0
			Temuan Tidak ada kerangka kerja pengelolaan risiko yang digunakan		
			Bukti Tidak ada		
3,16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan	0
			Temuan Pengelolaan risiko tidak dijadikan bagian dari kriteria penilaian kinerja pengamanan yang ada di DPTSI		
			Bukti Tidak ada		
			Total Skor Kategori Pengelolaan Risiko Keamanan Informasi	21	

C-4 Hasil Penilaian Aspek Kepatuhan Area III – Kerangka Kerja Pengelolaan Keamanan Informasi

No			Pertanyaan	Status	Skor
4,1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian	2
			Temuan Ada kebijakan dan prosedur yang terkait dengan keamanan informasi namun tidak semuanya dibuatkan prosedur dan kebijakannya.		
			Bukti Ada prosedur keamanan jaringan, prosedur legal perangkat lunak, prosedur layanan email, prosedur pengadaan barang, dan prosedur pemusnahan dokumen Bukti disertakan di **LAMPIRAN D (Foto D.27, Foto D.36, Foto D.37, Foto D.38, dan Foto D.39)**		
4,2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal,	Diterapkan Secara Menyeluruh	3

No			Pertanyaan	Status	Skor
			dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?		
			Temuan Prosedur dan kebijakan terkait keamanan informasi dipublikasikan kepada seluruh staff terkait dan mudah diakses karena prosedur dibentuk dalam softcopy dan juga hardcopy		
			Bukti Seluruh staff DPTSI mengetahui adanya prosedur keamanan informasi yang dimiliki di instansi. Hal ini diketahui saat melakukan wawancara dengan beberapa pihak dan semuanya mengetahui akan hal tersebut		
4,3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Tidak Dilakukan	0
			Temuan		

No			Pertanyaan	Status	Skor
			Tidak dilakukan mekanisme pengolahan dokumen prosedur dan kebijakan keamanan informasi yang dimiliki oleh DPTSI		
			Bukti Tidak ada		
4,4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Tidak Dilakukan	0
			Temuan Tidak dilakukan pengkomunikasian kebijakan dan prosedur keamanan informasi termasuk perubahannya karena sampai saat ini status dari masing-masing prosedur masih belum pernah diperbarui		
			Bukti Dalam setiap prosedur yang ada bertuliskan status perubahan dokumennya (pada poin 9) masih “belum ada” Bukti disertakan di **LAMPIRAN D (Foto D.40)**		

No			Pertanyaan	Status	Skor
4,5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?	Tidak Dilakukan	0
			Temuan Kebijakan dan prosedur keamanan informasi tidak merefleksikan kebutuhan dari mitigasi risiko keamanan informasi		
			Bukti Tidak adanya risiko yang dicantumkan dalam prosedur terkait keamanan informasi yang dimiliki DPTSI		
4,6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh	3
			Temuan		

No			Pertanyaan	Status	Skor
			Dilakukan identifikasi terhadap kondisi yang membahayakan keamanan informasi dengan menggunakan *log* ids "AlienVault OSSIM". Dengan aplikasi tersebut maka dapat diketahui serangan apa saja yang terjadi ada jaringan ITS dan dari negara mana saja. Jika ada yang melakukan tindakan berbahaya maka akan dilakukan blocking pada IP tersebut		
			Bukti Pemantauan setiap saat oleh staff SubDir IKTI pada *log* ids tersebut Bukti disertakan di **LAMPIRAN D (Foto D.28 dan Foto D.29)**		
4,7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan	0
			Temuan Aspek keamanan informasi tercantum dalam kontrak yang dijalankan oleh pihak DPTSI dengan pihak ketiga namun untuk dokumentasi kontraknya tidak didapatkan sebagai bukti		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
4,8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Diterapkan Secara Menyeluruh	6
			Temuan Terdapat unit layanan hukum di ITS yang menangani semua permasalahan/ pelanggaran etika di ITS. Sudah dijabarkan juga tugas dan kewenangan unit layanan hukum ini untuk menegakkan dan mengkomunikasikan pelanggaran di ITS termasuk yang menyerang keamanan informasi		
			Bukti Kewenangan dan tanggung jawab unit layanan hukum telah dijabarkan pada Peraturan Rektor ITS No.10 Tahun 2016 Pasal 89 Bukti disertakan di **LAMPIRAN D (Foto D.41)**		
4,9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			Temuan Tidak disediakan prosedur resmi untuk pengecualian penerapan keamanan informasi di DPTSI		
			Bukti Tidak ada		
4,10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan	0
			Temuan Dilakukan implementasi *security patch*, namun untuk kebijakan dan prosedur operasional untuk pengelolaan *security patch* masih belum dimiliki pihak DPTSI		
			Bukti Tidak ada		
4,11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam	Diterapkan Secara Menyeluruh	6

No			Pertanyaan	Status	Skor
			manajemen proyek yang terkait dengan ruang lingkup?		
			Temuan Dilakukan pembahasan aspek keamanan informasi saat rapat proyek yang sedang dilakukan pihak DPTSI ITS		
			Bukti Keamanan informasi menjadi bahasan saat penerapan manajemen proyek. Misalnya saat ada pengembangan proyek aplikasi/ sistem maka tidak bisa langsung dimasukkan server *live* karena berbahaya dan memungkinkan untuk diakses secara bebas		
4,12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Tidak Dilakukan	0
			Temuan Tidak dilakukan evaluasi risiko dalam penerapan sistem baru		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
4,13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Diterapkan Secara Menyeluruh	6
			Temuan Untuk pengembangan sistem menggunakan metode SDLC yang sesuai dengan kerangka kerja pengemabangan sistem aplikasi. Ada dokumen yang dibuat untuk setiap pengembangan sistem aplikasi yang dilakukan di DPTSI ITS		
			Bukti Adanya dokumen pengembangan sistem aplikasi yang berisikan kebutuhan sistem, diagram use case, diagram aktivitas, diagram class, dan lain sebagainya tentang kebutuhan sistem aplikasi Bukti disertakan di **LAMPIRAN D (Foto D.42 dan Foto D.43)**		
4,14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?		
			Temuan Tidak ada dokumen yang dibuat untuk mmenganalisis dan mendeskripsikan risiko baru dan pengamanannya saat dilakukan pengembangan sistem baru		
			Bukti Tidak ada		
4,15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Tidak Dilakukan	0
			Temuan Tidak tersedia kerangka kerja terkait BCP yang mendefinisikan persyaratan keamanan informasi di DPTSI		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
4,16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan	0
			Temuan Tidak ada dokumen terkait DRP yang digunakan di DPTSI		
			Bukti Tidak ada		
4,17	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak Dilakukan	0
			Temuan Tidak pernah dilakukan uji coba terkait DRP layanan TIK di DPTSI		
			Bukti Tidak ada		
4,18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster*	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			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?		
			Temuan Tidak dilakukan avaluasi terhadap DRP layanan TIK karena memang tidak pernah dilakukan uji coba/ penerapan DRP layanan TIK di DPTSI		
			Bukti Tidak ada		
4,19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan	0
			Temuan Tidak dilakukan evaluasi secara berkala pada kebijakan dan prosedur keamanan informasi yang dimiliki oleh pihak DPTSI		
			Bukti Pada dokumen prosedur keamanan informasi yang dimiliki terdapat keterangan bahwa belum pernah dilakukan perubahan pada dokumen tersebut		

No			Pertanyaan	Status	Skor
			Bukti disertakan di **LAMPIRAN D (Foto D.40)**		
4,20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Diterapkan Secara Menyeluruh	3
			Temuan Strategi penerapan keamanan informasi dilakukan dengan cara berintegrasi dengan SubDirektorat Pengembangan Sistem Informasi DPTSI		
			Bukti Komunikasi yang terarah dan terstruktur antara bagian IKTI dan Pengembangan Sistem Informasi terkait pembangunan,pemeliharaan, dan gangguan terhadap sistem yang dimiliki		
4,21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Diterapkan Secara Menyeluruh	3
			Temuan		

No			Pertanyaan	Status	Skor
			Strategi penggunaan teknologi informasi dilakukan dengan cara mencegah dan meng-*encourage* menggunakan https://		
			Bukti Semua website its yang beralamatkan “its.ac.id” diamankan dengan sertifikasi enkripsi dengan menggunakan https:// Bukti disertakan di **LAMPIRAN D (Foto D.44)**		
4,22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh	3
			Temuan Strategi keamanan informasi tersebut direalisasikan dengan baik hingga saat ini		
			Bukti Semua website its yang beralamatkan “its.ac.id” diamankan dengan sertifikasi enkripsi dengan menggunakan https:// Bukti disertakan di **LAMPIRAN D (Foto D.44)**		
4,23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?		
			Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada		
			Bukti Tidak ada		
4,24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Tidak Dilakukan	0
			Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
4,25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
			Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada		
			Bukti Tidak ada		
4,26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
			Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
4,27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan	0
			Temuan Tidak dilakukan revisi terhadap kebijakan dan prosedur yang berlaku di DPTSI dan tidak pernah dilakukan analisa aspek finansial atau perubahannya terhadap infrastruktur		
			Bukti Tidak ada		
4,28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?		
			Temuan Tidak dilakukan pengujian dan pengevaluasian terhadap kepatuhan program keamanan informasi yang ada		
			Bukti Tidak ada		
4,29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan	0
			Temuan Masih belum ada perencanaan		
			Bukti Tidak ada		
			Total Skor Kategori Kerangka Kerja Keamanan Informasi	35	

C-5 Hasil Penilaian Aspek Kepatuhan Area IV - Pengelolaan Aset Informasi

No			Pertanyaan	Status	Skor
5,1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	3
			Temuan Terdapat daftar aset informasi dan aset lainnya yang dimiliki oleh pihak DPTSI ITS. Didalam daftar aset tersebut juga terdapat status kepemilikan dari aset tersebut		
			Bukti Dalam daftar aset terdapat kolom kepemilikan dimana semua berisi milik DPTSI dan ada bagian pengelola aset informasi yang bertanggung jawab Bukti disertakan di **LAMPIRAN D (Foto D.30 dan Foto D.31)**		
5,2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
			Temuan Tidak ada undang-undang yang diberlakukan terkait klasifikasi aset di DPTSI		

No			Pertanyaan	Status	Skor
			Bukti Tidak ada		
5,3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Tidak Dilakukan	0
			Temuan Belum dilakukan evaluasi dan klasifikasi aset informasi sesuai dengan tingkat kepentingannya karena masih belum adanya undang-undang yang digunakan juga oleh DPTSI		
			Bukti Tidak ada		
5,4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	Diterapkan Secara Menyeluruh	3
			Temuan Tingkatan akses dibedakan dengan menggunakan proxy, namun hal ini sudah tidak digunakan lagi. Untuk saat ini tingkatan akses dibedakan dengan adanya user *login*		

No			Pertanyaan	Status	Skor
			integra. Tingkatan akses juga dibedakan dari menu-menu yang dapat diakses oleh user dalam akun integranya		
			Bukti Akun integra yang sudah dijadikan sebagai portal *single sign-on* Bukti disertakan di **LAMPIRAN D (Foto D.16 dan Foto D.17)**		
5,5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan konfigurasi terhadap sistem dan teknologi informasi yang diterapkan secara konsisten		
			Bukti Konfigurasi jaringan dilakukan dengan adanya firewall, router, dan switch. Untuk konfigurasi sistem juga dilakukan untuk password dan pemasangan time out untuk sistem yang sudah lama tidak digunakan		

No			Pertanyaan	Status	Skor
5,6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan konfigurasi terhadap sistem dan teknologi informasi yang diterapkan secara konsisten		
			Bukti Konfigurasi jaringan dilakukan dengan adanya firewall, router, dan switch. Untuk konfigurasi sistem juga dilakukan untuk password dan pemasangan time out untuk sistem yang sudah lama tidak digunakan Bukti disertakan di **LAMPIRAN D (Foto D.11, Foto D.12, Foto D.13, Foto D.14, dan Foto D.45)**		
5,7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan proses perilisan aset baru dalam lingkungan operasional dan dilakukan pembaruan terhadap daftar inventaris aset informasi		

No			Pertanyaan	Status	Skor
			Bukti Update daftar inventaris aset yang dimiliki oleh DPTSI terakhir dilakukan pada tanggal 29 November 2016 Bukti disertakan di **LAMPIRAN D (Foto D.46)**		
5,8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Diterapkan Secara Menyeluruh	3
			Temuan Terdapat daftar tanggung jawab masing-masing staff SubDir Infrastruktur & Keamanan Informasi DPTSI beserta target capaiannya dalam 1 tahun		
			Bukti File SKP untuk masing-masing staff SubDir IKTI DPTSI Bukti disertakan di **LAMPIRAN D (Foto D.47)**		
5,9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak Dilakukan	0
			Temuan Tidak ada tata tertib khusus untuk penggunaan komputer, email, internet, dan intranet		

No			Pertanyaan	Status	Skor
			Bukti Tidak ada		
5,10	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak Dilakukan	0
			Temuan Tidak ada tata tertib khusus untuk penggunaan dan pengamanan aset terkait HAKI		
			Bukti Tidak ada		
5,11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	Diterapkan Secara Menyeluruh	3
			Temuan Terdapat peraturan yang terkait dengan instalasi perangkat lunak yang diletakkan dalam website beserta file perangkat lunak yang dapat diunduh		
			Bukti Peraturan instalasi dapat dilihat di website https://unduh.its.ac.id/ Bukti disertakan di **LAMPIRAN D (Foto D.48)**		
5,12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			Temuan Tidak ada peraturan terkait penggunaan data pribadi yang mewajibkan adanya ijin untuk mengakses data pribadi		
			Bukti Tidak ada		
5,13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Tidak Dilakukan	0
			Temuan Tidak ada kebijakan terkait pengelolaan *username* & *password* beserta pelanggarannya		
			Bukti Tidak ada		
5,14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak Dilakukan	0
			Temuan		

No			Pertanyaan	Status	Skor
			Tidak ada prosedur terkait pengelolaan dan pemberian akses, otentikasi, dan otorisasi dalam penggunaan aset informasi		
			Bukti Tidak ada		
5,15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak Dilakukan	0
			Temuan Tidak ada patokan waktu untuk melakukan penyimpanan klasifikasi data dan syarat penghancuran data		
			Bukti Tidak ada		
5,16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan	0
			Temuan Tidak ada dokumentasi terkait ketepatan pertukaran data dan pengamanannya dengan pihak eksternal		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
5,17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Tidak Dilakukan	0
			Temuan Tidak adanya pencatatan insiden terkait kegagalan keamanan informasi		
			Bukti Tidak ada		
5,18	II	1	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	Tidak Dilakukan	0
			Temuan Tidak ada prosedur terkait *back-up* dan *restore* yang dibuat untuk DPTSI		
			Bukti Tidak ada		
5,19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya berkala?	Diterapkan Secara Menyeluruh	6
			Temuan Ada pengamanan fisik untuk aset-aset yang sudah diklasifikasikan kepentingannya. Untuk ruang server disediakan pengamanan fisik yang baik dan lengkap		

No			Pertanyaan	Status	Skor
			Bukti Ruang server dilengkapi dengan pintu berlapis, finger print, CCTV, gas pemadam kebakaran, anti petir, grounding, sensor kelembaban, dan sensor suhu Bukti disertakan di **LAMPIRAN D (Foto D.33, Foto D.34, Foto D.35, Foto D.49, dan Foto D.50)**		
5,20	III	2	Proses pengecekan latar belakang SDM	Tidak Dilakukan	0
			Temuan Pengecekan latar belakang SDM dilakukan pada awal pengambilan karyawan namun tidak ada pendokumentasian atas hal tersebut		
			Bukti Tidak ada		
5,21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Diterapkan Secara Menyeluruh	6
			Temuan Dilakukan pelaporan insiden keamanan informais dengan pihak eksternal, biasanya dilakukan dengan pihak ISP terkait. Koordinasi dilakukan secara 2 arah dengan baik		
			Bukti		

No			Pertanyaan	Status	Skor
			Email yang berisikan laporan insiden keamanan informasi atara staff SubDir IKTI DPTSI dengan pihak eksternal Bukti disertakan di **LAMPIRAN D (Foto D.22)**		
5,22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Diterapkan Secara Menyeluruh	6
			Temuan Terdapat prosedur untuk melakukan penghancuran dokumen yang sudah ditetapkan sejak lama		
			Bukti Ada prosedur penghancuran dokumen yang sudah tidak digunakan lagi Bukti disertakan di **LAMPIRAN D (Foto D.38)**		
5,23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Tidak Dilakukan	0
			Temuan		

No			Pertanyaan	Status	Skor
			Tidak ada prosedur yang mengatur tentang penggunaan hak akses dan langkah oembenahannya jika terjadi ketidak sesuaian dengan kebijakan yang berlaku		
			Bukti Tidak ada		
5,24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Perencanaan	2
			Temuan Sedang dalam proses pembuatan prosedur terkait *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya		
			Bukti Tim Pengembangan sedang melakukan perencanaan dan akan segera dieksekusi untuk tahun 2017		
5,25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan	0
			Temuan Tidak terdapat daftar data yang harus di *backup* dan prosedur *backup* yang disediakan oleh pihak DPTSI		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
5,26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan	0
			Temuan Tidak ada bukti daftar untuk melakukan pelaksanaan keamanan informasi yang disesuaikan dengan klasifikasinya		
			Bukti Tidak ada		
5,27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan	0
			Temuan Tidak ada prosedur penggunaan perangkat pengolah informasi milik pihak ketiga dengan memastikan aspek HAKI yang ada		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
5,28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Diterapkan Secara Menyeluruh	3
			Temuan Didepan pintu ruang server disediakan mesin *finger print* yang sudah disetting hanya untuk pihak tertentu yang boleh masuk kedalamnya		
			Bukti Mesin *finger print* yang ada di depan ruang server, CCTV yang ada dalam ruang server, dan buku tamu yang ada dalam ruang server Bukti disertakan di **LAMPIRAN D (Foto D.51 dan Foto D.35)**		
5,29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	3
			Temuan		

No			Pertanyaan	Status	Skor
			Dilakukan proses untuk melakukan pengolahan alokasi kunci masuk baik secara fisik maupun elektronik di DPTSI ITS untuk mengamankan fasilitas yang ada		
			Bukti Mesin *finger print* yang ada di depan ruang server, CCTV yang ada dalam ruang server, dan buku tamu yang ada dalam ruang server Bukti disertakan di **LAMPIRAN D (Foto D.51 dan Foto D.35)**		
5,30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
			Temuan Semua infratruktur komputasi sudah dilindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya		
			Bukti Terdapat tabung gas pemadam kebakaran, terdapat AC yang cukup, terdapat sesnsor suhu yang otomatis menyesuaikan , dan terdapat sensor kelembaban yang otomatis terkirim pada staff terkait jika terjadi masalah		

No			Pertanyaan	Status	Skor
			Bukti disertakan di **LAMPIRAN D (Foto D.33, Foto D.34, dan Foto D.50)**		
5,31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
			Temuan Semua infrastruktur komputasi telah dilindungi dari gangguan pasokan listrik dan dampak dari petir		
			Bukti Terdapat penangkal petir, UPS, box panel listrik, *grounding* untuk pembuangan arus listik yang berlebih kebumi, dan generator untuk memperkuat dan menjaga pasokan listrik yang dibutuhkan oleh server yang ada dalam DPTSI ITS Bukti disertakan di **LAMPIRAN D (Foto D.49 dan Foto D.34)**		
5,32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Diterapkan Secara Menyeluruh	3
			Temuan		

No			Pertanyaan	Status	Skor
			Adanya peraturan pengamanan perangkat komputasi milik DPTSI jika digunakan diluar kantor		
			Bukti Adanya surat serah terima untuk pemindahan alat komputasi Bukti disertakan di **LAMPIRAN D (Foto D.52)**		
5,33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	Diterapkan Secara Menyeluruh	3
			Temuan Terdapat proses untuk pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan		
			Bukti Adanya surat serah terima untuk pemindahan alat komputasi dan dilakukan pembaharuan pada daftar inventaris yang ada Bukti disertakan di **LAMPIRAN D (Foto D.46 dan Foto D.52)**		

No			Pertanyaan	Status	Skor
5,34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh	6
			Temuan Konstruksi ruang server DPTSI sudah dirancang dengan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai		
			Bukti Sudah terdapat pendeteksi asap, tabung gas pemadam kebakaran, alat sensor suhu, alat sensor kelembaban, dan *grounding* listrik Bukti disertakan di **LAMPIRAN D (Foto D.33, Foto D.34, Foto D.49, dan Foto D.50)**		
5,35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat	Dalam Penerapan / Diterapkan Sebagian	4

No			Pertanyaan	Status	Skor
			komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?		
			Temuan Dilakukan proses pemeriksaan dan perawatan pada fasilitas pendukung dan kelayakan keamanan lokasi kerja. Namun untuk proses pemeriksaan terhadap perangkat keras komputer tidak dilakukan secara rutin dan khusus		
			Bukti Proses pemeriksaan rutin pada jaringan yang digunakan di ITS Bukti disertakan di **LAMPIRAN D (Foto D.23, Foto D.24, Foto D.25, Foto D.28, dan Foto D.29)**		
5,36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	4
			Temuan Untuk pengamanan dalam pengiriman aset informasi yang melibatkan pihak ketiga sudah dilakukan sebagain		
			Bukti		

No			Pertanyaan	Status	Skor
			Dilakukan pengamanan aset informasi dengan penerapan password namun untuk pengamanan fisik masih tidak dilakukan		
5,37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Tidak Dilakukan	0
			Temuan Tidak ada peraturan khusus ntuk mengamankan lokasi ruang server dari risiko perangkat atau bahan yang dapat membahayakan aset informasi		
			Bukti Tidak ada larangan penggunaan alat komunikasi dan sejenisnya di ruang server		
5,38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Tidak Dilakukan	0

No			Pertanyaan	Status	Skor
			Temuan Tidak dilakukan proses pengamanan lokasi kerja dari keberadaan/kehadiran pihak ketiga		
			Bukti Tidak ada		
			Skor Total Kategori Pengelolaan Aset Informasi	73	

C-6 Hasil Penilaian Aspek Kepatuhan Area V – Teknologi dan Keamanan Informasi

No			Pertanyaan	Status	Skor
6,1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
			Temuan Sistem komputer yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan. Pengamanan pertama dilakukan dengan penerapan *firewall* yang digunakan dari Cisco ASA 5540. Untuk pengamanan tingkat kedua langsung ada pada sistem yang digunakan		

No			Pertanyaan	Status	Skor
			Bukti Adanya konfigurasi firewall dan penggunaan firewall dengan Cisco ASA 5540 Bukti disertakan di **LAMPIRAN D (Foto D.45 dan Foto D.53)**		
6,2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan segmentasi jaringan komunikasi di DPTSI yang sesuai dengan kepentingan (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)		
			Bukti Pembagian IP untuk pengaksesan di jaringan yang berbeda Bukti disertakan di **LAMPIRAN D (Foto D.54)**		
6,3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan	Diterapkan Secara Menyeluruh	3

No			Pertanyaan	Status	Skor
			(standar industri yang berlaku) dan kebutuhan?		
			Temuan Dilakukan konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan		
			Bukti Pembagian IP untuk pengaksesan di jaringan yang berbeda, pembatasan akses esurat diluar ip yang sudah ditentukan Bukti disertakan di **LAMPIRAN D (Foto D.54, Foto D.55, dan Foto D.56)**		
6,4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Diterapkan Secara Menyeluruh	3
			Temuan Pihak DPTSI melakukan analisa kepatuhan penerapan konfigurasi standar secara rutin		
			Bukti IP config yang ada selalu dipantau secararutin oleh staff IKTI DPTSI		
6,5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk	Dalam Penerapan/ Diterapkan Sebagian	2

No			Pertanyaan	Status	Skor
			mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?		
			Temuan Tidak dilakukan pemindaian secara rutin terhadap jaringan, sistem dan aplikasi yang digunakan untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi		
			Bukti Pemindaian hanya dilakukan jika terjadi masalah/ insiden		
6,6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Diterapkan Secara Menyeluruh	3
			Temuan Keseluruhan infrastruktur jaringan, sistem dan aplikasi telah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan		
			Bukti Ditentukan ketersediaan kuota penggunaan jaringan untuk masing-maisng user		

No			Pertanyaan	Status	Skor
			Bukti disertakan di **LAMPIRAN D (Foto D.57)**		
6,7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan monitoring terhadap keseluruhan infrastruktur jaringan, sistem dan aplikasi untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan		
			Bukti Diketahui pergerakan kuota penggunaan internet melalui pemantauan database email user ITS Bukti disertakan di **LAMPIRAN D (Foto D.57)**		
6,8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan perekaman secara otomatis jika terjadi perubahan dalam sistem informasi		
			Bukti		

No			Pertanyaan	Status	Skor
			Log ids untuk perubahan sistem yang dilakukan melalui jaringan Bukti disertakan di **LAMPIRAN D (Foto D.28)**		
6,9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan perekaman secara otomatis jika terjadi upaya akses oleh yang tidak berhak		
			Bukti *Log* pergerakan proxy ITS dan *log* upaya masuk dari user yang tidak berhak Bukti disertakan di **LAMPIRAN D (Foto D.28, Foto D.29, dan Foto D.26)**		
6,10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan analisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)		

No			Pertanyaan	Status	Skor
			Bukti Dashboard yang berisi aktivitas jaringan beserta report yang didapat perhari Bukti disertakan di **LAMPIRAN D (Foto D.28 dan Foto D.29)**		
6,11	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan penerapan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada		
			Bukti Enkripsi pada seluruh password user ITS dalam database dan enkripsi pada seluruh sistem yang memiliki domain its.ac.id Bukti disertakan di **LAMPIRAN D (Foto D.44)**		
6,12	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan	0
			Temuan Tidak ada standar khusus yang digunakan DPTSI untuk penggunaan enkripsi		
			Bukti		

No			Pertanyaan	Status	Skor
			Tidak ada		
6,13	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh	6
			Temuan Diterapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan di DPTSI ITS		
			Bukti Sertifikasi domain ITS dari DigiCert Inc Bukti disertakan di **LAMPIRAN D (Foto D.58)**		
6,14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Tidak Dilakukan	0
			Temuan		

No			Pertanyaan	Status	Skor
			Semua sistem dan aplikasi tidak secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama		
			Bukti Tidak ada		
6,15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh	6
			Temuan Ada penerapan akses untuk mengelola sistem dengan menggunakan pengamanan khusus		
			Bukti Akses pada database masing-masing sistem akan berbeda tergantung yang bertanggung jawab, akses pada eticket hanya untuk beberapa user yang terdaftar saja Bukti disertakan di **LAMPIRAN D (Foto D.55 dan Foto D.56))**		
6,16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan	Dalam Penerapan / Diterapkan Sebagian	4

No			Pertanyaan	Status	Skor
			waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?		
			Temuan Tidak semua sistem dan aplikasi yang digunakan menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses		
			Bukti Integra ITS menerapkan sistem *timeout* setelah kira-kira 30 menit tidak digunakan dan untuk akun share ITS tidak diterapkan *timeout*		
6,17	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh	6
			Temuan Sudah diterapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi di DPTSI		
			Bukti Penerapan firewall untuk jaringan dan sistem		

No			Pertanyaan	Status	Skor
			Bukti disertakan di **LAMPIRAN D (Foto D.45)**		
6,18	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Diterapkan Secara Menyeluruh	3
			Temuan Sudah diterapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi oleh pihak DPTSI ITS		
			Bukti Larangan untuk mengakses situs ITS yang diamankan dari luar instansi Bukti disertakan di **LAMPIRAN D (Foto D.55 dan Foto D.56)**		
6,19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Diterapkan Secara Menyeluruh	3
			Temuan Dilakukan pembaharuan pada sistem operasi untuk setiap perangkat *desktop* dan *server* yang diperlukan, misalnya untuk Windows. Untuk perangkat Linux tidak perlu dilakukan pembaharuan		
			Bukti		

No			Pertanyaan	Status	Skor
			Versi terbaru dari *desktop* dan *server*		
6,20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh	3
			Temuan Diterapkan penggunaan anti virus pada setiap *desktop* dan *server* untuk dilindungi dari penyerangan virus		
			Bukti Penggunaan anti virus dari Windows yaitu Windows Defender		
6,21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak Dilakukan	0
			Temuan Tidak dilakukan perekaman dan hasil analisa yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
6,22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan	0
			Temuan Tidak adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan		
			Bukti Tidak ada		
6,23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
			Temuan Sinkronisasi waktu sudah diterapkan secara keseluruhan pada jaringan, sistem dan aplikasi yang akurat, sesuai dengan standar yang ada		
			Bukti Sinkronisasi waktu pada akun ShareITS Bukti disertakan di **LAMPIRAN D (Foto D.59, Foto D.60, dan Foto D.61)**		

No			Pertanyaan	Status	Skor
6,24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?	Diterapkan Secara Menyeluruh	6
			Temuan Dilakukan diverifikasi/validasi spesifikasi dan fungsi keamanan pada saat proses pengembangan dan uji-coba pada setiap aplikasi di DPTSI		
			Bukti Uji coba dilakukan terkait fungsi keamanan dari aplikasi terkait		
6,25	III	3	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Tidak Dilakukan	0
			Temuan Tidak ada penggunaan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun		
			Bukti Tidak ada		

No			Pertanyaan	Status	Skor
6,26	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
			Temuan Tidak ada pihak independen yang bekerja sama untuk mengkaji kehandalan keamanan informasi		
			Bukti Tidak ada		
			Total Skor Kategori Teknologi dan Keamanan Informasi	75	

“Halaman ini sengaja dikosongkan”

LAMPIRAN D

Bukti Pendukung

Untuk bukti pendukung yang ada di LAMPIRAN D ini merupakan data-data confidentiality atau data rahasia yang tidak dapat diakses oleh pihak lain yang tidak berwenang. Maka dari itu bukti pendukung tidak dapat dilampirkan dalam buku tugas akhir dan hanya dilampirkan pada dokumen yang diberikan kepada pihak yang bersangkutan dan memiliki kewenangan untuk mengakses.

“Halaman ini sengaja dikosongkan”