TUGAS AKHIR – IS184853

ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/ IEC 27001:2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

GAP ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR PREPARATION OF ISOI IEC 27001: 2013 CERTIFICATION IN DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

RESTI NISAIDHA RAHMI
NRP. 05211640000016

Dosen Pembimbing
Hanim Maria Astuti, S.Kom, M.Sc, ITIL
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember
Surabaya 2020

TUGAS AKHIR – IS184853

ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/ IEC 27001:2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

RESTI NISAIDHA RAHMI
NRP. 05211640000016

Dosen Pembimbing
Hanim Maria Astuti, S.Kom, M.Sc, ITIL
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember
Surabaya 2020

UNDERGRADUATE THESIS – IS184853

GAP ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR PREPARATION OF ISO/ IEC 27001:2013 CERTIFICATION IN DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI

RESTI NISAIDHA RAHMI
NRP. 05211640000016

Supervisors
Hanim Maria Astuti, S.Kom, M.Sc, ITIL
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

INFORMATION SYSTEMS DEPARTMENT
Faculty of Intelligent Electrical and Informatics Technology
Sepuluh Nopember Institute of Technology
Surabaya 2020

LEMBAR PENGESAHAN

ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/ IEC 27001: 2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Elektro dan Informatika Cerdas

Oleh:

RESTI NISAIDHA RAHMI
NRP. 05211640000016

Surabaya, 20 Januari 2020

KEPALA
DEPARTEMEN SISTEM INFORMASI

Dr. Mudjahidin, S.T, M.T
NIP. 19701010 200302 1 001

LEMBAR PERSETUJUAN

ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/IEC 27001:2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

TUGAS AKHIR

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

Oleh:

RESTI NISAIDHA RAHMI
05211640000016

Disetujui Tim Penguji : Tanggal Ujian : 9 Januari 2020
Periode Wisuda : Maret 2020

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

Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom **(Pembimbing II)**

Feby Artwodini, S.Kom, MT **(Penguji I)**

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

ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMK) UNTUK PERSIAPAN SERTIFIKASI ISO/ IEC 27001: 2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

Nama Mahasiswa	: Resti Nisaidha Rahmi
NRP	: 05211640000016
Departemen	: Sistem Informasi FTEIC-ITS
Pembimbing 1	: Hanim Maria Astuti, S.Kom, M.Kom, ITIL
Pembimbing 2	: Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

ABSTRAK

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) merupakan suatu lembaga di bawah naungan Institut Teknologi Sepuluh Nopember (ITS) yang bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi di ITS. Meskipun DPTSI merupakan lembaga yang berkaitan dengan Teknologi Informasi, pada lembaga tersebut masih terdapat beberapa celah keamanan sistem informasi dan jaringan yang cukup berbahaya, di antaranya seperti adanya kasus pembobolan data Sistem Integra ITS dan pembobolan akun e-mail ITS. Hal tersebut mengindikasikan bahwa DPTSI belum menerapkan SMKI (Sistem Manajemen Keamanan Informasi) dengan baik. SMKI adalah suatu metode perencanaan manajemen yang mendetilkan seluruh kebutuhan yang akan digunakan untuk melakukan kontrol keamanan bagi kebutuhan suatu organisasi. Standar SMKI yang digunakan dalam kasus DPTSI ini adalah ISO/IEC 27001:2013. Standar tersebut berguna untuk membantu mengamankan aset-aset organisasi, seperti informasi finansial, informasi mengenai pegawai, maupun informasi yang telah dipercayakan dari pihak ketiga kepada suatu organisasi.

Salah satu aplikasi yang dapat mengukur penerapan SMKI yang sesuai dengan ISO/ IEC 27001:2013 adalah Indeks Keamanan Informasi (Indeks KAMI). Aplikasi ini berfungsi

untuk mengevaluasi tingkat kematangan dan tingkat kelengkapan penerapan standar ISO 27001, yang dikembangkan oleh Kominfo. Pada tahun 2017, pernah dilakukan evaluasi menggunakan Indeks KAMI 3.1 di DPTSI, namun sayangnya hasil penilaian tersebut masih dinyatakan tidak layak. Oleh karena itu, pada tahun 2019 evaluasi penerapan SMKI di DPTSI dilakukan kembali, namun dengan menggunakan Indeks KAMI 4.0. Evaluasi ini dilakukan agar bisa mewujudkan sertifikasi ISO 27001 di tahun 2020 sesuai dengan masterplan yang telah disusun.

Selain itu, dalam penelitian ini akan dilakukan analisis akar masalah guna mencari tahu penyebab penerapan SMKI di DPTSI yang belum optimal. Penyebab tersebut akan digambarkan dengan diagram ishikawa. Diagram ini dapat membantu DPTSI untuk melihat penyebab DPTSI masih dikatakan tidak layak untuk melakukan sertifikasi ISO 27001 berdasarkan penilaian Indeks KAMI. Output utama dari Tugas Akhir ini adalah checklist hasil analisis kesenjangan yang menunjukkan poin-poin ketidaksesuaian penerapan SMKI berdasarkan klausul ISO/IEC 27001:2013 dengan lebih mudah. Rekomendasi perbaikan pun juga akan diberikan pada poin-poin yang mengalami kesenjangan dengan menggunakan ISO/IEC 27001:2013. Dengan demikian, DPTSI dapat segera berbenah untuk melakukan perbaikan sehingga bisa melakukan sertifikasi ISO 27001 dalam waktu dekat.

Berangkat dari permasalahan tersebut, maka dibuatlah suatu penelitian Tugas Akhir yang berisikan tentang analisis kesenjangan SMKI di DPTSI dengan standar ISO/IEC 27001:2013 dengan judul "Analisis Kesenjangan Sistem Manajemen Keamanan Informasi (SMKI) untuk Persiapan Sertifikasi ISO/IEC 27001:2013 di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI)".

Kata Kunci : Analisis Kesenjangan, SMKI, ISO/IEC 27001:2013, Indeks KAMI 4.0

GAP ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR PREPARATION OF ISO/IEC 27001:2013 CERTIFICATION IN DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

Student Name	: Resti Nisaidha Rahmi
NRP	: 05211640000016
Departement	: Sistem Informasi FTEIC-ITS
Supervisor 1	: Hanim Maria Astuti, S.Kom, M.Kom, ITIL
Supervisor 2	: Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

ABSTRACT

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) is an institution under the auspices of Institut Teknologi Sepuluh Nopember (ITS) whose task is to provide and manage Information Technology services at ITS. Although DPTSI is an institution related to Information Technology, there are still number of vulnerabilities in information systems and network security that are quite dangerous, including cases of breaking through into ITS Integra System and ITS e-mail accounts. This indicates that the DPTSI has not implemented the ISMS (Information Security Management System) properly. The ISMS is a management planning method that details all the needs that will be used to exercise security control for the needs of an organization. One of the ISMS standards used in this case ISO / IEC 27001: 2013. These standards are useful to help secure organizational assets, such as financial information, information about employees, as well as information that has been entrusted from a third party to an organization.

One application that can measure the application of ISMS in accordance with ISO / IEC 27001: 2013 is Indeks Keamanan Informasi (Indeks KAMI). This application serves to evaluate the level of maturity and the level of completeness of the application of the ISO 27001 standard, developed by Kominfo. In 2017, an evaluation was conducted using the Indeks KAMI

3.1, but unfortunately the results of the assessment were still declared to be inappropriate. Therefore, in 2019 evaluating the ISMS will be conducted again, but using the Index KAMI 4.0. This evaluation is carried out in order to realize ISO 27001 certification in 2020 in accordance with the master plan that has been arranged by DPTSI.

In addition, in this study a root cause analysis will be carried out to find out the causes of the application of the ISMS in the DPTSI which are not optimal. The cause will be illustrated with Ishikawa diagram. This diagram can help DPTSI to see why DPTSI is still said to be unfit for ISO 27001 certification based on the Indeks KAMI assessment. The main output of this research study is a gap analysis checklist result to see the uncompliance point of ISMS implementation in DPTSI more easily. Recommendations for improvement will also be given to the gaps using ISO/IEC 27001:2013. Thus, DPTSI can immediately improve to make improvements so that it can do ISO 27001 certification in the near future.

Departing from these problems, a research study was made with the title "Gap Analysis of the Information Security Management System (ISMS) for Preparation for ISO/IEC 27001:2013 Certification in Directorate of Technology and Information Systems Development (DPTSI) ".

Keywords *: **Gap Analysis, ISMS, ISO/IEC 27001:2013, Indeks KAMI 4.0***

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertandatangan di bawah ini:

Nama	: Resti Nisaidha Rahmi
NRP	: 05211640000016
Tempat/ Tanggal Lahir	: Surabaya, 6 April 1998
Fakultas/ Departemen	: FTIK/ Sistem Informasi
Nomor Telp/ HP/e-mail	: 081224513616/ restinisaidharahmi@gmail.com

Dengan ini menyatakan dengan sesungguhnya bahwa penelitian/makalah/tugas akhir saya yang berjudul:

ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/IEC 27001:2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

Bebas Dari Plagiarisme Dan Bukan Hasil Karya Orang Lain.

Apabila dikemudian hari ditemukan seluruh atau sebagian penelitian/makalah/tugas akhir tersebut terdapat indikasi plagiarisme, maka saya bersedia menerima sanksi sesuai peraturan dan ketentuan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya dan untuk dipergunakan sebagaimana mestinya.

Surabaya, 20 Januari 2020

Resti Nisaidha Rahmi

NRP. 05211640000016

“Halaman ini sengaja dikosongkan”

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, penulis dapat menyelesaikan Tugas Akhir dengan judul:

"ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/ IEC 27001: 2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)

Penyusunan Tugas Akhir ini dilakukan sebagai salah satu syarat kelulusan di Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember (ITS), Surabaya. Dalam penyusunan Tugas Akhir ini, penulis mendapatkan banyak sekali doa, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih sebesar-besarnya kepada:

- Kedua orangtua dan kedua kakak yang selalu mengingatkan, memberi dukungan finansial dan moral, serta mendoakan penulis dari awal masuk Kampus Perjuangan hingga bisa menyelesaikan Tugas Akhir ini
- Pak Iyan, Bu Hanim, Pak Royyana, Pak Rizky, Mas Jananta, Pak Cahya, Bu Nuli, dan Bu Muji selaku pihak DPTSI yang bersedia meluangkan waktunya untuk melakukan wawancara dan mencarikan data/ bukti pendukung yang diperlukan untuk Tugas Akhir ini
- Ibu Hanim Maria Astuti, S.Kom, M.Sc, ITIL dan Bapak Dr. Eng Febriliyan Samopa, S.Kom, M.Kom yang telah memberikan saya bimbingan, arahan, dan motivasi dari awal pengerjaan proposal hingga Tugas Akhir ini selesai
- Bu Feby Artwodini, S.Kom, MT dan Bu Eko Wahyu Tyas D., S.Kom, MBA yang telah menguji dan memberikan saran untuk memperbaiki Tugas Akhir
- Ibu Anisah Herdiyanti, S.Kom, M.Sc yang telah membagikan ilmu dan pengalamannya kepada penulis

sehingga dapat memperkaya pengerjaan Tugas Akhir ini

- Bapak Dr. Eng Febriliyan Samopa, S.Kom, M.Kom selaku dosen wali yang senantiasa mendampingi sejak penulis menjadi Mahasiswa Baru hingga penulis bisa menyelesaikan Tugas Akhir
- Mas Ricky, selaku admin Laboratorium MSI yang membantu penulis dalam mengurus hal-hal administrasi, dari awal pendaftaran sidang TA hingga urusan bebas lab
- Teman-teman Lab MSI serta ARTEMIS yang banyak memberikan semangat dan dukungan moral dalam menyelesaikan Tugas Akhir
- Teman-teman "ANJAY", terdiri dari Tsani, Aelisa, Anggraini, Nadhifa, Dea, dan Afinda yang juga banyak memberikan dukungan materiil dan moril, serta memberikan motivasi dan saran dalam pengerjaan Tugas Akhir ini
- Abdul Muizzal Hafidz, selaku teman yang selalu memberi semangat, menjadi teman diskusi, dan banyak membantu selama proses pengerjaan Tugas Akhir
- Pihak lain yang telah membantu dan mendukung penyelesaian Tugas Akhir yang tidak bisa disebutkan satu persatu

Penulis sadar bahwa pengerjaan ini masih jauh dari kata sempurna dan banyak kekurangan. Namun, penulis berharap semoga penyusunan Tugas Akhir ini bisa memberi manfaat untuk menambah pengetahuan para pembaca serta dapat menjadi acuan bagi instansi terkait untuk berbenah. Penulis juga akan terbuka terhadap saran dan masukan dari semua pihak.

Surabaya, 20 Januari 2020
Penulis

DAFTAR ISI

“Halaman ini sengaja dikosongkan”

DAFTAR GAMBAR

“Halaman ini sengaja dikosongkan”

DAFTAR TABEL

BAB 1
PENDAHULUAN

Pada bab ini akan dibahas mengenai pendahuluan Tugas Akhir yang berisi latar belakang, perumusan masalah, batasan pengerjaan Tugas Akhir, tujuan dan manfaat dari pengerjaan Tugas Akhir, serta sistematika penulisan buku Tugas Akhir.

1.1. Latar Belakang

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) merupakan suatu lembaga di bawah naungan Institut Teknologi Sepuluh Nopember (ITS) yang bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi di ITS. DPTSI mempunyai fungsi untuk melakukan penyusunan rencana, program, dan anggaran lembaga, melaksanakan penelitian dan pengembangan teknologi dan sistem informasi, melaksanakan penjaminan keamanan sistem informasi, melaksanakan peningkatan kemampuan dan kompetensi tenaga pendidikan di bidang teknologi dan sistem informasi, pengelolaan sistem informasi berbasis web, melaksanakan pemberian layanan jasa di bidang teknologi dan sistem informasi, pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi, pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi, serta melaksanakan urusan administrasi lembaga [1].

Berdasarkan data dari DPTSI, ternyata pada DPTSI terdapat beberapa celah keamanan sistem informasi dan jaringan yang cukup berbahaya, yang mana telah dirasakan oleh civitas akademika ITS [2]**.** Celah keamanan tersebut di antaranya adanya kasus pembobolan data Sistem Integra ITS sehingga para mahasiswa tidak dapat *login*. Selain terjadi pada Sistem Integra ITS, hal serupa juga pernah terjadi pada akun e-mail ITS yang dibobol, sehingga harus dilakukan reset *password* untuk mengatasi permasalahan tersebut [2]. Kedua kasus tersebut terjadi pada tahun 2016 yang membuat baik dosen maupun mahasiswa panik dikarenakan adanya berita yang simpang siur bahwa data nilai sudah ter-*reset*.

Oleh karena itu, keamanan informasi mempunyai peranan yang vital bagi suatu organisasi. Karenanya dibutuhkan suatu manajemen sebagai aspek yang mengelola organisasi, yaitu Sistem Manajemen Keamanan Informasi (SMKI). SMKI telah dirancang sesuai dengan standar internasional, sehingga mampu menjadi acuan bagi organisasi untuk mengelola keamanan informasi di organisasinya. Selain itu, SMKI ini berfungsi untuk menjamin keamanan informasi suatu perusahaan dalam hal kerahasiaannya, integritasnya, dan ketersediaannya [3].

Salah satu standar SMKI internasional adalah ISO [4]. Standar ISO dapat diimplementasikan ke dalam organisasi baik untuk skala kecil-menengah maupun skala internasional sekalipun. Dalam studi kasus penelitian Tugas Akhir ini, standar ISO yang dapat diterapkan dan relevan dengan permasalahan yang sedang dihadapi DPTSI adalah ISO/IEC 27001:2013. Standar ISO/IEC 27001:2013 dapat membantu organisasi untuk menjaga keamanan informasinya, khususnya untuk membantu mengamankan aset-aset perusahaan, seperti informasi finansial, informasi mengenai pegawai, maupun informasi yang telah dipercayakan dari pihak ketiga kepada suatu organisasi [5].

Namun, apabila melihat kilas balik kasus keamanan informasi yang dihadapi oleh DPTSI mengindikasikan bahwa DPTSI masih belum menerapkan SMKI dengan baik berdasarkan standar ISO/IEC 27001:2013. Hal tersebut dapat terlihat dari adanya kasus pembobolan dan hasil evaluasi SMKI menggunakan Indeks KAMI versi 3.1 yang pernah dilakukan di tahun 2017 yang menunjukkan hasil masih menerapkan kerangka kerja dasar sehingga dikatakan tidak layak sertifikasi ISO 27001. Di sisi lain, DPTSI mencantumkan target di tahun 2020 untuk tersertifikasi ISO 27001 pada dokumen *masterplan*-nya [6].

Dengan demikian, diperlukan suatu intrumen berupa *checklist* yang dapat digunakan untuk melakukan analisis kesenjangan atau dikenal juga dengan *gap analysis*. Analisis kesenjangan merupakan suatu metode yang digunakan untuk

membandingkan kesenjangan antara kinerja dari suatu sistem yang sedang berjalan dengan sistem yang standar. Tujuan dari melakukan analisis kesenjangan adalah untuk mengetahui kondisi saat ini dari DPTSI dibandingkan dengan kondisi yang seharusnya menurut standar SMKI yang tercantum pada klausul-klausul ISO/IEC 27001:2013. Dengan melakukan analisis kesenjangan, DPTSI dapat memiliki gambaran sebagai dasar pengambilan tindakan apa saja yang harus diperbaiki DPTSI di masa yang akan datang.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah yang menjadi fokus untuk diselesaikan dalam Tugas Akhir ini adalah sebagai berikut.

1. Bagaimana hasil analisis kesenjangan SMKI di DPTSI dibandingkan dengan standar ISO/IEC 27001:2013?
    a. Bagaimana hasi1 penilaian Kategori Sistem Elektronik berdasarkan indeks KAMI 4.0?
    b. Bagaimana hasil penilaian Kategori 6 Area yang tercantum pada indeks KAMI 4.0?
    c. Bagaimana hasil analisis kesenjangan kesiapan sertifikasi ISO 27001 di DPTSI?
2. Apa rekomendasi perbaikan yang digunakan untuk mengurangi kesenjangan antara SMKI di DPTSI dengan standar ISO/ IEC 27001:2013?
3. Apa saja faktor penyebab dari adanya kesenjangan SMKI di DPTSI dengan ISO/ IEC 27001:2013?

1.3. Batasan Masalah

Berikut ini adalah batasan permasalahan yang menjadi ruang lingkup pengerjaan Tugas Akhir ini.

1. Metode penilaian analisis kesenjangan SMKI di DPTSI dilakukan dengan bantuan indeks KAMI versi 4.0

2. Hasil penilaian analisis kesenjangan SMKI di DPTSI menjadi hasil tingkat kesiapan DPTSI untuk melakukan sertifikasi ISO 27001
3. Untuk mengurangi kesenjangan SMKI di DPTSI dengan standar ISO/ IEC 27001:2013, diberikan rekomendasi perbaikan yang mencakup klausul utama dan *annex* ISO/IEC 27001:2013
4. Melakukan analisis akar masalah terhadap adanya kesenjangan dengan bantuan diagram *ishikawa*

1.4. Tujuan Tugas Akhir

Dari perumusan masalah yang disebutkan sebelumnya, tujuan yang akan dicapai melalui Tugas Akhir ini adalah sebagai berikut.

1. Mengetahui hasil analisis kesenjangan Sistem Manajemen Keamanan Informasi di DPTSI dibandingkan dengan standar ISO/IEC 27001:2013
    a. Mengetahui hasil penilaian Kategori Sistem Elektronik dari Indeks KAMI 4.0
    b. Mengetahui hasil penilaian 6 Area Indeks KAMI 4.0
    c. Menyusun *checklist* yang menunjukkan kesiapan DPTSI dalam melakukan sertifikasi ISO 27001
2. Memberikan rekomendasi perbaikan untuk mengurangi kesenjangan SMKI di DPTSI yang mengacu standar ISO/ IEC 27001:2013
3. Menyusun analisis akar permasalahan adanya kesenjangan SMKI di DPTSI dengan ISO/IEC 27001:2013

1.5. Manfaat Tugas Akhir

Adapun manfaat yang diharapkan dari penelitian Tugas Akhir ini, antara lain:

1. Bagi Organisasi

a. Dapat mengetahui bagaimana kesenjangan SMKI di DPTSI dengan standar ISO/IEC 27001:2013

b. Dapat menjadi evaluasi bagi DPTSI untuk memperbaiki SMKI-nya berdasarkan rekomendasi yang diberikan dalam rangka mempersiapkan sertifikasi ISO/IEC 27001

2. Bagi Akademisi

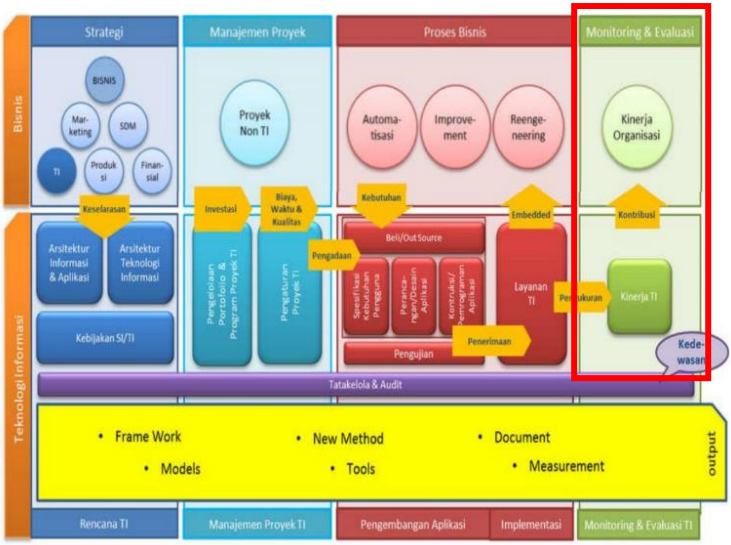
a. Dapat menambah referensi bagi peneliti selanjutnya mengenai metode analisis kesenjangan keamanan informasi

b. Dapat menambah referensi bagi peneliti selanjutnya untuk mengimplementasikan rekomendasi perbaikan yang telah diberikan.

1.6. Relevansi Tugas Akhir

Penelitian ini layak menjadi Tugas Akhir karena Tugas Akhir ini berinteraksi dengan manusia sebagai subjek pengguna teknologi dengan kebijakan sistem keamanan informasi yang diterapkan pada suatu organisasi. Topik permasalahan dan solusi yang diperlukan dalam menyelesaikan Tugas Akhir ini berfokus pada salah satu peta area Laboratorium Manajemen Sistem Informasi, yakni pengelolaan risiko Teknologi Informasi. Hal tersebut berkaitan dengan salah satu mata kuliah di Departemen Sistem Informasi, yaitu mata kuliah Manajemen Risiko dan Kualitas Teknologi Informasi (MRKTI).

Untuk bisa melakukan manajemen atau pengelolaan keamanan risiko, maka perlu untuk mengetahui aset-aset apa saja yang harus dilindungi serta bagaimana cara melindunginya. Hal tersebut diajarkan pada mata kuliah Proteksi Aset Informasi (PAI) di Departemen Sistem Informasi. Selain itu, kemampuan utama yang diperlukan dalam pengerjaan Tugas Akhir ini adalah melakukan evaluasi dan audit terhadap Teknologi Informasi, yang mana erat kaitannya dengan mata kuliah Evaluasi dan Audit (EA).



Gambar 1.1 *Roadmap* Laboratorium Manajemen Sistem Informasi

BAB 2
TINJAUAN PUSTAKA

Pada bab ini akan dibahan mengenai tinjauan pustaka dari Tugas Akhir. Bab ini berisi dasar teori yang mendukung Tugas Akhir, baik berdasarkan studi sebelumnya maupun referensi lain. Adapun hal yang ada di dalam Tinjauan Pustaka adalah sebagai berikut.

2.1. Studi Sebelumnya

Dalam pengerjaan Tugas Akhir ini, terdapat beberapa penelitian terkait yang telah dilakukan sebelumnya, yang mana penelitan sebelumnya tersebut dapat dijadikan sebagai bahan referensi untuk menyelesaikan Tugas Akhir. Berikut merupakan beberapa penelitian sebelumnya yang kasusnya berkaitan dengan pengerjaan Tugas Akhir ini yang disajikan pada Tabel 2.1.

Tabel 2.1 Penelitian Sebelumnya

Penelitian Pertama [2]	
Judul Penelitian	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 Peneliti, Tahun	Firzah Abdullah Basyarahil, 2017
Deskripsi Umum Penelitian	Penelitian ini merupakan Tugas Akhir dengan studi kasus DPTSI-ITS yang berisikan tentang evaluasi keamanan informasi pada DPTSI dengan menggunakan indeks KAMI dan mengacu pada *framework* ISO/IEC 27001:2013.
Hubungan dengan Tugas Akhir	Metode penelitian yang digunakan dalam penelitian tersebut juga akan digunakan di dalam penelitian ini. Penelitian akan mengacu pada *framework* ISO/IEC 27001:2013 dan menggunakan indeks KAMI sebagai alat bantu untuk melakukan analisis kesenjangan.

Kelebihan Penelitian	Penelitian ini mengevaluasi keamanan informasi di DPTSI dengan sangat terstruktur dan memiliki data yang komplit.
Kekurangan Penelitian	Indeks KAMI yang digunakan dalam penelitian ini masih menggunakan indeks KAMI versi 3.1, padahal saat ini sudah ada indeks KAMI versi terbaru yaitu indeks KAMI 4.0
Penelitian Kedua [1]	
Judul Penelitian	Penilaian dan Mitigasi Risiko Keamanan Sistem Informasi Berdasarkan Standar ISO/IEC 27001:2013 Menggunakan Metode PMBOK (Studi Kasus: DPTSI ITS)
Nama Peneliti, Tahun	Alif Satria Perdana, 2018
Deskripsi Umum Penelitian	Penelitian ini berfokus untuk melakukan penilaian keamanan risiko dari DPTSI. Penilaian tersebut didapat dari hasil analisis apa saja mitigasi yang diterapkan di DPTSI. *Framework* yang digunakan adalah ISO/IEC 27001:2013 dengan menggunakan metode PMBOK.
Hubungan dengan Tugas Akhir	Dalam melakukan analisis kesenjangan, maka metode penilaian keamanan risiko dapat menjadi referensi dalam melakukan analisis kesenjangan keamanan informasi di DPTSI dengan *framework* ISO/IEC 27001:2013.
Kelebihan Penelitian	Terdapat uraian mengenai dokumen rencana keamanan informasi, dimulai dari tahap identifkasi risiko dan penilaian,identifikasi ancaman dan kelemahan, serta aturan dan tanggungjawab sehingga memunculkan tabel strategi keamanan informasi.
Kekurangan Penelitian	Meskipun sama-sama mengacu ke *framework* ISO/IEC 27001:2013 dalam melakukan evaluasi keamanan risiko, metode yang digunakan adalah PMBOK, yang mana akan menjadi kurang relevan dengan penelitian ini.
Penelitian Ketiga [7]	

Judul Penelitian	Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005
Nama Peneliti, Tahun	I Gusti Ngurah Nyoman Bagiarta, 2012
Deskripsi Umum Penelitian	Berdasarkan hasil audit pada STMIK STIKOM Bali, tingkat ketergantungan perguruan tinggi tersebut dengan TIK termasuk dalam kategori sedang dengan tingkat kesiapanan Lembaga terhadap Indeks KAMI yang masih memerlukan perbaikan secara menyeluruh terhadap kelima area keamanan informasi.
Hubungan dengan Tugas Akhir	Manajemen tata kelola keamanan informasi yang dilakukan oleh STMIK STIKOM Bali bisa menjadi salah satu referensi bagaimana suatu organisasi mengelola keamanan informasi sebagai salah satu langkah dalam mepersiapkan sertifikasi ISO 27001 bagi organisasi.
Kelebihan Penelitian	Bisa menjadi acuan dalam melakukan evaluasi terhadap tata kelola keamanan informasi pada suatu organisasi
Kekurangan Penelitian	Penelitian ini masih mengacu kepada ISO 27001:2005.
Penelitian Keempat [8]	
Judul Penelitian	Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001:2013 (Studi Kasus KOMINFO Provinsi Jawa Timur)
Nama Peneliti, Tahun	Edo Rizky Pratama, Suprapto, Andi Reza Perdanakusuma
Deskripsi Umum Penelitian	Penelitian ini bertujuan untuk melakukan evaluasi keamanan informasi pada KOMINFO Provinsi Jawa Timur dengan menggunakan Indeks KAMI 3.1 dan ISO 27001. Luaran yang dihasilkan adalah berupa tingkat kematangan setiap area keamanan informasi berada pada tingkai I+ dan KOMINFO dinyatakan tidak layak untuk melakukan sertifikasi ISO 27001.

Hubungan dengan Tugas Akhir	Penelitian ini bisa menjadi rujukan untuk bagaimana penulis dari penelitian ini melakukan analisis tingkat kematangan suatu organisasi terhadap keamanan informasinya. Selain itu, penelitian ini juga dapat memberikan referensi mengenai seperti apa organisasi yang dikatakan tidak layak untuk melakukan sertifikasi ISO/IEC 27001:2013.
Kelebihan Penelitian	Bisa menjadi acuan bagaimana peneliti membandingkan kondisi keamanan informasi pada studi kasus dengan *framework* ISO/IEC 27001:2013 dan indeks KAMI 3.1.
Kekurangan Penelitian	Responden yang digunakan untuk membantu proses uji tingkat kematangan dengan menggunakan indeks KAMI 3.1 hanya berjumlah 2 orang.

Berikut ini adalah analisis kesenjangan dari keempat penelitan sebelumnya yang menjadi acuan untuk penulisan Tugas Akhir ini digambarkan pada Tabel 2.2

Tabel 2.2 *Gap Analysis* Penelitian Sebelumnya

Penelitian 1	**Penelitian 2**	**Penelitian 3**	**Penelitian 4**
Penelitian ini menggunakan indeks KAMI 3.1 dan ISO/IEC 27001:2013 untuk mengevaluasi SMKI	Penelitian ini menggunakan ISO/IEC 27001:2013 dan PMBOK untuk melakukan penilaian keamanan risiko	Penelitian ini menggunakan ISO/IEC 27001:2005 untuk melakukan audit keamanan informasi	Penelitian ini menggunakan ISO/IEC 27001:2013 dan Indeks KAMI untuk mengevaluasi keamanan informasi
Dilakukan di DPTSI	Dilakukan di DPTSI	Dilakukan di STMIK STIKOM Bali	Dilakukan di KOMINFO Jawa Timur
Pendukung	**Pendukung**	**Pendukung**	**Pendukung**
Standar yang digunakan sama, yaitu	Salah satu tandar yang digunakan sama, yaitu	Masih menggunakan standar	Masih menggunakan Indeks KAMI versi 3.1

ISO/IEC 27001:2013	ISO/IEC 27001:2013	ISO/IEC 27001:2005	
Masih menggunakan Indeks KAMI versi 3.1	Tempat yang menjadi studi kasus sama	Masih menggunakan Indeks KAMI versi 3.1	
Tempat yang menjadi studi kasus sama			
			
PENELITIAN YANG DIUSULKAN: ANALISIS KESENJANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) UNTUK PERSIAPAN SERTIFIKASI ISO/IEC 27001:2013 DI DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI)			
• Melakukan penilaian SMKI di DPTSI menggunakan indeks KAMI 4.0 • Melakukan analisis kesenjangan SMKI di DPTSI menggunakan bantuan ISO/IEC 27001:2013 *Gap Analysis Tool* • Menggunakan standar ISO/IEC 27001:2013 • Melakukan analisis akar masalah dengan menggunakan diagram *ishikawa* • Penelitian dilakukan oleh peneliti melalui wawancara, observasi, dan *review* dokumen			

2.2. Dasar Teori

2.2.1. Direktorat Pengembangan Teknologi dan Sistem Informasi

Pada awalnya, DPTSI merupakan pembaharuan nama dari suatu unit yang berfokus pada pengelolaan Teknologi Informasi di ITS yang dulunya bernama UPT Pusat Komputer yang didirikan pada tahun 1982. Menurut Peraturan Rektor Institut Teknologi Sepuluh Nopember No 10 Tahun 2016,

DPTSI memiliki struktur organisasi yang terdiri dari Direktur DPTSI yang membawahi Kasubdit Infrastruktur dan Keamanan Teknologi Informasi, Kasubdit Pengembangan Sistem Informasi yang membawahi Kasi Pengebangan aplikasi pada Perangkat Bergerak, dan Kasubdit Layanan Teknologi dan Sistem Informasi yang membawahi Kasi Layanan Data dan Informasi [1].

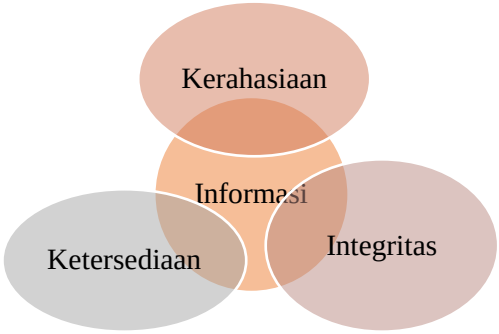
Gambar 2.1 Struktur Organisasi DPTSI

Secara umum, DPTSI memiliki beberapa fungsi dalam menjalankan tugasnya, di antaranya yaitu melakukan penyusunan rencana, program, dan anggaran lembaga, melaksanakan penelitian dan pengembangan teknologi dan sistem informasi, melaksanakan penjaminan keamanan sistem informasi, melaksanakan peningkatan kemampuan dan kompetensi tenaga pendidikan di bidang teknologi dan sistem informasi, pengelolaan sistem informasi berbasis web, melaksanakan pemberian layanan jasa di bidang teknologi dan sistem informasi, pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi, pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi, serta melaksanakan urusan administrasi lembaga [1].

2.2.2. Sistem Manajemen Keamanan Informasi

Keamanan sistem informasi memiliki beberapa aspek penting, di antaranya aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) [3].

Aspek kerahasiaan adalah aspek yang menjamin kerahasiaan data maupun informasi, yang mana data atau informasi tersebut hanya dapat diakses oleh orang yang memiliki wewenang. Di samping itu, aspek ini menjamin kerahasiaan data maupun informasi yang dikirim, diterima, serta disimpan [3]. Aspek integritas merupakan aspek yang menjamin data atau informasi tidak akan diubah tanpa adanya izin dari orang yang memiliki wewenang. Selain itu, aspek integritas juga menjamin keakuratan dan keutuhan informasi, serta metode prosesnya [3]. Aspek ketersediaan merupakan aspek yang menjamin bahwa data maupun informasi akan tersedia kapanpun saat dibutuhkan. Aspek ini juga berfungsi untuk memastikan bahwa pengguna yang memiliki wewenang dapat memakai data maupun informasi serta perangkat yang terkait apabila dibutuhkan [3].



Gambar 2.2 Aspek Keamanan Sistem Informasi

SMKI (Sistem Manajemen Kemanan Informasi) atau dikenal dengan istilah ISMS (*Information Security Management System*), adalah pendekatan sistematis untuk mengelola perusahaan, baik perusahaan kecil, menengah, dan perusahaan besar, yang memiliki informasi sensitif, sehingga informasi dari perusahaan tersebut tetap aman. SMKI merupakan bagian dari keseluruhan sistem manajemen organisasi, termasuk struktur organisasi, kebijakan, kegiatan perencanaan, tanggung jawab, praktik, prosedur, proses, serta sumber daya, yang berdasarkan pada pendekatan risiko bisnis

untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi [9]. Oleh karena itu, manajemen risiko teknologi informasi adalah fondasi dari implementasi Sistem Manajemen Keamanan Informasi [9].

Hal-hal yang perlu dilakukan dalam proses manajemen risiko di antaranya adalah manusia, proses, dan sistem Teknologi Informasi [10]. Dari segi internal, manusia harus memiliki kesadaran terkait SMKI dan terdapat delegasi keamanan informasi, sementara dari segi eksternal/ pihak ketiga harus menerapkan prinsip keamanan informasi manajemen proyek serta menerapkan klausul kerahasiaan. Proses sendiri terdiri dari kebijakan, baik dari kebijakan pengendalian hak akses, kriptografi, dan *backup* serta prosedur yang terdiri dari prosedur pengamanan area, *change management*, *disposal media*, *user access management*, serta *asset manafement*. Terakhir, dalam penggunaan teknologi juga harus diperhatikan apakah teknologi tersebut telah dilengkapi dengan *tools security* seperti *firewall* serta dilakukan *log management, access control, network monitoring, penetration test*, dan lain-lain [11].

Dengan menerapkan SMKI, manfaat yang akan diperoleh perusahaan secara umum di antaranya yaitu dapat meningkatkan reputasi perusahaan, meningkatkan kepercayaan pelanggan, dapat mengelola insiden dengan lebih baik, meningkatkan kualitas layanan, memperbaiki *response tim*, merubah proses reaktif menjadi proses proaktif, dapat melakukan *continuous improvement*, serta dapat mendukung proses bisnis [11].

Secara garis besar, penerapan Sistem Manajemen Keamanan Informasi terdiri dari 6 tahapan, di antaranya adalah persetujuan manajemen, pendefinisian ruang lingkup, melakukan *gap analysis*, melakukan *risk assessment* dan *risk treatment plan*, penyusunan SMKI, serta penerapan SMKI [5].

2.2.3. ISO/ IEC 27001: 2013 sebagai Standar SMKI

ISO 27000, atau juga dikenal sebagai ISO 27k, terdiri atas beberapa standar yang saling berhubungan satu sama lain. Standar-satandar tersebut ada yang telah dipublikasi dan ada yang masih dalam proses pengembangan oleh ISO, yang mana terdiri atas beberapa struktur komponen yang berfokus pada standar baku yang mendeskripsikan kebutuhan SMKI (ISO 27001), kebutuhan sertifikasi untuk kesesuaian dengan ISO 27001 (ISO 27006), dan kebutuhan tambahan lainnya untuk sektor implementasi yang spesifik (ISO 27009) [12]. Selain itu, standar-standar ISO lainnya juga menyediakan petunjuk untuk berbagai aspek seperti implementasi SMKI serta menangani proses-prosesnya [12].

ISO 27001 adalah standar yang dapat membantu organisasi untuk menjaga keamanan informasinya. Standar ini berguna untuk membantu mengamankan aset-aset perusahaan, seperti informasi finansial, informasi mengenai pegawai, maupun informasi yang telah dipercayakan dari pihak ketiga kepada suatu organisasi. Berdasarkan dokumentasi yang ada pada ISO 27001, standar ini dikembangkan dengan menggunakan pendekatan *top-down*, berdasarkan risiko, dan *technology-neutral* [4].

ISO 27001 berisi tentang persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi. Standar ini bersifat independen terhadap produk teknologi informasi. Selain itu, dalam standar ini mensyaratkan penggunaan pendekatan manajemen berbasis risiko, sehingga dapat menjamin bahwa kontrol keamanan yang dipilih dapat melindungi aset informasi dari berbagai risiko [5].

Secara garis besar, struktur ISO 27001 dibagi menjadi 2 bagian, yaitu klausul (*mandatory process*) dan Annex A (*security control*) [13]. Pada bagian klausul (*mandatory process*) berisi tentang persyaratan yang harus dipenuhi oleh organisasi yang menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang menggunakan *framework* ISO 27001 [13]. Sementara pada Annex A *(security control*) berisi

tentang dokumen referensi yang dapat dijadikan rujukan dalam menentukan kontrol keamanan yang harus diterapkan pada Sistem Manajemen Sistem Keamanan Informasi (SMKI) [13].

Di dalam ISO 27001:2013, terdapat beberapa klausul dan *domain* yang dapat digunakan untuk membantu organisasi dalam menerapkan SMKI [14]. Ada 34 Kontrol Tujuan (Tujuan Pengendalian) dan 114 Kontrol (Kontrol berlaku untuk diimplementasikan pada Sistem Manajemen Keamanan Informasi) [15]. Berikut adalah tabel klausul serta *domain* di dalam ISO 27001:2013 [14], yaitu:

Tabel 2.3 Klausul ISO/IEC 27001:2013

Klausul Utama		**Sub Klausul Utama**
Klausul 4	Konteks Organisasi	• *Understanding: The organization and its context,* • *The needs and expectations of interested parties,* • *Determining the scope of ISMS, Information Security Management System*
Klausul 5	Kepemimpinan	• *Leadership and Commitment,* • *Policy,* • *Organizational Roles,* • *Responsibilities and Authorities*
Klausul 6	Perencanaan	• *Actions to Address Risk and Opportunities,* • *Information security objectives and planning to achieve them*
Klausul 7	Pendukung	• *Resources,* • *Competence,* • *Awareness,* • *Communication,*

Klausul Utama		Sub Klausul Utama
		• *Documented information*
Klausul 8	Operasi	• *Operational planning and control,* • *Information security risk treatment*
Klausul 9	Evaluasi Kinerja	• *Monitoring,* • *Measurement,* • *Analysis and evaluation,* • *Internal audit,* • *Management review*
Klausul 10	Peningkatan	• *Non conformity and corrective action,* • *Continual Improvement*

2.2.4. Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan singkatan dari indeks Keamanan Informasi, merupakan suatu alat evaluasi untuk menganalisis tingkat kesiapan keamanan informasi pada suatu organisasi yang mengacu pada standar ISO/IEC 27001:2013. Luaran yang dihasilkan dari Indeks KAMI adalah gambaran mengenai kondisi kelengkapan serta kematangan kerangka kerja keamanan informasi, yang mana akan ditujukan kepada *top management* dari organisasi tersebut. Organisasi yang dapat menggunakan indeks ini adalah organisasi baik dengan skala nasional, maupun dengan skala kecil-menengah [2]. Sebaiknya, pengukuran indeks KAMI dilakukan sebanyak 2 kali dalam setahun untuk meninjau kembali kesiapan keamanan informasi serta untuk mengukur inisiatif perbaikan yang diterapkan organisasi yang dapat dilihat dari pencapaian kelengkapan maupun kematangan tertentu [16].

Indeks KAMI telah mengalami beberapa pembaharuan versi, di antaranya indeks KAMI versi 2.3, lalu diperbaharui menjadi indeks KAMI dengan versi 3.1, dan yang terakhir adalah indeks KAMI versi 4.0. Apabila dibandingkan dengan indeks KAMI versi sebelumnya, indeks KAMI 4.0 memiliki area evaluasi tambahan yaitu area suplemen yang berfungsi sebagai aspek pengamanan keterlibatan pihak ketiga

penyedia layanan, pengamanan layanan *cloud*, dan perlindungan data pribadi. Selain itu, area evaluasi yang ada pada indeks KAMI versi 3.1 dengan indeks KAMI versi 4.0 masih sama, di antaranya yaitu area Kategori Sistem Elektronik, Kategori Tata Kelola, Kategori Risiko, Kategori Kerangka Kerja, Kategori Pengelolaan Aset, serta kategori Teknologi. Proses evaluasi keamanan informasi menggunakan indeks KAMI akan dilakukan melalui sejumlah pertanyaan yang telah disediakan pada masing-masing area tersebut [16].

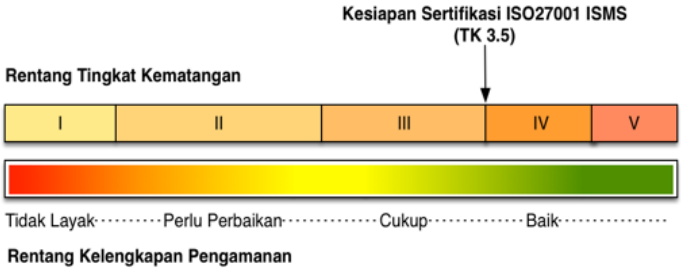
Pertanyaan-pertanyaan tersebut dikelompokkan untuk 2 keperluan, yaitu dikelompokkan berdasarkan tingkat kelengkapan yang diminta oleh standar ISO/IEC 27001:2013 dan tingkat kematangan pengamanan informasi. Untuk keperluan pertama, pertanyaan dari setiap area dibagi menjadi 3, yaitu pertanyaan dengan label 1 berhubungan dengan bentuk kerangka kerja dasar keamanan informasi, pertanyaan dengan label 2 terkait dengan efektivitas dan konsistensi penerapannya, serta pertanyaan dengan label 3 yaitu kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Masing-masing dari pertanyaan berlabel tersebut memiliki Status Pengamanan, yang terdiri dari Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, dan Diterapkan Secara Menyeluruh [16].

	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 2.3 Matriks Skor Pengamanan

Sementara untuk keperluan kedua, tingkat kematangan pada indeks KAMI dikategorisasikan ke dalam Tingkat I – Kondisi Awal, Tingkat II – Penerapan Kerangka Kerja Dasar, Tingkat

III – Terdefinisi dan Konsisten, Tingkat IV – Tekekola dan Terukur, serta Tingkat V – Optimal. Tingkatan tersebut kemudian didetilkan dengan cara menambah tingkatan tersebut dengan tingkatan antara – I+, II+, III+, dan IV+. Tingkat kesiapan sertifikasi yang diharapkan adalah minimum berada pada Tingkat III+ [16].



Gambar 2.4 Rentang Tingkat Kematangan dan Kelengkapan Pengamanan

Untuk memulai melakukan penilaian secara kuantitatif berdasarkan pertanyaan yang yang terdapat pada setiap area, responden diminta untuk mendefinisikan terlebih dahulu kategori Sistem Elektronik dari suatu instansi serta mendeskripsikan secara singkat infrastruktur Teknologi Informasi dari instansi tersebut [6]. Tujuan dari proses ini adalah untuk mengkategorisasikan Sistem Elektronik yang digunakan instansi tersebut ke dalam beberapa kelompok, yaitu rendah, tinggi, dan strategis Hasil kategorisasi tersebut didapatkan dari penjumlahan semua nilai kriteria pada setiap pertanyaan di dalam Kategori Sistem Elektronik. Setelah itu, pengkategorisasian Sistem Elektronik tersebut dikolerasikan dengan status Kesiapan melalui Gambar berikut ini [16].

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

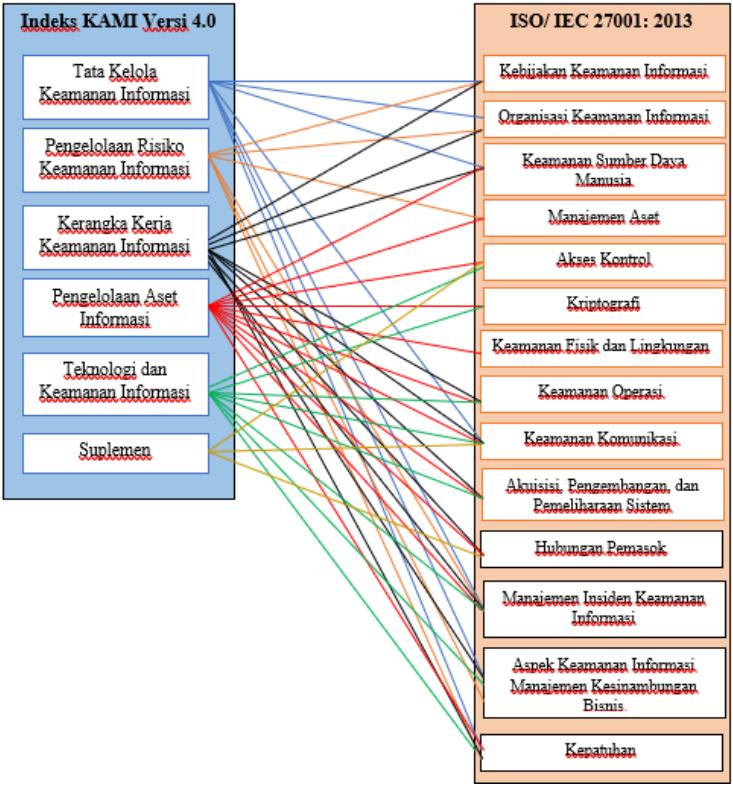
Gambar 2.5 Hubungan Nilai Kategori Sistem Elektronik dengan Status Kesiapan

Langkah selanjutnya adalah melakukan penilaian terhadap kelima area selain Kategori Sistem Informasi yang ada di Indeks KAMI versi 4.0 berdasarkan jawaban dari pertanyaan yang telah disediakan dari masing-masing area sehingga penilaian tersebut akan menghasilkan suatu diagram yang berbentuk jaring laba-laba (*spider chart*). Di dalam diagram tersebut terdapat *Radar Chart* yang menunjukkan 5 area utama (tanpa area Suplemen) di Indeks KAMI versi 4.0. Diagram tersebut memiliki 3 macam gradasi warna, yaitu dari hijau muda hingga hijau tua. Hal ini menunjukkan ambang batas dari kategori pengamanan 1 sampai 3 [16].

Gambar 2.6 *Radar Chart* Indeks KAMI

2.2.5. Hubungan Indeks KAMI dengan ISO/ IEC 27001:2013

Seperti yang telah dijelaskan sebelumnya, indeks KAMI versi 4.0 terdiri dari 5 area evaluasi yang sama seperti pada indeks KAMI versi 3.1 yang kemudian ditambah dengan 1 area evaluasi tambahan, yaitu area suplemen. Area-area tersebut merupakan rangkuman dari 14 sasaran pengendalian keamanan informasi yang tercantum pada *annex* dari ISO/IEC 27001:2013. Oleh karena itu, indeks KAMI pasti memiliki hubungan yang erat dengan ISO/IEC 27001:2013. Hubungan tersebut digambarkan dari area evaluasi yang ada pada indeks KAMI terhadap klausul *annex* yang ada pada ISO/ IEC 27001:2013. Sebagai contoh, area evaluasi Tata Kelola Keamanan Informasi memiliki hubungan dengan standar ISO/IEC 27001:2013 terhadap klausul Kebijakan Keamanan Informasi, Organisasi Keamanan Informasi, Keamanan Sumber Daya Manusia, Keamanan Komunikasi, Manajemen Insiden Keamanan Informasi, Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis, dan Kepatuhan. Berikut ini merupakan gambar yang menunjukkan hubungan Indeks KAMI dengan ISO/ IEC 27001:2013 [8].



Gambar 2.7 Hubungan Antara Indeks KAMI 4.0 dengan ISO/IEC 27001:2013

2.2.6. Analisis Kesenjangan

Gap analysis, atau analisis kesenjangan adalah suatu alat yang dapat digunakan untuk mengevaluasi kinerja perusahaan. Dengan kata lain, *gap analysis* merupakan suatu metode yang digunakan untuk membandingkan kesenjangan antara kinerja dari suatu sistem yang sedang berjalan dengan sistem yang standar. Selain itu, analisis kesenjangan juga bertujuan untuk mengidentifikasi tindakan-tindakan apa saja yang harus dilakukan untuk mengurangi kesenjangan atau mencapai kinerja yang diharapkan pada masa mendatang [17].

Sementara itu, analisis kesenjangan ISO 27001 merupakan aktivitas *mandatory* dalam ISO 27001, yang mana dimulai dari membaca setiap klausul dari ISO 27001 dan melakukan analisis apakah *requirement* dari ISO 27001 telah diimplementasikan oleh suatu organisasi [18]. Tujuan dari melakukan analisis kesenjangan ISO 27001 adalah untuk mengetahui kondisi kekinian dari suatu organisasi dan mencari tahu sumber daya apa yang akan diperlukan suatu organisasi untuk mengimplementasikan ISO 27001 [18]. Secara umum, tahapan dalam melakukan analisis kesenjangan ISO 27001 terdiri dari 2 fase, yaitu menilai kondisi kekinian Sistem Manajemen Keamanan Informasi (SMKI) dari suatu organisasi yang akan dibandingkan dengan standar ISO/ IEC 27001:2013 untuk mengidentifikasi berbagai kesempatan yang dapat meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) saat ini serta mengatasi kekurangan Sistem Manajemen Keamanan Informasi (SMKI) saat ini terhadap *requirement* yang ada pada standar ISO 27001. Tahapan selanjutnya yaitu menyusun laporan analisis kesenjangan yang berisi tentang kondisi kesiapan dan kematangan Sistem Manajemen Keamanan Informasi (SMKI) suatu organisasi, serta kesenjangan yang ada antara kondisi kekinian dengan yang seharusnya ada pada standar sehingga dapat membantu organisasi dalam mencapai sertifikasi ISO 27001 [19].

Dalam konteks penulisan Tugas Akhir ini, analisis kesenjangan yang dilakukan berkaitan dengan Sistem Manajemen Keamanan Informasi dari DPTSI. Kegiatan analisis ini dilakukan untuk membandingkan seberapa jauh DPTSI telah memenuhi persyaratan klausul-klausul pada ISO/IEC 27001:2013.

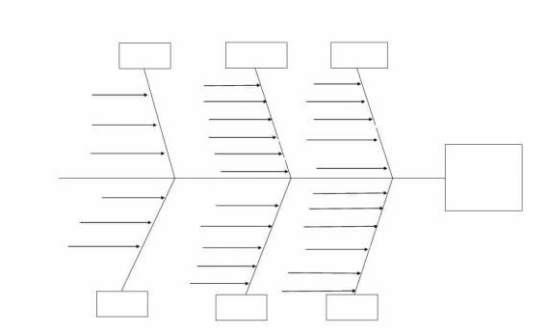
Persyaratan-persyaratan tersebut berupa aspek kerangka kerja, yaitu dari sisi kebijakan dan prosedur, serta aspek penerapannya. Dari segi aspek kerangka kerja, analisis kesenjangan yang dilakukan yaitu apakah kebijakan dan prosedur sebagaimana dicantumkan di ISO 27001:2013 telah dipenuhi. Sementara untuk aspek penerapan, ketersediaan

dokumentasi penerapan perlu diperiksa sebagai bukti penerapan. *Gap analysis* dari Sistem Manajemen Keamanan Informasi dari suatu organisasi umumnya dibantu dengan suatu instrumen, yaitu indeks KAMI.

Hasil analisis kesenjangan tersebut akan menjadi penilaian bagi suatu organisasi mengenai tingkat kesiapan sertifikasi ISO 27001. Selain itu, dapat menjadi masukan yang bermanfaat bagi organisasi karena dapat memberikan gambaran kondisi saat ini. Gambaran kondisi saat ini kemudian dibandingkan dengan standar ISO/IEC 27001: 2013 sebagai dasaran untuk mengambil tindakan apa saja yang harus diperbaiki oleh organisasi tersebut di masa yang akan datang, seperti kebijakan atau prosedur apa yang harus dibuat, dokumen-dokumen apa yang harus dilengkapi, serta hal apa yang harus diterapkan.

2.2.7. Analisis Akar Masalah

Analisis akar masalah, atau dikenal juga dengan *Root Cause Analysis* (RCA), adalah suatu metode untuk membantu identifikasi faktor apa saja yang mempengaruhi suatu kejadian. Tujuan dari dilakukannya analisis ini adalah untuk memudahkan suatu organisasi untuk mengetahui kondisi permasalahan yang terjadi, sehingga suatu organisasi dapat meningkatkan kinerjanya. Selain itu, permasalahan yang ada di suatu organisasi juga dapat terdokumentasi dengan baik. Dalam melakukan analisis akar masalah, diperlukan suatu proses pengumpulan data dari pihak organisasi, terutama pihak yang berhubungan langsung dengan suatu proses terkait, seperti seorang manajer. Proses pengumpulan data dapat dilakukan dengan wawancara dengan menanyakan mengapa pada setiap pertanyaan hingga menuju jawaban terakhir kepada manajer atau pimpinan lainnya.



Gambar 2.8 Diagram Fishbone

Salah satu metode untuk melakukan analisis akar masalah adalah dengan menggunakan diagram *ishikawa*. Diagram *ishikawa*, dikenal juga dengan diagram tulang ikan atau *fishbone diagram*. Diagram ini ditemukan oleh ilmuwan Jepang bernama Dr. Ishikawa pada tahun 1960-an . Diagram ini berbentuk mirip dengan tulang ikan yang moncong kepalanya menghadap ke kanan. Diagram ini akan menunjukkan akibat atau dampaknya pada bagian kepala dan penyebab-penyebabnya akan diisi pada tulang-tulang ikannya. Kelebihan melakukan analisis akar masalah dengan menggunakan diagram ini adalah bahwa diagram ini dapat menjabarkan setiap masalah yang terjadi dengan mudah. Namun, diagram ini memiliki tingkat subjektivitas yang cukup tinggi dikarenakan metode ini hanya menggambarkan masalah secara verbal (non kuantitatif) dengan bersumber pada hasil wawancara.

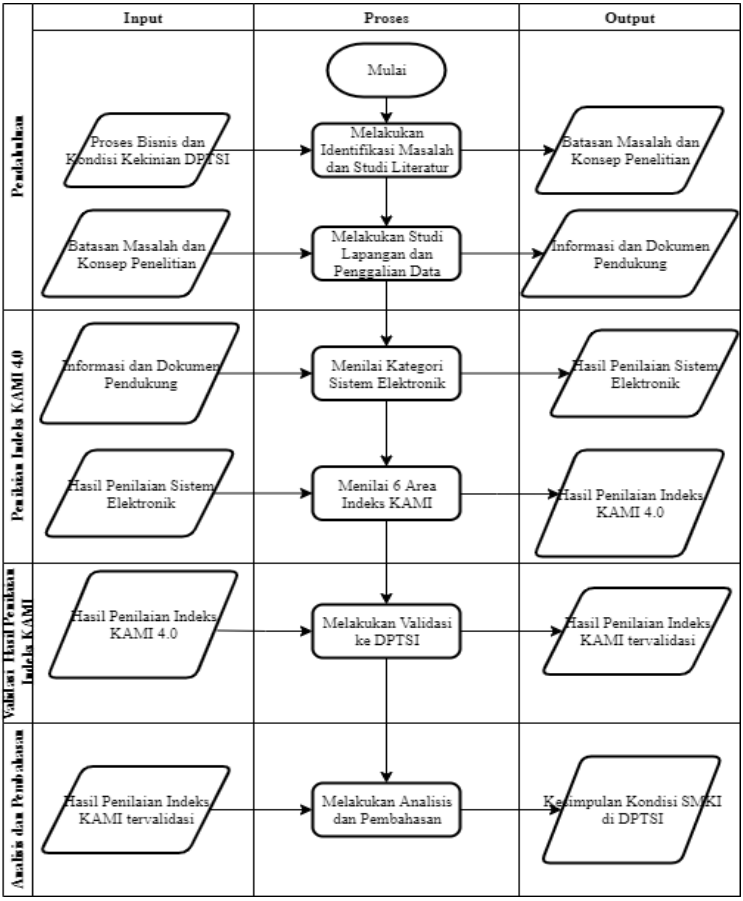
“Halaman ini sengaja dikosongkan”

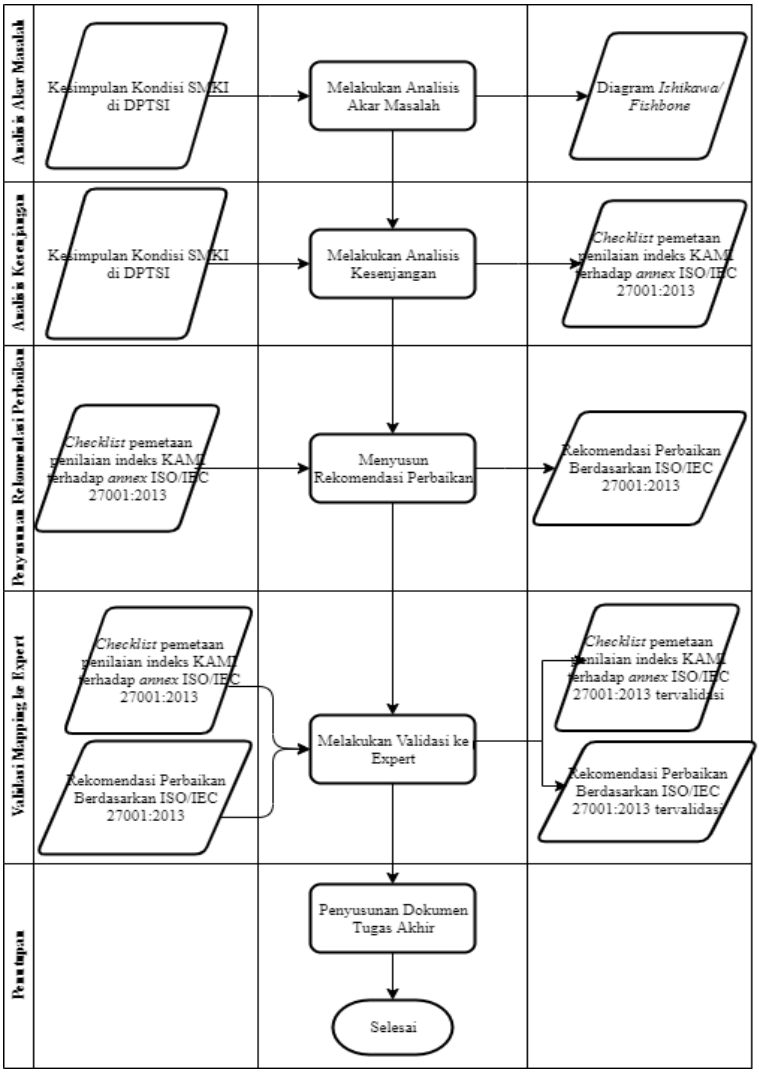
BAB 3
METODE PENGERJAAN TUGAS AKHIR

Bagian ini menjelaskan mengenai metodologi atau alur pengerjaan tugas akhir dengan memberikan rincian di setiap tahapan yang dilakukan.

3.1.Tahapan Pelaksaan Tugas Akhir

Pada penelitian tugas akhir ini terdapat langkah-langkah yang akan dilakukan sebagaimana tertuang pada gambar di bawah ini.





Gambar 3.1 Metodologi Penelitian Tugas Akhir

3.2.Uraian Metodologi

Pada bagian ini akan dijelaskan secara lebih rinci masing-masing tahapan yang dilakukan dalam penelitian Tugas Akhir.

3.2.1. Pembagian Tahapan Pengerjaan

Secara umum, pengerjaan penelitian tugas akhir ini dibagi menjadi empat bagian utama yaitu:

1. **Pendahuluan**

   Pada tahap ini akan membahas tentang pengidentifikasian masalah, pembahasan studi literatur yang terkait dengan penelitian, serta melakukan studi lapangan untuk pengambilan data.

2. **Melakukan Penilaian**

   Pada tahap ini akan dilakukan proses penilaian Sistem Manajemen Keamanan Informasi (SMKI) di DPTSI dengan bantuan instrumen indeks KAMI versi 4.0 mengacu ke standar ISO 27001:2013.

3. **Validasi Hasil Penilaian Indeks KAMI**

   Pada tahap ini akan dilakukan validasi terhadap hasil penilaian Indeks KAMI 4.0 untuk memastikan apa yang tertulis di dokumen sesuai dengan kondisi yang ada di lapangan. Validasi dilakukan dengan memastikan pertanyaan dijawab dengan narasumber yang tepat. Hal ini dilakukan dengan cara menanyakannya kepada Direktur DPTSI dan KaSubDit Layanan Teknologi Informasi sebagai representasi dari DPTSI. Selain itu, validasi juga dilakukan dengan menunjukkan hasil penilaian kepada kedua pihak tersebut untuk dipastikan sudah tidak ada lagi kesalahan.

4. **Analisis dan Pembahasan**

   Tahapan ini merupakan tahapan untuk melakukan analisis terhadap hasil penilaian yang telah valid dan melakukan penarikan kesimpulan.

5. **Melakukan Analisis Akar Masalah**

   Langkah selanjutnya yaitu melakukan analisis akar masalah sebagai gambaran mengapa kesenjangan bisa

terjadi. Harapannya, adanya analisis ini dapat membantu organisasi untuk mengatasi kesenjangan dengan tepat sasaran.

6. Melakukan Analisis Kesenjangan

Setelah mengetahui hasil penilaian Indeks KAMI, maka langkah selanjutnya yaitu melakukan analisis kesenjangan dengan melakukan pemetaan hasil penilaian terhadap ISO/IEC 27001:2013 sehingga menghasilkan suatu *checklist* kepatuhan SMKI DPTSI.

7. Penyusunan Rekomendasi Perbaikan

Pada tahap ini akan membahas tentang hasil analisis kesenjangan SMKI dengan bantuan instrumen yang telah disebutkan sebelumnya, lalu memberikan rekomendasi perbaikan untuk mengurangi kesenjangan dan meningkatkan kepatuhan yang mengacu pada ISO/IEC 27001:2013.

8. **Validasi *Mapping* ke *Expert***

Pada tahap ini akan dilakukan validasi kembali terhadap *checklist* pemetaan hasil penilaian Indeks KAMI 4.0 untuk memastikan setiap pertanyaan di Indeks KAMI 4.0 dipetakan dengan klausul *annex* ISO/IEC 27001:2013 secara tepat. Begitupun juga dengan hasil rekomendasi perbaikan yang telah disusun, akan dilakukan validasi juga untuk memastikan rekomendasi yang diberikan terhadap penilaian yang belum maksimal telah dilakukan dengan benar. Subjek yang dikatakan *expert* adalah seseorang yang telah sertifikasi ISO/IEC 27001:2013

9. Penutup

Setelah seluruh tahapan selesai maka penelitian Tugas Akhir ini akan diakhiri dengan pembuatan dokumentasi penelitian dalam bentuk laporan tugas akhir.

3.2.2. Identifikasi Permasalahan dan Studi Literatur

Tahapan ini merupakan tahap awal dalam pengerjaan Tugas Akhir. Pada tahap ini, akan dilakukan identifikasi masalah yang akan dijadikan topik Tugas Akhir. Setelah menemukan masalah yang akan diangkat, maka dilakukan studi literatur dengan mengumpulkan referensi dari buku, narasumber, jurnal, penelitian sebelumnya, dan dokumen terkait. Selain itu, pada tahap ini akan dilakukan kajian tentang konsep serta metode yang dapat digunakan untuk menyelesaikan permasalahan pada Tugas Akhir ini.

3.2.3. Studi Lapangan dan Penggalian Data

Selanjutnya, pada tahap ini akan dilakukan pengumpulan data dari DPTSI yang berkaitan dengan permasalahan pada Tugas Akhir ini. Data-data tersebut akan didapat melalui wawancara, observasi secara langsung, dan melakukan *review* dokumen.

3.2.4. Penilaian Tingkat Kategori Sistem Elektronik

Pada tahap ini akan dilakukan penilaian terhadap tingkat kategori SE di DPTSI. Hasil dari penilaian ini akan menunjukkan seberapa jauh tingkat ketergantungan suatu organisasi terhadap sistem elektronik. Kategori SE (Sistem Elektronik) ini akan dibagi menjadi tiga tingkat, yaitu rendah, tinggi, dan strategis. Penilaian ini dapat diperoleh dari responden yang diwawancara dan observasi secara langsung.

3.2.5. Penilaian 6 Area Indeks KAMI 4.0

Setelah dilakukan penilaian tingkat kategori SE di DPTSI, maka akan dilanjutkan dengan penilaian 6 area yang ada di Indeks KAMI sebagai insstrumen dalam melakukan analisis kesenjangan SMKI DPTSI dengan standar ISO/IEC 27001:2013.

3.2.6. Validasi Hasil Penilaian Indeks KAMI ke DPTSI

Tahapan berikutnya yaitu validasi terhadap hasil indeks KAMI untuk memastikan agar hasil penilaian Indeks KAMI tersebut sesuai dengan kondisi yang ada di lapangan.

3.2.7. Analisis dan Pembahasan

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.

3.2.8. Analisis Akar Masalah

Berikutnya yaitu melakukan analisis akar masalah. Analisis ini merupakan tahapan untuk mencari tahu akar penyebab dari kondisi SMKI di DPTSI berdasarkan hasil penilaian Indeks KAMI dan adanya kesenjangan dengan ISO/IEC 27001:2013. Dalam melakukan tahapan ini, *tool* yang digunakan untuk membantu analisis akar masalah adalah diagram *iskhikawa*. Sebelum bisa menuliskan faktor-faktor masalahnya, penilaian Indeks KAMI yang masih belum dijawab DPTSI dengan maksimal akan dikategorisasi. Setelah itu, untuk membantu proses analisis, akan dilakukan wawancara kembali untuk menggali penyebab terdasar dari masalah-masalah yang telah dikategorikan sebelumnya.

3.2.9. Analisis Kesenjangan

Kemudian, di tahap ini akan dilakukan pemetaan hasil penilaian Indeks KAMI dengan ISO/IEC 27001:2013 berupa *checklist* yang menunjukkan klausul mana yang belum dipenuhi DPTSI berdasarkan Indeks KAMI 4.0. Tujuan dari dilakukan pemetaan ini adalah untuk memudahkan organisasi dalam memahami kondisi SMKI di DPTSI secara umum, sehingga dapat mempercepat langkah pengambilan keputusan.

3.2.10. Penyusunan Rekomendasi Perbaikan

Langkah selanjutnya yaitu memberikan rekomendasi perbaikan untuk mengurangi kesenjangan SMKI di DPTSI dengan standar ISO/IEC 27001:2013. Rekomendasi perbaikan yang diberikan mengacu pada standar ISO/IEC 27001:2013, yang terdiri dari klausul utama dan klausul *annex*-nya.

3.2.11. Validasi ke *Expert*

Di tahapan ini akan dilakukan validasi kembali, namun validasi dilakukan ke pihak *expert* untuk memastikan bahwa *checklist* pemetaan penilaian Indeks KAMI 4.0 terhadap klausul-klausul ISO/IEC 27001:2013 yang tercantum telah dilakukan dengan benar. Selain itu, penyusunan rekomendasi terhadap hasil penilaian Indeks KAMI 4.0 yang belum maksimal juga akan divalidasi, sehingga rekomendasi yang diberikan kepada DPTSI dilakukan dengan tepat sehingga dapat diimplementasikan oleh DPTSI. Validasi dilakukan kepada seorang *expert*, yaitu seseorang yang telah tersertifikasi ISO 27001.

3.2.12. Pembuatan Dokumen Tugas Akhir

Penelitian Tugas Akhir ini diakhiri dengan tahap pembuatan dokumen laporan Tugas Akhir. Dokumen ini akan mendokumentasikan setiap langkah dan tahapan yang telah dilakukan, hasil yang didapat pada setiap langkah, kesimpulan serta saran untuk penelitian selanjutnya.

“Halaman ini sengaja dikosongkan”

BAB 4
PERANCANGAN

Pada bab ini akan dijelaskan mengenai proses perancangan penelitian tugas akhir. Proses perancangan ini dilakukan agar dapat menjadi panduan dalam mengerjakan penelitian Tugas Akhir.

4.1. Perancangan Penelitian

Dalam melakukan penelitian, sudah menjadi suatu keharusan untuk menyiapkan segala hal yang berkaitan dengan pengerjaan Tugas Akhir sebelum terjun ke lapangan. Menurut Margono, rancangan merupakan alur kegiatan penulis dalam memecahkan masalah. Menurut Sukardi, rancangan penelitian adalah bayangan seorang penulis mengenai apa yang akan dilakukan saat melakukan penelitian dan menjawab permasalahan yang mejadi objek penelitian, yang kemudian dituangkan ke dalam langkah sistematis [21]. Perancangan penelitian yang digunakan dalam pengerjaan Tugas Akhir ini adalah eksplorasi-deskriptif, yang mana melakukan penggalian fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk peulis dan menggambarkannya dalam bentuk narasi.

Selain itu, Menurut Yin, perancangan penelitian terbagi menjadi dua jenis, antara lain *single-case design* yang mana pengujian dilakukan dengan hanya menggunakan satu kasus, serta *multiple-case design* yang mana penguujian dilakukan dengan menggunakan dua atau lebih kasus [2]. Kemudian, Yin membagi *single-case design* menjadi *single unit of analysis* yang mana digunakan dalam penelitian dengan kasus kritis atau unik, serta meguji teori yang telah dirumuskan, dan *multiple unit of analysis* yang mana digunakan dalam penelitian dengan tujuan melakukan eksplorasi perbedaan dengan membandingkan sub-unitnya. Oleh karena itu, berdasarkan teori jenis perancangan penelitian Yin, pengerjaan Tugas Akhir ini menerapkan *single-case design* dan *multiple unit of analysis*.

Tujuan dari penelitian Tugas Akhir kali ini adalah untuk melakukan analisis kesenjangan Sistem Manajemen Keamanan

Informasi di DPTSI dibandingkan dengan standar ISO/IEC 27001:2013, mengetahui tingkat kesiapan DPTSI untuk melakukan sertifikasi ISO 27001, memberikan rekomendasi perbaikan untuk mengurangi kesenjangan SMKI di DPTSI dengan menggunakan bantuan Indeks KAMI 4.0, serta melakukan analisis akar masalah atas adanya kesenjangan tersebut.

Oleh karena itu, untuk menjawab tujuan penelitian Tugas Akhir, maka diperlukan beberapa masukan data yang telah dijabarkan pada bab sebelumnya mengenai metodologi, di antaranya kondisi kekinian DPTSI yang meliputi Sistem Elektronik di DPTSI serta tata kelola risiko, teknologi, dan aset di DPTSI, yang selanjutnya data tersebut akan dioleh sehingga menghasilkan penilaian Indeks KAMI 4.0. Setelah itu, hasil penilaian tersebut menjadi masukan untuk dipetakan menjadi sebuah *checklist* kesenjangan untuk mengetahui kesenjangan SMKI di DTPSI dengan ISO/IEC 27001:2013.

4.2. Subjek dan Objek Penelitian

Subjek dari penelitian Tugas Akhir ini adalah salah satu instansi yang ada di Institut Teknologi Sepuluh Nopember (ITS) yaitu Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI). Instansi ini terdiri dari Ketua DPTSI, Kepala Pusat Pengelolaan & Layanan TIK, Kepala Pusat Pengembangan Sistem Informasi, Kepala Pusat dan Staf Infrastruktur & Keamanan Informasi, yang mana orang-orang pada posisi tersebut akan menjadi sumber peneliti dalam melakukan penilaian Indeks KAMI 4.0.

Objek dari penelitan tugas akhir ini adalah SMKI pada DPTSI ITS, yang mana setelah dilakukan penilaian terhadap SMKI pada DPTSI ITS untuk melihat sejauh mana kesiapan DPTSI untuk melakukan sertifikasi ISO 27001, melakukan analisis akar masalah, memberikan hasil kesenjangan DPTSI dengan ISO 27001:2013, serta memberikan rekomendasi perbaikan untuk DPTSI.

4.3. Data yang Diperlukan

Berikut ini akan dijelaskan data yang diperlukan peneliti dalam menjawab tujuan penelitian tugas akhir, data-data tersebut, antara lain: 1) Tugas pokok dan fungsi dari DPTSI ITS, 2) Gambaran kondisi Tata Kelola Keamanan Informasi, 3) Gambaran kondisi Pengelolaan Risiko Keamanan Informasi, 4) Gambaran kondisi Kerangka Kerja Keamanan Informasi, 5) Gambaran kondisi Pengelolaan Aset Informasi, 6) Gambaran kondisi Teknologi dan Keamanan Informasi, dan 7) Informasi suplemen, seperti pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan, dan perlindungan data pribadi. Meskipun data-data tersebut telah diperoleh untuk kepentingan pengerjaan Tugas Akhir dengan objek yang sama pada tahun 2017, pengerjaan Tugas Akhir kali ini tetap membutuhkan data-data tersebut untuk membandingkan hasil penelitian yang pernah dilakukan di tahun 2017 dengan penelitian yang dilakukan saat ini.

4.4. Penentuan Metode Pengumpulan Data

4.4.1 Wawancara

Menurut Robert Khan dan Channel, wawancara merupakan pola khusus dari interaksi dimulai secara lisan untuk tujuan tertentu, dan difokuskan pada daerah konten yang spesifik, dengan proses eliminasi dari bahan-bahan yang tidak ada hubungannya secara berkelanjutan [22]. Berdasarkan pengertian tersebut, wawancara ini dilakukan dengan konten penilaian SMKI dengan menggunakan pertanyaan Indeks KAMI 4.0 sebagai instrumen utamanya. Pertanyaan yang telah disediakan dari Indeks KAMI 4.0 ini merupakan pertanyaan terbuka, sehingga jawaban dari narasumber dapat dieksplorasi lebih lanjut.

Berdasarkan poin subjek penelitian yang telah dijabarkan sebelumnya, wawancara akan dilakukan kepada Ketua DPTSI, Kepala Pusat Pengelolaan & Layanan TIK, Kepala Pusat Pengembangan Sistem Informasi, Kepala Pusat dan Staf Infrastruktur & Keamanan Informasi. Subjek tersebut

dipilih berdasarkan kapasitas dan kewenangannya, mengingat instrumen yang digunakan dalam mewawancara subjek tersebut berkaitan erat dengan penerapan SMKI pada DPTSI. Berikut ini adalah pemetaan pertanyaan yang ada di Indeks KAMI 4.0 dengan subjek yang terkait.

Tabel 4.1 Tabel Pemetaan Narasumber dengan Pertanyaan Indeks KAMI 4.0

Subjek	Pertanyaan Indeks KAMI 4.0
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
Kepala Pusat Pengelolaan & Layanan TIK Hanim Maria Astuti, S.Kom, M.Sc, ITIL	1-SE; 2-SE; 3-SE; 4-SE; 5-SE; 6-SE; 7-SE; 8-SE; 9-SE; 10-SE 7.1.1; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.3.9
Kepala Pusat dan Staf Infrastruktur & Keamanan Informasi Royyana Muslim Itjihadie, 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;

Subjek	Pertanyaan Indeks KAMI 4.0
	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 7.2; 7.3.1; 7.3.3; 7.3.4; 7.3.5; 7.3.6; 7.3.7; 7.3.8; 7.3.11; 7.3.13; 7.3.14; 7.3.16
Admin pusat infrastruktur dan keamanan informasi • 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
Kepala Pusat Pengembangan Sistem Informasi Rizky Januar Akbar, S.Kom, M.Eng	4.12; 4.13; 4.14; 4.23; 4.24; 4.25; 4.26; 6.24; 6.25 7.3.2; 7.3.10; 7.3.12; 7.3.15;

4.4.2 Observasi

Observasi adalah proses untuk mengamati kondisi kekinian dari DPTSI secara langsung. Observasi dilakukan dengan tujuan untuk mendukung hasil wawancara. Luaran dari proses ini adalah dokumentasi bukti penerapan SMKI di DPTSI ITS.

4.4.3 Review Dokumen

Selain melakukan wawancara dan observasi, metode lain yang digunakan adalah *review* dokumen. Metode ini

merupakan metode yang digunakan untuk memberikan informasi lebih jauh dari hasil wawancara dan hasil observasi. Informasi ini dapat menjadi bukti sudah sejauh mana penerapan SMKI di DPTSI ITS. Informasi-informasi yang diperlukan dalam melakukan *review* dokumen adalah informasi struktur organisasi, fungsi, tupoksi, log aktivitas, serta kebijakan-kebijakan terkait keamanan informasi dalam bentuk dokumen fisik maupun dokumen digital.

4.4.4 Pemetaan Metode Pengumpulan Data dengan Tujuan dan Sasaran

Dengan adanya banyak metode pengumpulan data yang digunakan dalam pengerjaan Tugas Akhir ini, diharapkan dapat membuat data yang diperoleh menjadi lebih valid dan akurat. Namun di sisi lain, menggunakan lebih dari satu metode pengumpulan data dapat membuat bias terkait data apa saja yang harus diperoleh dari setiap metode pengumpulan data yang dilakukan. Oleh karena itu, perlu adanya penjabaran mengenai tujuan dan sasaran yang bersumber dari Indeks KAMI 4.0 dan ISO/IEC 27001:2013 pada setiap metode pengumpulan data yang dilakukan, antara lain.

Tabel 4.2 Tujuan dan Sasaran Metode Pengumpulan Data

Tujuan	Sasaran
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
Mengetahui standar dan algoritma keamanan informasi pada sistem elektronik	• Standar keamanan informasi pada sistem elektronik • Jenis algoritma khusus pada sistem elektronik

Tujuan	Sasaran
Mengetahui jenis data yang dikelola, tingkat kekritisan data, dan tingkat kekritisan proses pada ancaman yang ada di sistem elektronik	• Data pribadi yang dikelola sistem elektronik • Tingkat klasifikasi data dalam sistem elektronik • Tingkat kekritisan proses dalam sistem elektronik
Mengetahui dampak dan kerugian dari kegagalan sistem elektronik	• Dampak dari kegagalan sistem elektronik • Kerugian dari insiden keamanan sistem elektronik
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 informasi • Program khusus untuk pengamanan informasi

Tujuan	Sasaran
	• 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
Mengetahui rencana, penerapan, dan evaluasi dari pengelolaan kebijakan & prosedur keamanan informasi	• Kebijakan & prosedur keamanan informasi • Mekanisme pengelolaan dokumen kebijakan & prosedur keamanan informasi

Tujuan	Sasaran
	• 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

Tujuan	Sasaran
	• Framework keberlanjutan 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
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,

Tujuan	Sasaran
	pengamanan aset, instalasi software, dan penggunaan data pribadi • 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

Tujuan	Sasaran
	infomasi terkait pihak ketiga
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 • Penindaklanjutan dari adanya virus & malware sinkronisasi waktu jaringan, sistem, dan aplikasi sesuai standar • Verifikasi/ validasi saat proses pengembangan setiap aplikasi

Tujuan	Sasaran
	• Pengamanan lingkungan pengembangan sesuai standar yang digunakan untuk sikus hidup sistem • Pihak independan untuk mengkaji keamanan informasi
Metode Observasi	
Tujuan	**Sasaran**
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
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

Tujuan	Sasaran
Mengetahui kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengamanan aset teknologi	• Perlindungan pada iternet 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
Metode Review Dokumen	
Tujuan	**Sasaran**
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
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

Tujuan	Sasaran
	• Dokumen keberlanjutan bisnis mengenai layanan TIK • Dokumen hasil laporan kondisi keamanan informasi • Dokumen standar dan perangkat hukum terkait keamanan informasi
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 • Dokumen mitigasi risiko beserta prioritas penyelesaiannya • Dokumen evaluasi langkah mitigasi secara berkala • Dokumen evaluasi framework pengelolaan risiko

Tujuan	Sasaran
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
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
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

4.5. Penentuan Metode Pengolahan Data

Setelah melakukan pengumpulan data dari wawancara, observasi, dan *review* dokumen, maka tahapan selanjutnya yaitu melakukan pengolahan data. Metode yang digunakan dalam melakukan pengolahan data yang diperoleh di antaranya untuk untuk metode pengumpulan data melalui wawancara, metode pengolahan data yang dilakukan adalah menulis ulang catatan hasil wawancara peneliti dan rekaman wawancara menggunakan media *recorder* dengan menggunakan Microsoft Word. Selanjutnya, untuk hasil data penilaian Indeks KAMI 4.0 dilakukan pembobotan dan menjumlahkan seluruh skor yang diperoleh dari masing-masing pertanyaan. Sementara, untuk metode pengumpulan data melalui observasi dan *review* dokumen, data yang diperoleh akan dimasukkan ke dalam buku laporan Tugas Akhir, khususnya di bagian lampiran sebagai bukti pendukung dari hasil wawancara.

4.6. Penentuan Metode Analisis

Setelah memperoleh dan mengolah data yang diperlukan, maka langkah berikutnya yang dilakukan adalah melakukan analisis. Analisis ini dilakukan dengan menggunakan pendekatan kategori yang telah disediakan oleh Indeks KAMI 4.0 yang kemudian akan dipetakan ke dalam *checklist* kelengkapan dan kepatuhan sebagai output dari analisis kesenjangan. Setelah itu, akan dilakukan penyusunan rekomendasi perbaikan berdasarkan ISO/IEC 27001:2013 dan *root-caused analysis*. Berikut adalah penjabaran dari pendekatan yang dilakukan, antara lain:

- **Pendekatan Kategori Sistem Elektronik Indeks KAMI 4.0**

  Kategori Sistem Elektronik adalah kategori pertama yang harus diisi dalam melakukan penilaian Sistem Manajemen Keamanan Informasi dari DPTSI.

- **Pendekatan 6 Area Keamanan Informasi Indeks KAMI 4.0**

  Setelah mengisi kategori Sistem Elektronik, maka langkah selanjutnya yaitu melakukan pengisian pada 6 area yang disediakan oleh Indeks KAMI 4.0 untuk membantu proses penilaian Sistem Manajemen Keamanan Informasi dari DPTSI. Keenam area tersebut di antaranya Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, serta Suplemen

- **Melakukan Analisis Akar Masalah**

  Langkah selanjutnya adalah melakukan *root-caused analysis* atau analisis akar masalah. Langkah ini dilakukan untuk mengetahui akar penyebab dari permasalahan DPTSI yang masih belum sepenuhnya mematuhi standar ISO/IEC 27001:2013, sehingga masih belum siap dalam melakukan sertifikasi ISO 27001. Pertanyaan-pertanyaan pada Indeks KAMI 4.0 akan dipetakan dengan klausul-klausul ISO 27001:2013 sebagai kategorisasi permasalahan yang sedang dihadapi DPTSI. Klausul-klausul tersebut akan menjadi tulang ikan utama dari diagram *ishikawa* yang kemudian akan didetilkan dengan penyebab adanya permasalahan pada klausul tersebut.

- **Melakukan Analisis Kesenjangan**

  Hasil penilaian Indeks KAMI 4.0 yang telah dilakukan sebelumnya akan dipetakan menjadi suatu *checklist*, untuk mengetahui kepatuhan DPTSI dalam menerapkan *annex* ISO/IEC 27001:2013. Bentuk pemetaan yang dilakukan yaitu mengkelompokkan setiap poin pertanyaan Indeks KAMI di semua area ke dalam klausul *annex* ISO/IEC 27001:2013. Pemetaan dilakukan dengan mengacu ke referensi yang menunjukkan hubungan area Indeks KAMI dengan ISO/IEC 27001:2013 yang telah digambarkan pada Gambar 2.7.

Berikut adalah *checklist* kepatuhan terhadap klausul ISO/IEC 27001:2013 yang ditunjukkan pada Tabel 4.3. Kolom Indeks KAMI 4.0 akan diisi dengan kode pertanyaan Indeks KAMI 4.0 Kolom *checked* dapat diisi dengan Y yang berarti *Yes* (sudah patuh dan sudah terdokumentasi) yang dapat dilihat dari hasil penilaian Indeks KAMI yang diperoleh secara penuh, N yang berarti *No* (tidak patuh dan tidak terdokumentasi yang dapat dilihat bahwa skor pada Indeks KAMI terisi 0, dan QY yang berarti *Qualified Yes* (hanya patuh atau terdokumentasi sebagian), yang mana perolehan skor dari Indeks KAMI.

Tabel 4.3 Bentuk *Checklist* Pemetaan Penilaian Indeks KAMI

Annex A	**Pertanyaan Indeks KAMI**	***Checklist (Y, QY, N)***
A.5 Kebijakan Keamanan Informasi		
A.6 Organisasi Keamanan Informasi		
A.7 Keamanan Sumber Daya Manusia		
A.8 Manajemen Aset Sumber		
A.9 Akses Kontrol		
A.10 Kriptografi		
A.11 Keamanan Fisik dan Lingkungan		
A.12 Keamanan Operasi		
A.13 Keamanan Komunikasi		
A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem		
A.15 Hubungan Pemasok		
A.16 Manajemen Insiden Keamanan Informasi		

Annex A	Pertanyaan Indeks KAMI	*Checklist (Y, QY, N)*
A.17 Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis		
A.18 Kepatuhan		

- **Penyusunan Rekomendasi Perbaikan**

  Penyusunan rekomendasi perbaikan yang dilakukan berdasarkan hasil penilaian Indeks KAMI 4.0 akan mengacu pada ISO/IEC 27001:2013 yang mana merupakan standar perancangan Sistem Manajemen Keamanan Informasi. Standar tersebut terdiri dari klausul-klausul utama dan klausul annex. Indeks KAMI hanya mengacu pada ke klausul *annex* dari ISO/IEC 27001:2013 saja, padahal untuk melakukan sertifikasi ISO 27001 organisasi perlu memenuhi seluruh ISO/IEC 27001:2013, baik klausul utama maupun klausul *annex*. Oleh karena itu, rekomendasi perbaikan akan mencakup hal-hal yang diharuskan klausul utama dan klausul *annex* dari ISO/IEC 27001:2013 dalam menerapkan SMKI dan melakukan sertifikasi ISO 27001.

BAB 5
IMPLEMENTASI

Pada bab ini akan dijelaskan mengenai hasil eksekusi dari proses perancangan yang telah dijelaskan pada bab sebelumnya. Bagian ini akan menjabarkan data yang diperoleh dari pengumpulan data menggunakan metode wawancara, observasi, dan review dokumen.

5.1. Profil DPTSI

Pada awalnya, DPTSI merupakan pembaharuan nama dari suatu unit yang berfokus pada pengelolaan Teknologi Informasi di ITS yang dulunya bernama UPT Pusat Komputer yang didirikan pada tahun 1982. Menurut Peraturan Rektor Institut Teknologi Sepuluh Nopember No 10 Tahun 2016, DPTSI memiliki struktur organisasi yang terdiri dari Direktur DPTSI yang membawahi Kasubdit Infrastruktur dan Keamanan Teknologi Informasi, Kasubdit Pengembangan Sistem Informasi yang membawahi Kasi Pengebangan aplikasi pada Perangkat Bergerak, dan Kasubdit Layanan Teknologi dan Sistem Informasi yang membawahi Kasi Layanan Data dan Informasi [1].

Secara umum, DPTSI memiliki beberapa fungsi dalam menjalankan tugasnya, di antaranya yaitu melakukan penyusunan rencana, program, dan anggaran lembaga, melaksanakan penelitian dan pengembangan teknologi dan sistem informasi, melaksanakan penjaminan keamanan sistem informasi, melaksanakan peningkatan kemampuan dan kompetensi tenaga pendidikan di bidang teknologi dan sistem informasi, pengelolaan sistem informasi berbasis web, melaksanakan pemberian layanan jasa di bidang teknologi dan sistem informasi, pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi, pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi, serta melaksanakan urusan administrasi lembaga [1].

Gambar 5.1 Struktur Organisasi DPTSI

Setiap Unit di DPTSI memiliki tanggung jawab masing-masing yang dijabarkan ke dalam Tugas Pokok dan Fungsi. Tanggung jawab tersebut harus dikerjakan untuk membantu menjawab tujuan dari DPTSI ITS. Berikut adalah pemetaan Tugas Pokok dan Fungsi (Tupoksi) dari DPTSI dengan Unit Pusat Layanan (PusYan), Pusat Infratruktur dan Teknologi Informasi (PusNet), dan Pusat Pengembangan (PusBang).

Tabel 5.1 Tugas, Pokok, dan Fungsi DPTSI

No.	Tupoksi DPTSI	PusYan	PusNet	PusBang
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

No.	Tupoksi DPTSI	PusYan	PusNet	PusBang
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		
10.	Menjamin keamanan sistem informasi		V	

No.	Tupoksi DPTSI	PusYan	PusNet	PusBang
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	

No.	Tupoksi DPTSI	PusYan	PusNet	PusBang
16.	Menyediakan jasa di bidang teknologi dan sistem informasi dengan berbagai pihak	V	V	V

5.2. Hasil Wawancara dan Observasi

Pada Bab 4, telah dijelaskan bahwa untuk mendapatkan hasil penilaian Indeks KAMI 4.0, akan dilakukan wawancara dengan beberapa narasumber yang telah dipetakan dengan seluruh area pertanyaan Indeks KAMI 4.0 pada Tabel 4.1. Wawancara tersebut dilaksanakan di Gedung DPTSI. Hasil wawancara dan observasi dapat dilihat lebih detail pada **Lampiran A**.

5.3. Hasil Review Dokumen

Seperti yang telah dijelaskan pada bab sebelumnya, setelah melakukan wawancara dan observasi, diperlukan *review* dokumen yang akan digunakan sebagai penunjang/ bukti dari jawaban wawancara dan observasi. Bukti tersebut akan menggambarkan sejauh mana pelaksanaan SMKI yang dilakukan DPTSI Surabaya. Berikut adalah daftar dokumen yang perlu untuk dilakukan *review* beserta keterangan ada atau tidaknya dokumen yang diperlukan.

Tabel 5.2 Tabel Ketersediaan Dokumen untuk *Review* Dokumen

No.	Dokumen	Ada/ Tidak Ada
1	Dokumen anggaran sistem elektronik	Ada
2	Dokumen dampak dan kerugian kegagalan sistem elektronik	Tidak Ada

No.	Dokumen	Ada/ Tidak Ada
3	Dokumen Tupoksi dan struktur organisasi bagian keamanan informasi	Ada
4	Dokumen standar kompetensi SDM Keamanan Informasi	Tidak Ada
5	Dokumen Undang-Undang identifikasi data pribadi	Tidak Ada
6	Dokumen keberlanjutan bisnis layanan TIK	Tidak Ada
7	Dokumen hasil laporan kondisi keamanan informasi	Tidak Ada
8	Dokumen standar dan perangkat hokum terkait keamanan informasi	Tidak Ada
9	Dokumen program kerja pengelolaan risiko keamanan informasi	Tidak Ada
10	Dokumen struktur organisasi dan Tupoksi manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi	Tidak Ada
11	Dokumen *framework* pengelolaan risiko keamanan informasi	Tidak Ada

No.	Dokumen	Ada/ Tidak Ada
12	Dokumen klasifikasi aset, tingkat ancaman, dan dampak kerugian keamanan informasi	Tidak Ada
13	Dokumen analisis/ kajian risiko keamanan informasi	Tidak Ada
14	Dokumen mitigasi risiko berdasarkan prioritas	Ada
15	Dokumen evaluasi langkah mitigasi secara berkala	Ada
16	Dokumen evaluasi *framework* pengelolaan risiko	Tidak Ada
17	Dokumen daftar inventaris aset informasi dan aset TI	Tidak Ada
18	Dokumen pengelolaan konfigurasi	Tidak Ada
19	Tata tertib penggunaan computer, e-mail, internet, dan internet	Tidak Ada
20	Tata tertib penggunaan dan pengaman aset	Tidak Ada
21	Dokumen peraturan instalasi software dan penggunaan data	Tidak Ada
22	Dokumen syarat serta prosedur penghancuran data dan	Tidak Ada

No.	Dokumen	Ada/ Tidak Ada
	pertukaran data dengan pihak eksternal	
23	Dokumen prosedur *backup* dan *restore*	Tidak Ada
24	Dokumen pelaporan insiden keamanan informasi pada pihak internal dan eksternal	Tidak Ada
25	Dokumen pengelolaan fasilitas fisik/ lokasi kerja	Tidak Ada
26	Dokumen peraturan pengamanan lokasi ruang server dan ruang arsip	Ada
27	Dokumen log perubahan sistem informasi dan upaya akses yang tidak pantas	Ada
28	Dokumen standar penggunaan enkripsi	Tidak Ada
29	Dokumen verifikasi dan validasi pengembangan aplikasi	Ada
30	SOP mitigasi risiko implementasi sistem baru	Ada
31	SOP pengelolaan dan pemantauan layanan	Tidak Ada

No.	Dokumen	Ada/ Tidak Ada
32	Dokumen mekanisme identifikasi risiko kerjasama dengan vendor	Tidak Ada
33	Dokumen alur pemrosesan dan pertukaran data pribadi dengan pihak ketiga	Tiadak Ada
34	Dokumen proses pengungkapan data pribadi dengan pihak ketiga yang membutuhkan	Tidak Ada

5.4. Hasil Penilaian Indeks KAMI 4.0

Berikut ini adalah hasil penilaian Indeks KAMI versi 4.0 yang didapatkan dari wawancara, observasi, dan *review* dokumen. Penilaian Indeks KAMI 4.0 ini terdiri dari penilaian kategori Sistem Elektronik dan penilaian 6 area yang terdiri dari area tata kelola, risiko, kerangka kerja, pengelolaan aset, teknologi, dan suplemen.

Penilaian 6 area tersebut dilakukan untuk mengetahui kondisi kematangan keamanan informasi sesuai dengan standar ISO/IEC 27001:2013. Area kematangan tersebut digambarkan dengan tingkatan warna yang berbeda yang telah ditentukan oleh aplikasi Indeks KAMI 4.0, yang digambarkan pada Tabel 5.3.

Tabel 5.3 Tingkatan Warna pada Indeks KAMI 4.0

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 Dilaksanakan
		Dalam Perencanaan
		Dalam Penerapan/ Diterapkan Sebagian
		Diterapkan secara Menyeluruh

Penilaian terhadap setiap pertanyaan dilakukan dengan mengisi pertanyaan dengan jawaban Status Pengamanan yang terdiri dari Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, serta Diterapkan secara Menyeluruh, yang mana skor untuk setiap pertanyaan dengan status pengamanan yang sama memiliki *range* skor yang berbeda, yang telah digambarkan pada Gambar 2.3.

5.4.1Penilaian Kategori Sistem Elektronik

Penilaian Kategori Sistem Elektronik adalah penilaian yang harus dilakukan sebelum mengisi penilaian terhadap 6 area Indeks KAMI. Hal ini bertujuan untuk mengklasifikasikan penggunaan Sistem Elektronik dalam suatu organisasi. Hasil klasifikasi penggunaan Sistem Elektronik dibagi menjadi 3,

yaitu Rendah, Tinggi, dan Strategis. Tingkat klasifikasi tersebut didapatkan dari menjawab pertanyaan tertutup yang disediakan oleh Indeks KAMI, yang mana memiliki 3 pilihan yaitu A, B, dan C. Berdasarkan tingkat klasifikasi tersebut, maka skor yang diperlukan untuk mencapai status kesiapan sertifikasi ISO 27001 memiliki *range* skor yang berbeda. Pada Gambar telah dijelaskan pemetaan klasifikasi Sistem Elektronik dengan Skor Status Kesiapan.

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

Gambar 5.2 Hubungan Nilai Kategori Sistem Elektronik dengan Status Kesiapan

Setelah dilakukan penilaian, skor kategori Sistem Elektronik pada DPTSI mencapai 31. Hal ini menunjukkan bahwa tingkat ketergantungan DPTSI terhadap Sistem Elektronik masuk ke dalam kategori Tinggi. Hasil penilaian yang lebih lengkap dapat melihat pada **Lampiran A**.

5.4.2Penilaian 6 Area Indeks KAMI 4.0

Hasil penilaian 6 area Indeks KAMI 4.0 terdiri dari area tata kelola keamanan informasi yang mencapai 49, area pengelolaan risiko keamanan informasi yang mencapai 18, area kerangka kerja pengelolaan keamanan informasi yang mencapai 35, area pengelolaan aset informasi mencapai 76, dan penilaian area teknologi dan keamanan informasi mencapai 75. Selain itu, area suplemen yang terbagi terbagi menjadi 3 bagian penilaian, yaitu untuk pengamanan

keterlibatan pihak ketiga penyedia layanan mencapai 0,37, penilaian pengamanan layanan infrastruktur awan mencapai 0,40, dan penilaian perlindungan data pribadi mencapai 0,81 Untuk hasil penilaian yang lebih lengkap dapat melihat pada **Lampiran A**.

BAB 6
HASIL DAN PEMBAHASAN

6.1 Analisis Hasil Akhir Indeks KAMI 4.0

Berdasarkan hasil penilaian kategori Sistem Elektronik dan hasil penilaian 6 area yang telah ditulis pada bab sebelumnya, dapat dilihat hasil penilaian secara keseluruhan pada Gambar 6.1. Dari gambar *dashboard* di bawah ini dapat dilihat bahwa hasil evaluasi Indeks KAMI secara keseluruhan di DPTSI dengan tingkat Sistem Elektronik masuk dalam kategori tinggi adalah Tidak Layak. Hal tersebut disebabkan karena skor tingkat kelengkapan penerapan standar di DPTSI hanya mencapai 255.

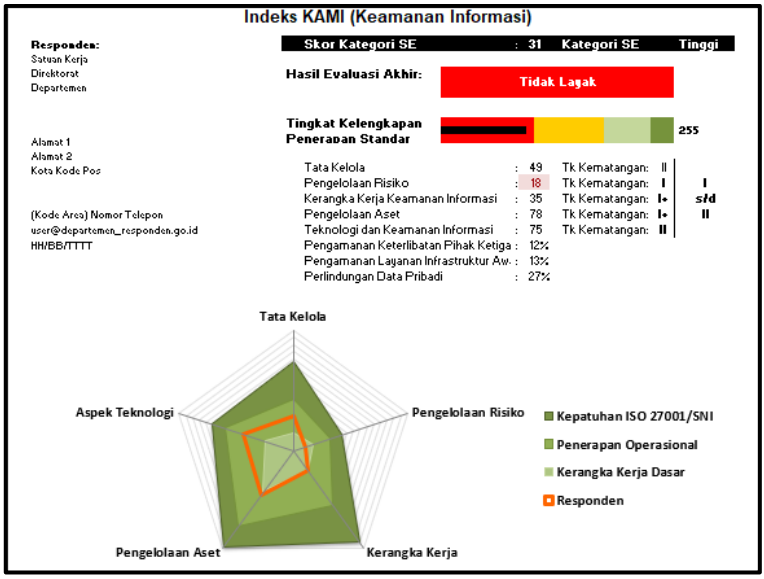
Skor total tersebut didapatkan dari hasil penilaian area tata kelola yang mencapai 49 dengan tingkat kematangan II, area pengelolaan risiko sebesar 18 dengan tingkat kematangan I, area kerangka kerja keamanan informasi sebesar 35 dengan tingkat kematangan I+, area pengelolaan aset sebesar 78 dengan tingkat kematangan I+, serta area teknologi informasi sebesar 75 dengan tingkat kematangan II. Dari penilaian tingkat kematangan setiap area tersebut menunjukkan bahwa kondisi tingkat kematangan SMKI di DPTSI baru mencapai I-II. Hal ini dapat diketahui bahwa tingkat kematangan SMKI di DPTSI bisa dikatakan masih cukup jauh dari target sertifikasi ISO 27001 yang mana adalah sebesar III+. Berikut adalah uraian tingkat kematangan SMKI di DPTSI berdasarkan penilaian Indeks KAMI 4.0.

Tabel 6.1 Uraian Hasil Tingkat Kematangan DPTSI Secara Keseluruhan

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

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
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
	II	**I**	**I+**	**I+**	**II**

Selain itu, untuk penilaian area suplemen, dapat dilihat bahwa untuk kategori pengamanan keterlibatan pihak ketiga sebesar 12%, pengamanan layanan infrastruktur awan sebesar 13%, dan perlindungan data pribadi sebesar 27%. Sementara, jika dilihat dengan menggunakan *radar chart*, dapat diketahui bahwa tingkat kepatuhan DPTSI terhadap ISO 27001 baru mencapai penerapan operasional pada area tata kelola, area kerangka kerja, pengelolaan aset, dan aspek teknologi serta mencapai kerangka kerja dasar untuk area pengelolaan risiko.



Gambar 6.1 Dashboard Hasil Penilaian Indeks KAMI 4.0

6.1.1 Tingkat Kelengkapan dan Tingkat Kematangan 6 Area

Area tata kelola memiliki total pertanyaan sebesar 22, yang terdiri dari pertanyaan dengan tahap penerapan 1 dan 2 sebanyak 8 serta tahap penerapan 3 sebanyak 6. Skor tahap penerapan 1 adalah 16, skor tahap penerapan 2 adalah 34, dan skor tahap penerapan 3 adalah 0, sehingga nilai total tingkat kelengkapan area ini adalah sebesar 49. Nilai ini meningkat sebanyak 5 poin dari evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017 yang semula skor area ini hanya mencapai 45. Hal ini dikarenakan adanya perubahan penilaian yang terjadi pada beberapa pertanyaan, yang diuraikan pada tabel berikut ini.

Tabel 6.2 Perubahan Penilaian Indeks KAMI tahun 2017 dan tahun 2019 Area Tata Kelola

Pertanyaan Area Tata Kelola	Penilaian Sebelumnya		Penilaian Saat ini	
	Status	Skor	Status	Skor
2.1	Diterapkan secara Menyeluruh	3	Dalam Penerapan/ Diterapkan Sebagian	2
2.4	Tidak Dilakukan	0	Dalam Perencanaan	1
2.5	Tidak Dilakukan	0	Dalam Penerapan/ Diterapkan Sebagian	2
2.6	Tidak Dilakukan	0	Dalam Perencanaan	1
2.7	Tidak Dilakukan	0	Dalam Perencanaan	1
2.8	Tidak Dilakukan	0	Dalam Penerapan/ Diterapkan Sebagian	2

Pertanyaan Area Tata Kelola	Penilaian Sebelumnya		Penilaian Saat ini	
	Status	Skor	Status	Skor
2.15	Diterapkan Secara Menyeluruh	6	Dalam Penerapan/ Diterapkan Sebagian	4

Nilai tingkat kelengkapan setiap tahapan pengamanan menentukan tingkat kematangan area ini. Semakin besar nilai tingkat kelengkapan, maka semakin besar pula nilai tingkat kematangannya. Pada area ini, tingkat kematangan baru mencapai tingkat kematangan II. Berikut adalah tabel yang menjelaskan tingkat kelengkapan dan tingkat kematangan area tata kelola.

Tabel 6.3 Tingkat Kelengkapan dan Tingkat Kematangan Area Tata Kelola

Tingkat Kelengkapan Area Tata Kelola			
Kategori Kontrol (Tahapan)	**Pertanyaan Tata Kelola**	**Nilai**	
1	8	15	
2	8	34	
3	6	0	
Total	**22**	**49**	
Tingkat Kematangan Area Tata Kelola			
Kategori Tk. Kematangan	**Pertanyaan Tata Kelola**	**Nilai**	**Validitas Kematangan**
II	13	39	II
III	3	10	No
IV	6	0	No
Total	22	49	

Selanjutnya, area pengelolaan risiko keamanan informasi memiliki total pertanyaan sebesar 16, yang terdiri dari pertanyaan dengan tahap penerapan 1 sebanyak 10, tahap penerapan 2 sebanyak 4, serta tahap penerapan 3 sebanyak 2. Skor tahap penerapan 1 adalah 16, skor tahap penerapan

2 adalah 34, dan skor tahap penerapan 3 adalah 0, sehingga nilai total tingkat kelengkapan area ini adalah sebesar 18. Nilai ini menurun sebanyak 3 poin dari evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017 yang semula skor area ini mencapai 21. Hal ini dikarenakan adanya perubahan penilaian yang terjadi pada beberapa pertanyaan, yang diuraikan pada tabel berikut ini.

Tabel 6.4 Perubahan Penilaian Indeks KAMI tahun 2017 dan tahun 2019 Area Risiko

Pertanyaan Area Risiko	Penilaian Sebelumnya		Penilaian Saat ini	
	Status	Skor	Status	Skor
3.5	Diterapkan Secara Menyeluruh	3	Dalam Penerapan/ Diterapkan Sebagian	2
3.6	Diterapkan Secara Menyeluruh	3	Dalam Penerapan/ Diterapkan Sebagian	2
3.10	Diterapkan Secara Menyeluruh	3	Dalam Penerapan/ Diterapkan Sebagian	2
3.11	Diterapkan Secara Menyeluruh	6	Dalam Penerapan/ Diterapkan Sebagian	4

Pada area ini, tingkat kematangan baru mencapai tingkat kematangan I. Berikut adalah tabel yang menjelaskan tingkat kelengkapan dan tingkat kematangan area pengelolaan risiko keamanan informasi.

Tabel 6.5 Tingkat Kelengkapan dan Tingkat Kematangan Area Risiko

Tingkat Kelengkapan Area Risiko		
Kategori Kontrol (Tahapan)	Pertanyaan Tata Kelola	Nilai

1	10	6
2	4	12
3	2	0
Total	**16**	**18**

Tingkat Kematangan Area Risiko			
Kategori Tk. Kematangan	**Pertanyaan Tata Kelola**	**Nilai**	**Validitas Kematangan**
II	10	6	No
III	2	12	No
IV	2	0	No
V	3	0	No
Total	16	18	

Pada area kerangka kerja memiliki total pertanyaan sebesar 29, yang terdiri dari pertanyaan dengan tahap penerapan 1 sebanyak 12, tahap penerapan 2 sebanyak 10 serta tahap penerapan 3 sebanyak 7. Skor tahap penerapan 1 adalah 16, skor tahap penerapan 2 adalah 34, dan skor tahap penerapan 3 adalah 0, sehingga nilai total tingkat kelengkapan area ini adalah sebesar 35. Nilai ini tidak mengalami perubahan poin dari evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017. Namun, terdapat perubahan penilaian yang terjadi pada beberapa pertanyaan, yang diuraikan pada tabel berikut ini.

Tabel 6.6 Perubahan Penilaian Indeks KAMI tahun 2017 dan tahun 2019 Area Kerangka Kerja

Pertanyaan Area Kerangka Kerja	**Penilaian Sebelumnya**		**Penilaian Saat ini**	
	Status	**Skor**	**Status**	**Skor**
4.6	Diterapkan Secara Menyeluruh	3	Dalam Penerapan/ Diterapkan Sebagian	2
4.8	Diterapkan Secara Menyeluruh	6	Dalam Penerapan/ Diterapkan Sebagian	4

Pertanyaan Area Kerangka Kerja	Penilaian Sebelumnya		Penilaian Saat ini	
	Status	Skor	Status	Skor
4.14	Tidak Dilakukan	0	Dalam Penerapan/ Diterapkan Sebagian	4
4 .17	Tidak Dilakukan	0	Diterapkan Secara Menyeluruh	0
4.18	Tidak Dilakukan	0	Diterapkan Secara Menyeluruh	0
4.21	Diterapkan Secara Menyeluruh	3	Dalam Penerapan/ Diterapkan Sebagian	2
4.28	Tidak Dilakukan	0	Diterapkan Secara Menyeluruh	0
4.29	Tidak Dilakukan	0	Diterapkan Secara Menyeluruh	0

Nilai tingkat kelengkapan setiap tahapan pengamanan menentukan tingkat kematangan area ini. Semakin besar nilai tingkat kelengkapan, maka semakin besar pula nilai tingkat kematangannya. Pada area ini, tingkat kematangan baru mencapai tingkat kematangan I+. Berikut adalah tabel yang menjelaskan tingkat kelengkapan dan tingkat kematangan area kerangka kerja.

Tabel 6.7 Tingkat Kelengkapan dan Tingkat Kematangan Area Kerangka Kerja

Tingkat Kelengkapan Area Kerangka Kerja		
Kategori Kontrol (Tahapan)	**Pertanyaan Tata Kelola**	**Nilai**
1	12	15
2	10	20

3	7	0	
Total	**29**	**35**	
Tingkat Kematangan Area Kerangka Kerja			
Kategori Tk. Kematangan	**Pertanyaan Tata Kelola**	**Nilai**	**Validitas Kematangan**
II	11	16	I+
III	13	19	No
IV	3	0	No
V	2	0	No
Total	**29**	**35**	

Pada area pengelolaan aset memiliki total pertanyaan sebesar 38, yang terdiri dari pertanyaan dengan tahap penerapan 1 sebanyak 24, tahap penerapan 2 sebanyak 10 serta tahap penerapan 3 sebanyak 4. Skor tahap penerapan 1 adalah 38, skor tahap penerapan 2 adalah 38, dan skor tahap penerapan 3 adalah 0, sehingga nilai total tingkat kelengkapan area ini adalah sebesar 78. Nilai ini mengalami peningkatan sebesar 5 poin dari evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017 yang semula sebesar 73. Hal ini dikarenakan adanya perubahan penilaian yang terjadi pada beberapa pertanyaan, yang diuraikan pada tabel berikut ini.

Tabel 6.8 Perubahan Penilaian Indeks KAMI tahun 2017 dan tahun 2019 Area Pengelolaan Aset

Pertanyaan Pengelolaan Aset	**Penilaian Sebelumnya**		**Penilaian Saat ini**	
	Status	**Skor**	**Status**	**Skor**
5.20	Tidak Dilakukan	0	Dalam Penerapan/ Diterapkan Sebagian	4
5.24	Dalam Perencanaan	2	Dalam Penerapan/ Diterapkan Sebagian	4
5.32	Diterapkan secara Menyeluruh	3	Dalam Penerapan/	2

Pertanyaan Pengelolaan Aset	Penilaian Sebelumnya		Penilaian Saat ini	
	Status	Skor	Status	Skor
			Diterapkan Sebagian	

Nilai tingkat kelengkapan setiap tahapan pengamanan menentukan tingkat kematangan area ini. Semakin besar nilai tingkat kelengkapan, maka semakin besar pula nilai tingkat kematangannya. Pada area ini, tingkat kematangan baru mencapai tingkat kematangan II. Berikut adalah tabel yang menjelaskan tingkat kelengkapan dan tingkat kematangan area pengelolaan aset.

Tabel 6.9 Tingkat Kelengkapan dan Tingkat Kematangan Area Pengelolaan Aset

Tingkat Kelengkapan Area Pengelolaan Aset			
Kategori Kontrol (Tahapan)	**Pertanyaan Tata Kelola**	**Nilai**	
1	24	38	
2	10	40	
3	4	0	
Total	**38**	**78**	
Tingkat Kematangan Area Pengelolaan Aset			
Kategori Tk. Kematangan	**Pertanyaan Tata Kelola**	**Nilai**	**Validitas Kematangan**
II	29	58	I+
III	9	20	No
Total	**38**	**78**	

Berikutnya yaitu pada area teknologi keamanan informasi memiliki total pertanyaan sebesar 26, yang terdiri dari pertanyaan dengan tahap penerapan 1 sebanyak 12, tahap penerapan 2 sebanyak 10 serta tahap penerapan 3 sebanyak 7. Skor tahap penerapan 1 adalah 16, skor tahap penerapan 2 adalah 34, dan skor tahap penerapan 3 adalah 0, sehingga nilai total tingkat kelengkapan area ini adalah sebesar 35. Nilai ini tidak mengalami perubahan poin dari evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017.

Nilai tingkat kelengkapan setiap tahapan pengamanan menentukan tingkat kematangan area ini. Semakin besar nilai tingkat kelengkapan, maka semakin besar pula nilai tingkat kematangannya. Pada area ini, tingkat kematangan baru mencapai tingkat kematangan II. Berikut adalah tabel yang menjelaskan tingkat kelengkapan dan tingkat kematangan area teknologi.

Tabel 6.10 Tingkat Kelengkapan dan Tingkat Kematangan Area Teknologi

Tingkat Kelengkapan Area Teknologi			
Kategori Kontrol (Tahapan)	**Pertanyaan Tata Kelola**	**Nilai**	
1	14	41	
2	10	34	
3	2	0	
Total	**26**	**75**	
Tingkat Kematangan Area Teknologi			
Kategori Tk. Kematangan	**Pertanyaan Tata Kelola**	**Nilai**	**Validitas Kematangan**
II	14	41	II
III	11	34	Yes
IV	1	0	No
Total	**26**	**75**	

Terakhir adalah area suplemen, yang mana area ini merupakan area baru yang ditambahkan pada Indeks KAMI versi 4.0. Area ini menilai seberapa jauh suatu organisasi dalam melakukan pengamanan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur, dan perlindungan data pribadi. Penilaian setiap kategori pada area ini dilakukan dengan cara menghitung rata-rata penilaiannya, yang mana untuk kategori pengamanan keterlibatan pihak ketiga, DPTSI memperoleh skor sebesar 0.37. Selanjutnya, untuk kategori pengamanan layanan infrastruktur awan, DPTSI memperoleh skor sebesar 0.40 serta untuk kategori perlindungan data pribadi, DPTSI memperoleh skor sebesar 0.81. Skor-skor tersebut akan

dirata-rata kembali (dengan membagi 3 skor tiap kategori) untuk mendapatkan hasil secara keseluruhan, sehingga didapatkan skor pengamanan keterlibatan pihak ketiga penyedia layanan sebesar 0.12, skor pengamanan layanan infrastruktur awan sebesar 0.13, dan perlindungan data pribadi sebesar 0.27.

Tabel 6.11 Tingkat Kelengkapan Area Suplemen

Tingkat KelengkapanArea Suplemen			
Kategori Tk. Kematangan	**Rata-Rata Pertanyaan Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**	**Rata-Rata Pertanyaan Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**	**Rata-Rata Pertanyaan Perlindungan Data Pribadi**
1	0.37	0.40	0.81
Rata-Rata Total	**0.12**	**0.13**	**0.27**

6.2 Hasil Validasi Penilaian Indeks KAMI

Validasi hasil penilaian Indeks KAMI dilakukan untuk memastikan bahwa nilai yang diberikan terhadap evaluasi Indeks KAMI sesuai dengan kondisi di lapangan, yang diketahui dari hasil wawancara, observasi, dan *review* dokumen. Validasi juga dilakukan untuk memastikan setiap poin pertanyaan Indeks KAMI dijawab oleh narasumber yang tepat. Dokumen wawancara dan observasi telah dilampirkan pada LAMPIRAN A dan hasil *review* dokumen telah dilampirkan pada Tabel 5.2. Validasi dilakukan kepada Direktur DPTSI dan KaSubdit Layanan Teknologi Informasi. Hasil validasi penilaian Indeks KAMI dapat dilihat pada bagian nilai-nilai yang mengalami perubahan, yang telah dijelaskan pada sub bab 6.1. Selain itu, daftar pemetaan poin pertanyaan Indeks KAMI dengan narasumber telah dijelaskan pada Tabel 4.1.

6.3 Analisis Akar Masalah

Berdasarkan hasil penilaian Indeks KAMI yang telah dijelaskan pada sub bab sebelumnya, dapat diketahui bahwa terdapat banyak sekali pertanyaan yang tidak bisa dijawab dengan nilai yang sempurna. Hal tersebut terjadi dikarenakan adanya masalah yang sedang dihadapi DPTSI saat ini. Masalah-masalah tersebut dapat dikategorisasi berdasarkan klausul-klausul pada ISO/IEC 27001:2013. Kemudian, dilakukan wawancara kembali terkait penyebab adanya masalah tersebut dengan menanyakan beberapa kali pertanyaan mengapa hingga jawaban dari pertanyaan mengapa sudah tidak lagi bisa ditanyakan penyebabnya. Berikut adalah tabel pemetaan pertanyaan Indeks KAMI dengan klausul ISO 27001:2013 yang dianggap sebagai kategorisasi permasalahan beserta justifikasinya.

Tabel 6.12 Kategorisasi Masalah Berdasarkan Klausul ISO 27001:2013

Klausul ISO 27001:2013	Pertanyaan Indeks KAMI 4.0	Justifikasi (Hasil Wawancara)

Konteks Organisasi	4.4
	4.6
	4.14
	4.15
	7.2.9
	7.2.10
	7.3.11
	7.3.12
	7.3.13
	7.3.15
	7.3.16
		• Tidak ada *role*/fungsi yang fokus mengurus pembuatan, pembaruan, pendokumentasian, dan mengkomunikasikan kebijakan/ prosedur
		  • Hal tersebut terjadi karena DPTSI masih fokus ke ranah operasional
		  • Selain itu tidak ada kewajiban untuk melakukan

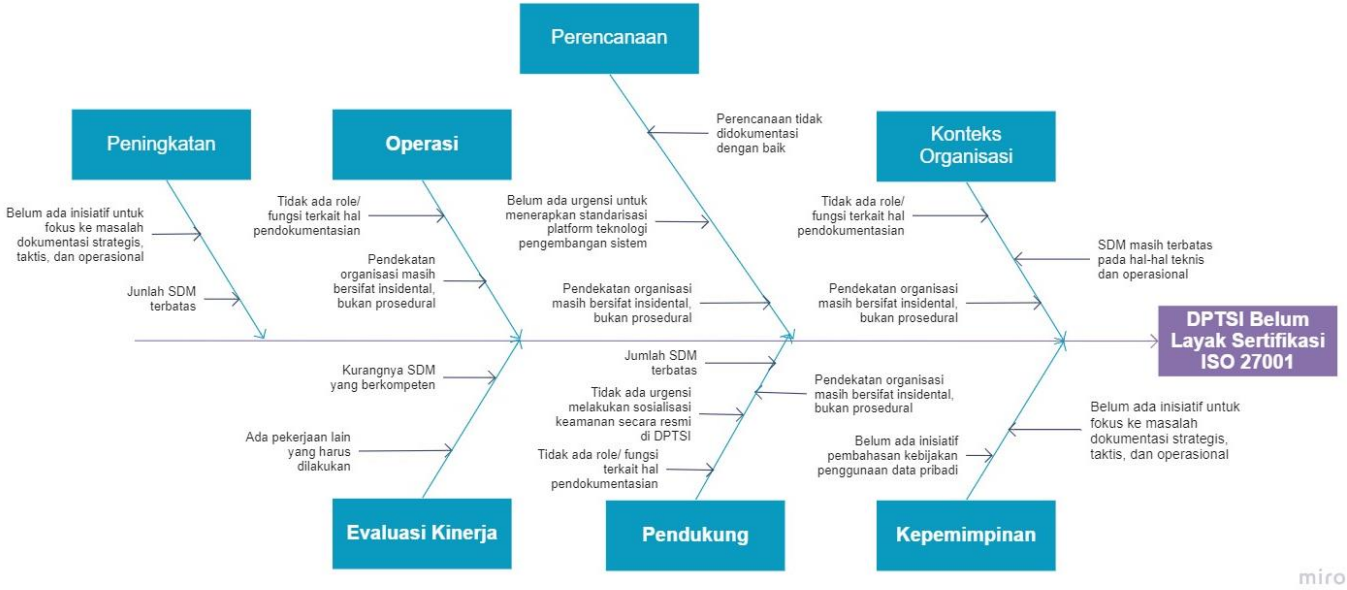
Klausul ISO 27001:2013	Pertanyaan Indeks KAMI 4.0	Justifikasi (Hasil Wawancara)
		tersebut di organisasi • Kapabilitas pegawai SubDit IKTI bukan untuk membuat SOP, sehingga bingung bagaimana cara membuatnya
Kepemimpinan	4.8 2.6 2.11 2.21 2.22 4.10 5.12 5.13 5.15 5.16 5.32 5.37 2.14 3.2 4.1 7.1.1.5 7.1.3.8 7.1.2.1 7.2.8 7.3.4 7.3.5	• Belum ada inisiatif untuk fokus membenahi masalah dokumentasi strategis, taktis, dan operasional • Belum ada inisiatif pembahasan terkait kebijakan penggunaan data pribadi • Perencanaan tidak didokumentasi dengan baik • Hal tersebut terjadi karena DPTSI masih fokus ke ranah operasional sehingga cara memecahkan masalahnya masih bersifat insidental bukan prosedural • Belum ada urgensi untuk menerapkan standarisasi platform teknologi pengembangan sistem dan standarisasi fungsi timeout pada aplikasi
Perencanaan	3.1 6.14 6.16 6.25 7.1.1.1 7.1.1.2 7.1.1.3	

Klausul ISO 27001:2013	Pertanyaan Indeks KAMI 4.0	Justifikasi (Hasil Wawancara)
	7.1.1.4	
	7.1.2.2	
	7.1.4.2	
	7.1.7.3	
	7.2.1	
	7.2.3	
	7.3.6	
	7.3.7	
	7.3.8	
Pendukung	2.4	• Jumlah SDM terbatas • Tidak ada urgensi melakukan sosialisasi keamanan informasi secara resmi di DPTSI • DPTSI masih fokus ke ranah operasional sehingga cara memecahkan masalahnya masih bersifat insidental bukan prosedural • Tidak ada *role*/fungsi yang fokus mengurus pembuatan, pembaruan, pendokumentasian, dan mengkomunikasikan kebijakan/ prosedur
	3.6	
	2.7	
	2.8	
	3.3	
	3.4	
	4.3	
	4.9	
	5.2	
	5.3	
	5.9	
	5.10	
	5.14	
	5.17	
	5.18	
	5.20	
	5.23	
	5.24	
	5.25	
	5.26	
	5.27	
	5.35	
	5.36	
	5.38	
	6.12	
	7.1.3.1	
	7.1.5.1	
	7.1.6.1	

Klausul ISO 27001:2013	Pertanyaan Indeks KAMI 4.0	Justifikasi (Hasil Wawancara)
	7.1.7.1	
	7.2.2	
	7.2.6	
	7.3.1	
	7.3.2	
	7.3.3	
	7.3.9	
Operasi	3.5	• DPTSI masih fokus ke ranah operasional sehingga cara memecahkan masalahnya masih bersifat insidental bukan procedural • Tidak ada *role*/fungsi yang fokus mengurus pembuatan, pembaruan, pendokumentasian, dan mengkomunikasikan kebijakan/ prosedur
	3.7	
	3.8	
	3.9	
	3.14	
	3.10	
	3.15	
	4.5	
	4.16	
	7.1.1.6	
	7.1.1.7	
	7.1.4.1	
	7.1.5.2	
	7.1.6.2	
	7.3.10	
Evaluasi Kerja	2.15	• Kurangnya SDM yang berkompeten • Ada pekerjaan lain yang harus dilakukan
	2.18	
	2.19	
	3.13	
	3.16	
	4.12	
	2.5	
	4.23	
	4.24	
	4.25	
	4.26	
	2.20	
	4.7	
	4.21	
	4.27	

Klausul ISO 27001:2013	Pertanyaan Indeks KAMI 4.0	Justifikasi (Hasil Wawancara)
	6.26	
	7.1.2.3	
	7.1.3.4	
	7.1.3.5	
	7.1.3.6	
	7.1.7.2	
	7.2.4	
	7.2.5	
	7.2.7	
Peningkatan	6.22	Tidak berfokus untuk menyelesaikan masalah dokumentasi strategis, taktis, dan operasional
	7.1.3.7	Jumlah SDM terbatas

Berdasarkan tabel di atas, dapat diketahui bahwa terdapat beberapa permasalahan yang menyebabkan DPTSI belum dikatakan layak dalam melakukan sertifikasi ISO 27001. Hal ini tentu menjadi pertanyaan mengapa hasil evaluasi SMKI menggunakan Indeks KAMI di tahun 2019 hanya mengalami peningkatan sebesar 3 poin, dari semula sebesar 252 berdasarkan hasil evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017 menjadi 255 di tahun 2019. Oleh karena itu, untuk mengetahui akar permasalahan ini, akan dibuat suatu diagram *ishikawa* atau juga dikenal dengan istilah diagram *fishbone*, sehingga DPTSI dapat berbenah dari berinstropeksi dengan kondisi eksisting yang ada.



Gambar 6.2 Diagram Ishikawa DPTSI

6.4 Analisis Kesenjangan

Berdasarkan hasil penilaian Indeks KAMI 4.0, dapat dilihat adanya beberapa masalah yang dihadapi DPTSI pada sub bab Analisis Akar Masalah. Sementara, pada sub bab ini akan dijelaskan dampak dari adanya masalah-masalah pada DPTSI, yaitu DPTSI yang belum layak untuk melakukan sertifikasi ISO 27001, yang dikarenakan masih banyaknya kesenjangan penerapan SMKI di DPTSI terhadap *annex* ISO/IEC 27001:2013.

Apabila pada kolom *checked* telah terisi Y, maka DPTSI telah menerapkan sepenuhnya salah satu persyaratan pada ISO/IEC 27001:2013 yang dirupakan dalam bentuk pertanyaan di Indeks KAMI. Namun, apabila masih terisi QY, maka DPTSI hanya menerapkan sebagian, sementara N berarti DPTSI masih belum menerapkan sama sekali.

Berdasarkan hasil analisis kesenjangan yang telah dilakukan, dapat dilihat pada kolom *checklist* bertanda Y adalah sebesar 56 poin, QY sebesar 29 poin, dan N sebesar 93. Tabel yang menjelaskan analisis kesenjangan SMKI di DPTSI telah terlampir pada LAMPIRAN C.

6.5 Hasil Validasi *Mapping* ke *Expert*

Tujuan dari melakukan validasi pemetaan Indeks KAMI terhadap ISO/IEC 27001:2013 adalah untuk memastikan bahwa pemetaan telah dilakukan dengan benar, mengingat inti dari pengerjaan Tugas Akhir ini adalah untuk melakukan analisis kesenjangan. Oleh karena itu, perlu dilakukan validasi kepada seorang *expert*. Seperti yang telah dijelaskan pada bab 3, seorang *expert* adalah seseorang yang telah tersertifikasi ISO/IEC 27001, yaitu Rahadian Bisma, S.Kom, M.Kom, ITILF, ISO27001:2013.

Luaran dari validasi *mapping* ke *expert* adalah tabel analisis kesenjangan. Sebelum dilakukan validasi, bentuk awal tabel analisis kesenjangan merupakan pemetaan poin pertanyaan Indeks KAMI terhadap klausul utama ISO/IEC 27001:2013 beserta *checklist* yang berisikan Y (*yes*) apabila poin pertanyaan

indeks KAMI telah dipenuhi secara maskimal, QY (*qualified yes*) apabila masih dalam perencanaan atau diterapkan sebagian, dan N (*no)* apabila tidak dilakukan sama sekali. Namun, setelah dilakukan validasi ke *expert* ternyata pemetaan tersebut masih kurang tepat dikarenakan Indeks KAMI hanya memiliki hubungan dengan klausul Annex ISO/IEC 27001:2013 saja, bukan klausul utamanya.

Oleh karena itu, dilakukan perubahan bentuk tabel analisis yang memetakan poin pertanyaan Indeks KAMI terhadap klausul Annex ISO/IEC 27001:2013. Pemetaan juga dilakukan dengan mengacu kepada referensi yang telah terlampir pada Gambar 2.7. Dengan demikian, tabel *mapping* Indeks KAMI terhadap klausul Annex ISO/IEC 27001:2013 yang kemudian akan menjadi hasil analisis kesenjangan yang terlampir pada LAMPIRAN C dapat dikatakan telah *valid*.

6.6 Penyusunan Rekomendasi Perbaikan

Penyusunan rekomendasi perbaikan dilakukan berdasarkan hasil *checklist* analisis kesenjangan. *Checklist* tersebut berisi pemetaan Indeks KAMI 4.0 terhadap klausul *annex* dari ISO/IEC 27001:2013. Rekomendasi perbaikan akan dilakukan pada bagian yang masih belum terpenuhi yang mana masih terdapat kesenjangan (kolom *checked* masih berisi QY dan N). Selain itu, DPTSI tetap harus memperhatikan klausul utama dari ISO/IEC 27001:2013, di samping memperhatikan rekomendasi perbaikan dari klausul *annex*-nya. Hal tersebut dilakukan karena organisasi yang ingin melakukan sertifikasi ISO 27001 harus memenuhi seluruh komponen pada ISO/IEC 27001:2013, baik klausul utama maupun klausul *annex.*

BAB 7
KESIMPULAN DAN SARAN

Bab ini merupakan bab penutup dari dokumen Tugas Akhir ini. Pada bab ini, akan dijelaskan kesimpulan dari Tugas Akhir yang telah dikerjakan oleh penulis serta saran-saran penulis bagi penelitian selanjutnya.

7.1 Kesimpulan

Berdasarkan pengerjaan Tugas Akhir yang telah tertuang dari Bab 1 hingga Bab 6, terdapat beberapa hal yang dapat menjadi sorotan utama. Berikut adalah penjabaran dari kesimpulan penulisan Tugas Akhir.

- Berdasarkan penilaian Indeks KAMI 4.0 yang dilakukan dalam penelitian ini, skor dari Kategori Sistem Elektronik dari DPTSI mencapai 31 dari total keseluruhan sebesar 48. Hal tersebut mengindikasikan bahwa tingkat ketergantungan DPTSI terhadap Sistem Elektronik masuk ke dalam kategori tinggi. Selain itu, untuk hasil penilaian 5 area Indeks KAMI, DPTSI mencapai 255 dari total keseluruhan sebesar 645. Poin tersebut hanya meningkat sebanyak 3 poin berdasarkan evaluasi Indeks KAMI yang pernah dilakukan di tahun 2017. Berdasarkan penilaian Indeks KAMI, dapat dilihat bahwa tingkat kematangan penerapan SMKI di DPTSI masih berada di level I-II yang mana masih menerapkan kerangka kerja dasar dan operasional.
- Berdasarkan hasil *checklist* pemetaan Indeks KAMI 4.0 terhadap ISO 27001, dapat dilihat bahwa kolom *checklist* berlabel Y hanya dipenuhi sebesar 56 poin, sementara kolom QY adalah sebesar 29 poin, dan kolom N sebesar 93 poin. *Checklist* berlabel Y tidak mencapai 50% dari total keseluruhan poin pertanyaan Indeks KAMI 4.0 menandakan DPTSI perlu melakukan banyak perbaikan.
- Penilaian Indeks KAMI merupakan turunan dari ISO/IEC 27001:2013 klausul *annex* saja. Apabila penilaian untuk bagian *annex* saja masih belum maksimal, maka DPTSI

dikatakan sangat tidak siap untuk melakukan sertifikasi ISO 27001, sebab masih ada klausul utama dari ISO/IEC 27001:2013 yang juga harus dipenuhi oleh organisasi yang ingin melakukan sertifikasi ISO 27001.

- DPTSI harus melaksanakan seluruh rekomendasi perbaikan yang mengacu pada bagian a*nnex* ISO/IEC 27001:2013 seperti yang telah terlampir pada LAMPIRAN D tanpa melupakan klausul utamanya untuk dapat melakukan sertifikasi ISO 27001.

7.2 Saran

Saran yang bisa diberikan penulis bagi penelitian selanjutnya yang terkait dengan melakukan analisis kesenjangan Sistem Manajemen Keamanan Informasi di DPTSI menggunakan Indeks KAMI 4.0 adalah sebagai berikut:

- Sebaiknya peneliti selanjutnya mengikuti bimbingan teknis penggunaan Indeks KAMI 4.0 untuk membantu dalam memahami cara penggunaan *tool* ini
- Sebaiknya peneliti selanjutnya dapat lebih memahami setiap poin pertanyaan, sehingga dapat melakukan evaluasi yang lebih detail berdasarkan poin-poin yang diminta dalam setiap pertanyaan pada Indeks KAMI 4.0
- Sebaiknya peneliti selanjutnya tidak hanya memberikan rekomendasi perbaikan berdasarkan klausul *annex* ISO/IEC 27001:2013, tapi juga dapat mencantumkan rekomendasi perbaikan yang mengacu ke klausul utama ISO/IEC 27001:2013

DAFTAR PUSTAKA

[1] A. S. Perdana, “Sistem Informasi Berdasarkan Standar Iso / Iec Pmbok (Studi Kasus Direktorat Pengembangan Teknologi Dan Sistem Informasi (Dptsi) Its) Assessment and Mitigation of Security Risk of Information System Based on Iso / Iec 27001 : 2013 Standard Using Pmbok,” p. 281, 2018.

[2] A. Basyarahil, Firzah, “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,” 2013.

[3] C. Chazar and A. Ramdani, “Model perencanaan keamanan sistem informasi menggunakan pendekatan metode octave dan iso 27001:2005,” *Semin. Nas. Telekomun. dan Inform. (SELISIK 2016)*, no. Selisik, pp. 80–85, 2016.

[4] “What is ISO 27001? - Definition from WhatIs.com.” [Online]. Available: https://whatis.techtarget.com/definition/ISO-27001. [Accessed: 29-Mar-2019].

[5] S. Manajemen and K. Informasi, “Panduan Penerapan,” no. September, 2017.

[6] “Masterplan ICT - DPTSI.” [Online]. Available: https://www.its.ac.id/dptsi/masterplan-ict/. [Accessed: 21-Dec-2019].

[7] Adityaputri, Alitya Novianda, "Analisis Kesenjangan Kualitas Layanan Teknologi Informasi Berdasarkan Perspektif Pengguna dan Penyedia Layanan (Layanan TIK DPTSI ITS)". 2017.

[8] “Indeks KAMI | bssn.go.id.” [Online]. Available: https://bssn.go.id/indeks-kami/. [Accessed: 16-May-2019].

[9] Departemen Sistem Informasi ITS, “Roadmap Laboraorium 2018 - 2022,” Surabaya, 2017.

[10] A. Fitriansyah and H. Budiarto, “Tata kelola keamanan informasi berbasis iso/iec 27001:2005,” vol. VIII, no. 02, pp. 18–32, 2012.

[11] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, “Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018.

[12] R. Fauzi, “Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002,” *J. Teknol. Rekayasa*, vol. 3, no. 2, p. 145, 2018.

[13] “ISO/IEC 27001 Information security management.” [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed: 29-Mar-2019].

[14] “Penerapan ISO 27001 : 2013 Sistem Manajemen Keamanan Informasi DCN & DCO GSIT BCA,” 2017.

[15] E. Kurniawan and I. Riadi, “Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM,” *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 2, no. 1, p. 12, 2018.

[16] “ISO 27001 gap analysis vs. risk assessment.” [Online]. Available: https://advisera.com/27001academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment/. [Accessed: 31-May-2019].

[17] “What exactly is an ISO 27001 gap analysis, anyway? - IT Governance Blog.” [Online]. Available: https://www.itgovernance.co.uk/blog/what-exactly-is-an-iso-27001-gap-analysis-anyway. [Accessed: 31-May-2019].

[18] T. Iso, I. E. Commission, and T. Isms, “An Overview of ISO / IEC 27000 family of Information Security Management System Standards An Overview of ISO / IEC 27000 family of Information Security Management System Standards,” vol. 2015, no. November, pp. 1–10,

2018.

[19] A. T. Informasi, M. Manajemen, and T. Its, “malware , spam , spoofing , sniffing),” pp. 2013–2016, 2015.

[20] Candiwan, “Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia,” no. 1, pp. 50–58, 2014.

[21] Muhammad Bakri and Nia Irmayana, “Analisis dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001,” *Teknokompak*, vol. 11, no. 2, pp. 41–44, 2017.

[22] “Home page - Mirosław Dąbrowski.” [Online]. Available: https://miroslawdabrowski.com/. [Accessed: 16-May-2019].

[23] N. Ibrachim *et al.*, “Bakuan Audit Keamanan Informasi Kemenpora,” *Bakuan Audit Keamanan Inf. Kemenpora*, p. 98 + xii, 2012.

“Halaman ini sengaja dikosongkan”

BIODATA PENULIS

Resti Nisaidha Rahmi, adalah anak ke-3 dari tiga bersaudara, lahir di Surabaya, 6 April 1998. Riwayat pendidikan yang pernah ditempuh penulis di antaranya SDN Margorejo I/403 Surabaya, SMPN 1 Surabaya, dan SMAN 9 Surabaya. Setelah itu, penulis masuk Departemen Sistem Informasi ITS melalui Jalur SNMPTN. Penulis pernah mengikuti beberapa kegiatan, yakni Drum Band "Gita Siswa Anoraga" pada saat duduk di bangku SD dan meraih Juara 1 pada Lomba Unjuk Gelar, *Pop Group* Spensa saat duduk di bangku SMP dan mendapatkan Juara 2 DETCON *Pop Group Competition*, menjadi anggota OSIS ketika duduk di bangku SMA, serta pernah menjuarai beberapa perlombaan, yakni Juara 3 Lomba Karya Tulis Ilmiah tingkat kota yang diselenggarakan oleh BLH Surabaya dan Juara 2 Olimpiade Koperasi tingkat kota yang diselenggarakan oleh Dinas Koperasi Surabaya. Selama perkuliahan, penulis juga aktif menjadi panitia ISE! 2016 dan ISE! 2017, menjadi pengurus Himpunan Sistem Informasi (HMSI) dengan posisi terakhir Vice Head I. Selain itu, penulis merupakan salah satu penerima beasiswa Bank Indonesia pada tahun 2018/2019. Selanjutnya, penulis memutuskan untuk mengerjakan Tugas Akhir yang berkaitan dengan laboratorium MSI. Untuk kepentingan penelitian penulis, silahkan menghubungi restinisaidharahmi@gmail.com.

LAMPIRAN A

Instrumen Wawancara dan Hasil Penilaian Indeks KAMI 4.0

Form Wawancara Kategori Sistem Elektronik

Hari/ Tanggal : Selasa, 5 November 2019
Pukul : 11.56 WIB
Lokasi : SI-4202 dan Ruang DPTSI
Narasumber : Hanim Maria Astuti, S.Kom, M.Sc, ITIL dan
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
Jabatan : Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi
Direktur DPTSI

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
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	1	Status: B Skor: 2	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	[C] Kurang dari Rp.3 Miliar				
	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				
	Perubahan/ Tambahan Nilai investasi yang dikeluarkan oleh DPTSI untuk pengadaan barang Sistem Elektronik pada tahun 2019 adalah > Rp 10 Miliar Bukti telah terlampir pada Lampiran B (Gambar B.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	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	Temuan Untuk anggaran operasional terkait pengelolaan sistem elektronik DPTSI ITS tahun 2019 masih memiliki nilai yang sama seperti tahun 2016, yaitu mencapai lebih dari 3 miliar				
	Bukti Daftar anggaran untuk operasional Sistem Elektronik adalah sebanyak ± 3 miliar Bukti telah terlampir pada Lampiran B (Gambar B.1)				
	Perubahan/ Tambahan -				
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	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
	Temuan				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	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 2010 tentang pengadaan barang/jasa pemerintah yang ketentuan teknis operasionalnya diatur oleh Peraturan Kepala LKPP Nomor 2 Tahun 2010 tentang Layanan pengadaan Secara Elektronik. Selain itu, DPTSI ITS juga mengacu pada POB, yaitu aturan yang dikeluarkan oleh ITS mengenai pengelolaan aset, yaitu Peraturan Rektor No. 12/ 2018				
	Bukti Website LPSE yang sudah bekerja sama dengan ITS dapat diakses pada alamat http://www.lpse.its.ac.id/eproc4# Penjelasan tentang peraturan LPSE sendiri dapat diakses pada https://jdih.lkpp.go.id/ Peraturan Rektor ITS No. 12/2018 Bukti telah terlampir pada Lampiran B (Gambar B.2 dan Gambar B.3)				
	Perubahan/ Tambahan -				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	C	1	Status: B Skor: 2	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan Tidak digunakan algoritma khusus untuk keamanan informasi dalam sistem elektronik yang digunakan				
	Bukti Tidak Ada				
	Perubahan/ Tambahan Adanya teknik kriptografi yang yang diterapkan pada sistem yang dikembangkan oleh DPTSI dengan menggunakan standar OpenID				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
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	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
	Temuan Jumlah pengguna sistem elektronik yang dikembangkan oleh DPTSI dapat dilihat dari jumlah mahasiswa ITS tahun 2018/2019 yaitu sebesar 22.158 orang dan jumlah dosen tetap yang mencapai 986 orang.				
	Bukti Pangkalan Data Pendidikan Tinggi Kemenristek Dikti yang tercantum dalam website yang beralamatkan https://forlap.ristekdikti.go.id/perguruantinggi/detail/ Bukti telah terlampir pada Lampiran B (Gambar B.4 dan Gambar B.5)				
	Perubahan/ Tambahan -				
1.6	Data pribadi yang dikelola Sistem Elektronik	A	5	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	[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				
	Temuan Data pribadi yang dikelola Sistem Elektronik memiliki keterkaitan dengan data pribadi lainnya, sebagai contoh data pribadi pada Integra, pada SIM Akademik terdiri dari data nilai mahasiswa, data ekivalensi, dan biaya pendidikan yang memiliki hubungan dengan SIM Beasiswa yang terdiri dari data mahasiswa, gaji orangtua, dan biaya pendidikan				
	Bukti Bukti telah terlampir pada Lampiran B (Gambar B.6)				
	Perubahan/ Tambahan -				
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif	B	2	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/atau Terbatas [C] Biasa				
	Temuan Data yang dikelola DPTSI ada yang bersifat rahasia, seperti data pada Integra, ShareITS, dan unduh aplikasi berlisensi yang mana hanya mahasiswa/ dosen yang bersangkutan yang dapat mengakses Integra menggunakan akun *user* yang telah dimiliki (harus login).				
	Bukti Data bersifat rahasia: https://integra.its.ac.id/ http://share.its.ac.id/ https://unduh.its.ac.id/ Bukti telah terlampir pada Lampiran B (Gambar B.7)				
	Perubahan/ Tambahan				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	-				
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 hanya berdampak pada bisnis perusahaan	B	2	Status: A Skor: 5	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	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				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	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 langsung pada layanan publik yang diberikan ITS. Akibat dari tidak bisa *login* Integra maka tidak bisa juga *login* ke akun lainnya dan tidak bisa tersambung ke internet yang ada di ITS karena akun Integra digunakan sebagai portal *single sign-on* Bukti telah terlampir pada Lampiran B (Gambar B.8 dan B.9)				
	Perubahan/ Tambahan Secara garis besar, Sistem Elektronik yang disediakan DPTSI terdiri dari SIM Keuangan dan SIM Non-Keuangan. Pada dasarnya, SIM Keuangan diperuntukkan hanya untuk dosen/ karyawan ITS yang hanya bisa diakses oleh jaringan lokal ITS atau menggunakan VPN, yang mana data tersebut bukanlah data yang bersifat kritis, sehingga penyerangan/ penerobosan terhadap sistem tersebut tidak begitu besar. Sementara, untuk SIM Non-Keuangan seperti Integra, sistem tersebut dipakai oleh mahasiswa dan dosen, yang mana data yang berada di dalamnya bersifat sangat kritis, sehingga apabila terjadi penyerangan dalam sistem tersebut maka dapat menimbulkan dampak yang besar yang bersifat secara langsung terhadap layanan **Bukti**				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	Adanya kejadian mahasiswa dapat membobol akun Integra sehingga dapat melakukan Perubahan/ Tambahan nilai dari mahasiswa tersebut. Hal ini tentu akan memberi dampak secara langsung terhadap layanan publik yang disediakan oleh DPTSI				
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	A	5	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
	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 Peraturan Rektor No. 10 Tahun 2016 yang menjabarkan pengesahan ITS sebagai Perguruan Tinggi Negeri Badan Hukum (PTNBH) yang didukung dengan berbagai macam Undang-Undang Negara Republik Indonesia				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	Bukti telah terlampir pada Lampiran B (Gambar B.10)				
	Perubahan/ Tambahan -				
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 mengakibatkan kerugian finansial)	C	1	x	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
	Temuan Dampaknya hanya mengganggu proses bisnis organisasi dan tidak sampai membahayakan jiwa. Dampak mengenai finansial masih belum dipengaruhi hingga saat ini.				
	Bukti				

Bagian I: Kategori Sistem Elektronik					
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis					
No.	**Pertanyaan Kategori Sistem Elektronik**	**Status**	**Skor**	**Pembaruan**	**Narasumber**
	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				
	Perubahan/ Tambahan -				
Skor Penetapan Kategori Sistem Elektronik			**31 (Tingkat Ketergantungan: Sangat Tinggi)**		

Form Wawancara Kategori Tata Kelola Keamanan Informasi

Hari/ Tanggal : Selasa, 29 Oktober 2019
Pukul : 10.12 WIB
Lokasi : Ruang DPTSI
Narasumber : Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
Jabatan : Direktur DPTSI
Kepala SubDirektorat Infrastruktur dan Keamanan Teknologi Informasi

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan	Sudah dijalankan	Diterapkan Secara Menyeluruh	3		Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?					
	Temuan Direktur DPTSI memiliki peran dan tanggung jawab dalam melaksanakan program keamanan informasi yang tercantum dalam Peraturan Rektor ITS No.10/ 2016. Namun di dalam peraturan tersebut masih belum dijelaskan peran dan tanggungjawab seorang pimpinan secara eksplisit dalam program keamanan informasi di DPTSI							
	Bukti Berdasarkan Peraturan Rektor ITS No. 10/ 2016 Pasal 62, Direktur DPTSI bertanggung jawab pada Wakil Rektor III yang bertugas untuk menyelenggarakan perumusan dan pelaksanaan kebijakan dalam bidang teknologi dan sistem informasi Bukti telah terlampir pada Lampiran B (Gambar B.10)							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Perubahan/ Tambahan Disampaikan juga oleh narasumber bahwa peran pimpinan DPTSI dibuktikan dengan adanya sebagian staf yang akan mengikuti pelatihan program keamanan informasi							
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Sudah ada bagian khusus yang menangani yaitu bagian infrastruktur & keamanan, namun tidak terlalu dispesifikkan untuk perorangan	Diterapkan Secara Menyeluruh	3	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan DPTSI sudah memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya, yang diampu oleh Sub Direktorat Infrastruktur dan Keamanan Informasi (IKTI)							
	Bukti Struktur organisasi DPTSI yang membawahi Sub Direktorat Infrastruktur dan Keamanan Informasi (IKTI) Bukti telah terlampir pada Lampiran B (Gambar B.10 dan Gambar B.11)							
	Perubahan/ Tambahan -							
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai	Wewenang dibagi kedalam bagian listrik, jaringan, dan	Diterapkan Secara	3	x	Dr. Eng. Febriliyan Samopa,

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	sistem namun tidak ada tugas khusus dan tidak dilakukan pengkotakan bagian secara tertulis dan paten	Menyelu ruh			S.Kom, M.Kom
	Temuan Pelaksana pengamanan informasi mempunyai hak untuk melakukan penerapan dan penjaminan terhadap kepatuhan program keamanan informasi							
	Bukti Pasal 64 Peraturan Rektor ITS No. 10/ 2016 telah menjabarkan Tupoksi bagian Sub Direktorat Infrastruktur dan Keamanan Informasi							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti telah terlampir pada Lampiran B (Gambar B.10)							
	Perubahan/ Tambahan -							
2.4	II	1	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 karena hanya terdiri dari 8 orang saja	Tidak Dilakukan	0	Status: Dalam Perencanaan Skor: 1	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Alokasi sumber daya dalam bentuk uang sudah cukup, namun untuk 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. Per tanggal 1 November 2019 akan ada tambahan pegawai sebanyak 4 orang dikarenakan untuk menggantikan pegawai yang keluar sebanyak 2 orang. Bukti telah terlampir pada Lampiran B (Gambar B.12)							
	Perubahan/ Tambahan Adanya rencana untuk mengalokasikan sumber daya baru ke dalam Sub Direktorat IKTI							
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap,	Belum ada pemetaan secara tertulis dan tidak	Tidak Dilakukan	0	Status: Dalam Penerapan/	Royyana Muslim Itjihadie, S.Kom,

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	dilakukan audit internal			Diterapkan Sebagian Skor: 2	M.Kom, Ph.D
	Temuan Tidak dilakukan segregasi kewenangan dan rencana kebutuhan audit internal							
	Bukti Tidak Ada							
	Perubahan/ Tambahan Saat ini sudah ada pemetaan kewenangan dan segregasi, namun tidak ada dokumen tertulis							
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan	Untuk staff ada standar kompetensi khusus namun	Tidak Dilakuka n	0	Status: Dalam Perencanaan	Dr. Eng. Febriliyan Samopa,

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	tidak ada secara tertulis			Skor: 1	S.Kom, M.Kom
	Temuan Belum ada standar kompetensi yang harus dimiliki staff Sub Direktorat Infrastruktur dan Keamanan Informasi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan Sedang mengajukan standar kompetensi keahlian pelaksana pengelolaan keamanan informasi ke Biro Umum Bagian Kepegawaian dan Wakil Rektor 3, namun masih belum ada dokumen resmi secara tertulis							
2.7	II	1	Apakah semua pelaksana pengamanan informasi di	Kompetensi yang dimiliki sudah cukup	Tidak Dilakuka n	0	Status: Dalam Perencanaan	Dr. Eng. Febriliyan Samopa,

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	baik namun kembali lagi bahwa tidak ada persyaratan secara tertulis			Skor: 1	S.Kom, M.Kom Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	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							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Perubahan/ Tambahan Kompetensi/ keahlian pelaksana cukup memadai, namun untuk standar kompetensi masih diajukan ke Biro Umum Bagian Kepegawaian dan Wakil Rektor 3							
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Belum pernah ada sosialisasi secara resmi namun untuk semua pihak sudah paham dan sadar akan keamanan informasi di instansi	Tidak Dilakuka n	0	Status: Dalam Penerapan/ Diterapkan Sebagian Skor: 2	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan Sosialisasi tidak dilakukan secara resmi karena dianggap semua SDM di DPTSI ITS sudah paham tentang keamanan informasi							
	Bukti Tidak ada							
	Perubahan/ Tambahan DPTSI sudah melakukan sosialisasi hanya ke bagian admin IT di setiap unit dan ke perwakilan setiap departemen, meskipun sosialisasi tersebut tidak secara resmi							
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan	Dilakukan beberapa pelatihan yang dirasa penting dan terkait keamanan.	Diterapkan Secara Menyeluruh	6	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			petugas pelaksana pengelolaan keamanan informasi?	Tahun 2016 ini dilakukan pelatihan tentang *honeypot* yang diadakan oleh Kominfo bagi beberapa staff infrastruktur				
	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							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti telah dilampirkan pada Lampiran B (Gambar B.13)							
	Perubahan/ Tambahan Tahun 2019 ini pegawai DPTSI telah diikutkan *training* keamanan siber ID SIRTII (Indonesia-Security Incident)							
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Integrasi dilakukan di bagian internet dan intranet. Namun tidak ada pengamanan khusus pada intranet	Diterapkan Secara Menyeluruh	6	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan Integrasi pengamanan informasi dilakukan pada bagian internet dan intranet yang ada di ITS							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan	Belum ada identifikasi data pribadi sesuai undang-undang. Belum ada penerapan perundang-undangan	Tidak Dilakuka n	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			perundangan yang berlaku?					
	Temuan Tidak ada undang-undang yang digunakan terkait pendefinisian data pribadi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan	Ada koordinasi dengan pihak lain yang terkait namun masih belum ada dokumen	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			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?	yang resmi untuk hal tersebut				
	Temuan Dilakukan koordinasi dengan pihak pengguna aset yang berkepentingan. Koordinasi dapat dilakukan melalui email untuk pihak eksternal dan melalui chat untuk pihak internal ITS							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti Selalu dilakukan koordinasi dengan pihak eksternal malalui e-mail untuk dilakukan pertukaran informasi dan penyelesaian masalah mulai dari awal hingga akhir Bukti telah terlampir pada Lampiran B (Gambar B.14)							
	Perubahan/ Tambahan Koordinasi dengan pihak internal untuk menyelesaikan permasalahan juga dibahas dalam rapat internal DPTSI							
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang	Proaktif dilakukan. Biasanya dengan pihak ISP dan ke bagian developer jika ada masalah di	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	aplikasi yang dibuat				
	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 e-mail untuk dilakukan pertukaran informasi dan penyelesaian masalah mulai dari awal hingga akhir masalah ditutup							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti telah terlampir pada Lampiran B (Gambar B.14)							
	Perubahan/ Tambahan -							
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?	Belum ada dokumen BCP dan DRP secara formal	Tidak Dilakuka n	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan Rancangan dan pelaksanaan BCP dan DRP dilakukan permasing-masing bagian namun tidak ada dokumentasi secara formal							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program	Dilakukan pelaporan ke kepala instansi secara rutin. Bisa setiap hari, mingguan, dan	Diterapkan Secara Menyeluruh	6	Status: Dalam Penerapan/ Diterapkan sebagian Skor: 4	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	bulanan namun untuk dokumen pelaporan secara tertulis masih belum ada				
	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 telah terlampir pada Lampiran B (Gambar B.15)							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Perubahan/ Tambahan Penanggungjawab pengelolaan tidak melakukan pelaporan secara rutin. Pelaporan yang dilakukan baru bersifat ad hoc, yaitu apabila ada insiden saja serta pelaporan tiap tahun yang tidak resmi							
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Dibahas sebelum mengambil keputusan karena memang kamanan informasi sangat penting. Seperti misalnya mengeluarkan	Diterapkan Secara Menyeluruh	6	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
				kebijakan terkait email untuk menghindari risiko-risiko				
	Temuan Diutamakan tentang keamanan informasi saat dilakukan rapat. Untuk saat ini telah ditetapkan kebijakan tentang e-mail							
	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. Selain itu ada kebijakan strategis dari DPTSI ITS yang menghasilkan ketentuan portal S*ingle-Sign On* Bukti telah terlampir pada LAMPIRAN B (Gambar B.8 dan Gambar B.16)							
	Perubahan/ Tambahan							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Dibuatnya kebijakan penggunaan portal *Single-Sign On*							
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak dilakukan penerapan program khusus	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan Belum ada program khusus untuk keamanan informasi							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran,	Tidak ada parameter dan pengukuran untuk kinerja pengelolaan keamanan	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			pelaksananya, pemantauannya, dan eskalasi pelaporannya?					
	Temuan Belum dilakukan pendefinisian parameter dan pengukuran kinerja pengelolaan keamanan informasi							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan	Tidak ada program untuk melakukan penilaian kinerja	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	pengelolaan keamanan				
	Temuan Belum dilakukan penilaian kinerja staff keamanan informasi secara individu							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan	Tidak ada target dan sasaran khusus	Tidak Dilakuka n	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?					
	Temuan Belum dilakukan penerapan target dan sasaran keamanan informasi diberbagai area lain yang relevan dan belum dilakukan langkah perbaikannya							
	Bukti							

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Tidak ada							
	Perubahan/ Tambahan -							
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak ada perangkat hukum yang digunakan untuk keamanan informasinya	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan Tidak ada perangkat hukum yang dijadikan patokan untuk keamanan informasi							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut	Tidak ada kebijakan khusus yang diterapkan	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian II: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			pelanggaran hukum (pidana dan perdata)?					
	Temuan Belum ada kebijakan terkait penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							
Total Nilai Evaluasi Tata Kelola				**49**				

Form Wawancara Pengelolaan Risiko Keamanan Informasi

Hari/ Tanggal : Kamis, 31 Oktober 2019
Pukul : 11.00 WIB
Lokasi : Ruang DPTSI
Narasumber : Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
Jabatan : Kepala Sub Direktorat Infrastruktur dan Keamanan Informasi

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Belum ada pengelolaan risiko secara tertulis dan resmi	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan Belum ada proker terkait pengelolaan risiko apalagi pendokumentasianya							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan	Masih belum ada penanggung jawab risiko yang ditugaskan khusus	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			informasi sampai ke tingkat pimpinan?					
	Temuan Belum ada bagian yang bertugas khusus menangani manajemen risiko dan pengelolaannya							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi	Belum ada, masih perencanaan untuk menggunakan ISO 27001	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			dan secara resmi digunakan?					
	Temuan Belum digunakan *framework* khusus terkait pengelolaan risiko keamanan informasi							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan	Masih belum ada karena kerangka kerjanya masih belum diterapkan	Tidak Dilakukan	0		Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?					
	Temuan Belum digunakan *framework* khusus terkait pengelolaan risiko keamanan informasi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang	Ada catatan risiko yang diterima, dicatat di dalam log	Diterapkan Secara Menyeluruh	3	Status: Dalam Penerapan/ Diterapkan Sebagian	Royyana Muslim Itjihadie, S.Kom,

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			batas tingkat risiko yang dapat diterima?	sensor ids terkait upaya masuk dari pihak yang tidak berhak			Skor: 2	M.Kom, Ph.D
	Temuan Sudah ada ambang batas tingkat risiko yang direkap dalam *log* sensor, dimana ITS menggunakan AlienVault sebagai aplikasi untuk keperluan melakukan monitoring jaringan, HIDS, dan NIDS untuk memantau serangan dari luar instansi							
	Bukti *Log sensor* selalu dipantau setiap harinya dan jika ada ada yang aktivitas yang mencurigakan maka akan dilakukan blok oleh admin Bukti telah terlampir pada LAMPIRAN B (Gambar B.15)							
	Perubahan/ Tambahan Namun tidak ada dokumentasi penetapan ambang batas risiko							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
3.6	II	1	Apakah instansi/perusahaan 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	Diterapkan Secara Menyeluruh	3	Status: Dalam Penerapan/ Diterapkan Sebagian Skor: 2	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Dalam daftar aset informasi yang dimiliki oleh DPTSI ITS terdaftar seluruh aset informasi yang dimiliki beserta pihak-pihak yang bertanggung jawab							
	Bukti							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Dalam daftar aset terdapat kolom kepemilikan dimana semua berisi milik DPTSI dan ada bagian pengelola aset informasi yang bertanggung jawab Bukti telah terlampir pada LAMPIRAN B (Gambar B.17)							
	Perubahan/ Tambahan -							
3.7	II	1	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	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Untuk ancaman dan kelemahan yang terkait dengan aset informasi belum diidentifikasi dan dicatat dalam dokumen risiko keamanan informasi							
	Bukti							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Tidak ada							
	Perubahan/ Tambahan -							
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Sudah ada dampak yang dipikirkan dan juga langkah-langkah mitigasinya	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Dampak dari kerugian terkait terganggunya fungsi aset utama tidak diidentifikasikan dan tidak ada pendokumentasian							
	Bukti Tidak ada							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Perubahan/ Tambahan -							
3.9	II	1	Apakah instansi/perusahaan 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	Sudah ada kajian risiko saat rapat dibahas biasanya, seperti saat rilis layanan baru itu harus diketahui *performance* keamanannya dan akhirnya dilakukan balancing dan penerapan	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			program pengelolaan keamanan informasi)?	firewall. Namun untuk dokumennya memang masih belum ada				
	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							
	Perubahan/ Tambahan -							
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan	Saat memikirkan risiko yang akan terjadi	Diterapkan Secara Menyeluruh	3	Status: Dalam Penerapan/ Diterapkan	Royyana Muslim Itjihadie, S.Kom,

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			penanggulangan risiko yang ada?	otomatis juga langsung dipikirkan langkah mitigasinya			Sebagian Skor: 2	M.Kom, Ph.D
	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 telah terlampir pada LAMPIRAN B (Gambar B.18)							
	Perubahan/ Tambahan -							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
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?	Untuk dokumentasi masih belum ada namun tingkat prioritasnya berdasarkan *urgency*nya. Biasanya yang harus dipulihkan cepat itu terkait data user dan infrastruktur	Diterapkan Secara Menyeluruh	6	Status: Dalam Penerapan/ Diterapkan Sebagian Skor: 4	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Penyelesaian risiko diprioritaskan berdasarkan tingkat kepentingannya. Hal yang diprioritaskan adalah risiko terkait dengan data user dan infrastruktur penting, seperti server							
	Bukti Tidak Ada							
	Perubahan/ Tambahan Tidak ada dokumentasi prioritas risiko, meskipun sudah ada penerapan pemulihan terkait data user dan infrastruktur biasanya menjadi proritas							
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak dilakukan secara resmi, biasanya dibahas melalui grup chat	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan							

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	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 telah terlampir pada LAMPIRAN B (Gambar B.14)							
	Perubahan/ Tambahan -							
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Masih belum dilakukan evaluasi secara terukur	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan Tidak dilakukan evaluasi terhadap mitigasi yang telah dijalankan sebelumnya							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
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/ Tambahan kondisi	Tidak dilakukan pengkajian ulang terhadap profil risiko dan bentuk mitigasinya , karena mitigasi yang biasanya	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			yang signifikan atau keperluan penerapan bentuk pengamanan baru?	dilakukan sudah dianggap baik dan membantu menyelesaikan masalah				
	Temuan Tidak dilakukan pengkajian ulang terhadap profil risiko dan bentuk mitigasinya , karena mitigasi yang biasanya dilakukan sudah dianggap baik dan membantu menyelesaikan masalah							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji	Tidak, karena belum ada kerangka kerja	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie,

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			untuk memastikan/meningkatkan efektifitasnya?					S.Kom, M.Kom, Ph.D
	Temuan Tidak ada kerangka kerja pengelolaan risiko yang digunakan							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak dimasukkan sebagai kriteria penilaian kinerja pengamanan	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian III: Tata Kelola Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Temuan Pengelolaan risiko tidak dijadikan bagian dari kriteria penilaian kinerja pengamanan yang ada di DPTSI							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
Total Nilai Evaluasi Pengelolaan Keamanan Risiko				**18**				

Form Wawancara Kerangka Kerja Pengelolaan Keamanan Informasi

Hari/ Tanggal : Kamis, 31 Oktober 2019
Pukul : 11.49 WIB
Lokasi : Ruang DPTSI
Narasumber : Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D,
Rizky Januar Akbar, S.Kom, M.Eng,
Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
Jabatan : Kepala SubDirektorat Infrastruktur dan Keamanan Informasi,
KepalaSub Direktorat Pengembangan Sistem Informasi,
Direktur DPTSI

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya	Sudah ada kebijakan terkait keamanan informasi namun	Dalam Penerapan / Diterapkan Sebagian	2	x	Royyana Muslim Itjihadie,

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	belum lengkap untuk peran masing-masing pihak				S.Kom, M.Kom, Ph.D
	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							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Bukti telah terlampir pada LAMPIRAN B (Gambar B.16, Gambar B.19, Gambar B.20, Gambar B.21, Gambar B.22)							
	Perubahan/ Tambahan -							
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Sudah pernah dipublikasikan, namun semua dokumen kebijakan disimpan oleh 1 orang di bagian helpdesk/ layanan dan dalam bentuk hardcopy	Diterapkan Secara Menyeluruh	3	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	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							
	Perubahan/ Tambahan -							
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari	Masih belum ada	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			peredaran dan penyimpanannya?					
	Temuan Tidak dilakukan mekanisme pengolahan dokumen prosedur dan kebijakan keamanan informasi yang dimiliki oleh DPTSI							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya untuk mengkomunikasikan	Masih belum dilakukan	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			kebijakan keamanan informasi dan perubahannya kepada semua pihak terkait, termasuk pihak ketiga?					
	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/ Tambahan dokumennya (pada poin 9) masih “belum ada” Bukti telah terlampir pada LAMPIRAN B (Gambar B.23)							
	Perubahan/ Tambahan -							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	Untuk mitigasi dan risiko seperti yang sudah dijelaskan sebelumnya bahwa masih belum ada penerapannya	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Kebijakan dan prosedur keamanan informasi tidak merefleksikan kebutuhan dari mitigasi risiko keamanan informasi							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Bukti Tidak adanya risiko yang dicantumkan dalam prosedur terkait keamanan informasi yang dimiliki DPTSI							
	Perubahan/ Tambahan -							
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?	Untuk dokumentasinya masih belum ada, namun sudah dilakukan. Untuk semua identifikasinya dilakukan dengan menggunakan log ids dan log file	Diterapkan Secara Menyeluruh	3	Status: Dalam Penerapan/ Diterapkan Sebagian Skor: 2	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Temuan 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 telah terlampir pada LAMPIRAN B (Gambar B.15)							
	Perubahan/ Tambahan -							
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan,	Sudah ada. Kontrak yang terkait itu dengan bagian pengadaan & perawatan	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom,

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	server dan dengan bagian penyambungan kabel				M.Kom, Ph.D
	Temuan Aspek keamanan informasi tercantum dalam kontrak yang dijalankan oleh pihak DPTSI dengan pihak ketiga namun untuk dokumentasi kontraknya tidak didapatkan sebagai bukti							
	Bukti Tidak ada							
	Perubahan/ Tambahan -							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
4.8	II	2	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	Diterapkan Secara Menyeluruh	6	Status: Dalam Penerap an/ Diterap kan Sebagia n Skor: 4	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	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 telah terlampir pada LAMPIRAN B (Gambar B.24)							
	Perubahan/ Tambahan Sudah ada unit yang mengurusi layanan hukum, namun konsekwensi pelanggaran kebijakan keamanan informasi tidak secara resmi ditegakkan							
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk	Tidak ada secara resmi	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom,

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			proses untuk menindak lanjuti konsekwensi dari kondisi ini?					M.Kom, Ph.D
	Temuan Tidak disediakan prosedur resmi untuk pengecualian penerapan keamanan informasi di DPTSI							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola	Untuk *security patch* sudah dilakukan namun tidak ada kebijakan khusus yang diterapkan	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya?					
	Temuan Dilakukan implementasi *security patch*, namun untuk kebijakan dan prosedur operasional untuk pengelolaan *security patch* masih belum dimiliki pihak DPTSI							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
4.11	III	2	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	Diterapkan Secara Menyeluruh	6	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan Dilakukan pembahasan aspek keamanan informasi saat rapat proyek yang sedang dilakukan pihak DPTSI ITS							
	Bukti							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	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							
	Perubahan/ Tambahan -							
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?	Secara informal sudah menerapkan, tapi secara formal (beserta dokumentasinya) tidak melakukan.	Tidak Dilakukan	0	x	Rizky Januar Akbar, S.Kom, M.Eng

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Temuan Tidak dilakukan evaluasi risiko dalam penerapan sistem baru							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
4.13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform	SDLC pasti diterapkan dan berbeda-beda dari setiap proyeknya dan tidak semua ada dokumentasinya.	Diterapkan Secara Menyeluruh	6	x	Rizky Januar Akbar, S.Kom, M.Eng

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			teknologi yang digunakan?					
	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 telah terlampir pada LAMPIRAN B (Gambar B.25, Gambar B.26)							
	Perubahan/ Tambahan -							
4.14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru	Untuk penerapan pengamanan sudah dilakukan, namun untuk	Tidak Dilakukan	0	Status Dalam Penerap an/	Rizky Januar Akbar,

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	dokumentasi risikonya masih belum ada sudah			Sebagia n Diterap kan Skor: 4	S.Kom, M.Eng
	Temuan Tidak ada dokumen yang dibuat untuk menganalisis dan mendeskripsikan risiko baru dan pengamanannya saat dilakukan pengembangan sistem baru							
	Bukti Tidak Ada							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Perubahan/ Tambahan Adanya SOP untuk menanggulangi timbulnya risiko atau terjadi ketidakpatuhan terhadap kebijakan yang sudah diunggah di laman https://www.its.ac.id/dptsi/id/dokumen-layanan-tik/, tapi belum disosialisasikan dan dilaksanakan. SOP tersebut adalah SOP layanan SIM, yang mana terdiri dari SOP permintaan pengembangan SIM, SOP permintaan perawatan SIM, SOP Pengajuan Perubahan SIM, SOP Pengelolaan Insiden SIM, SOP Migrasi SIM, dan SOP Terminasi SIM. Bukti telah terlampir pada LAMPIRAN B (Gambar B.27, B.28, B.29, B.30, B.31, B.32, dan, B.33)							
4.15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsidera	Masih belum punya untuk dokumen BCP	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			ns keamanan informasi, termasuk penjadwalan uji cobanya?					
	Temuan Tidak tersedia kerangka kerja terkait BCP yang mendefinisikan persyaratan keamanan informasi di DPTSI							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan	Untuk DRP sendiri DPTSI masih belum punya. Belum ada tim dan pendefinisian	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	wewenang karena hanya ada 1 orang yang menangani pemulihan bencana terhadap layanan. Namun, untuk rencana pemulihan sudah diterapkan dan DPTSI memiliki DRC dibeberapa tempat yang terpisah				
	Temuan Tidak ada dokumen terkait DRP yang digunakan di DPTSI							
	Bukti Tidak Ada							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Perubahan/ Tambahan Belum ada tim, karena hanya seorang individu yang bertanggungjawab							
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	Belum Pernah Dilakukan	Tidak Dilakukan	0	Status: Diterap kan secara menyel uruh Skor: 0	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan Uji coba DRC dilakukan oleh pihak eksternal yang mana tempat membeli peralatan tersebut							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Adanya temuan uji coba DRC sebanyak 2x dalam 1 tahun yang dilakukan oleh pihak eksternal yang maan tempat membeli peralatan tersebut							
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)	Belum dilakukan evaluasi	Tidak Dilakukan	0	Status: Dilakuk an Secara Menyel uruh Skor: 0	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			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							
	Perubahan/ Tambahan Iya, dilakukan setiap setelah melakukan uji coba. Namun, belum ada dokumentasi laporannya							
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak ada evaluasi secara berkala terkait kebijakan dan prosedur keamanan informasi	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom Royyana Muslim

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
								Itjihadie, S.Kom, M.Kom, Ph.D
	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/ Tambahan pada dokumen tersebut Bukti telah terlampir pada LAMPIRAN B (Gambar B.23)							
	Perubahan/ Tambahan -							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
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?	Sudah ada strateginya dan biasanya dilakukan integrasi dengan bagian pengembangan	Diterapkan Secara Menyeluruh	3	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Strategi penerapan keamanan informasi dilakukan dengan cara berintegrasi dengan SubDirektorat Pengembangan Sistem Informasi DPTSI							
	Bukti							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Komunikasi yang terarah dan terstruktur antara bagian IKTI dan Pengembangan Sistem Informasi terkait pembangunan,pemeliharaan, dan gangguan terhadap sistem yang dimiliki							
	Perubahan/ Tambahan							
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan Perubahan/ Tambahan profil risiko?	Lebih ke mencegah dengan cara mengencourage dan menenkripsi dengan menggunakan https. Namun tidak ada secara tertulis dalam dokumen	Diterapkan Secara Menyeluruh	3	Status: Dalam Penerapan/ Diterapkan Sebagian Skor: 2	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Temuan 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 telah terlampir pada LAMPIRAN B (Gambar B.34)							
	Perubahan/ Tambahan Pembahasan strategi dilakukan melalui rapat, namun tidak ada dokumentasi profil risiko sehingga tidak ada yang bisa menjamin penerapan strateginya sesuai dengan profil risiko							
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari	Direalisasikan untuk penerapan strategi keamanan informasinya	Diterapkan Secara Menyeluruh	3	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			pelaksanaan program kerja organisasi anda?					Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	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 telah terlampir pada LAMPIRAN B (Gambar B.34)							
	Perubahan/ Tambahan -							
4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan	Belum pernah dilakukan audit internal	Tidak Dilakukan	0	x	Rizky Januar Akbar,

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			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)?					S.Kom, M.Eng
	Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada							
	Bukti Tidak Ada							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Perubahan/ Tambahan							
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Belum ada	Tidak Dilakukan	0	x	Rizky Januar Akbar, S.Kom, M.Eng
	Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Belum ada	Tidak Dilakukan	0	x	Rizky Januar Akbar, S.Kom, M.Eng
	Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Belum dilakukan	Tidak Dilakukan	0	x	Rizky Januar Akbar, S.Kom, M.Eng
	Temuan Tidak pernah dilakukan audit internal oleh pihak independen terkait aset informasi, kebijakan, dan prosedur keamanan yang ada							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
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/ Tambahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat	Belum ada penilaian aspek finansial untuk Perubahan/ Tambahan infrastruktur dan pengelolaan perubahannya	Tidak Dilakukan	0	x	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			untuk menerapkannya?					
	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							
	Perubahan/ Tambahan -							
4.28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi	Tidak dilakukan pengujian secara rutin dan efektif terhadap kepatuhan program	Tidak Dilakukan	0	Status: Diterap kan secara menyel uruh Skor: 0	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
			yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	keamanan informasi				
	Temuan Tidak dilakukan pengujian dan pengevaluasian terhadap kepatuhan program keamanan informasi yang ada							
	Bukti Tidak Ada							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Perubahan/ Tambahan Adanya suatu program pemberian *reward* berdasarkan penilaian terhadap 10 website terbaik yang dilaporkan kepada Wakil Rektor 3							
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?	Belum diterapkan, masih mau disesuaikan dengan ISO	Tidak Dilakukan	0	Status: Diterapkan Secara Menyeluruh Skor: 0	Dr. Eng. Febriliyan Samopa, S.Kom, M.Kom
	Temuan Masih belum ada perencanaan							
	Bukti							

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembar uan**	**Nara-sumber**
	Tidak Ada							
	Perubahan/ Tambahan Terdapat dokumentasi masterplan perencanaan keamanan informasi yang direalisasikan secara konsisten							
Total Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi				**35**				

Form Wawancara Pengelolaan Aset Informasi

Hari/ Tanggal : Selasa, 29 Oktober 2019
Pukul : 09.31 WIB
Lokasi : Ruang DPTSI
Narasumber : Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
Jananta Permata Putra, S.ST
Cahya Purnama Dani, A.Md
Jabatan : Kepala SubDirektorat Infrastruktur dan Keamanan Teknologi Informasi
Staf Bagian Sistem
Staf Bagian Inventaris & Sistem

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara? (termasuk kepemilikan aset)	Ada daftar inventaris aset milik ITS	Diterapkan Secara Menyeluruh	3	x	Cahya Purnama Dani, A.Md.
	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 telah terlampir pada LAMPIRAN B (Gambar B.17)							
	Bukti							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Dalam daftar aset terdapat kolom kepemilikan dimana semua berisi milik DPTSI dan ada bagian pengelola aset informasi yang bertanggung jawab							
	Perubahan/ Tambahan -							
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak ada undang-undang yang digunakan untuk klasifikasi aset	Tidak Dilaku kan	0	x	Cahya Purnama Dani, A.Md
	Temuan Tidak ada undang-undang yang diberlakukan terkait klasifikasi aset di DPTSI							
	Bukti Tidak Ada							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Perubahan/ Tambahan -							
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Belum dilakukan juga karena masih belum ada undang-undang yang dipakai	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Belum dilakukan evaluasi dan klasifikasi aset informasi sesuai dengan tingkat kepentingannya karena masih belum adanya undang-undang yang digunakan juga oleh DPTSI							
	Bukti							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Tidak Ada							
	Perubahan/ Tambahan							
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?	Tingkatan akses dulu dibedakan dengan menggunakan proxy, namun sekarang sudah tidak lagi	Diterapkan Secara Menyeluruh	3	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Tingkatan akses dibedakan dengan menggunakan proxy, namun hal ini sudah tidak digunakan lagi. Untuk saat ini tingkatan akses dibedakan dengan adanya user *login* integra. Tingkatan akses juga dibedakan dari menu-menu yang dapat diakses oleh user dalam akun integranya							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Bukti Akun integra yang sudah dijadikan sebagai portal *single sign-on* Bukti telah terlampir pada LAMPIRAN B (Gambar B.8 dan Gambar B.9)							
	Perubahan/ Tambahan -							
5.5	II	1	Apakah tersedia proses pengelolaan Perubahan/ Tambahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk Perubahan/ Tambahan konfigurasi) yang	Ada pengelolaan Perubahan/ Tambahan sistem dan konfigurasi	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			diterapkan secara konsisten?					
	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							
	Perubahan/ Tambahan Untuk konfigurasi switch, setiap terdapat perubahan maka otomatis langsung tersimpan di server tertentu. Namun untuk beberapa konfigurasi lainnya, ada yang hanya melakukan konfigurasi sebanyak 1x untuk selamanya tanpa ada perubahan							
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi	Sudah dilakukan untuk pengelolaan konfigurasi	Ditera pkan Secara	3	x	Jananta Permata

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			yang diterapkan secara konsisten?		Menye luruh			Putra, S.ST
	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 telah terlampir pada LAMPIRAN B (Gambar B.7 dan Gambar B.26)							
	Perubahan/ Tambahan -							
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset	Ada dengan cara menambahkan aset	Ditera pkan	3	x	Cahya Purnama

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	baru ke daftar inventaris yang dimiliki	Secara Menye luruh			Dani, A.Md.
	Temuan Dilakukan proses perilisan aset baru dalam lingkungan operasional dan dilakukan pembaruan terhadap daftar inventaris aset informasi							
	Bukti Update daftar inventaris aset yang dimiliki oleh DPTSI terakhir dilakukan pada tanggal 18 Desember 2019							
	Perubahan/ Tambahan -							
5.8	II	1	Definisi tanggungjawab pengamanan informasi	Untuk secara individu adanya	Ditera pkan	3	x	Royyana Muslim

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			secara individual untuk semua personil di instansi/perusahaan anda	hanya dibagian sistem bukan untuk semua bagian	Secara Menye luruh			Itjihadie, S.Kom, M.Kom, Ph.D
	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 telah terlampir pada LAMPIRAN B (Gambar B.35)							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak ada tata tertib	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Tidak ada tata tertib khusus untuk penggunaan komputer, email, internet, dan intranet							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Tidak ada secara tertulis	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Tidak ada tata tertib khusus untuk penggunaan dan pengamanan aset terkait HAKI							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Hanya ada beberapa di website namun tidak semuanya	Diterapkan Secara Menyeluruh	3	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	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 telah terlampir pada LAMPIRAN B (Gambar B.36)							
	Perubahan/ Tambahan							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	-							
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Masih belum diterapkan	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak ada peraturan terkait penggunaan data pribadi yang mewajibkan adanya ijin untuk mengakses data pribadi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.13	II	1	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	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak ada kebijakan terkait pengelolaan *username* & *password* beserta pelanggarannya							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	-							
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak ada prosedur secara tertulis	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Tidak ada prosedur terkait pengelolaan dan pemberian akses, otentikasi, dan otorisasi dalam penggunaan aset informasi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak pernah dilakukan penghancuran data sebelumnya	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak ada patokan waktu untuk melakukan penyimpanan klasifikasi data dan syarat penghancuran data							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
5.16	II	1	Ketetapan terkait pertukaran data dengan	Tidak pernah dilakukan pertukaran data	Tidak Dilaku kan	0	x	Jananta Permata

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			pihak eksternal dan pengamanannya	dengan pihak eksternal				Putra, S.ST
	Temuan Tidak ada dokumentasi terkait ketepatan pertukaran data dan pengamanannya dengan pihak eksternal							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dilakukan secara keseluruhan dan ada pencatatan insiden	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Temuan Tidak adanya pencatatan insiden terkait kegagalan keamanan informasi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
5.18	II	1	Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	Dilakukan backup secara berkala dan ada prosedur yang mengaturnya	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak ada prosedur terkait *back-up* dan *restore* yang dibuat untuk DPTSI							
	Bukti							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Tidak Ada							
	Perubahan/ Tambahan -							
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	ada pembagian zona dan klasifikasi aset	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Ada pengamanan fisik untuk aset-aset yang sudah diklasifikasikan kepentingannya. Untuk ruang server disediakan pengamanan fisik yang baik dan lengkap							
	Bukti							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Ruang server dilengkapi dengan pintu berlapis, *fingerprint*, CCTV, gas pemadam kebakaran, anti petir, *grounding*, sensor kelembaban, dan sensor suhu Bukti telah terlampir pada LAMPIRAN B (Gambar B.18, Gambar B.37) dan Gambar B.38)							
	Perubahan/ Tambahan -							
5.20	III	2	Proses pengecekan latar belakang SDM	Dilakukan saat diawal perekrutan karyawan, dilakukan penilaian terhadap bidang terkait	Tidak Dilaku kan	0	Status: Dalam Penerapa n/ Diterapk an Sebagian Skor: 4	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Temuan Pengecekan latar belakang SDM dilakukan pada awal pengambilan karyawan namun tidak ada pendokumentasian atas hal tersebut							
	Bukti Tidak Ada							
	Perubahan/ Tambahan Adanya perubahan status penerapan dari yang semula tidak dilakukan menjadi dalam penerapan/ diterapkan sebagian. Sebab, proses ini pasti dilakukan ketika perekrutan SDM, namun tidak ada dokumentasi yang bisa membuktikannya							
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Ada koordinasi dengan pihak lain, biasanya dengan pihak ISP terkait	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom,

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
								M.Kom, Ph.D
	Temuan Dilakukan pelaporan insiden keamanan informais dengan pihak eksternal, biasanya dilakukan dengan pihak ISP terkait. Koordinasi dilakukan secara 2 arah dengan baik							
	Bukti Email yang berisikan laporan insiden keamanan informasi atara staff SubDir IKTI DPTSI dengan pihak eksternal Bukti telah terlampir pada LAMPIRAN B (Gambar B.14)							
	Perubahan/ Tambahan -							
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Sudah ada prosedur penghancuran dokumen	Ditera pkan Secara	6	x	Royyana Muslim Itjihadie,

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
					Menye luruh			S.Kom, M.Kom, Ph.D
	Temuan Terdapat prosedur untuk melakukan penghancuran dokumen yang sudah ditetapkan sejak lama							
	Bukti Ada prosedur penghancuran dokumen yang sudah tidak digunakan lagi Bukti telah terlampir pada LAMPIRAN B (Gambar B.21)							
	Perubahan/ Tambahan -							
5.23	III	2	Prosedur kajian penggunaan akses (user access review) dan hak	Sudah dimiliki. Sekarang akses	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie,

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku	menggunakan integra				S.Kom, M.Kom, Ph.D
	Temuan Tidak ada prosedur yang mengatur tentang penggunaan hak akses dan langkah pembenahannya jika terjadi ketidak sesuaian dengan kebijakan yang berlaku							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.24	III	2	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.	Belum ada prosedur, namun sekarang sedang dalam tahap pembuatan	Dalam Perencanaan	2	Status: Dalam Penerapan/ Diterapkan Sebagian Skor: 4	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	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. Namun, di dalam kontrak kerja telah tercantum peraturan yang saling mengikat kedua belah pihak, yang terdiri dari: Pasal 1 Kewajiban							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Pihak Pertama, Pasal 2 Kewajiban Pihak Kedua, Pasal 3 Hak Pihak Pertama, Pasal 4 Hak Pihak Kedua, Pasal 5 Tata Cara Pembayaran Upah, Pasal 6 Jangka Waktu dan Pengakhiran Perjanjian, Pasal 7 Penyelesaian Perselisihan, dan Pasal 8 Addendum.							
	Perubahan/ Tambahan							
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?	Tidak ada daftar khusus untuk di-*backup.*	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak terdapat daftar data yang harus di *backup* dan prosedur *backup* yang disediakan oleh pihak DPTSI							
	Bukti							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Tidak Ada							
	Perubahan/ Tambahan -							
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak ada	Tidak Dilaku kan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak ada bukti daftar untuk melakukan pelaksanaan keamanan informasi yang disesuaikan dengan klasifikasinya							
	Bukti Tidak Ada							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Perubahan/ Tambahan -							
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?	Belum ada prosedur khusus yang mengatur	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Tidak ada prosedur penggunaan perangkat pengolah informasi milik pihak ketiga dengan memastikan aspek HAKI yang ada							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
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	Sudah ada pengamanan berlapis, misalnya dengan menggunakan firewall dengan tingkatan yang berbeda	Diterapkan Secara Menyeluruh	3	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			oleh pihak yang tidak berwenang?					
	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 telah terlampir pada LAMPIRAN B (Gambar B.18 dan B.37)							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Sudah ada dengan menggunakan *finger print*	Diterapkan Secara Menyeluruh	3	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan 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 telah terlampir pada LAMPIRAN B (Gambar B.18 dan B.37)							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Perubahan/ Tambahan -							
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?	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	Diterapkan Secara Menyeluruh	3	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
				minimal yang ditentukan				
	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 Bukti telah terlampir pada LAMPIRAN B (Gambar B.18 dan B.38)							
	Perubahan/ Tambahan -							
5.31	II	1	Apakah infrastruktur komputasi yang	Sudah ada didalam ruang server	Ditera pkan	3	x	Jananta Permata

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?		Secara Menyeluruh			Putra, S.ST
	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							
	Perubahan/ Tambahan -							
5.32	II	1	Apakah tersedia peraturan pengamanan	Ada surat terima, biasanya dilakukan	Diterapkan	3	Status: Dalam	Royyana Muslim

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	dengan jurusan-jurusan yang ada di ITS	Secara Menyeluruh		Penerapan/ Diterapkan Sebagian Skor: 2	Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Adanya peraturan pengamanan perangkat komputasi milik DPTSI jika digunakan diluar kantor							
	Bukti Adanya surat serah terima untuk pemindahan alat komputasi Bukti telah terlampir pada LAMPIRAN B (Gambar B.39)							
	Perubahan/ Tambahan							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Untuk pemindahannya menggunakan berita acara lalu didaftar inventaris akan diperbaharui	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	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							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Bukti telah terlampir pada LAMPIRAN B (Gambar B.39)							
	Perubahan/ Tambahan -							
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,	Sangat penting dan sudah ada semua standarnya untuk ruang server yang di DPTSI, namun untuk yang ruang server di lantai 6 masih belum mengikuti standar	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			pemadam api, pengatur suhu dan kelembaban) yang sesuai?					
	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 telah terlampir pada LAMPIRAN B (Gambar B.18, B.37, dan B.38)							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Tidak dilakukan perawatan komputer secara khusus jika ada kerusakan. Biasanya dilakukan pada jaringan	Dalam Penera pan / Ditera pkan Sebagi an	4	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	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							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Bukti telah terlampir pada LAMPIRAN B (Gambar B.15)							
	Perubahan/ Tambahan -							
5.36	II	2	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	Dalam Penera pan / Ditera pkan Sebagi an	4	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Untuk pengamanan dalam pengiriman aset informasi yang melibatkan pihak ketiga sudah dilakukan sebagain							
	Bukti							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	Dilakukan pengamanan aset informasi dengan penerapan password namun untuk pengamanan fisik masih tidak dilakukan							
	Perubahan/ Tambahan -							
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	Tidak ada peraturan resmi dan tanda larangan. Untuk orang yang masuk juga tidak diperingatkan ataupun diingatkan dan tidak diperiksa	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
			dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)					
	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							
	Perubahan/ Tambahan -							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Tidak dilakukan	Tidak Dilaku kan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Tidak dilakukan proses pengamanan lokasi kerja dari keberadaan/kehadiran pihak ketiga							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian V: Pengelolaan Aset Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pemba-ruan**	**Nara-sumber**
	-							
Total Penilaian Pengelolaan Aset Informasi					**78**			

Form Wawancara Teknologi dan Keamanan Informasi

Hari/ Tanggal	: Selasa, 29 Oktober 2019
Pukul	: 09.31
Lokasi	: Ruang DPTSI
Narasumber	: Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Jananta Permata Putra, S.ST
	Rizky Januar Akbar, S.Kom, M.Eng
Jabatan	: Kepala SubDirektorat Infrastruktur dan Keamanan Teknologi Informasi
	Staf Bagian Sistem
	Kepala SubDirektorat Pengembangan Sistem Informasi

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
6.1	II	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	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	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							
	Bukti Adanya konfigurasi firewall dan penggunaan firewall dengan Cisco ASA 5540 Bukti telah terlampir pada LAMPIRAN B (Gambar B.26 dan B.40)							
	Perubahan/ Tambahan -							
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian	Sudah ada segmentasinya	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?					
	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							
	Perubahan/ Tambahan -							
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan	Ada yang sudah ada dan ada yang tidak	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	ada. Yang ada itu untuk server jaringan dan aplikasi				
	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 e-surat diluar ip yang sudah ditentukan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti telah terlampir pada LAMPIRAN B (Gambar B.41, Gambar B.42, dan Gambar B.43)							
	Perubahan/ Tambahan -							
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dilakukan analisa	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan Pihak DPTSI melakukan analisa kepatuhan penerapan konfigurasi standar secara rutin							
	Bukti IP config yang ada selalu dipantau secararutin oleh staff IKTI DPTSI							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Perubahan/ Tambahan -							
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau Perubahan/ Tambahan/keutuhan konfigurasi?	Dilakukan tetapi tidak secara rutin, hanya dilakukan jika ada insiden saja	Dalam Penerapan/ Diterapkan Sebagian	2	x	Jananta Permata Putra, S.ST
	Temuan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Tidak dilakukan pemindaian secara rutin terhadap jaringan, sistem dan aplikasi yang digunakan untuk mengidentifikasi kemungkinan adanya celah kelemahan atau Perubahan/ Tambahan/keutuhan konfigurasi							
	Bukti Pemindaian hanya dilakukan jika terjadi masalah/ insiden							
	Perubahan/ Tambahan -							
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai	Iya, dan sekarang sudah disamakan semua dengan menggunakan *single sign-on*	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			kebutuhan/persyaratan yang ada?					
	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-masing *user* Bukti telah terlampir pada LAMPIRAN B (Gambar B.44)							
	Perubahan/ Tambahan -							
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk	Ada monitoring kapasitas	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?					
	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 e-mail *user* ITS Bukti telah terlampir pada LAMPIRAN B (Gambar B.44)							
	Perubahan/ Tambahan -							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
6.8	II	1	Apakah setiap Perubahan/ Tambahan dalam sistem informasi secara otomatis terekam di dalam log?	Terekam dalam log yang dipegang oleh staff infrastruktur	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan Dilakukan perekaman secara otomatis jika terjadi Perubahan/ Tambahan dalam sistem informasi							
	Bukti *Log ids* untuk Perubahan/ Tambahan sistem yang dilakukan melalui jaringan Bukti terlampir pada LAMPIRAN B (Gambar B.15)							
	Perubahan/ Tambahan -							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Ada notifikasi yang masuk ke bagian admin	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan Dilakukan perekaman secara otomatis jika terjadi upaya akses oleh yang tidak berhak							
	Bukti Pelatihan dan workshop pemasangan honeynet terakhir dilakukan tahun 2016 yang diadakan oleh komunitas dan dibantu pihak Kominfo Bukti terlampir pada LAMPIRAN B (Gambar B.15 dan Gambar B.19)							
	Perubahan/ Tambahan -							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
6.10	II	1	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	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan Dilakukan analisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)							
	Bukti Dashboard yang berisi aktivitas jaringan beserta report yang didapat perhari							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti terlampir pada LAMPIRAN B (Gambar B.15)							
	Perubahan/ Tambahan -							
6.11	III	2	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Pasti ada enkripsi	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan Dilakukan penerapan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti Enkripsi pada seluruh *password user* ITS dalam *database* dan enkripsi pada seluruh sistem yang memiliki domain its.ac.id Bukti telah dilampirkan pada LAMPIRAN B (Gambar B.34)							
	Perubahan/ Tambahan -							
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Untuk standar tertentu tidak ada, namun sudah diterapkan enkripsi dari password dan	Tidak Dilakukan	0	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
				penggunaan https				
	Temuan Tidak ada standar khusus yang digunakan DPTSI untuk penggunaan enkripsi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk	Ada sertifikasi enkripsi yang diambil dari digicert	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?					
	Temuan Diterapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan di DPTSI ITS							
	Bukti Sertifikasi domain ITS dari DigiCert Inc Bukti telah terlampir pada LAMPIRAN B (Gambar B.45)							
	Perubahan/ Tambahan -							
6.14	III	2	Apakah semua sistem dan aplikasi secara	Ada peraturan tetapi tidak	Tidak Dilakukan	0	x	Royyana Muslim

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjang nya dan penggunaan kembali password lama?	tertulis. Untuk ganti password juga kembali lagi ke orangnya masing-masing				Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan 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							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Tidak Ada							
	Perubahan/ Tambahan							
6.15	III	2	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	Diterapkan Secara Menyeluruh	6	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Ada penerapan akses untuk mengelola sistem dengan menggunakan pengamanan khusus							
	Bukti							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Akses pada database masing-masing sistem akan berbeda tergantung yang bertanggung jawab, akses pada esurat hanya untuk beberapa *user* yang terdaftar saja Bukti telah terlampir pada LAMPIRAN B (Gambar B.42 dan B.43)							
	Perubahan/ Tambahan -							
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan	Sudah diterapkan kesemuanya. Jika untuk jaringan biasanya akan diputus kalau sudah lama tidak dipakai	Dalam Penerapan / Diterapkan Sebagian	4	x	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			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*							
	Perubahan/ Tambahan -							
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk	Ada dengan menggunakan firewall	Diterapkan Secara Menyeluruh	6	x	Jananta Permata Putra, S.ST

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?					
	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 Bukti telah dilampirkan pada LAMPIRAN B (Gambar B.26)							
	Perubahan/ Tambahan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	-							
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Sudah diterapkan	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	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							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti telah dilampirkan pada LAMPIRAN B (Gambar B.42 dan Gambar B.43)							
	Perubahan/ Tambahan -							
6.19	II	1	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,	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
				jika ada fungsi yang terganggu maka tetap memakai versi yang lama				
	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 Versi terbaru dari *desktop* dan *server*							
	Perubahan/ Tambahan -							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
6.20	II	1	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	Diterapkan Secara Menyeluruh	3	x	Jananta Permata Putra, S.ST
	Temuan Diterapkan penggunaan anti virus pada setiap *desktop* dan *server* untuk dilindungi dari penyerangan virus							
	Bukti Penggunaan anti virus dari Windows yaitu Windows Defender							
	Perubahan/ Tambahan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	-							
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 ada	Tidak Dilakukan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak dilakukan perekaman dan hasil analisa yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti Tidak Ada							
	Perubahan/ Tambahan -							
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak ada laporan khusus	Tidak Dilakukan	0	x	Jananta Permata Putra, S.ST
	Temuan Tidak adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan							
	Bukti Tidak Ada							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Perubahan/ Tambahan -							
6.23	III	2	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	Diterapkan Secara Menyeluruh	6	x	Jananta Permata Putra, S.ST
	Temuan Sinkronisasi waktu sudah diterapkan secara keseluruhan pada jaringan, sistem dan aplikasi yang akurat, sesuai dengan standar yang ada							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
	Bukti Sinkronisasi waktu pada akun ShareITS dan Integra Bukti telah terlampir pada LAMPIRAN B (Gambar B.46, Gambar B.47, Gambar B.48)							
	Perubahan/ Tambahan -							
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses	Sudah dilakukan verifikasi dan validasi namun untuk dokumentasi masih belum diterapkan	Diterapkan Secara Menyeluruh	6	x	Rizky Januar Akbar, S.Kom, M.Eng

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			pengembangan dan uji coba?					
	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							
	Perubahan/ Tambahan							
6.25	III	3	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan	Ada pengamanan untuk tempat pengembangan namun tidak	Tidak Dilakukan	0		Rizky Januar Akbar, S.Kom, M.Eng

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
			uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	menggunakan standar tertentu				Yuniarti, S.Kom, M.Comp.Sc
	Temuan Tidak ada penggunaan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun							
	Bukti Tidak ada							
	Perubahan/ Tambahan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak dilakukan secara rutin, namun dahulu pernah dilakukan	Tidak Dilakukan	0		Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
	Temuan Tidak ada pihak independen yang bekerja sama untuk mengkaji kehandalan keamanan informasi							
	Bukti Tidak Ada							
	Perubahan/ Tambahan							

Bagian VI: Teknologi dan Keamanan Informasi								
[Penilaian] Tidak Dilakukan, Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh								
No.	**Tk. Kema-tangan**	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Pembaruan**	**Nara-sumber**
Total Penilaian Teknologi dan Keamanan Informasi				**75**				

Form Wawancara Suplemen

Hari/ Tanggal : Jumat, 1 November 2019
Pukul : 14.51 WIB
Lokasi : Ruang DPTSI
Narasumber : Hanim Maria Astuti, S.Kom, M.Sc, ITIL
Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
Rizky Januar Akbar, S.Kom, M.Eng
Jabatan : Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi
Kepala SubDirektorat Infrastruktur dan Keamanan Teknologi Informasi
Kepala SubDirektorat Pengembangan Sistem Informasi

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.1 Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan						
7.1.1 Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga						

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.1.1.1	1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	DPTSI melakukan identifikasi risiko keamanan informasi terkait vendor, biasanya melalui rapat. Namun tidak ada dokumentasi untuk hal tersebut	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.1.2	1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	DPTSI mengkomunikasikan dan mengklarifikasi, namun tidak ada dokumentasinya	Dalam Penerapan/ Diterapkan Sebagian	2	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.1.3	1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan	DPTSI mengklarifikasi persyaratan mitigasi risiko, namun tidak ada dokumentasinya	Dalam Penerapan/ Diterapkan Sebagian	2	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?				
7.1.1.4	1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Rencana mitigasi yang sudah diidentifikasi tidak selalu disetujui oleh vendor, sehingga DPTSI dan vendor sama-sama mencari solusinya	Dalam Penerapan/ Diterapkan Sebagian	2	
7.1.1.5	1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan	DPTSI belum menerapkan kebijakan keamanan informasi. Saat ini masih baru dalam proses pembuatan SOP-nya	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?				
7.1.1.6	1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Dikarenakan tidak ada kebijakannya, maka tidak dikomunikasikan	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.1.7	1	Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit	Tidak dilakukan audit	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		internal/eksternal tentang kondisi kontrol keamanan informasi pihak ketiga?				
7.1.2 Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga						
7.1.2.1	1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/ infrastruktur yang digunakan dalam layanannya?	Pihak ketiga belum mengidentifikasi risiko terkait alihdaya penyedia teknologi/ informasi	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.2.2	1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Pihak ketiga tidak melakukan pengendalian risiko	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.1.2.3	1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Pihak ketiga belum melakukan pemantauan dan evaluasi	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.3 Pengelolaan Layanan dan Keamanan Pihak Ketiga						
7.1.3.1	1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang	Tidak ada prosedur yang terdokumentasi	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		diakses) dalam hubungan kerjasama dengan pihak ketiga?				
7.1.3.2	1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	Tidak ada audit sehingga tidak ada pembagian peran dan tanggung jawab	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.3.3	1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	Tidak ada laporan berkala terkait pencapaian SLA	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.1.3.4	1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Tidak ada rapat secara berkala untuk membahas pencapaian SLA	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.3.5	1	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	Tidak ada rapat, sehingga tidak ada pendokumentasiannya	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.3.6	1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap	Tidak ada audit	Tidak Dilakukan	0	Hanim Maria Astuti,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		pemenuhan persyaratan keamanan informasi oleh pihak ketiga?				S.Kom, M.Sc, ITIL
7.1.3.7	1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	Tidak ada audit sehingga tidak ada tindak lanjut	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.3.8	1	Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan,	Tidak ada dokumentasi kondisi ketidakpatuhan pihak ketiga	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		dikomunikasikan, dipahami dan diterapkan?				
7.1.4 Pengelolaan Perubahan/ Tambahan Layanan dan Kebijakan Pihak Ketiga						
7.1.4.1	1	Apakah instansi/perusahaan mengelola Perubahan/ Tambahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan/ Tambahan layanan pihak ketiga; - Perubahan/ Tambahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	DPTSI melakukan pengelolaan perubahan	Dalam Penerapan/ Diterapkan Sebagian	2	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.1.4.2	1	Apakah risiko yang menyertai Perubahan/ Tambahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Tidak dikaji dan didokumentasikan sebagai rencana mitigasi	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.5 Penanganan Aset						
7.1.5.1	1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, Perubahan/ Tambahan, dan penghapusan/penghancuran aset?	DPTSI tidak diberikan informasi mengenai prosedur formal dari pihak ketiga dalam menangani data selama siklus hidupnya	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.5.2	1	Apakah per untuk penghancuran (disposal) data secara aman telah	Tidak ada kesepakatan penghancuran data	Tidak Dilakukan	0	Hanim Maria Astuti,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		disepakati bersama pihak ketiga (pihak ketiga)?	dengan pihak ketiga. Terdapat data penting, biasanya data masih disimpan			S.Kom, M.Sc, ITIL
7.1.6 Pengelolaan Insiden oleh Pihak Ketiga						
7.1.6.1	1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	DPTSI tidak diberikan prosedur terkait hal tersebut. Namun, terdapat perwakilan dari Telkom (Mas Wahyu) yang mengawasi jaringan di DPTSI	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.6.2	1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang	DPTSI tidak diberikan bukti-bukti penerapan	Tidak Dilakukan	0	Hanim Maria Astuti,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		memadai dalam menangani insiden keamanan informasi?	insiden keamanan informasi			S.Kom, M.Sc, ITIL
7.1.7 Rencana Kelangsungan Layanan Pihak Ketiga						
7.1.7.1	1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	DPTSI tidak diberikan prosedur terkait hal tersebut. Namun, terdapat perwakilan dari Telkom (Mas Wahyu) yang mengawasi jaringan di DPTSI	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.1.7.2	1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	DPTSI tidak melakukan ujicoba terkait efektivitas prosedur rencana keberlangsungan bisnis	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.1.7.3	1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Hanya terdapat seorang perwakilan dari Telkom untuk mengawasi jaringan di DPTSI	Dalam penerapan/ Diterapkan Sebagian	2	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
Temuan Adanya perwakilan Telkom yang mengawasi jaringan di DPTSI, yaitu Mas Khusnul						
Bukti -						
Rata-Rata Penilaian Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan					0.37	
7.2 Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)						
7.2.1	1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan	Belum melakukan kajian	Tidak Dilakukan	0	Royyana Muslim Itjihadie,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?				S.Kom, M.Kom, Ph.D
7.2.2	1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	Sebenarnya penggunaan cloud di DPTSI tidak direncanakan. Namun karena DPTSI menggunakan layanan Office 365, yang mana menyediakan layanan cloud, maka DPTSI menggunakan layanan cloud dari Office 365. Tidak ada dokumentasi khusus yang mengatur data apa saja yang	Dalam Penerapan/ Diterapkan Sebagian	2	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
			disimpan ke dalam cloud.			
Temuan Terdapat 2 kategori data, yaitu data yang berkaitan dengan layanan umum, seperti e-mail dan storage serta data yang berkaitan dengan akademik dan keuangan, seperti Integra dan Sistem Informasi lain yang dikelola ITS. Untuk data yang berkaitan dengan layanan umum diletakkan ke dalam cloud, sementara untuk data yang berkaitan dengan akademik dan keuangan diletakkan di luar cloud						
Bukti -						
7.2.3	1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?	Belum ada langkah pengamanan, ketika rapat juga hanya dibahas secara implisit saja	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
7.2.4	1	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	Tidak dilakukan pengkajian dan penetapan kriteria	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.2.5	1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	Sebenarnya penggunaan cloud di DPTSI tidak direncanakan dan bukan merupakan tujuan DPTSI. Namun karena DPTSI menggunakan layanan Office 365, yang mana menyediakan layanan cloud, maka DPTSI	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
			menggunakan layanan cloud dari Office 365. Oleh karena itu belum ada evaluasi penyelanggaraan cloud untuk Microsoft Cloud. Namun, pernah dilakukan evaluasi sederhana, sebelum menggunakan Microsoft, DPTSI menggunakan layanan dari Google, sehingga kelebihannya tidak perlu mengeluarkan ongkos tapi tidak bisa mencukupi seluruh			

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
			kebutuhan user, sedangkan dengan Microsoft Cloud, DPTSI lebih mudah karena tinggal meng-outsource-kan semua kebutuhan ke Microsoft			
7.2.6	1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Tidak ada penetapan standar keamanan teknis penggunaan dari DPTSI, karena teknis penggunaan mengikuti cloud provider yang bersangkutan	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.2.7	1	Apakah instansi/perusahaan sudah mengevaluasi kelaikan	DPTSI melakukan evaluasi kelaikan	Tidak Dilakukan	0	Royyana Muslim

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	keamanan namun tidak ada dokumentasinya. DPTSI juga tidak melakukan evaluasi kelaiakan terkait pemenuhan sertifikasi layanan berbasis ISO 27001			Itjihadie, S.Kom, M.Kom, Ph.D
7.2.8	1	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Sudah ada strategi pemulihan data terkait e-mail dalam cloud, yaitu dengan mengembalikannya ke on premis. Namun, untuk data-data yang ada di One Drive maupun Google Drive,	Dalam Penerapan/ Dilakukan Sebagian	2	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
			tidak ada strategi fasilitas pengganti			
Temuan Apabila terjadi gangguan terhadap data e-mail, DPTSI akan mengembalikan data tersebut ke on-premis						
Bukti Tidak Ada						
7.2.9	1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	Proses pelaporan insiden mengikuti layanan support yang disediakan oleh layanan cloud	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.2.10	1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan	Tidak ada proses terkait penghentian layanan cloud	Tidak Dilakukan	0	Royyana Muslim Itjihadie,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		data yang ada (memindahkan dan menghapus data)?				S.Kom, M.Kom, Ph.D
Rata-Rata Penilaian Pengamanan Layanan Infrastruktur Awan (Cloud Service)					**0.40**	
7.3 Perlindungan Data Pribadi						
7.3.1	1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Terdapat log activity terkait pihak ketiga yang sedang membangun sesuatu di DPTSI, tapi itu tidak berisi data pribadi	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.3.2	1	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak	Secara informal, sudah ada acuan untuk memetakan alur	Dalam Penerapan/ Diterapkan Sebagian	2	Rizky Januar Akbar, S.Kom, M.Eng

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	pertukaran data pribadi dengan pihak eksternal			
7.3.3	1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Tidak ada dokumentasi	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.3.4	1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Tidak ada kebijakan perlindungan data pribadi	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.3.5	1	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data	Tidak ada kebijakan perlindungan data pribadi dan tidak ada	Tidak Dilakukan	0	Hanim Maria Astuti,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	pembagian peran dan tanggung jawab atas kebijakan tersebut			S.Kom, M.Sc, ITIL Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.3.6	1	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	Sudah menganalisis dampaknya, namun tidak secara resmi dan tidak ada dokumentasinya	Dalam Penerapan/ Diterapkan Sebagian	2	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
Temuan Adanya analisis disalahgunakannya data pribadi oleh pihak eksternal, misalnya dijual untuk kepentingan pihak eksternal						

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
Bukti Tidak Ada						
7.3.7	1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Belum pernah didefinisikan apa saja cakupan data pribadi	Tidak Dilakukan	0	Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.3.8	1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Belum ada mekanisme perlindungan data pribadi, sehingga belum diterapkan	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL Royyana Muslim Itjihadie,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
						S.Kom, M.Kom, Ph.D
7.3.9	1	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Tidak ada program seperti itu	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL
7.3.10	1	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik	Tidak ada mekanisme untuk mendapatkan persetujuan user, aplikasi yang	Tidak Dilakukan	0	Rizky Januar Akbar, S.Kom, M.Eng

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?	dikembangkan ITS juga tidak didesain seperti itu			
7.3.11	1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Di SubDit IKTI belum ada proses pelaporan insiden. DPTSI belum memiliki proses pelaporan insiden terungkapnya data pribadi	Tidak Dilakukan	0	Hanim Maria Astuti, S.Kom, M.Sc, ITIL Royyana Muslim Itjihadie, S.Kom, M.Kom, Ph.D
7.3.12	1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data	User dapat mengakses data dirinya sendiri	Diterapkan Secara Menyeluruh	4	Rizky Januar Akbar,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		pribadi untuk mengakses data tersebut?	dengan melalui proses autentikasi pada Integra			S.Kom, M.Eng
Temuan Setiap mahasiswa yang mengakses Integra dapat mengakses data Indeks Prestasi, beasiswa yang diperoleh, SKEM, dan data pribadi lain seperti No. HP, e-mail, dan lain-lain						
Bukti						
7.3.13	1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Proses untuk memastikan data yang diakses akurat dilakukan by system	Diterapkan Secara Menyeluruh	3	Rizky Januar Akbar, S.Kom, M.Eng
Temuan Sistem di Integra dapat menampilkan data yang akurat sesuai dengan user yang sudah terautentikasi						

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
Bukti Tidak Ada						
7.3.14	1	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	Tidak ada proses penghapusan, hanya proses pemindahan/ backup data ke teknologi yang membutuhkan waktu lebih lama dalam mengaksesnya. tidak dilakukan atas perjanjian dengan pemilik data	Dalam Penerapan/ Diterapkan Sebagian	2	Rizky Januar Akbar, S.Kom, M.Eng
Temuan Proses pemindahan data-data lama atau data yang sudah tidak begitu dibutuhkan dilakukan oleh Pak Radit						

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
Bukti Tidak Ada						
7.3.15	1	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?	Semua data masih tersimpan	Tidak Dilakukan	0	Rizky Januar Akbar, S.Kom, M.Eng
7.3.16	1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas	Belum menerapkan proses pengungkapan data pribadi, kemungkinan jika itu terjadi biasanya akan	Dalam Perencanaan	1	Royyana Muslim Itjihadie,

Bagian VII: Suplemen						
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh						
No.	**Kate-gori**	**Pertanyaan**	**Jawaban Wawancara**	**Status**	**Skor**	**Narasumber**
		permintaan resmi aparat penegak hukum?	dibuatkan Surat Pengantar atau Surat Perintah dari Direktur DPTSI untuk melakukan pengungkapan data			S.Kom, M.Kom, Ph.D
Rata-Rata Penilaian Perlindungan Data Pribadi					**0.81**	

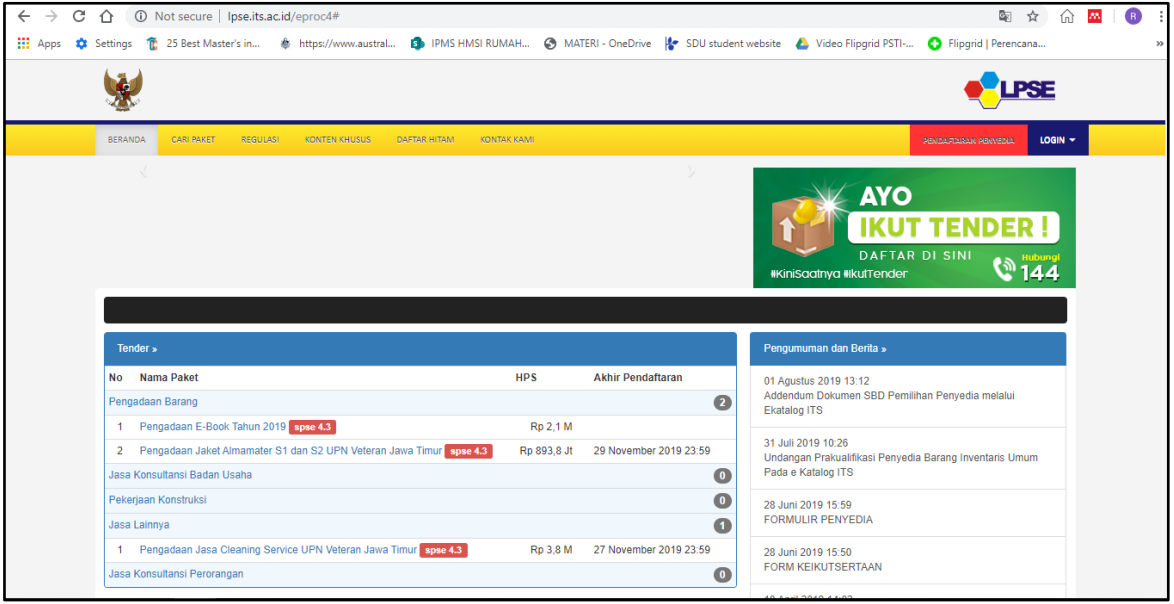
LAMPIRAN B

Bukti Penilaian Indeks KAMI Versi 4.0
DPTSI ITS Surabaya

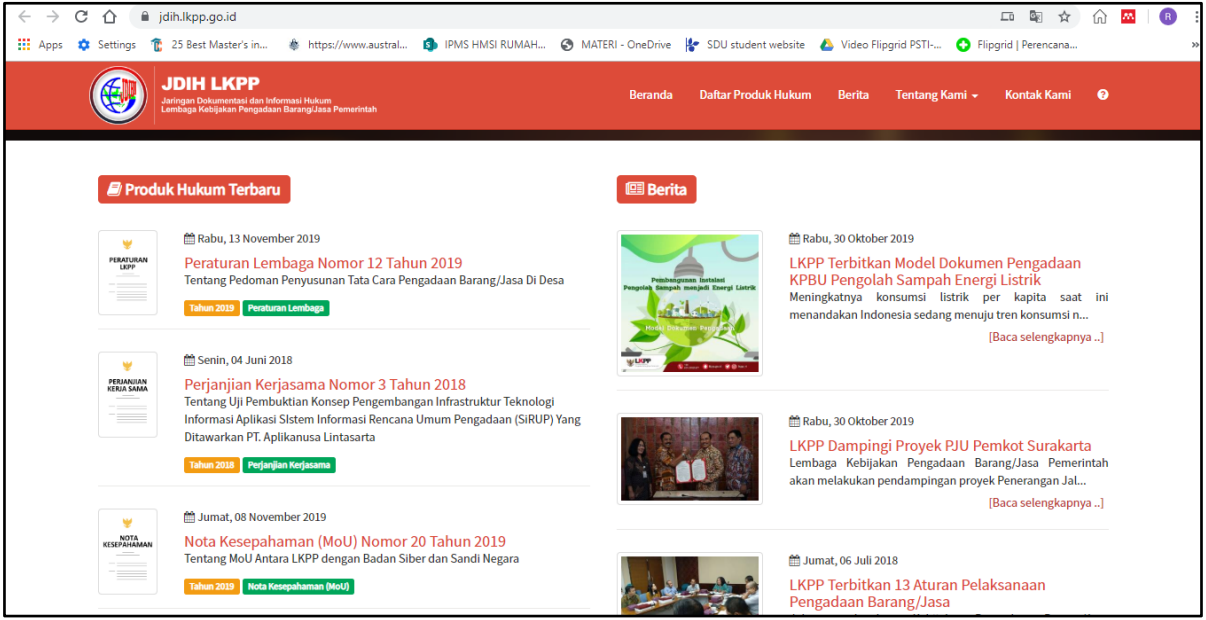
PENGEMBANGAN DIREKTORAT PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI
Laporan Penyerapan Anggaran Belanja per MAK Dana NON PNBP
Periode Januari s.d. Desember TA 2019

Mata Anggaran	Anggaran	UMK Bruto	Pengembalian	UMK Netto	Daya Serap (%)	Sisa Anggaran	SPJ	Realisasi (%)	Sisa UMK
5742.005.001.051 - Pengadaan/pemeliharaan Peralatan Pendukung Perkantoran									
525114 - Belanja Pemeliharaan	762.928.380	894.640.360	270.491.640	624.148.720	81,81	138.779.660	581.855.420	93,22	42.293.300
537112 - Belanja Modal Peralatan dan	747.637.000	477.348.500	114.337.000	363.011.500	48,55	384.625.500	338.879.000	93,35	24.132.500
5742.005.001.052 - Pengadaan/pemeliharaan Meubelair Pendukung Perkantoran									
537112 - Belanja Modal Peralatan dan	130.405.000	0	0	0	0	130.405.000	0	0	0
5742.005.001.053 - Pembangunan/pemeliharaan Gedung Dan Bangunan Pendukung Perkantoran									
537113 - Belanja Modal Gedung dan B	41.598.000	47.195.600	5.597.600	41.598.000	100	0	38.799.200	93,27	2.798.800
5742.994.001.051 - Penyelenggaraan Operasional Perkantoran									
525112 - Belanja Barang	108.894.425	177.220.940	74.722.790	102.498.150	94,13	6.396.275	72.088.790	70,33	30.409.360
525119 - Belanja Penyediaan Barang	0	0	0	0	0	0	0	0	0
5742.994.001.054 - Pembayaran Honor Tenaga Pendidik/tenaga Kependidikan Tenaga Tidak Tetap									
525111 - Belanja Gaji & Tunjangan	396.800.000	286.164.000	42.356.000	243.808.000	61,44	152.992.000	201.620.000	82,7	42.188.000
5742.994.001.055 - Seminar/workshop/promosi Penjaminan Mutu Kelembagaan/organisasi									
525113 - Belanja Jasa	2.500.000	0	0	0	0	2.500.000	0	0	0
525115 - Belanja Perjalanan	9.913.000	16.888.940	8.340.940	8.548.000	86,23	1.365.000	2.603.530	30,46	5.944.470
5742.994.001.057 - Penyusunan Dokumen/laporan Sistem Tata Kelola, Kelembagaan Dan Kegiatan World Class University (wcu)									
525112 - Belanja Barang	20.495.000	36.100.500	16.035.400	20.065.100	97,9	429.900	19.092.500	95,15	972.600
TOTAL	**2.221.170.805**	**1.935.558.840**	**531.881.370**	**1.403.677.470**	**63,2**	**817.493.335**	**1.254.938.440**	**89,4**	**148.739.030**

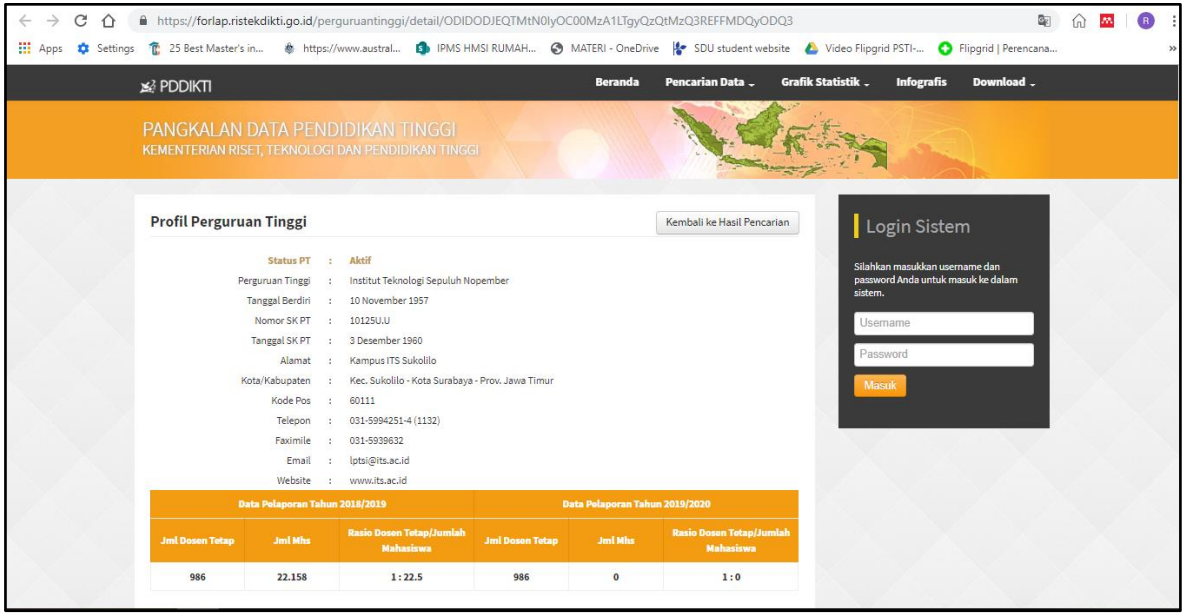
Gambar B.1 Nilai Investasi dan Anggaran Operasional Sistem Elektronik DPTSI



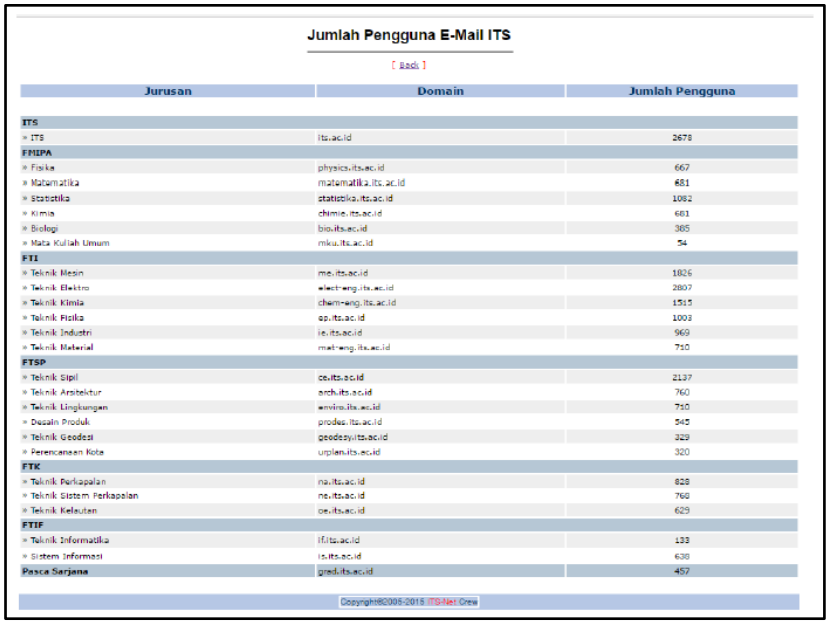
Gambar B.2 Tampilan Website LPSE yang Bekerjsasama dengan ITS



Gambar B.3 Tampilan Website Regulasi LPSE



Gambar B.4 Jumlah Mahasiswa dan Dosen di ITS

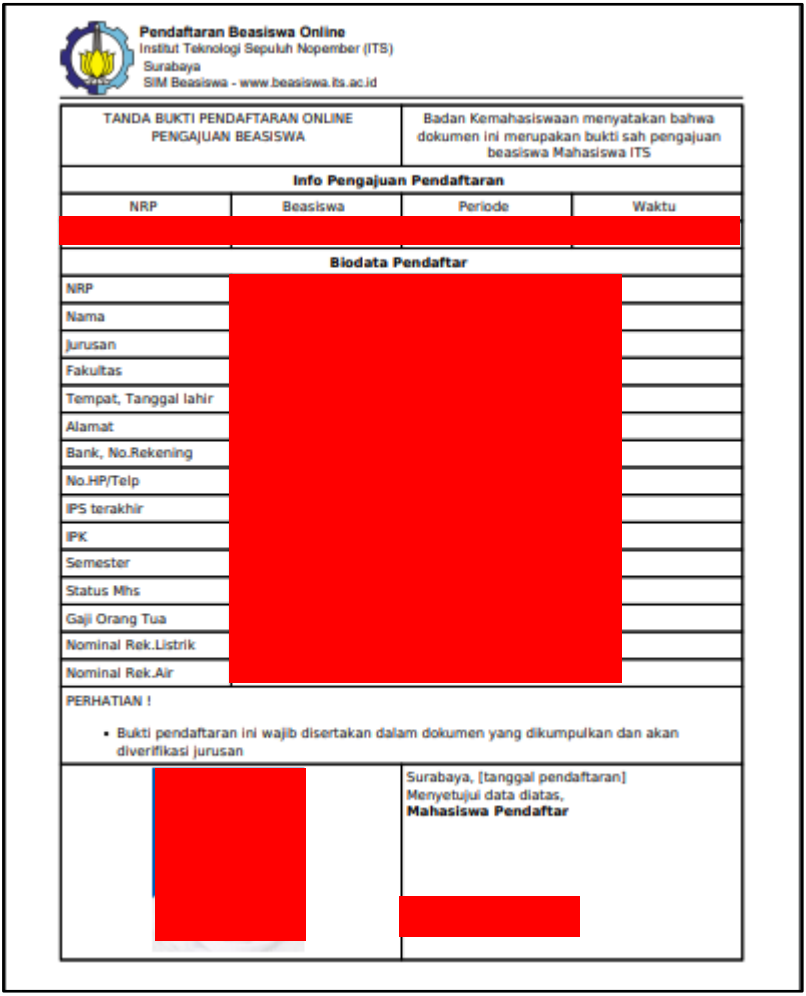


Jumlah Pengguna E-Mail ITS

[Back]

Jurusan	Domain	Jumlah Pengguna
ITS		
» ITS	its.ac.id	2678
FMIPA		
» Fisika	physics.its.ac.id	667
» Matematika	matematika.its.ac.id	681
» Statistika	statistika.its.ac.id	1052
» Kimia	chimie.its.ac.id	681
» Biologi	bio.its.ac.id	385
» Mata Kuliah Umum	mku.its.ac.id	54
FTI		
» Teknik Mesin	me.its.ac.id	1826
» Teknik Elektro	elect-eng.its.ac.id	2807
» Teknik Kimia	chem-eng.its.ac.id	1515
» Teknik Fisika	ep.its.ac.id	1003
» Teknik Industri	ie.its.ac.id	969
» Teknik Material	mat-eng.its.ac.id	750
FTSP		
» Teknik Sipil	ce.its.ac.id	2137
» Teknik Arsitektur	arch.its.ac.id	760
» Teknik Lingkungan	enviro.its.ac.id	750
» Desain Produk	prodes.its.ac.id	545
» Teknik Geodesi	geodesy.its.ac.id	329
» Perencanaan Kota	urplan.its.ac.id	320
FTK		
» Teknik Perkapalan	na.its.ac.id	828
» Teknik Sistem Perkapalan	ne.its.ac.id	760
» Teknik Kelautan	oe.its.ac.id	629
FTIF		
» Teknik Informatika	if.its.ac.id	133
» Sistem Informasi	is.its.ac.id	636
Pasca Sarjana	grad.its.ac.id	457

Gambar B.5 Jumlah Pengguna e-mail ITS



Pendaftaran Beasiswa Online
Institut Teknologi Sepuluh Nopember (ITS)
Surabaya
SIM Beasiswa - www.beasiswa.its.ac.id

TANDA BUKTI PENDAFTARAN ONLINE PENGAJUAN BEASISWA	Badan Kemahasiswaan menyatakan bahwa dokumen ini merupakan bukti sah pengajuan beasiswa Mahasiswa ITS

Info Pengajuan Pendaftaran

NRP	Beasiswa	Periode	Waktu
[redacted]			

Biodata Pendaftar

NRP	[redacted]
Nama	
Jurusan	
Fakultas	
Tempat, Tanggal lahir	
Alamat	
Bank, No.Rekening	
No.HP/Telp	
IPS terakhir	
IPK	
Semester	
Status Mhs	
Gaji Orang Tua	
Nominal Rek.Listrik	
Nominal Rek.Air	

PERHATIAN !

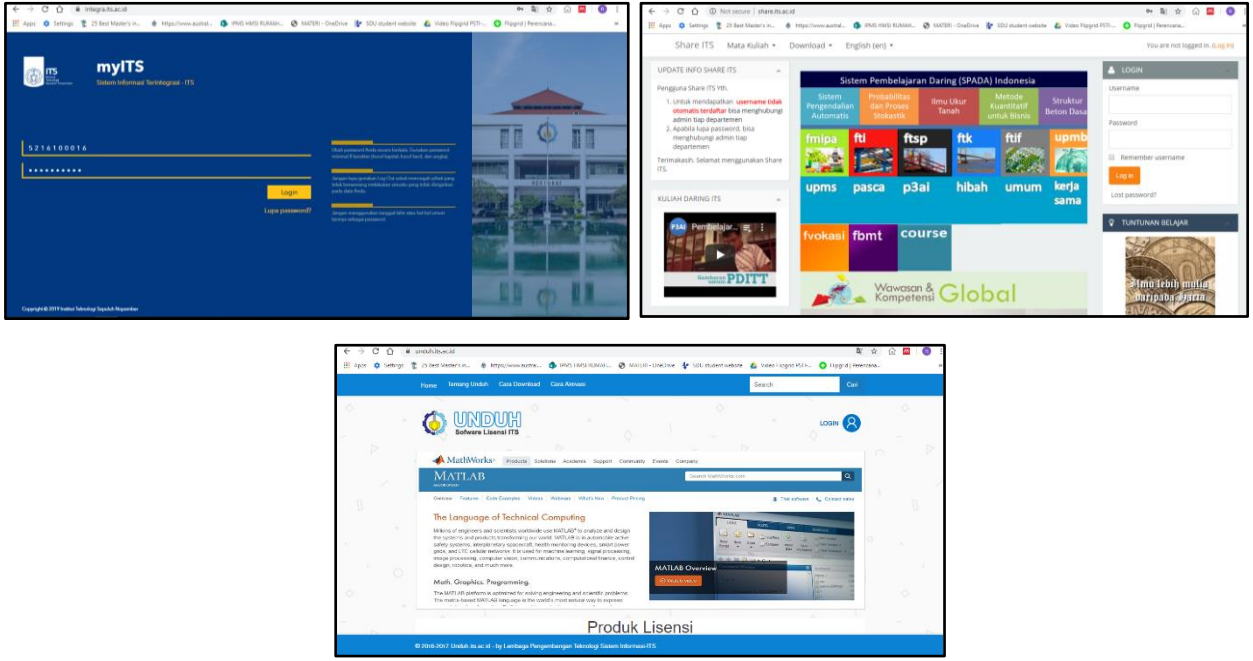
- Bukti pendaftaran ini wajib disertakan dalam dokumen yang dikumpulkan dan akan diverifikasi jurusan

[redacted]

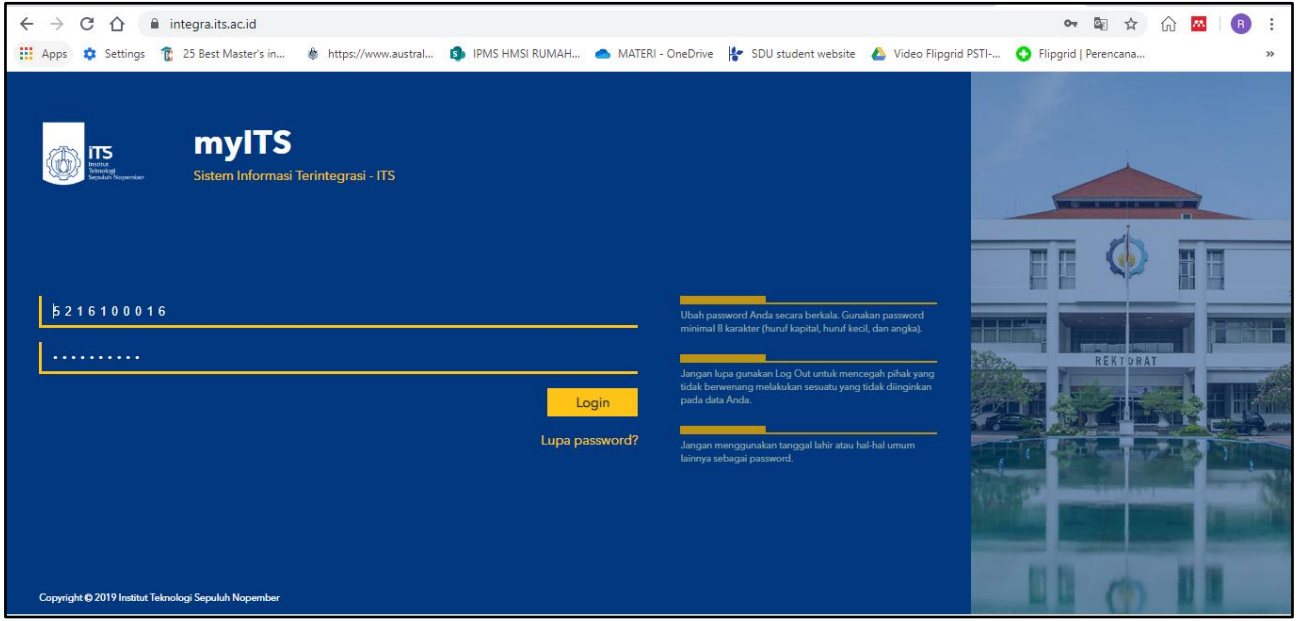
Surabaya, [tanggal pendaftaran]
Menyetujui data diatas,
Mahasiswa Pendaftar

[redacted]

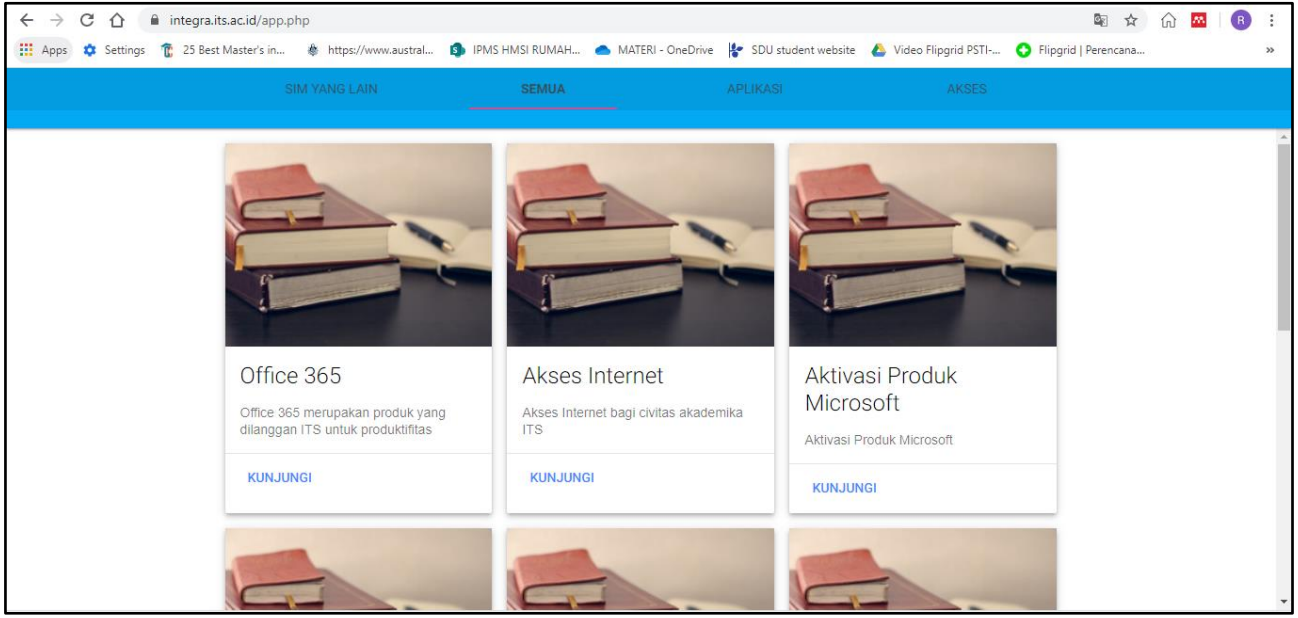
Gambar B.6 Data Pribadi SIM Beasiswa pada Integra



Gambar B.7 Data yang Bersifat Rahasia (Integra, ShareITS, dan UnduhITS)



Gambar B.8 Portal Integra



Gambar B.9 Portal *Single Sign On* (*Redirect* ke *Website* Office 365 ITS)

KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
Kampus ITS Sukolilo-Surabaya 60111
Telp : 031-5994251-54, 5947274, 5945472 (Hunting)
Fax : 031-5947264, 5950806
http://www.its.ac.id

PERATURAN REKTOR INSTITUT TEKNOLOGI SEPULUH NOPEMBER
NOMOR 10 TAHUN 2016

TENTANG

ORGANISASI DAN TATA KERJA INSTITUT TEKNOLOGI SEPULUH NOPEMBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

REKTOR INSTITUT TEKNOLOGI SEPULUH NOPEMBER,

Menimbang :
a. bahwa dalam rangka penetapan Institut Teknologi Sepuluh Nopember sebagai Perguruan Tinggi Negeri Badan Hukum yang akan berimplikasi terhadap pelayanan dan kinerja pelaksanaan kegiatan tridharma perguruan tinggi, maka dibutuhkan organisasi dan tata kerja yang selaras dengan tujuan Institut Teknologi Sepuluh Nopember;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a perlu menetapkan Peraturan Rektor tentang Organisasi dan Tata Kerja ITS;

Mengingat :
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 4286);
2. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 158, Tambahan Lembaran Negara Republik Indonesia Nomor 5336);
3. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 16, Tambahan Lembaran Negara Republik Indonesia Nomor 5500);
4. Peraturan Pemerintah Nomor 83 Tahun 2014 tentang Penetapan Institut Teknologi Sepuluh Nopember sebagai Perguruan Tinggi Negeri Badan Hukum (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 304);
5. Peraturan Pemerintah Nomor 54 Tahun 2015 tentang Statuta Institut Teknologi Sepuluh Nopember (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 172, Tambahan Lembaran Negara Republik Indonesia Nomor 5723);
6. Keputusan Menteri Riset, Teknologi dan Pendidikan Tinggi Nomor 138/M/Kp/IV/2015 tentang Pengangkatan Rektor Institut Teknologi Sepuluh Nopember Masa Jabatan 2015-2019;

MEMUTUSKAN:

Menetapkan : PERATURAN REKTOR INSTITUT TEKNOLOGI SEPULUH NOPEMBER TENTANG ORGANISASI DAN TATA KERJA INSTITUT TEKNOLOGI SEPULUH NOPEMBER.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam peraturan ini yang dimaksud dengan:
1. Institut Teknologi Sepuluh Nopember yang selanjutnya disebut ITS adalah perguruan tinggi negeri badan hukum.
2. Statuta ITS adalah peraturan dasar pengelolaan ITS yang digunakan sebagai landasan penyusunan peraturan dan prosedur operasional di ITS.
3. Rektor adalah organ ITS yang memimpin penyelenggaraan dan pengelolaan ITS.
4. Wakil Rektor adalah pembantu Rektor dalam penyelenggaraan dan pengelolaan ITS pada bidang strategis tertentu.

BAB VI
WAKIL REKTOR III

Bagian Kesatu
Tugas, Fungsi, dan Organisasi

Pasal 55

(1) Wakil Rektor III sebagaimana dimaksud dalam pasal 3 huruf c, mempunyai tugas menyelenggarakan perumusan dan pelaksanaan kebijakan dalam bidang sumber daya manusia, organisasi, dan teknologi dan sistem informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Wakil Rektor III menyelenggarakan fungsi:
    a. penyusunan rencana pengembangan di bidang sumber daya manusia, organisasi, dan teknologi dan sistem informasi;
    b. penyusunan rencana strategis bidang sumber daya manusia, organisasi, dan teknologi dan sistem informasi;
    c. penyusunan program kerja bidang sumber daya manusia, organisasi, dan teknologi dan sistem informasi;
    d. pengelolaan dan pelaporan di bidang sumber daya manusia, organisasi, dan teknologi dan sistem informasi; dan
    e. penyusunan rencana umum pengembangan sumber daya manusia, organisasi, dan teknologi dan sistem informasi.

Pasal 56

Wakil Rektor III terdiri atas:
a. Direktorat Sumber Daya Manusia dan Organisasi;
b. Direktorat Pengembangan Teknologi dan Sistem Informasi; dan
c. Biro Umum.

Bagian Ketiga
Direktorat Pengembangan Teknologi dan Sistem Informasi

Pasal 62

(1) Direktorat Pengembangan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan perumusan kebijakan pengembangan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan di bidang teknologi dan sistem informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Direktorat Pengembangan Teknologi dan Sistem Informasi menyelenggarakan fungsi:
    a. pengelolaan dan pengembangan infrastruktur dan keamanan informasi;
    b. pengelolaan dan pengembangan sistem informasi; dan
    c. pengelolaan dan pengembangan layanan sistem dan teknologi informasi.
(3) Direktorat Pengembangan Teknologi dan Sistem Informasi dipimpin oleh seorang Direktur, yang dalam menjalankan tugasnya bertanggung jawab kepada Wakil Rektor III.

Pasal 63

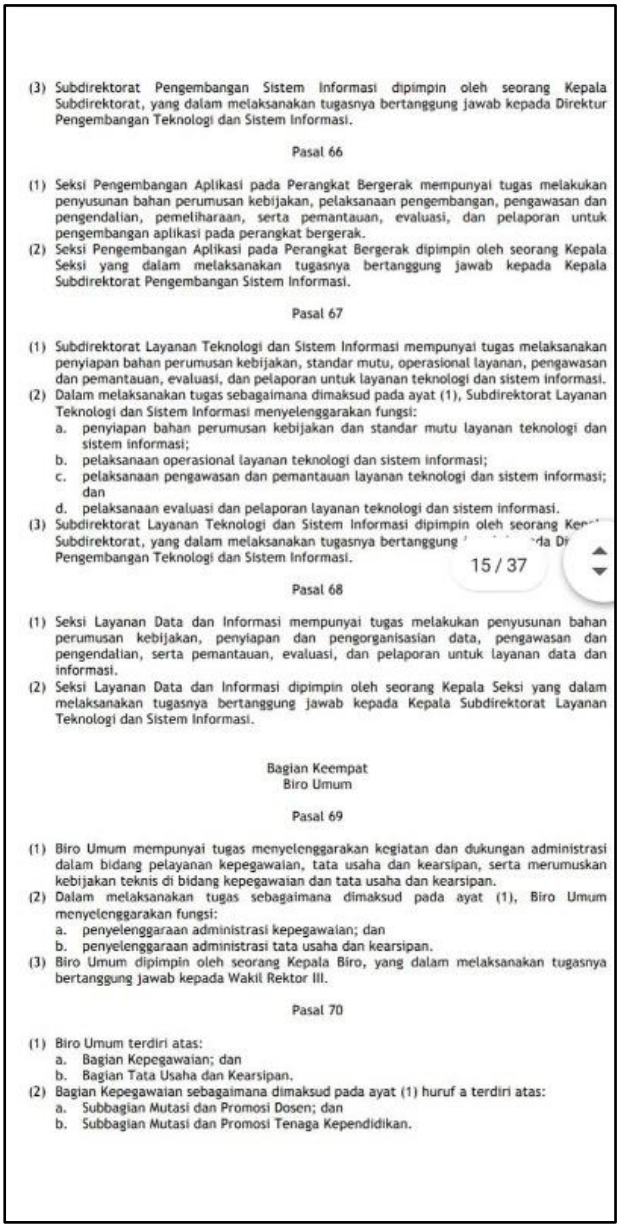
(1) Direktorat Pengembangan Teknologi dan Sistem Informasi terdiri atas:
    a. Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi;
    b. Subdirektorat Pengembangan Sistem Informasi; dan
    c. Subdirektorat Layanan Teknologi dan Sistem Informasi.
(2) Subdirektorat Pengembangan Sistem Informasi, sebagaimana dimaksud pada ayat (1) huruf b, dibantu oleh Seksi Pengembangan Aplikasi pada Perangkat Bergerak.
(3) Subdirektorat Layanan Teknologi dan Sistem Informasi sebagaimana dimaksud pada ayat (1) huruf c, dibantu oleh Seksi Layanan Data dan Informasi.

Pasal 64

(1) 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.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi menyelenggarakan fungsi:
    a. penyiapan bahan perumusan kebijakan dan standar mutu pengembangan infrastruktur dan keamanan teknologi informasi;
    b. pelaksanaan pengembangan infrastruktur dan keamanan teknologi informasi;
    c. pelaksanaan pengawasan dan pemantauan pengembangan infrastruktur dan keamanan teknologi informasi;
    d. pelaksanaan pemeliharaan infrastruktur dan keamanan teknologi informasi; dan
    e. pelaksanaan evaluasi dan pelaporan infrastruktur dan keamanan teknologi informasi.
(3) Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi dipimpin oleh seorang Kepala Subdirektorat, yang dalam melaksanakan tugasnya bertanggung jawab kepada Direktur Pengembangan Teknologi dan Sistem Informasi.

Pasal 65

(1) 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.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdirektorat Pengembangan Sistem Informasi menyelenggarakan fungsi:
    a. penyiapan bahan perumusan kebijakan dan standar mutu pengembangan sistem informasi;
    b. pelaksanaan pengembangan sistem informasi;
    c. pelaksanaan pengawasan dan pemantauan pengembangan sistem informasi;
    d. pelaksanaan pemeliharaan data dan sistem informasi; dan
    e. pelaksanaan evaluasi dan pelaporan pengembangan sistem informasi.



(3) Subdirektorat Pengembangan Sistem Informasi dipimpin oleh seorang Kepala Subdirektorat, yang dalam melaksanakan tugasnya bertanggung jawab kepada Direktur Pengembangan Teknologi dan Sistem Informasi.

Pasal 66

(1) Seksi Pengembangan Aplikasi pada Perangkat Bergerak mempunyai tugas melakukan penyusunan bahan perumusan kebijakan, pelaksanaan pengembangan, pengawasan dan pengendalian, pemeliharaan, serta pemantauan, evaluasi, dan pelaporan untuk pengembangan aplikasi pada perangkat bergerak.
(2) Seksi Pengembangan Aplikasi pada Perangkat Bergerak dipimpin oleh seorang Kepala Seksi yang dalam melaksanakan tugasnya bertanggung jawab kepada Kepala Subdirektorat Pengembangan Sistem Informasi.

Pasal 67

(1) Subdirektorat Layanan Teknologi dan Sistem Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, operasional layanan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk layanan teknologi dan sistem informasi.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Subdirektorat Layanan Teknologi dan Sistem Informasi menyelenggarakan fungsi:
   a. penyiapan bahan perumusan kebijakan dan standar mutu layanan teknologi dan sistem informasi;
   b. pelaksanaan operasional layanan teknologi dan sistem informasi;
   c. pelaksanaan pengawasan dan pemantauan layanan teknologi dan sistem informasi; dan
   d. pelaksanaan evaluasi dan pelaporan layanan teknologi dan sistem informasi.
(3) Subdirektorat Layanan Teknologi dan Sistem Informasi dipimpin oleh seorang Ker[illegible] Subdirektorat, yang dalam melaksanakan tugasnya bertanggung [illegible]da Di[illegible] Pengembangan Teknologi dan Sistem Informasi.

15 / 37

Pasal 68

(1) Seksi Layanan Data dan Informasi mempunyai tugas melakukan penyusunan bahan perumusan kebijakan, penyiapan dan pengorganisasian data, pengawasan dan pengendalian, serta pemantauan, evaluasi, dan pelaporan untuk layanan data dan informasi.
(2) Seksi Layanan Data dan Informasi dipimpin oleh seorang Kepala Seksi yang dalam melaksanakan tugasnya bertanggung jawab kepada Kepala Subdirektorat Layanan Teknologi dan Sistem Informasi.

Bagian Keempat
Biro Umum

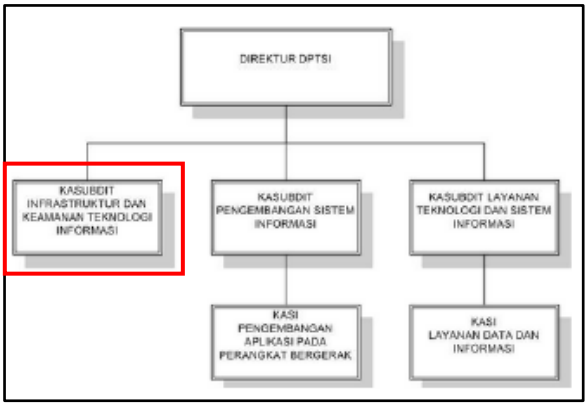
Pasal 69

(1) Biro Umum mempunyai tugas menyelenggarakan kegiatan dan dukungan administrasi dalam bidang pelayanan kepegawaian, tata usaha dan kearsipan, serta merumuskan kebijakan teknis di bidang kepegawaian dan tata usaha dan kearsipan.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Biro Umum menyelenggarakan fungsi:
   a. penyelenggaraan administrasi kepegawaian; dan
   b. penyelenggaraan administrasi tata usaha dan kearsipan.
(3) Biro Umum dipimpin oleh seorang Kepala Biro, yang dalam melaksanakan tugasnya bertanggung jawab kepada Wakil Rektor III.

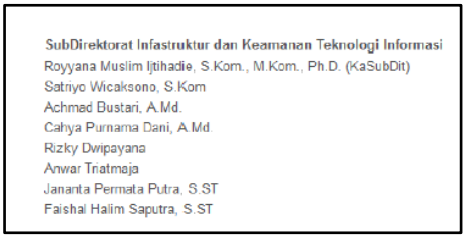
Pasal 70

(1) Biro Umum terdiri atas:
   a. Bagian Kepegawaian; dan
   b. Bagian Tata Usaha dan Kearsipan.
(2) Bagian Kepegawaian sebagaimana dimaksud pada ayat (1) huruf a terdiri atas:
   a. Subbagian Mutasi dan Promosi Dosen; dan
   b. Subbagian Mutasi dan Promosi Tenaga Kependidikan.

Gambar B.10 Peraturan Rektor ITS No. 10 tahun 2016



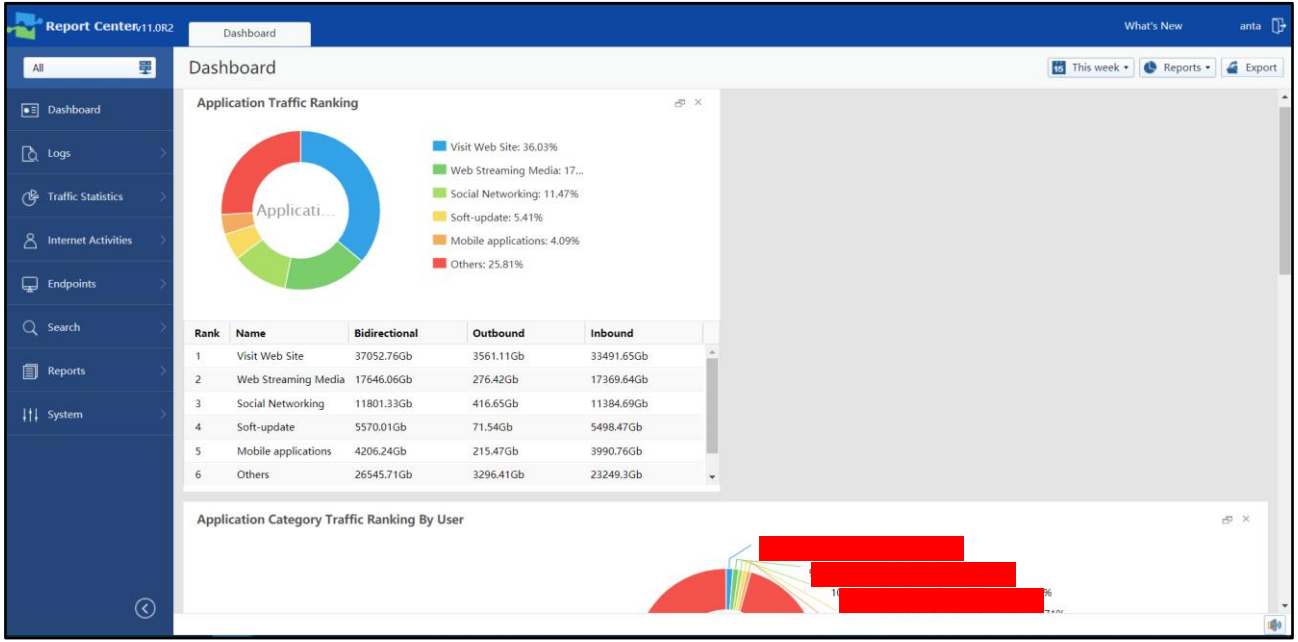
Gambar B.11 Struktur Organisasi DPTSI



Gambar B.12 Jumlah Pegawai Sub Direktorat Infrastruktur dan Keamanan Informasi DPTSI

Gambar B.13 Pemasangan Honeynet Penghubung Honeypot di ITS

Gambar B.14 Koordinasi Penyelesaian Masalah dengan Pihak Eksternal via e-mail



Gambar B.15 *Report Internet Access Management* ITS

1. **Tujuan**
   Membuat akun e-mail yang diminta oleh pengguna layanan (user) BTSI.

2. **Ruang Lingkup**
   Mengatur proses pembuatan E-mail ITS yang diminta oleh pengguna layanan (user)BTSI, yaitu:
   - Tenaga pendidik (Dosen ITS)
   - Tenaga kependidikan (Karyawan ITS)
   - Pejabat di lingkungan ITS
   - Unit kerja yang terdapat di lingkungan ITS
   - Mahasiswa ITS.

3. **Definisi**
   - E-mail ITS merupakan akun surat elektronik yang disediakan oleh BTSI yang dapat digunakan oleh pihak-pihak tertentu di lingkungan ITS. Selain sebagai sarana komunikasi, e-mail tersebut juga digunakan untuk proses *autentifikasi* penggunaan fasilitas IT seperti Wi-Fi dan Internet.
   - Tenaga pendidik ialah PNS kementerian di bidang pendidikan nasional yang ditempatkan di ITS, dan non PNS yang diangkat Rektor sesuai dengan peraturan perundang-undangan.
   - Tenaga kependidikan ialah mereka yang bekerja di ITS baik yang berstatus PNS maupun non PNS.
   - Pejabat adalah para pemegang jabatan struktural di ITS.
   - Unit kerja merupakan unsur pelaksana administrasi, pelaksana akademik, pengembang dan pelaksana tugas strategis, dan unsur penunjang yang berada di ITS.
   - Mahasiswa adalah mereka yang terdaftar sebagai peserta didik pendidikan akademik, vokasi, dan profesi di ITS.

4. **Dokumen terkait**
   - Manual cara pendaftaran
   - Standardisasi penamaan e-mail
   - ketentuan layanan pembuatan e-mail
   - ketentuan penggunaan e-mail
   - Surat permohonan pembuatan E-Mail ITS.

5. **Rincian Prosedur**
   - Melalui **website (webmail.its.ac.id atau gmail.its.ac.id)**, khusus untuk **Mahasiswa dan Tenaga Pendidik**:

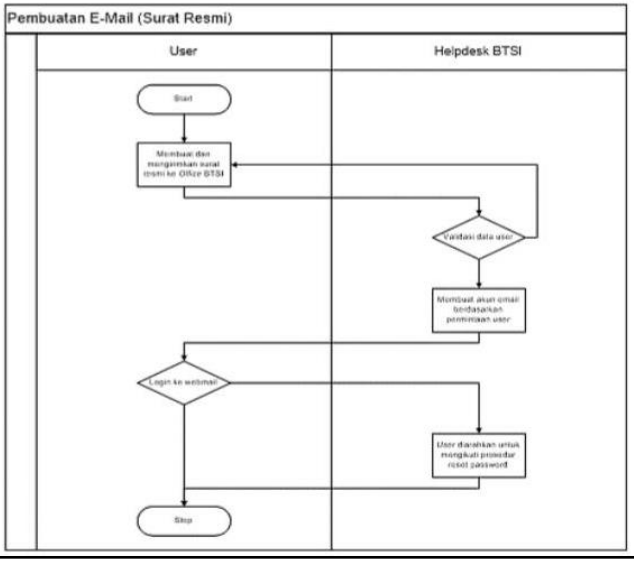
NO	ENTITAS	AKTIVITAS
1.	User	- Mengentrikan NRP/NIP dan password integra - Memilih alamat email dan memasukkan password yang diinginkan - Menunggu validasi, maksimal 1x24 jam kerja.
2.	Operator BTSI	Melakukan validasi.
3.	User	- Login ke webmail. Jika gagal, user disrahkan untuk mengikuti prosedur reset password atau manual reset password email ITS.

– Melalui surat resmi, khusus untuk Pejabat dan Unit yang ada di lingkungan ITS.

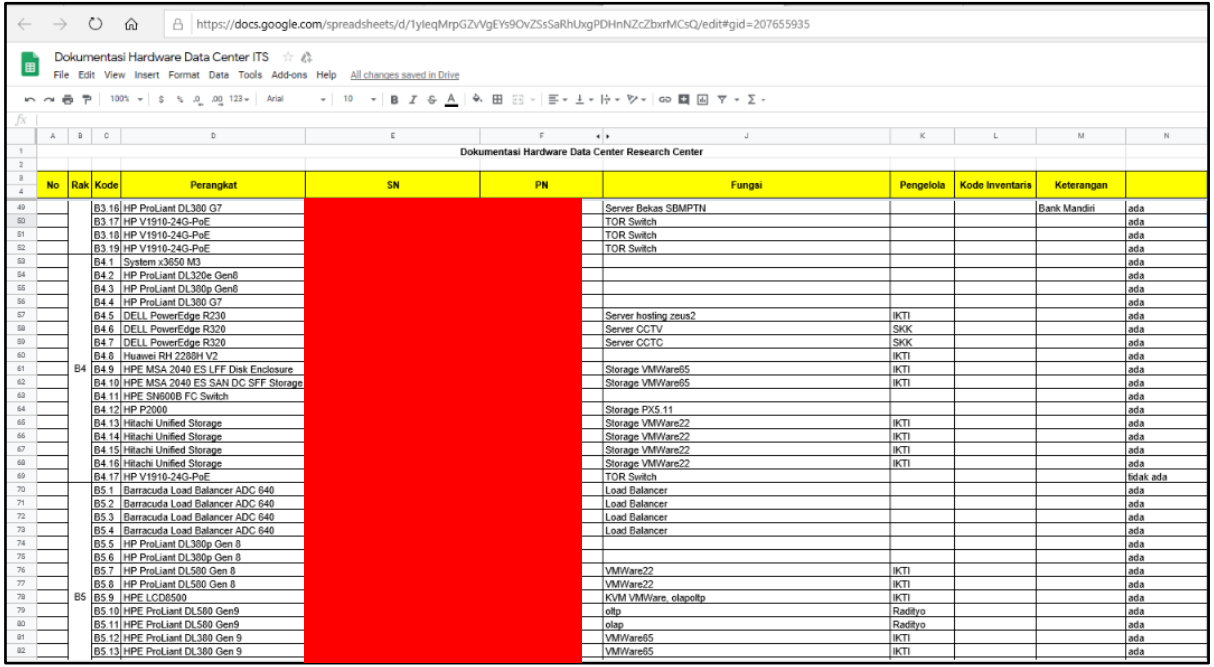
NO	ENTITAS	AKTIVITAS
1.	*User*	- Membuat dan mengirimkan surat resmi ke *Office* BTSI dengan menyebutkan nama, NIP, jabatan, alamat e-mail yang diminta, dan password sementara - Selain terdapat tanda tangan *user*, surat resmi harus disetujui oleh Pejabat Struktural terdekat. - Menunggu proses pendaftaran, maksimal 1x24 jam kerja.
2.	Operator BTSI	- Melakukan validasi data *user* - Membuat akun email berdasarkan permintaan *user*, dengan memasukkan data nama, NIP, jabatan, alamat e-mail yang diminta, dan password sementara.
3.	*User*	- Login ke webmail. Jika gagal, *user* diarahkan untuk mengikuti prosedur reset password atau manual reset password email ITS.

Bagi Tenaga Kependidikan:

NO	ENTITAS	AKTIVITAS
1.	*User*	- Menghubungi *Office* BTSI dengan menyebutkan nama, NIP, alamat e-mail yang diminta, dan password sementara. - Menunggu proses pendaftaran, maksimal 1x24 jam kerja.
2.	Operator BTSI	- Melakukan validasi data *user* - Membuat akun email berdasarkan permintaan *user*, dengan memasukkan data nama, NIP, alamat e-mail yang diminta, dan password sementara
3.	*User*	- Login ke webmail. Jika gagal, *user* diarahkan untuk mengikuti prosedur reset password atau manual reset password email ITS.



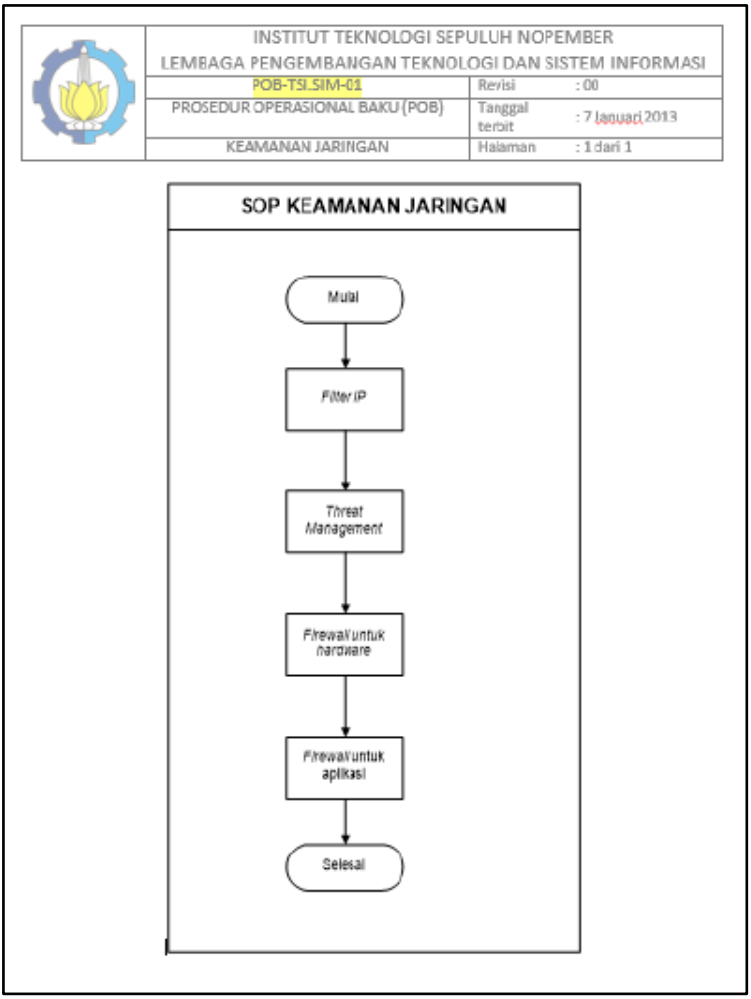
Gambar B.16 Prosedur Pembuatan e-mail ITS



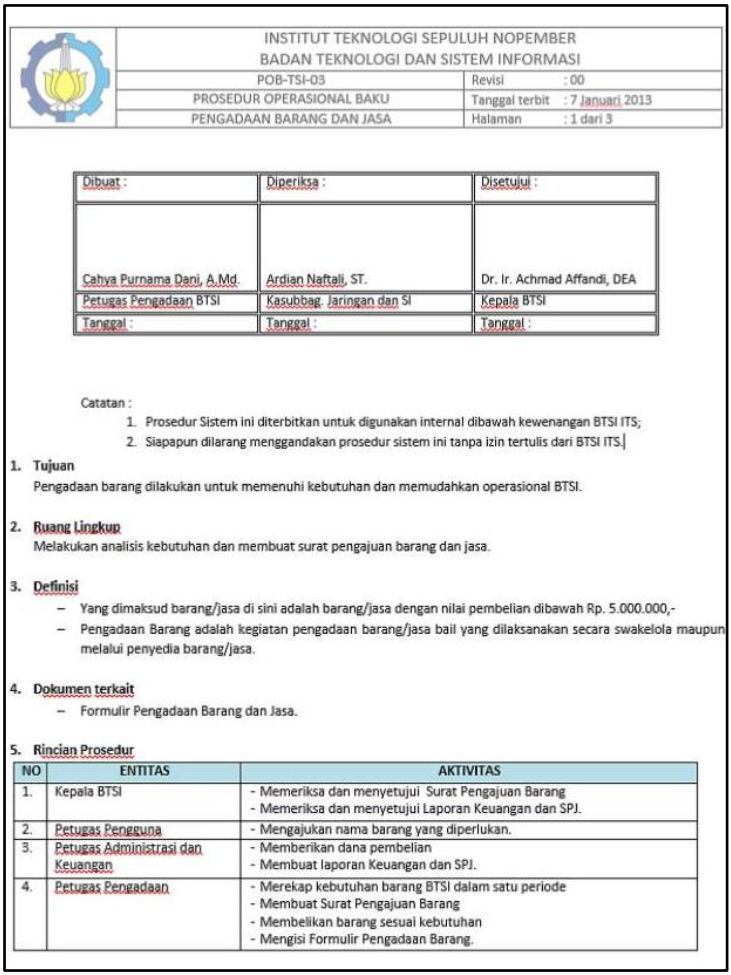
No	Rak	Kode	Perangkat	SN	PN	Fungsi	Pengelola	Kode Inventaris	Keterangan	
		B3.16	HP ProLiant DL380 G7			Server Bekas SBMPTN			Bank Mandiri	ada
		B3.17	HP V1910-24G-PoE			TOR Switch				ada
		B3.18	HP V1910-24G-PoE			TOR Switch				ada
		B3.19	HP V1910-24G-PoE			TOR Switch				ada
		B4.1	System x3650 M3							ada
		B4.2	HP ProLiant DL320e Gen8							ada
		B4.3	HP ProLiant DL380p Gen8							ada
		B4.4	HP ProLiant DL380 G7							ada
		B4.5	DELL PowerEdge R230			Server hosting zeus2	IKTI			ada
		B4.6	DELL PowerEdge R320			Server CCTV	SKK			ada
		B4.7	DELL PowerEdge R320			Server CCTC	SKK			ada
		B4.8	Huawei RH 2288H V2				IKTI			ada
	B4	B4.9	HPE MSA 2040 ES LFF Disk Enclosure			Storage VMWare65	IKTI			ada
		B4.10	HPE MSA 2040 ES SAN DC SFF Storage			Storage VMWare65	IKTI			ada
		B4.11	HPE SN600B FC Switch							ada
		B4.12	HP P2000			Storage PX5.11				ada
		B4.13	Hitachi Unified Storage			Storage VMWare22	IKTI			ada
		B4.14	Hitachi Unified Storage			Storage VMWare22	IKTI			ada
		B4.15	Hitachi Unified Storage			Storage VMWare22	IKTI			ada
		B4.16	Hitachi Unified Storage			Storage VMWare22	IKTI			ada
		B4.17	HP V1910-24G-PoE			TOR Switch				tidak ada
		B5.1	Barracuda Load Balancer ADC 640			Load Balancer				ada
		B5.2	Barracuda Load Balancer ADC 640			Load Balancer				ada
		B5.3	Barracuda Load Balancer ADC 640			Load Balancer				ada
		B5.4	Barracuda Load Balancer ADC 640			Load Balancer				ada
		B5.5	HP ProLiant DL380p Gen 8							ada
		B5.6	HP ProLiant DL380p Gen 8							ada
		B5.7	HP ProLiant DL580 Gen 8			VMWare22	IKTI			ada
		B5.8	HP ProLiant DL580 Gen 8			VMWare22	IKTI			ada
	B5	B5.9	HPE LCD8500			KVM VMWare, olapoltp	IKTI			ada
		B5.10	HPE ProLiant DL580 Gen9			oltp	Radityo			ada
		B5.11	HPE ProLiant DL580 Gen9			olap	Radityo			ada
		B5.12	HPE ProLiant DL380 Gen 9			VMWare65	IKTI			ada
		B5.13	HPE ProLiant DL380 Gen 9			VMWare65	IKTI			ada

Gambar B. 17 Daftar Aset DPTSI

Gambar B.18 Tabung Gas Pemadam Kebakaran, Box Panel Listrik, dan CCTV



Gambar B.19 Prosedur Keamanan Jaringan



	INSTITUT TEKNOLOGI SEPULUH NOPEMBER BADAN TEKNOLOGI DAN SISTEM INFORMASI	
	POB-TSI-03	Revisi : 00
	PROSEDUR OPERASIONAL BAKU	Tanggal terbit : 7 Januari 2013
	PENGADAAN BARANG DAN JASA	Halaman : 1 dari 3

Dibuat :	Diperiksa :	Disetujui :
Cahya Purnama Dani, A.Md.	Ardian Naftali, ST.	Dr. Ir. Achmad Affandi, DEA
Petugas Pengadaan BTSI	Kasubbag. Jaringan dan SI	Kepala BTSI
Tanggal :	Tanggal :	Tanggal :

Catatan :

1. Prosedur Sistem ini diterbitkan untuk digunakan internal dibawah kewenangan BTSI ITS;
2. Siapapun dilarang menggandakan prosedur sistem ini tanpa izin tertulis dari BTSI ITS.

1. Tujuan

Pengadaan barang dilakukan untuk memenuhi kebutuhan dan memudahkan operasional BTSI.

2. Ruang Lingkup

Melakukan analisis kebutuhan dan membuat surat pengajuan barang dan jasa.

3. Definisi

- Yang dimaksud barang/jasa di sini adalah barang/jasa dengan nilai pembelian dibawah Rp. 5.000.000,-
- Pengadaan Barang adalah kegiatan pengadaan barang/jasa bail yang dilaksanakan secara swakelola maupun melalui penyedia barang/jasa.

4. Dokumen terkait

- Formulir Pengadaan Barang dan Jasa.

5. Rincian Prosedur

NO	ENTITAS	AKTIVITAS
1.	Kepala BTSI	- Memeriksa dan menyetujui Surat Pengajuan Barang - Memeriksa dan menyetujui Laporan Keuangan dan SPJ.
2.	Petugas Pengguna	- Mengajukan nama barang yang diperlukan.
3.	Petugas Administrasi dan Keuangan	- Memberikan dana pembelian - Membuat laporan Keuangan dan SPJ.
4.	Petugas Pengadaan	- Merekap kebutuhan barang BTSI dalam satu periode - Membuat Surat Pengajuan Barang - Membelikan barang sesuai kebutuhan - Mengisi Formulir Pengadaan Barang.

Gambar B.20 Prosedur Pengadaan Barang dan Jasa

	INSTITUT TEKNOLOGI SEPULUH NOPEMBER BADAN TEKNOLOGI DAN SISTEM INFORMASI		
	POB-TSI-05	Revisi	: 00
	PROSEDUR OPERASIONAL BAKU (POB)	Tanggal terbit	: 7 Januari 2013
	PEMUSNAHAN DOKUMEN	Halaman	: 1 dari 3

Dibuat :	Disetujui :
Suroso	Dr. Ir. Achmad Affandi, DEA.
Staf BTSI	Kepala BTSI
Tanggal : 7 Januari 2013	Tanggal : 7 Januari 2013

Catatan :

1. Prosedur Sistem ini diterbitkan untuk digunakan internal dibawah kewenangan BTSI
2. Siapapun dilarang menggandakan prosedur sistem ini tanpa izin tertulis dari BTSI ITS

1. **Tujuan**

   Tertib administrasi

2. **Ruang Lingkup**

   Pelanggan, Bagian Arsip

3. **Definisi**

   Pelanggan adalah orang/lembaga/instansi yang menggunakan jasa UPT PUSKOM

   Bagian Arsip adalah petugas UPT PUSKOM yang bertanggungjawab terhadap pengarsipan dokumen Pelanggan

4. **Dokumen terkait**

   Berita Acara Pemusnahan Dokumen Pelanggan

5. **Rincian Prosedur**

NO	PENANGGUNG JAWAB	AKTIVITAS
1	Pelanggan	○ Mengambil dokumen pelanggan atau memberikan kewenangan untuk memusnahkan dokumen kepada UPT PUSKOM
2	Bagian Arsip	○ Mengirim surat pemberitahuan kepada pelanggan bahwa dokumen miliknya sudah habis masa simpan ○ Membuat Berita Acara Pemusnahan Dokumen Pelanggan

Gambar B.21 Prosedur Penghancuran Dokumen

	INSTITUT TEKNOLOGI SEPULUH NOPEMBER BADAN TEKNOLOGI DAN SISTEM INFORMASI	
	POB-TSI.YAN-05	Revisi : 00
	PROSEDUR OPERASIONAL BAKU (POB)	Tanggal terbit : 7 Januari 2013
	LAYANAN PENYEDIAAN LEGAL SOFTWARE	Halaman : 1 dari 4

Dibuat :	Diperiksa :	Disetujui :
Mudjiatin	Arief Rahman, ST., M.Sc.	Dr. Ir. Achmad Affandi, DEA
Staf Pusyan	Kapus. Pengelolaan dan Pelayanan TIK	Kepala BTSI
Tanggal : 7 Januari 2013	Tanggal : 7 Januari 2013	Tanggal : 7 Januari 2013

1. **Tujuan**
   Mengatur ketentuan-ketentuan terkait layanan legal software.

2. **Ruang Lingkup**
   Mengatur proses layanan penyediaan *legal software*, yang meliputi proses analisis kebutuhan, pembelian, dan pengunggahan ke *server* ITS.

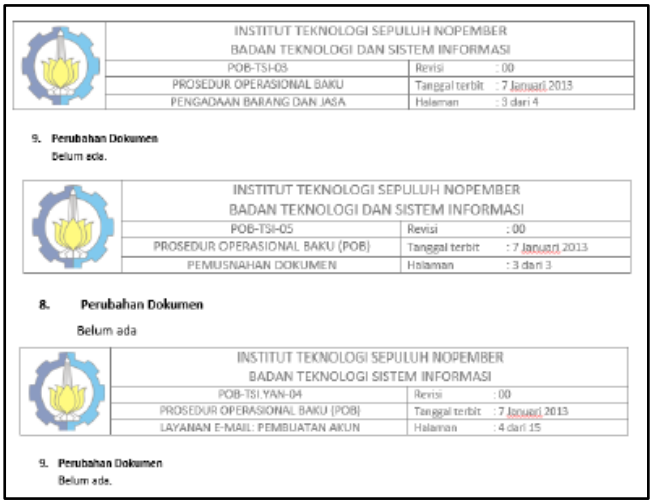
3. **Definisi**
   - *Legal software* merupakan segala perangkat lunak resmi yang disediakan oleh ITS untuk kebutuhan civitas akademika.

4. **Dokumen terkait**
   - Form kebutuhan *software*

5. **Rincian Prosedur**

NO	ENTITAS	AKTIVITAS
1.	Unit/Jurusan	- Masing-masing unit/jurusan memberikan daftar kebutuhan software beserta spesifikasinya ke Kepala Pusat Layanan BTSI.
2.	Kepala Pusat Layanan	- Mengumpulkan daftar *software* yang menjadi kebutuhan dari semua unit di ITS, baik yang baru maupun yang perlu pembaruan lisensi. Pengumpulan juga dapat dilakukan dengan meminta masing-masing unit untuk mengirimkan daftar kebutuhan software beserta spesifikasinya. - Melakukan analisis spesifikasi dan harga *software*, sekaligus melakukan pencarian penawaran yang berkaitan dengan *software-software* tersebut. - Membuat/menyusun daftar prioritas *software* yang akan dibeli. - Memeriksa anggaran yang ada. Jika tidak mencukupi, harus dilakukan lagi analisis untuk mengurangi jumlah pengeluaran. - Jika anggaran tercukupi, maka proposal pengadaan dibuat, kemudian diteruskan pada Kepala BTSI.
3.	Kepala BTSI	Melakukan evaluasi terhadap proposal pengadaan. Apakah dinilai boleh atau tidak untuk dikerjakan. Jika: – Boleh, Kepala BTSI mengirimkan surat permintaan pengadaan *software* ke Unit Layanan Pengadaan. – Tidak, maka proposal harus direvisi berdasarkan rekomendasi Kepala BTSI.
4.	Unit Layanan Pengadaan	Melakukan proses pengadaan (pembelian).
5.	Panitia Penerima *Software*	- Melakukan pemeriksaan terhadap *software* yang baru dibeli sebelum diputuskan untuk dipakai/diterima. Jika *software* yang bersangkutan tidak sesuai dengan harapan, maka dikembalikan pada ULP. - Software yang sesuai akan dilakukan penerimaan secara legal/resmi.
6.	Subbag Jaringan	Menerima *software* yang telah diterima secara resmi, dan melakukan pengunggahan ke *server* ITS.

Gambar B.22 Prosedur Legal Perangkat Lunak



INSTITUT TEKNOLOGI SEPULUH NOPEMBER BADAN TEKNOLOGI DAN SISTEM INFORMASI		
POB-TSI-03	Revisi	: 00
PROSEDUR OPERASIONAL BAKU	Tanggal terbit	: 7 Januari 2013
PENGADAAN BARANG DAN JASA	Halaman	: 3 dari 4

9. **Perubahan Dokumen**
Belum ada.

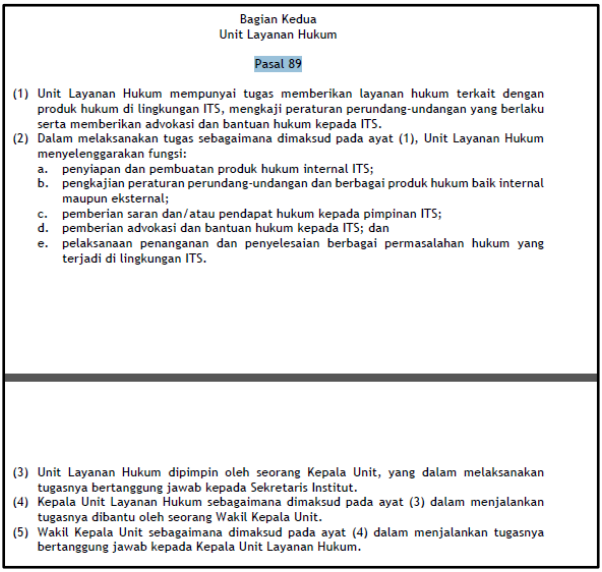
INSTITUT TEKNOLOGI SEPULUH NOPEMBER BADAN TEKNOLOGI DAN SISTEM INFORMASI		
POB-TSI-05	Revisi	: 00
PROSEDUR OPERASIONAL BAKU (POB)	Tanggal terbit	: 7 Januari 2013
PEMUSNAHAN DOKUMEN	Halaman	: 3 dari 3

8. **Perubahan Dokumen**
Belum ada

INSTITUT TEKNOLOGI SEPULUH NOPEMBER BADAN TEKNOLOGI SISTEM INFORMASI		
POB-TSI YAN-04	Revisi	: 00
PROSEDUR OPERASIONAL BAKU (POB)	Tanggal terbit	: 7 Januari 2013
LAYANAN E-MAIL: PEMBUATAN AKUN	Halaman	: 4 dari 15

9. **Perubahan Dokumen**
Belum ada.

Gambar B.23 Bukti Belum Ada Pembaruan Dokumen Prosedur



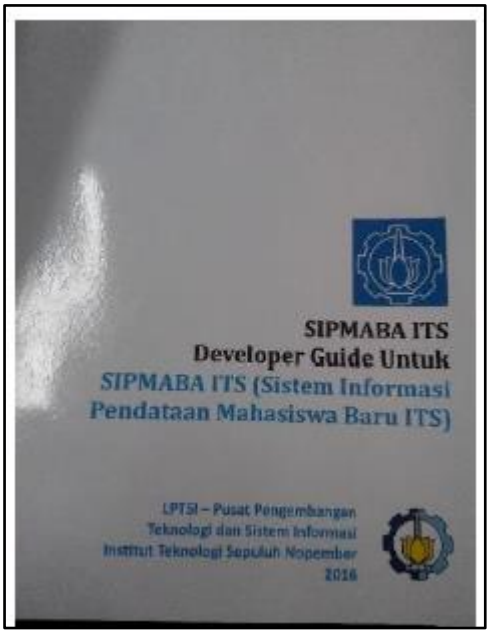
Bagian Kedua
Unit Layanan Hukum

Pasal 89

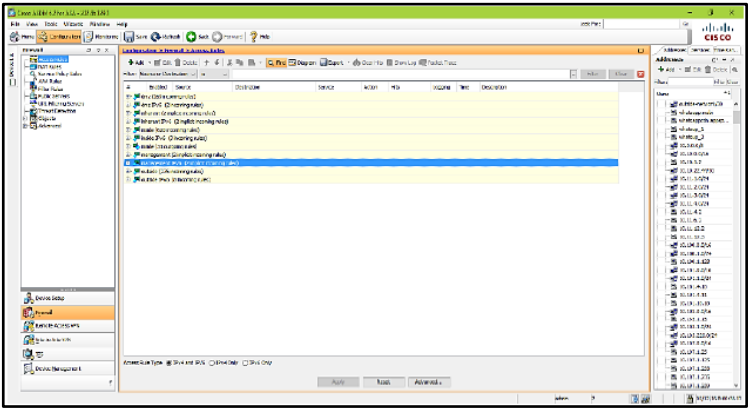
(1) Unit Layanan Hukum mempunyai tugas memberikan layanan hukum terkait dengan produk hukum di lingkungan ITS, mengkaji peraturan perundang-undangan yang berlaku serta memberikan advokasi dan bantuan hukum kepada ITS.
(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Unit Layanan Hukum menyelenggarakan fungsi:
   a. penyiapan dan pembuatan produk hukum internal ITS;
   b. pengkajian peraturan perundang-undangan dan berbagai produk hukum baik internal maupun eksternal;
   c. pemberian saran dan/atau pendapat hukum kepada pimpinan ITS;
   d. pemberian advokasi dan bantuan hukum kepada ITS; dan
   e. pelaksanaan penanganan dan penyelesaian berbagai permasalahan hukum yang terjadi di lingkungan ITS.

(3) Unit Layanan Hukum dipimpin oleh seorang Kepala Unit, yang dalam melaksanakan tugasnya bertanggung jawab kepada Sekretaris Institut.
(4) Kepala Unit Layanan Hukum sebagaimana dimaksud pada ayat (3) dalam menjalankan tugasnya dibantu oleh seorang Wakil Kepala Unit.
(5) Wakil Kepala Unit sebagaimana dimaksud pada ayat (4) dalam menjalankan tugasnya bertanggung jawab kepada Kepala Unit Layanan Hukum.

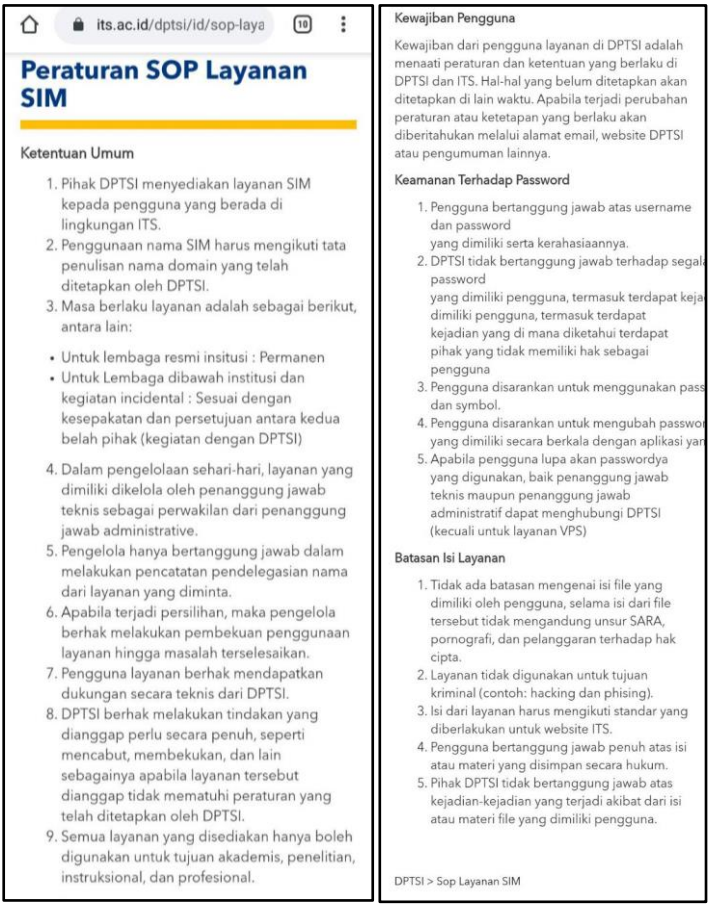
Gambar B 24 Pasal 89 Peraturan Rektor ITS No. 10 Tahun 2016



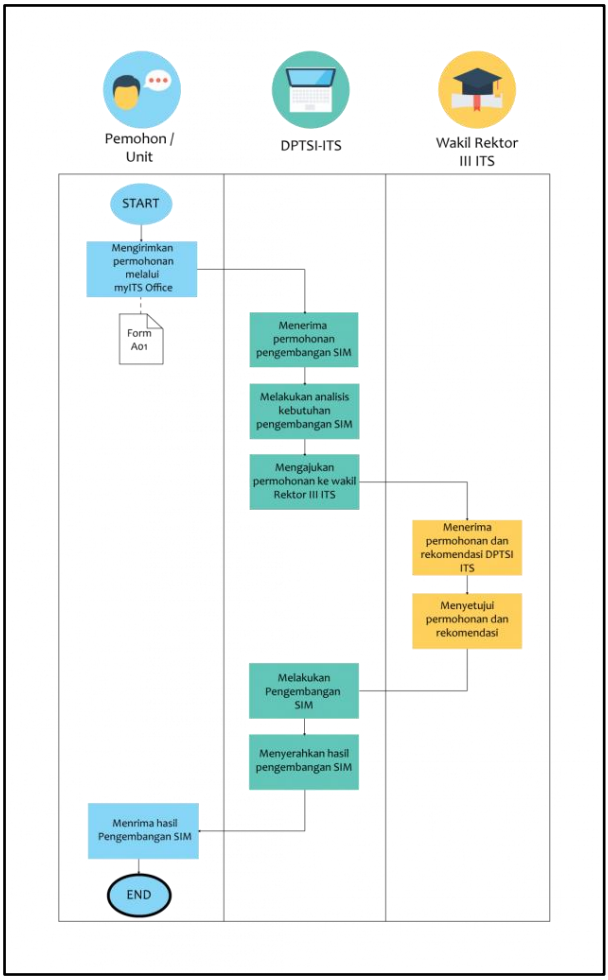
Gambar B.25 Dokumen Developer Guide SIPMABA ITS



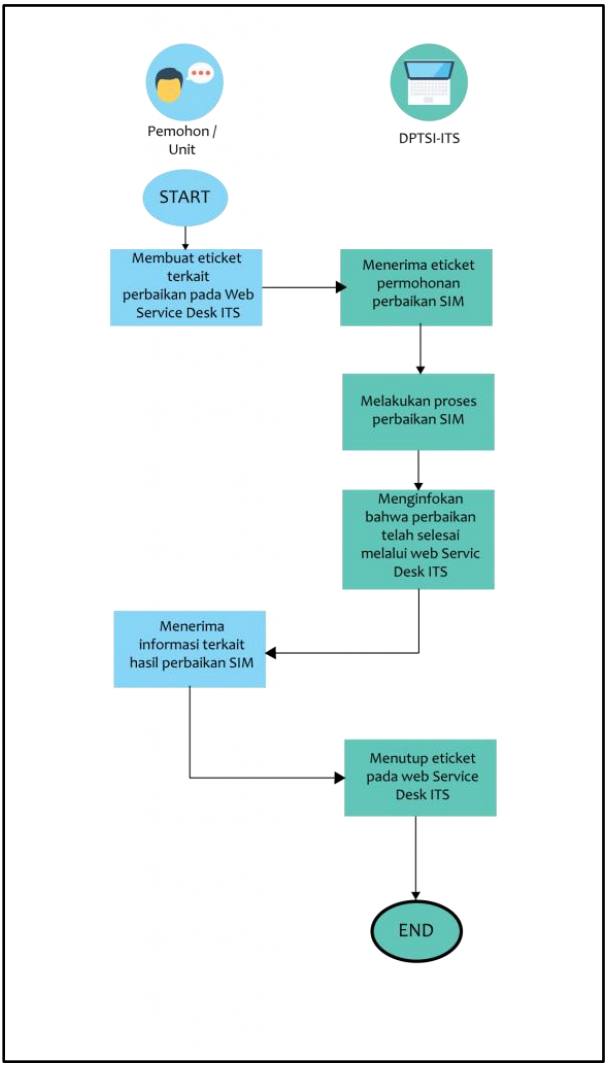
Gambar B.26 Konfigurasi Firewall



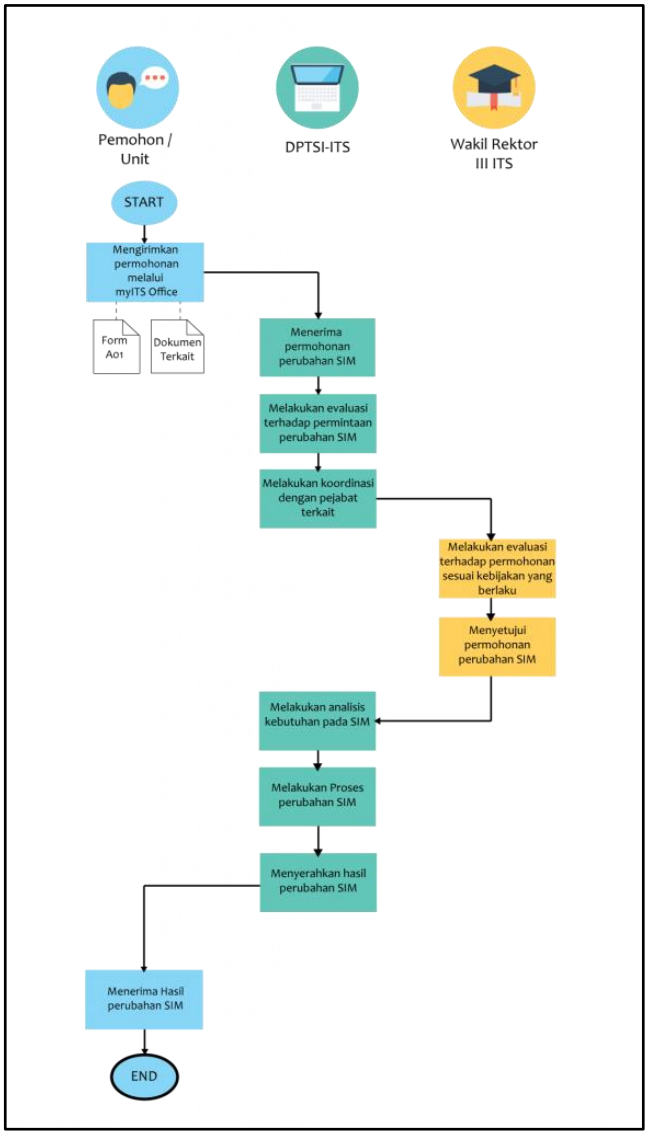
Gambar B.27 SOP Layanan SIM



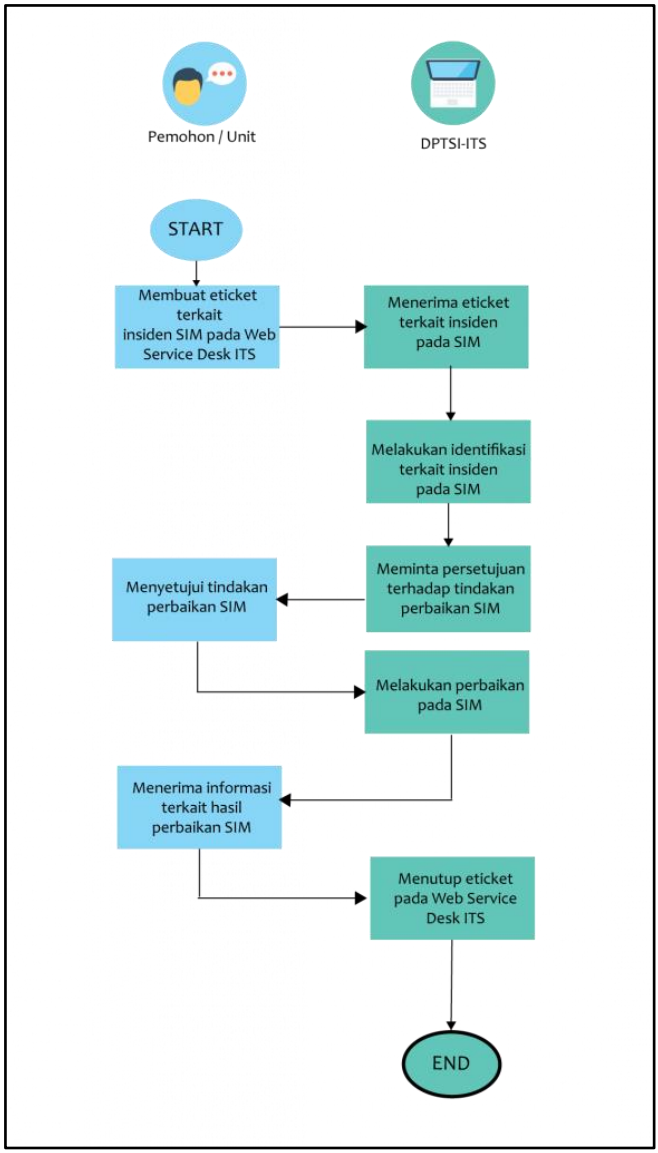
Gambar B.28 SOP Pengajuan Pengembangan SIM



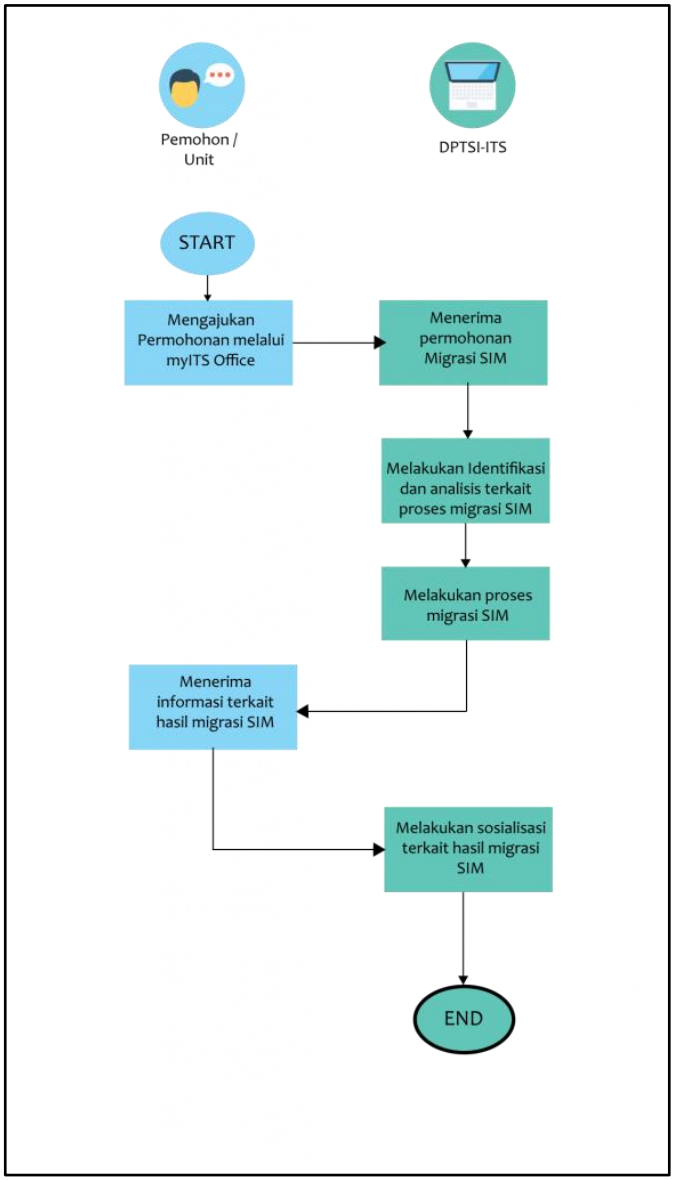
Gambar B 29 SOP Pengajuan Perbaikan SIM



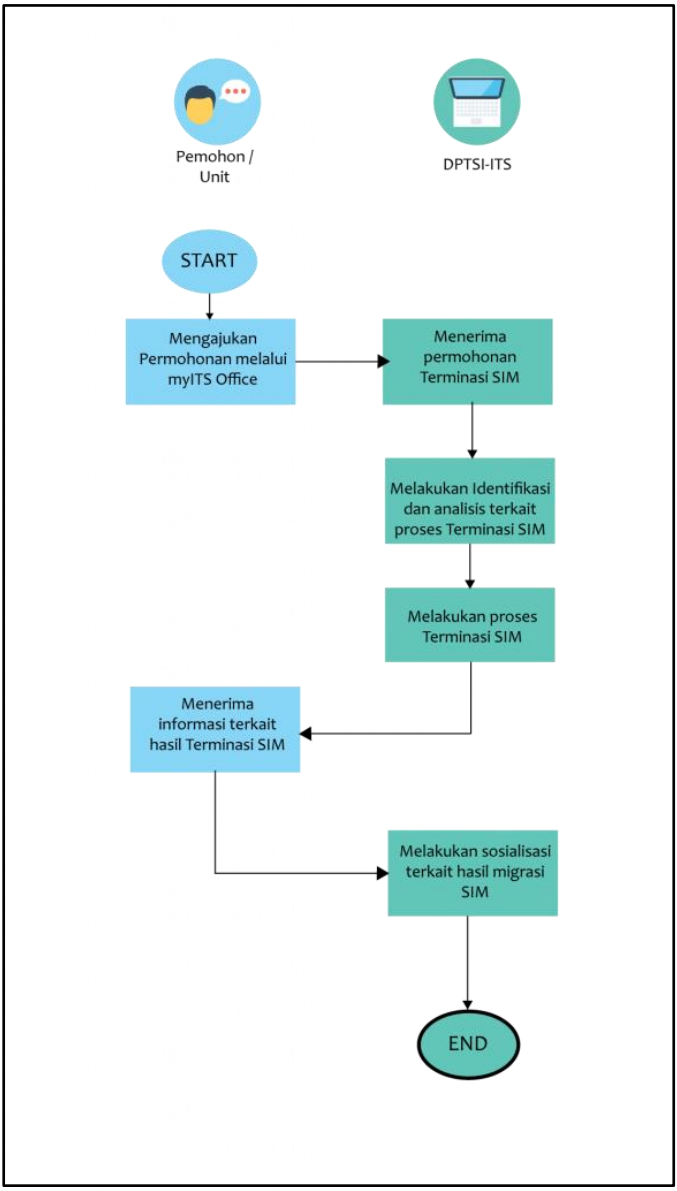
Gambar B 30 SOP Pengajuan Perubahan SIM



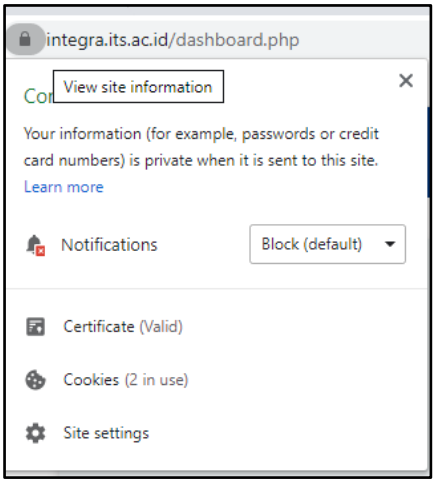
Gambar B.31 SOP Pengelolaan Insiden SIM



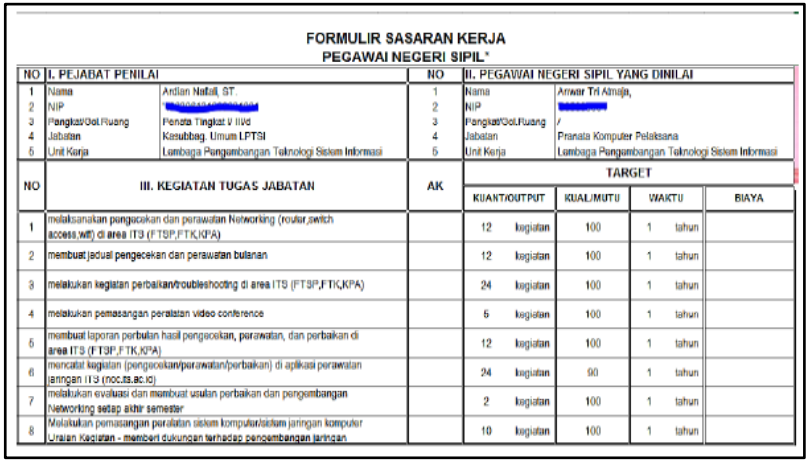
Gambar B.32 SOP Migrasi SIM



Gambar B.33 SOP Terminasi SIM



Gambar B.34 Sertifikasi https

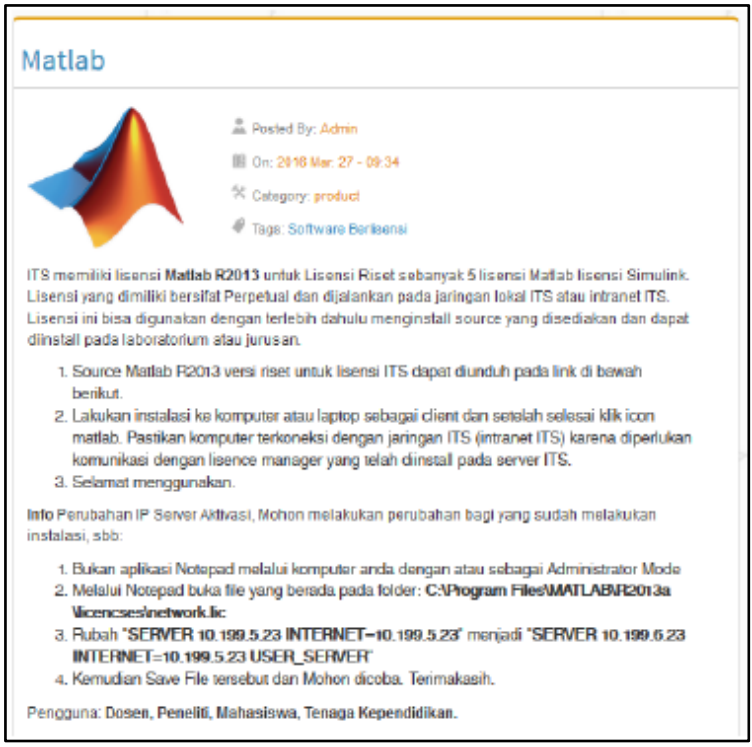


FORMULIR SASARAN KERJA
PEGAWAI NEGERI SIPIL*

NO	I. PEJABAT PENILAI		NO	II. PEGAWAI NEGERI SIPIL YANG DINILAI	
1	Nama	Ardian Natali, ST	1	Nama	Anwar Tri Atmaja,
2	NIP	[redacted]	2	NIP	[redacted]
3	Pangkat/Gol.Ruang	Penata Tingkat.I /IIId	3	Pangkat/Gol.Ruang	/
4	Jabatan	Kasubbag. Umum LPTSI	4	Jabatan	Pranata Komputer Pelaksana
5	Unit Kerja	Lembaga Pengambangan Teknologi Sistem Informasi	5	Unit Kerja	Lembaga Pengambangan Teknologi Sistem Informasi

NO	III. KEGIATAN TUGAS JABATAN	AK	TARGET			
			KUANT/OUTPUT	KUAL/MUTU	WAKTU	BIAYA
1	melaksanakan pengecekan dan perawatan Networking (router,switch access,wifi) di area ITS (FTSP,FTK,KPA)		12 kegiatan	100	1 tahun	
2	membuat jadual pengecekan dan perawatan bulanan		12 kegiatan	100	1 tahun	
3	melakukan kegiatan perbaikan/troubleshooting di area ITS (FTSP,FTK,KPA)		24 kegiatan	100	1 tahun	
4	melakukan pemasangan peralatan video conference		5 kegiatan	100	1 tahun	
5	membuat laporan perbulan hasil pengecekan, perawatan, dan perbaikan di area ITS (FTSP,FTK,KPA)		12 kegiatan	100	1 tahun	
6	mencatat kegiatan (pengecekan/perawatan/perbaikan) di aplikasi perawatan jaringan ITS (noc.its.ac.id)		24 kegiatan	90	1 tahun	
7	melakukan evaluasi dan membuat usulan perbaikan dan pengembangan Networking setap akhir semester		2 kegiatan	100	1 tahun	
8	Melakukan pemasangan peralatan sistem komputer/sistem jaringan komputer Uraian Kegiatan - memberi dukungan terhadap pengembangan jaringan		10 kegiatan	100	1 tahun	

Gambar B.35 Dokumen SKP Pegawai SubDit IKTI



Matlab

Posted By: Admin

On: 2016 Mar 27 - 09:34

Category: product

Tags: Software Berlisensi

ITS memiliki lisensi **Matlab R2013** untuk Lisensi Riset sebanyak 5 lisensi Matlab lisensi Simulink. Lisensi yang dimiliki bersifat Perpetual dan dijalankan pada jaringan lokal ITS atau intranet ITS. Lisensi ini bisa digunakan dengan terlebih dahulu menginstall source yang disediakan dan dapat diinstall pada laboratorium atau jurusan.

1. Source Matlab R2013 versi riset untuk lisensi ITS dapat diunduh pada link di bawah berikut.
2. Lakukan instalasi ke komputer atau laptop sebagai client dan setelah selesai klik icon matlab. Pastikan komputer terkoneksi dengan jaringan ITS (intranet ITS) karena diperlukan komunikasi dengan lisence manager yang telah diinstall pada server ITS.
3. Selamat menggunakan.

Info Perubahan IP Server Aktivasi, Mohon melakukan perubahan bagi yang sudah melakukan instalasi, sbb:

1. Bukan aplikasi Notepad melalui komputer anda dengan atau sebagai Administrator Mode
2. Melalui Notepad buka file yang berada pada folder: **C:\Program Files\MATLAB\R2013a \licences\network.lic**
3. Rubah "**SERVER 10.199.5.23 INTERNET=10.199.5.23**" menjadi "**SERVER 10.199.5.23 INTERNET=10.199.5.23 USER_SERVER**"
4. Kemudian Save File tersebut dan Mohon dicoba. Terimakasih.

Pengguna: **Dosen, Peneliti, Mahasiswa, Tenaga Kependidikan.**

Gambar B.36 Peraturan Instalasi Matlab

Gambar B.37 Grounding dan Fingerprint pada Ruangan Server

Gambar B.38 Sensor Suhu Ruangan Server

SURAT TANDA TERIMA BARANG

Pada hari Rabu tanggal 10 Agustus 2016. Telah terima dari:

Nama : Dony Kusuma W.P.K

Jabatan : Administrator Sistem Teknologi Informasi

Alamat :

Barang berupa :

No	Jenis Barang	Nomor Serial	Jumlah
1	Fujitsu Primergy RX300 S7	MAA8006691	1
2	Fujitsu Primergy RX300 S7	MAA8006774	1

Dalam rangka layanan colocation LPTSI-ITS.

Yang Menerima

(Surendra Perwira Putra)

Yang Menyerahkan,

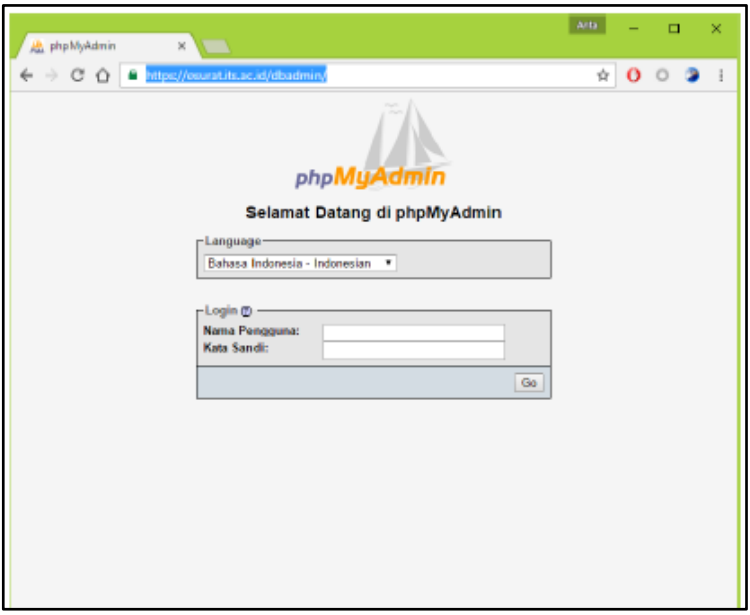
(Dony Kusuma W.P.K)

Gambar B.39 Surat Serah Terima Pemindahan Alat Komputasi

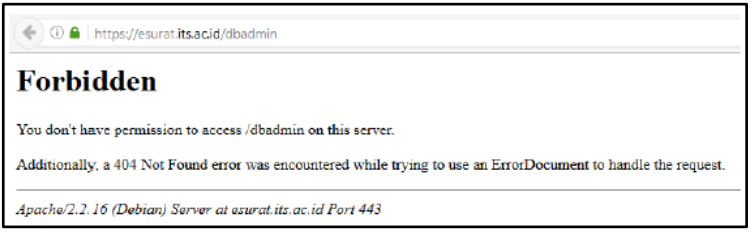
Gambar B.40 Firewall Cisco ASA 5540 DPTSI

ITSNET-AS-6FL		
ITSnet	10.	2001:df0:426:10:1101::/80
?	10.	2001:df0:426:10:1102::/80
?	10.	2001:df0:426:10:1103::/80
	10.	2001:df0:426:10:1104::/80
?	10.	2001:df0:426:10:1105::/80
MMT	10.	2001:df0:426:10:1106::/80
D3 Sipil	10.	2001:df0:426:10:1107::/80
ITSRSC-AS-RSC		
	10.	2001:df0:426:10:1201::/80
	10.	2001:df0:426:10:1202::/80
ITSPSC-AS-PSC		
Pasca	10.	2001:df0:426:10:1301::/80
LPPM	10.	2001:df0:426:10:1302::/80
	10.	2001:df0:426:10:1303::/80
	10.	2001:df0:426:10:1304::/80
ITSPSC-AS-TSB		
	10.	2001:df0:426:10:1401::/80
	10.	2001:df0:426:10:1402::/80
	10.	2001:df0:426:10:1403::/80
	10.	2001:df0:426:10:1404::/80
ITSSTK-DS-STK		
ITSSTK-AS-ASR		
	10.	2001:df0:426:10:2101::/80
	10.	2001:df0:426:10:2102::/80
	10.	2001:df0:426:10:2103::/80
	10.	2001:df0:426:10:2104::/80
	10.	2001:df0:426:10:2105::/80
	10.	2001:df0:426:10:2106::/80
	10.	2001:df0:426:10:2107::/80

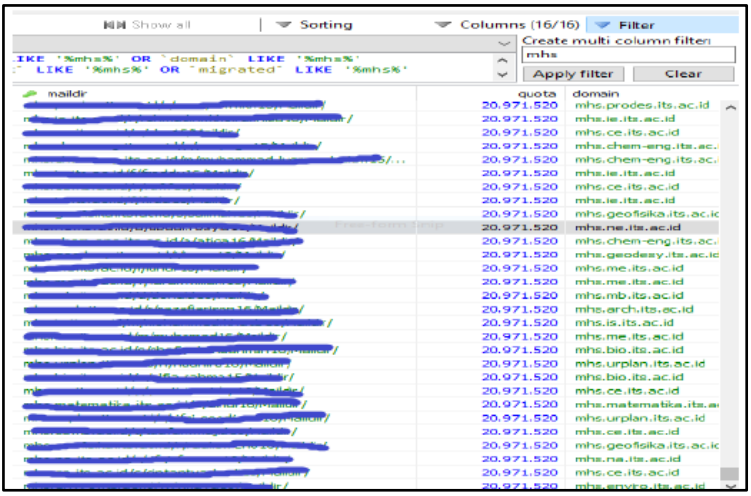
Gambar B.41 IP Config di ITS



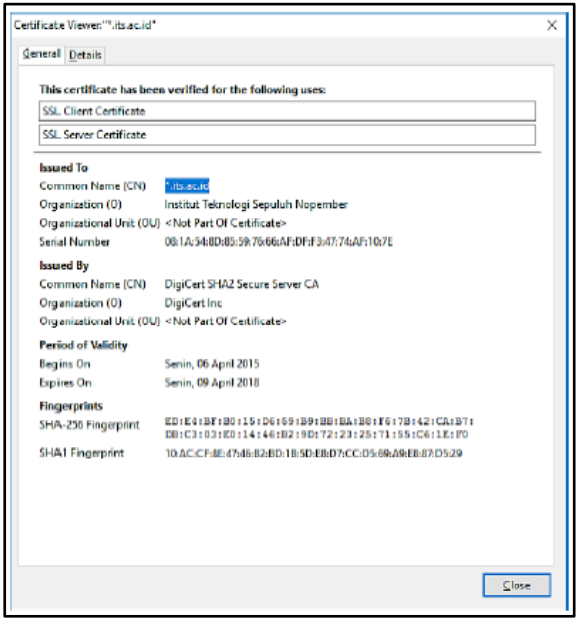
Gambar B.42 Akses e-Surat dengan IP ITS



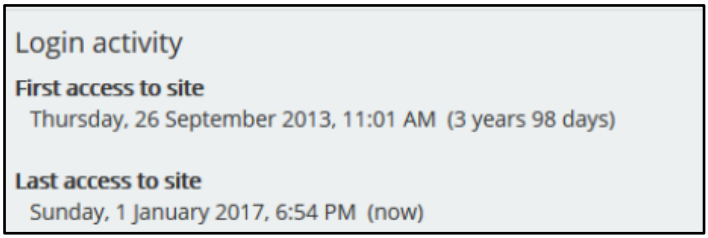
Gambar B.43 Gagal Akses e-Surat



Gambar B.44 Pembagian Kuota Jaringan di ITS

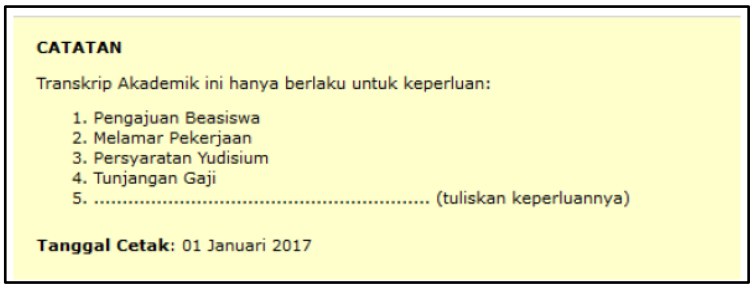


Gambar B.45 Sertifikat DigiCert ITS



Gambar B.46 Sinkronisasi Waktu pada ShareITS

Gambar B.47 Sinkronisasi Waktu pada FRS Integra



Gambar B.48 Sinkronisasi Waktu pada Transkrip Integra

LAMPIRAN C

Tabel *Checklist* Analisis Kesenjangan

Annex A	Pertanyaan Indeks KAMI	*Checklist*
A.5 Kebijakan Keamanan Informasi	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?	N
	4.1 Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	QY
	2.17 Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	N
	4.5 Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	ditetapkan oleh pimpinan instansi/ perusahaan?	
	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?	N
	4.11 Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Y
	2.10 Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Y
	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?	Y
	2.16 Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Y
	4.19 Apakah seluruh kebijakan dan prosedur keamanan informasi	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	dievaluasi kelayakannya secara berkala?	
	4.20 Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Y
	4.22 Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Y
	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?	Y
	4.29 Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Y
A.6 Organisasi Keamanan Informasi	3.2 Apakah instansi/ perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	7.3.5 Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	N
	2.19 Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	N
	2.5 Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	QY
	4.21 Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	QY
	2.2 Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Y
	2.3 Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	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?	Y
	5.8 Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Y
	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?	Y
A.7 Keamanan Sumber Daya Manusia	5.20 Proses Pengecekan Latar Belakang	QY
	4.8 Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	QY
	2.6 Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	QY

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	N
	2.7 Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	QY
	2.8 Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	QY
	2.9 Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Y
A.8 Manajemen Aset Sumber	5.32 Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	QY
	3.6 Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	QY
	3.4 Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	
	5.3 Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	N
	5.9 Tata tertib penggunaan komputer, email, internet dan intranet	N
	5.10 Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	N
	3.7 Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	N
	5.19 Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Y
	5.1 Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	Y
	5.22 Prosedur penghancuran data/aset yang sudah tidak diperlukan	Y
	5.33 Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras,	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	
	5.7 Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Y
A.9 Akses Kontrol	5.13 Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya	N
	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?	N
	5.23 Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku	N
	5.24 Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.	QY
	5.4 Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	7.3.12 Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Y
	7.3.13 Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Y
	6.15 Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Y
	6.17 Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Y
	6.18 Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Y
	5.29 Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Y
A.10 Kriptografi	6.12 Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	N
	6.11 Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	6.13 Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Y
A.11 Keamanan Fisik dan Lingkungan	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)	N
	5.35 Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	QY
	5.38 Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	N
	4.17 Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	Y
	5.28 Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	dapat mencegah upaya akses oleh pihak yang tidak berwenang?	
	5.30 Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Y
	5.31 Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Y
A.12 Keamanan Operasi	4.10 Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya?	N
	7.2.8 Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	QY
	2.4 Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	QY
	5.18 Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	N
	5.25 Apakah tersedia daftar data/informasi yang harus di-	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?	
	5.26 Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	N
	3.10 Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	QY
	2.15 Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	QY
	6.21 Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	N
	4.25 Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	N
	4.26 Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	N
	6.22 Apakah adanya laporan penyerangan virus/malware yang	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	gagal/sukses ditindaklanjuti dan diselesaikan?	
	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?	Y
	6.6 Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Y
	6.7 Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Y
	6.1 Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Y
	6.5 Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Y
	6.19 Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Y
	6.20 Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	5.11 Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Y
	6.4 Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Y
	6.9 Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Y
	6.10 Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Y
	6.21 Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Y
A.13 Keamanan Komunikasi	5.17 Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	N
	5.36 Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	QY
	6.2 Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Y
A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem	3.5 Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	QY

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	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?	QY
	6.25 Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	N
	4.12 Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	N
	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?	Y
	6.23 Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	6.24 Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Y
	5.5 Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Y
	5.6 Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Y
	6.8 Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Y
A.15 Hubungan Pemasok	7.2.9 Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	N
	7.3.11 Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	N
	7.1.3.8 Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	N
	7.3.4 Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	5.16 Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	N
	7.1.1.5 Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	N
	7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	N
	7.1.1.2 Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	N
	7.1.1.3 Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	QY
	7.1.1.4 Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	QY
	7.1.2.1 Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	QY

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	7.1.7.3 Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	N
	7.2.1 Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	QY
	7.1.2.2 Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	N
	7.1.4.2 Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	N
	7.1.3.1 Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	N
	7.1.6.1 Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	7.1. Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	N
	7.2.2 Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	N
	7.1.1.6 Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	QY
	7.1.1.7 Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal/eksternal tentang kondisi kontrol keamanan informasi pihak ketiga?	N
	7.1.4.1 "Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?"	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	7.1.5.2 Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	QY
	7.1.6.2 Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	N
	7.1.2.3 Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/ infrastruktur terhadap persyaratan keamanan yang ditetapkan?	N
	7.1.3.3 Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	N
	7.1.3.4 Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	N
	7.1.3.5 Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	N
	7.2.4 Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	kewenangan) terkait penggunaan layanan berbasis cloud?	
	7.2.5 Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	N
	7.2.7 Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	N
	7.1.3.6 Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	N
	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?	N
	7.1.3.7 Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	N
A.16 Manajemen Insiden Keamanan Informasi	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?	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	3.1 Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	N
	3.3 Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	N
	7.3.2 Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	N
	3.8 Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	QY
	3.9 Apakah instansi/perusahaan 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)?	N
	3.14 Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	
	3.15 Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	N
	2.18 Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	N
	3.13 Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	N
	3.16 Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	N
	5.21 Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Y
	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	Y

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	dengan meminimalisir dampak terhadap operasional layanan TIK?	
	3.12 Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Y
	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?	Y
A.17 Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis	7.1.7.2 Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	N
	4.15 Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	N
	2.14 Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	4.16 Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	N
A.18 Kepatuhan	7.3.14 Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/ pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	N
	7.3.15 Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?	QY
	7.3.16 Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	N
	2.11 Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	QY
	2.21 Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	menganalisa tingkat kepatuhannya?	
	2.22 Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	N
	5.15 Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	N
	7.2.3 Apakah instansi/ perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/ diolah/ dipertukarkan melalui layanan cloud?	N
	7.3.6 Apakah instansi/ perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	N
	7.3.7 Apakah kajian risiko keamanan pada instansi/ perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	QY
	7.3.8 Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	N
	7.3.9 Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi,	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	
	4.3 Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	N
	4.9 Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	N
	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?	N
	7.1.5.1 Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/ penghancuran aset?	N
	7.3.1 Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	dipertukarkan dengan pihak eksternal?	
	7.3.3 Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	N
	7.1.5.2 Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	N
	7.3.10 Apakah instansi/ perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?	N
	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)?	N
	4.24 Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	N

Annex A	Pertanyaan Indeks KAMI	*Checklist*
	2.20 Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	N
	6.26 Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	N

“Halaman ini sengaja dikosongkan”

LAMPIRAN D

Penyusunan Rekomendasi Perbaikan Berdasarkan ISO/IEC 27001:2013 (Klausul *Annex*)

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
A.5 Kebijakan Keamanan Informasi	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?	N	***Control 5.1.1 Policies for Information Security*** Seluruh kebijakan keamanan informasi harus didefinisikan, disetujui oleh manajemen, dipublikasikan, dan dikomunikasikan kepada seluruh pegawai serta pihak ketiga yang relevan. Kebijakan keamanan informasi terdiri dari strategi bisnis, peraturan dan kontrak serta ancaman lingkungan keamanan informasi saat ini dan masa depan.
	4.1 Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab	QY	***Control 5.1.1 Policies for Information Security*** Kumpulan kebijakan keamanan informasi harus didefinisikan,m disetujui oleh manajemen,

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	pihak-pihak yang diberikan wewenang untuk menerapkannya?		dipunlikasikan, dan dikomunikasikan kepada pegawai dan pihak ketiga yang relevan.
	2.17 Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	N	***Control 5.1.1 Policies for information security*** DPTSI seharusnya mendefinisikan beberapa kebijakan untuk keamanan informasi yang berfokus memenuhi tujuan pengamanan informasi. Setelah itu, kebijakan ini harus diseutujui oleh pihak manajemen, dipublikasikan dan dikomunikasikan kepada semua pegawai dan semua pihak eksternal yang terkait. Kebijakan ini harus mengandung pernyataan yang berisi tentang : • Definisi kemanan informasi, tujuan, dan petunjuk untuk arahan semua proses yang berkaitan dengan kemanan informasi • Penunjukan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			personel yang berkaitan dan deskripsi tanggung jawab yang jelas. • Proses untuk mengelola penyimpangan dan pengecualian.
	4.5 Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/ perusahaan?	N	***Control 5.1.1 Policies for Information Security*** Kumpulan kebijakan keamanan informasi harus didefinisikan, disetujui oleh manajemen, dipublikasikan, dan dikomunikasikan kepada seluruh pegawai dan pihak ketiga. Kebijakan tersebut harus dibuat berdasarkan strategi bisnis, regulasi, serta ancaman saat ini dan perkiraan di masa mendatang
	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	N	***Control 5.1.2 Review of the Policies for Information Security*** Kebijakan keamanan informasi harus ditinjau dalam interval yang telah ditentukan atau

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?		aapbila perubahan signifikan terjadi maka harus dipastikan efektifvitas, kesesuaian, dan kecukupannya secara berkelanjutan. Peninjauan kebijakan keamanan informasi harus mempertimbangkan hasil tinjauan manajemen.
A.6 Organisasi Keamanan Informasi	3.2 Apakah instansi/ perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	N	***Control 6.1.1 Information Security Roles and Responsibilities*** Seluruh penanggungjawab keamanan informasi harus didefinisikan dan dialokasikan.
	2.1 Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	QY	***Control 6.1.1 Information Security Roles and Responsibilities*** Seluruh penanggungjawab keamanan informasi harus didefinisikan dan dialokasikan, termasuk tugas dan wewenang dari pimpinan DPTSI dalam melaksanakan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			program keamanan informasi.
	7.3.5 Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	N	***Control 6.1.1 Information Security Roles and Responsibilities*** Seluruh penanggungjawab keamanan informasi harus didefinisikan dan dialokasikan, termasuk penanggungjawab peribasi dan perlindungan data pribadi yang tercantum pada klasul control nomor 18.
	2.19 Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	N	***Control 6.1.1 Information security roles and responsibilities*** DPTSI seharusnya menetapkan sebuah penilaian kinerja pengelola keamanan informasi untuk mencegah terjadinya risiko yang lebih serius. Hal ini perlu diperhatikan karena ketika individu yang diberi tanggung jawab bisa jadi dia menyerahkan wewenang tersebut kepada orang lain untuk

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			mengerjakannya. Walaupun begitu, individu yang telah ditunjuk ini harus tetap bertanggung jawab atas pekerjaan yang telah diselesaikan apakah sudah benar atau belum. Penilaian individu ini harus mencakup: • Aset dan proses keamanan informasi harus didefinisikan. • Setiap orang yang bertanggung jawab atas setiap aset harus didokumentasikan dengan detail. Tingkat otorisasi harus harus jelas ditetapkan dan didokumentasikan.
	2.5 Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	QY	***Control 6.1.2 Segregation of duties*** Tugas dan area kerja yang saling berbenturan harus segera dilakukan segregasi atau pemisahan kewenangan untuk meminimalisir campur tangan pihak yang tidak berkepentingan menyalahgunakan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			aset perusahaan. Selain itu, pemetaan para pelaksana pengamanan informasi harus dilakukan secara lengkap.
	4.21 Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	QY	***Control 6.1.5 Information Security in Project Management*** Keamanan informasi harus ditujukan pada manajemen proyek, apapun tipe proyeknya untuk memastikan risiko keamanan informasi telah teridentifikasi sebagai bagian dari proyek.
A.7 Keamanan Sumber Daya Manusia	5.20 Proses Pengecekan Latar Belakang	QY	***Control 7.1.1 Screening*** Organisasi harus melakukan proses verifikasi latar belakang SDM sesuai dengan Undang-Undang yang berlaku, yang meliputi kelengkapan dan verifikasi dari riwayat hidup pemohon, konfirmasi kualifikasi akademik dan profesionalitas,

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			serta verifikasi identitas independent seperti paspor/ sejenis dan verifikasi catatan kriminal
	4.8 Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	QY	***Control 7.2.1 Management Responsibilities*** Manajemen harus mewajibkan seluruh pegawai dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur organisasi yang diterapkan. Dalam hal ini, manajemen harus menyediakan media pelaporan untuk melaporkan pelanggaran kebijakan atau prosedur keamanan informasi.
	2.6 Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	QY	***Control 7.2.1 Management responsibilities*** Pihak manajemen harus memberikan standar kompetensi untuk semua pegawai yang akan melamar di posisi keamanan informasi berdsarkan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			kebijakan dan prosedur yang telah ditetapkan di dalam DPTSI.
	7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	N	***Control 7.1.1 Screening*** ***Control 15.1.1 Information Security Policy for Supplier Relationshop*** Organisasi harus melakukan verifikasi latar belakang seluruh pegawai dan melakukan klasifikasi risiko yang akan dirasakan. Selain itu organisasi harus membuat kebijakan dan kontrol yang mewajibkan supplier untuk mengimplementasikan persyaratan keamanan informasi minimum berdasarkan kebutuhan bisnis organisasi dan profil risionya.
	2.7 Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan	QY	***Control 7.2.2 Information security awareness, education and training*** Harus dilakukan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	keahlian yang memadai sesuai persyaratan/standar yang berlaku?		program yang terkait dengan kesadaran kemanan informasi yang selaras dengan kebijakan dan standar kemanan informasi yang ada di DPTSI untuk memastikan semua pelaksana pengamanan informasi memiliki kompetensi yang memadai. Program ini harus berkaitan dengan posisi dan peran pegawai yang relevan. Program ini juga harus mencakup hal – hal yang umum seperti berikut : • Pernyataan komitmen manajemen DPTSI terhadap kemanan informasi di seluruh organisasi • Kebutuhan untuk memenuhi standar dan kebijakan kemanan informasi yang berlaku Prosedur keamanan informasi standar.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	2.8 Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	QY	***Control 7.2.2 Information security awareness, education and training*** Perlu diadakan program kesadaran akan kebijakan kemanan informasi yang sesuai dengan standar dan kebijakan keamanan informasi yang berlaku di DPTSI. Program ini sedikitnya harus memenuhi aspek sebagai berikut : • Pernyataan komitmen manajemen DPTSI terhadap kemanan informasi di seluruh organisasi • Kebutuhan untuk memenuhi standar dan kebijakan kemanan informasi yang berlaku • Sosialisasi prosedur keamanan informasi standar.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
A.8 Manajemen Aset Sumber	5.32 Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	QY	***Control 8.1.1 Inventory for Assets*** Aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi dan inventaris aset ini harus dipersiapkan dan selalu di-maintain.
	3.6 Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	QY	***Control 8.1.2 Ownership of assets*** Pengelolaan aset yang dimiliki oleh DPTSI harus juga didefinisikan kepemilikannya. Baik itu individu ataupun kepemilikan oleh entitas lain, harus ditetapkan kepemilikannya untuk menjaga kualitas siklus hidup aset tersebut. Kepemilikan ini juga harus disetujui oleh pihak manajemen.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	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/perusahaan anda?	N	***Control 8.2.1 Classification of Information*** Langkah pertama yaitu menerapkan kerangka kerja pengelolaan risiko. Selanjutnya yaitu melakukan klasifikasi aset informasi dan kepemilikan aset informasi, sehingga dapat menentukan langkah penanggulangan insiden keamanan informasi yang berhubungan dgn pelanggaran hukum
	5.3 Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	N	***Control 8.2.3 Handling of Assets*** Prosedur untuk mengelola aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi, yang mempertimbangkan pembaatsan akses yang mendukung persyaratan perlindungan klasifikasi aset pada level tertentu.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	5.9 Tata tertib penggunaan komputer, email, internet dan intranet	N	***Control 8.2.3 Handling of Assets*** Prosedur untuk mengelola aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi, yang mempertimbangkan pembaatsan akses yang mendukung persyaratan perlindungan klasifikasi aset pada level tertentu.
	5.10 Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	N	***Control 8.1.3 Acceptable Use of Assets*** Organisasi harus membuat standar persyaratan keamanan informasi dalam penggunaan aset.
	3.7 Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	N	***Control 8.2.3 Handling of Assets*** Sebaiknya, ancaman dan kelemahan aset informasi harus dilakukan pencatatan. Lalu, disusunlah prosedur dalam menangani, mengelola, menyimpan, dan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			mengkomunikasikan informasi yang harus mencakup pembatasan hak akses dan perlindungan terhadap Salinan informasi serta penyimpanan aset TI sesuai dgn spesifikasi
A.9 Akses Kontrol	5.13 Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya	N	***Control 9.2.4 Management of Secret Authentication Information of Users*** Alokasi informasi otentikasi rahasia harus dikendalikan melalui proses manajemen secara formal. Proses tersebut meliputi pewajiban user untuk menjaga informasi otentikasi serta pembuatan prosedur untuk memverifikasi identitas user, dan sebagainya.
	6.14 Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis,	N	***Control 9.4.3 Password management system*** DPTSI seharusnya menerapkan standar atau kebijakan untuk menjamin kualitas

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?		password yang dimiliki oleh pihak terkait.
	5.23 Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku	N	***Control 9.2.3 Management of Privileged Access Right*** Organisasi harus membuat prosedur terkait pengalokasian hak akses yang dikontrol dengan proses otorisasi resmi.
	5.24 Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.	QY	***Control 9.2.6 Removal or Adjustment of Access Rights*** Organisasi harus membuat kebijakan dan prosedur penghapusan hak akses user terhadap informasi dan aset layanan ketika user telah keluar dari instansi.
A.10 Kriptografi	6.12 Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	N	***Control 10.1.1 Policy on the use of cryptographic controls*** DPTSI harus mengembangkan standar dan kebijakan dalam

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			menggunakan enkripsi yang sedikitnya memuat hal di bawah ini: • Pendekatan manajemen terhadap kebijakan kriptografi yang ada • Identifikasi jenis, kekuatan, dan kualitas enkripsi Dampak penggunaan informasi terenkripsi
A.11 Keamanan Fisik dan Lingkungan	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)	N	***Control 11.1.1 Physical Security Perimeter*** Keamanan fisik harus didefinisikan dan digunakan untuk melindungi area yang mengandung informasi yang sensitive atau kritis, denga membuat tidak ada celah pada keamanan tersebut, seperti membangun dinding dan lantai dengan konstruksi yang solid dan semua pintu eksternal harus dilindungi.
	5.35 Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat:	QY	***Control 11.2.4 Equipment Maintenance*** Organisasi harus

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?		menerapkan proses pemeriksaan dan perawatan perangkat computer dan fasilitas pendukung dengan cara membuat panduan pemeliharaan yang meliputi pemeliharaan peralatan sesuai dengan jadwal servis yang direkomendasikan supplier dan dilakukan oleh pihak yang berwenang.
	5.38 Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	N	***Control 11.1.2 Physical Entry Controls*** Organisasi harus melakukan pengamanan terhadap pintu masuk untuk menghindari akses oleh pihak yang tidak berwenang dengan membuat pedoman yang meliputi pencatatan waktu pengunjung dan pembatasan area kunjungan terutama area yang kritis.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
A.12 Keamanan Operasi	4.10 Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya?	N	Control 12.6.2 Peraturan untuk mengelola instalasi perangkat lunak oleh user harus dibuat dan diimplementasikan. Organisasi harus mengidentifikasi jenis instalasi yang diperbolehkan dan yang tidak.
	7.2.8 Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	QY	***Control 12.3.1 Information Backup*** Kebijakan backup harus dibuat dan didefinisikan sebagai syarat untuk melakukan backup terhadap informasi, perangkat lunak dan sistem. Kebijakan tersebut harus mendefinisikan periode dan persyaratan perlindungan, serta menyediakan fasilitas backup yang memadai untuk me-recover apabila terjadi bencana atau kerusakan.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	2.4 Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	QY	***Control 12.1.3 Capacity management*** Alokasi sumber daya harus dipantau dan dilakukan sesuai proyeksi kebutuhan masa mendatang untuk memastikan kebutuhan performa sistem. Perhatian khusus juga perlu dilakukan terkait dengan proses pengadaan yang panjang dan biaya yang tinggi. Maka dari itu, manager harus memantau penggunaan sumber daya utama. Mereka harus mengidentifikasi tren penggunaan aplikasi bisnis dan manajemen sistem informasi.
	5.18 Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	N	***Control 12.3.1 Information Backup*** Organisasi harus membuat kebijakan backup data, perangkat lunak, dan sistem. Kebijakan atau prosedur tersebut harus

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			diujicoba untuk memastikan semua data penting dan perangkat lunak dapat dipulihkan setelah adanya bencana/ kerusakan.
	5.25 Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?	N	***Control 12.3.1 Information Backup*** Organisasi harus membuat kebijakan backup data, perangkat lunak, dan sistem. Kebijakan tersebut harus meliputi catatan yang akurat dan lengkap.
	5.26 Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	N	***Control 12.4.1 Event Logging*** Organisasi harus membuat daftar log aktivitas pengguna, kesalahan, dan kejadian keamanan informasi yang tersimpan secara berkala. Pencatatan tersebut meliputi ID pengguna, kegiatan sistem, waktu kejadian, identitas perangkat/ lokasi, perubahan konfigurasi sistem, dan sebagainya.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	3.10 Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	QY	***Control 12.2.1 Controls against malware*** DPTSI harus menyusun langkah deteksi, penanggulangan, dan pemulihan dari risiko untuk meningkatkan kesadaran semua pihak.
	2.15 Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	QY	***Control 12.4.1 Event logging*** DPTSI harus membuat event log yang teratur dikaji berisikan aktivitas pengguna, exceptions, kesalahan, dan kejadian terkait keamanan informasi. Event log harus memuat : • ID pengguna; • kegiatan sistem; • tanggal, waktu, dan detail acara utama, mis. log-on dan log-off; • identitas atau lokasi perangkat jika memungkinkan dan pengidentifikasi sistem; • catatan upaya

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			akses sistem yang berhasil dan ditolak; • rekaman data yang berhasil dan ditolak dan upaya akses sumber daya lainnya
	6.21 Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	N	***Control 12.2.1 Controls against malware*** DPTSI seharusnya melakukan rekaman dan analisis terhadap jejak rekam malware yang ada.
	4.25 Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	N	Control 12.7.1 Information Systems Audit Controls Persyaratan audit dan aktivitas yang meliputi operasional sistem harus direncanakan dengan baik dan disetujui untuk meminimalisir perubahan pada proses bisnis. Apabila ditemukan isu yang terkait hasil audit, maka organisasi harus melakukan inisiatif tindakan perbaikan, yang tercantum pada klausul kontrol 18.2.1.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	4.26 Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	N	***Control 12.7.1 Information Systems Audit Controls*** Persyaratan audit dan aktivitas yang meliputi operasional sistem harus direncanakan dengan baik dan disetujui untuk meminimalisir perubahan pada proses bisnis.
	6.22 Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	N	***Control 12.2.1 Controls against malware*** Selain DPTSI harus membuat jejak rekam dari malware atau virus yang ada, DPTSI juga seharusnya membuat laporan tentang adanya penyerangan virus dan ditindaklanjuti dengan tepat
A.13 Keamanan Komunikasi	5.17 Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	N	***Control 13.2.4 Confidentiality or Non-Disclosure Agreements*** Organisasi harus melakukan pencatatan terkait insiden yang telah diselesiakan untuk membantu melakukan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			investigasi terkait kesesuaian tindakan penyelesaian insiden yang dilakukan.
	5.36 Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	QY	***Control 13.2.2 Agreements on Information Transfer*** Organisasi harus menetapkan kebijakan, prosedur, dan standar untuk melindungi pengiriman informasi dan media fisik.
A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem	3.5 Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	QY	***Control 14.1 Security requirements of information systems*** Kebutuhan yang terkait keamanan informasi harus didefinisikan untuk semua sistem keamanan informasi baru maupun lama. Hal ini termasuk juga penetapan ambang batas tingkat risiko yang dapat diterima untuk mencegah terjadinya risiko yang lebih besar terjadi.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	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?	QY	***Control 14.2.2 System Change Control Procedures*** Perubahan terhada sistem harus dikontrol dengan menggunakan prosedur kontrol perubahan secara formal. Prosedur ini harus didokumentasikan untuk memastikan integritas sistem. Selain itu, proses ini juga termasuk melakukan risk assessment, analisis dampak dari perubahan dan spesifikasi kontrol keamanan yang diperlukan.
	6.25 Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	N	***Control 14.2.6 Secure development environment*** Standar untuk platform teknologi yang digunakan DPTSI harus ditetapkan oleh DPTSI untuk menjamin keamanan informasi dan siklus hidupnya.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	4.12 Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	N	***Control 14.1.1 Security Requirements of Information Systems*** Persyaratan keamanan informasi harus meliputi persyaratan sistem informasi baru dan peningkatan terhadap sistem informasi.
A.15 Hubungan Pemasok	7.2.9 Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	N	***Control 15.2.1 Monitoring and Review of Supplier Services*** Organisasi harus mempertahankan visibilitas ke dalam aktivitas keamanan informasi, seperti manajemen perubahan, identifikasi kerentanan, dan pelaporan dan respons insiden keamanan informasi melalui proses pelaporan yang ditetapkan.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.3.11 Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Perjanjian dengan pemasok layanan harus didokumentasikan, termasuk kebijakan keamanan informasi yang relevan dengan kontrak apabila terjadi suatu insiden
	7.1.3.8 Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	N	***Control 15.1.1 Information Security Policy for Supplier Relationship*** Organisasi harus mengidentifikasi kontrol keamanan informasi yang terkait dengan supplier dalam suatu kebijakan, termasuk mengidentifikasi dan mendokumentasi jenis supplier, menstandarisasi proses dan siklus hidup untuk mengelola hubungan dengan supplier, dan mengelola insiden termasuk tanggungjawab organisasi dan supplier

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.3.4 Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh informasi yang relevan dengan persyaratan keamanan harus dibuat dan disetujui oleh seluruh supplier yang memiliki akses terhadap organisasi. Dalam hal ini termasuk membuat persyaratan/ peraturan termasuk perlindungan data, hak kekayaan intelektual, dan hak cipta.
	5.16 Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	N	***Control 15.1.1 Information Security Policy for Supplier Relationship*** Organisasi harus mengidentifikasi kontrol keamanan informasi yang terkait dengan supplier, termasuk kontrol akurasi dan kelengkapan untuk memastikan integritas data atau pemrosesan data yang disediakan oleh supplier.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.1.1.5 Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh informasi yang relevan dengan persyaratan keamanan harus dibuat dan disetujui oleh seluruh supplier yang memiliki akses terhadap organisasi.
	7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	N	***Control 7.1.1 Screening Control 15.1.1 Information Security Policy for Supplier Relationshop*** Organisasi harus melakukan verifikasi latar belakang seluruh pegawai dan melakukan klasifikasi risiko yang akan dirasakan. Selain itu organisasi harus membuat kebijakan dan kontrol yang mewajibkan supplier untuk mengimplementasikan persyaratan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			keamanan informasi minimum berdasarkan kebutuhan bisnis organisasi dan profil risionya.
	7.1.1.2 Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	QY	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh persyaratan keamanan informasi yang relevan harus disusun dan disetujui oleh seluruh supplier yang memiliki akses dan menyediakan infrastruktur TI untuk organisasi agar tidak terjadi kesalahpahaman dan untuk memastikan kedua belah pihak memenuhi kewajiban untuk memenuhi persyaratan keamanan inforrmasi.
	7.1.1.3 Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang	QY	***Control 15.1.2 Addressing Security within Supplier Agreements Control Managing Changes to Supplier Services*** Seluruh persyaratan keamanan informasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	harus dipatuhi oleh pihak ketiga?		yang relevan harus disusun dan disetujui oleh seluruh supplier yang memiliki akses dan menyediakan infrastruktur TI untuk organisasi agar tidak terjadi kesalahpahaman dan untuk memastikan kedua belah pihak memenuhi kewajiban untuk memenuhi persyaratan keamanan inforrmasi. Apabila terjadi perubahan terkait layanan yang diberikan oleh supplier, maka supplier harus melakukan pengelolaan dan perubahan pada kebijakan keamanan informasi, prosedur, dan kontrol.
	7.1.1.4 Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	QY	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh persyaratan keamanan informasi yang relevan harus disusun dan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			disetujui oleh seluruh supplier yang memiliki akses dan menyediakan infrastruktur TI untuk organisasi agar tidak terjadi kesalahpahaman dan untuk memastikan kedua belah pihak memenuhi kewajiban untuk memenuhi persyaratan keamanan inforrmasi.
	7.1.2.1 Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	N	***Control 15.1.2 Addressing Security within Supplier Agreement*** Organisasi harus membuat dan mendokumentasikan perjanjian dengan supplier termasuk peraturan yang terkait subkontrakting, termasuk kontrol yang harus diimplementasikan.
	7.1.7.3 Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	QY	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh perjanjian yang dilakukan dengan supplier harus dibuat dan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			didokumentasikan termasuk perjanjian yang mencantumkan narahubung untuk mengatasi isu terkait keamanan informasi
	7.2.1 Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	N	***Control 15.1.3 Information and Communication Technology Supply Chain*** Organisasi disarankan untuk bekerjasama dengan supplier untuk memahami informasi dan teknologi komunikasi supply chain serta dampak yang akan ditimbulkan. Organisasi dapat membuat perjanjian yang jelas dengan supplier untuk mempengaruji praktik teknologi tersebut, termasuk data-data apa saja yang akan dioleh, disimpan, dan dipertukarkan. Teknologi komunikasi supply chain yang dimaksud termasuk layanan cloud computing.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.1.2.2 Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Perjanjian dengan pemasok layanan harus didokumentasikan, termasuk kebijakan keamanan informasi yang relevan dengan kontrak apabila terjadi suatu insiden
	7.1.4.2 Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	N	***Control 15.2.1 Monitoring and Review of Supplier Services*** ***Control 15.2.2 Managing Changes to Supplier Services*** Organisasi harus melakukan pengawasan, peninjauan, dan audit terhadap pemberian layanan oleh supplier, termasuk bagaimana supplier mengatasi keadaan merugikan/ bencana. Apabila terjadi perubahan oleh supplier, maka kebijakan, prosedur, dan kontrol keamanan informasi suatu perusahaan harus disesuaikan dan dilakukan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			penilaian risiko kembali.
	7.1.3.1 Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	N	***Control 15.2.1 Monitoring and Review of Supplier Services*** Organisasi harus melakukan pengawasan, peninjauan, dan audit terhadap layanan yang diberikan oleh supplier secara berkala.
	7.1.6.1 Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	N	***Control 15.2.1 Monitoring and Review of Supplier Services*** Organisasi harus melakukan pemantauan, peninjauan, dan audit terhadap pemberian layanan oleh supplier dengan cara memastikan supplier memberikan informasi mengenai insiden keamanan informasi dan melakukan peninjauan terhadap perjanjian dan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			panduan atau prosedur pendukung lainnya.
	7.1. Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	N	***Control 15.2.1 Monitoring and Review of Supplier Services*** ***Control 15.2.2 Managing Changes to Supplier Services*** Organisasi harus melakukan pengawasan, peninjauan, dan audit terhadap pemberian layanan oleh supplier, termasuk bagaimana supplier mengatasi keadaan merugikan/ bencana. Apabila terjadi perubahan oleh supplier, maka kebijakan, prosedur, dan kontrol keamanan informasi suatu perusahaan harus disesuaikan dan dilakukan penilaian risiko kembali.
	7.2.2 Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui	QY	***Control 15.1.3 Information and Communication Technology Supply Chain*** Organisasi disarankan untuk bekerjasama dengan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	layanan berbasis cloud?		supplier untuk memahami informasi dan teknologi komunikasi supply chain serta dampak yang akan ditimbulkan. Organisasi dapat membuat perjanjian yang jelas dengan supplier untuk mempengaruji praktik teknologi tersebut, termasuk data-data apa saja yang akan dioleh, disimpan, dan dipertukarkan. Teknologi komunikasi supply chain yang dimaksud termasuk layanan cloud computing.
	7.1.1.6 Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Perjanjian dengan supplier harus dibuat dan didokumentasikan untuk memastikan tidak terjadinya kesalahpahaman antara organisasi dengan supplier, termasuk perjanjian

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			untuk melakukan audit terhadap proses dan kontrol terhadap perjanjian dengan supplier. Hasil audit tersebut harus didokumentasikan dan dilaporkan kepada manajemen organisasi.
	7.1.1.7 Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal/eksternal tentang kondisi kontrol keamanan informasi pihak ketiga?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Perjanjian dengan supplier harus dibuat dan didokumentasikan untuk memastikan tidak terjadinya kesalahpahaman antara organisasi dengan supplier, termasuk perjanjian untuk melakukan audit terhadap proses dan kontrol terhadap perjanjian dengan supplier. Hasil audit tersebut harus didokumentasikan dan dilaporkan kepada manajemen organisasi.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.1.4.1 "Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?"	QY	***Control 15.2.2 Managing Changes to Supplier Services*** Perubahan yang terjadi pada penyedia layanan baik berupa perubahan kebijakan, prosedur, dan kontrol keamanan informasi harus dikelola dengan mempertimbangkan kekritisan informasi bisnis, sistem, dan proses yang terlibat pada penilaian risiko.
	7.1.5.2 Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	N	***Control 18.1.3 Protection of Records*** ***Control 15.1.2 Addressing Security within Supplier Agreements*** Organisasi harus membuat panduan terkait isu penyimpanan dan pembuangan data/ informasi. Panduan tersebut harus disetujui oleh kedua belah pihak dengan mencantumkan perjanjian skema klasifikasi informasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			organisasi dan supplier.
	7.1.6.2 Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Supplier memiliki kewajiban untuk memberikan laporan independent secara periodic terkait efektivitas kontrol dan melakukan tindakan perbaikan dengan tepat waktu berdasarkan isu yang muncul pada laporan tersebut.
	7.1.2.3 Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/ infrastruktur terhadap persyaratan keamanan yang ditetapkan?	N	***Control 15.2.1 Monitoring and Review of Supplier Services*** Organisasi harus melakukan pengawasan, peninjauan dan audit terhadap layanan yang diberikan oleh supplier. Dalam hal ini meninjau aspek kamanan informasi dari hubungan supplier dengan supplier mereka.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.1.3.3 Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh persyaratan keamanan informasi harus disusun dan disetujui oleh seluruh supplier yang memiliki akses atau menyediakan infrastruktur TI kepada organisasi dalam bentuk perjanjian yang meliputi kewajiban supplier untuk memberikan laporan indepen secara periodic terhadap kontrol dan perjanjian dan tindakan perbaikan yang dilakukan terhadap isu yang ada sesuai dengan laporan tersebut.
	7.1.3.4 Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh persyaratan keamanan informasi harus disusun dan disetujui oleh seluruh supplier yang memiliki akses atau menyediakan infrastruktur TI

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			kepada organisasi dalam bentuk perjanjian yang meliputi kewajiban supplier untuk memberikan laporan indepen secara periodic terhadap kontrol dan perjanjian dan tindakan perbaikan yang dilakukan terhadap isu yang ada sesuai dengan laporan tersebut.
	7.1.3.5 Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh persyaratan keamanan informasi harus disusun dan disetujui oleh seluruh supplier yang memiliki akses atau menyediakan infrastruktur TI kepada organisasi dalam bentuk perjanjian yang meliputi kewajiban supplier untuk memberikan laporan indepen secara periodic terhadap kontrol dan perjanjian dan tindakan perbaikan yang dilakukan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			terhadap isu yang ada sesuai dengan laporan tersebut.
	7.2.4 Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	N	***Control 15.1.1 Information Security Policy for Supplier Relationship*** Organisasi harus mengidentifikasi dan mengamanatkan kontrol keamanan untuk menangani akses supplier ke informasi milik organisasi dalam suatu kebijakan. Kontrol ini harus membahas proses dan prosedur yang akan dilaksakan oleh organisasi serta proses dan prosedur tersebut harus diterapkan oleh supplier.
	7.2.5 Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	N	***Control 15.1.1 Information Security Policy for Supplier Relationship*** Organisasi harus mengidentifikasi dan mengamanatkan kontrol keamanan untuk menangani akses supplier ke informasi milik organisasi dalam

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			suatu kebijakan. Kontrol ini harus membahas proses dan prosedur yang akan dilaksakan oleh organisasi serta proses dan prosedur tersebut harus diterapkan oleh supplier.
	7.2.7 Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	N	***Control 15.1.1 Information Security Policy for Supplier Relationship*** Organisasi harus mengidentifikasi dan mengamanatkan kontrol keamanan untuk menangani akses supplier ke informasi milik organisasi dalam suatu kebijakan. Kontrol ini harus membahas proses dan prosedur yang akan dilaksakan oleh organisasi serta proses dan prosedur tersebut harus diterapkan oleh supplier.
	7.1.3.6 Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh informasi yang relevan dengan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	persyaratan keamanan informasi oleh pihak ketiga?		persyaratan keamanan harus dibuat dan disetujui oleh seluruh supplier yang memiliki akses terhadap organisasi. Dalam hal ini termasuk melakukan audit dengan tepat terhadap proses yang berkaitan dengan supplier dan kontrol yang berakitan dengan perjanjian kontrak.
	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?	N	***Control 15.1.2 Addressing Security within Supplier Agreements*** Seluruh informasi yang relevan dengan persyaratan keamanan harus dibuat dan disetujui oleh seluruh supplier yang memiliki akses terhadap organisasi. Dalam hal ini termasuk membuat persyaratan/ peraturan termasuk perlindungan data, hak kekayaan intelektual, dan hak cipta.
	7.1.3.7 Apakah hasil audit tersebut	N	***Control 15.2.1 Monitoring and***

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?		***Review of Supplier Services*** Organisasi harus mengawasi, meninjau dan mengaudit pemberian layanan dari supplier secara rutin. Proses tersebut termasuk mengawasi kinerja layanan, laporan layanan, dan melakukan audit terhadap supplier, termasuk melakukan follow up terhadap isu-isu yang telah teridifentifikasi dalam audit.
A.16 Manajemen Insiden Keamanan Informasi	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?	N	***Control 16.1.1 Responsibilities and Procedures*** Tanggungjawab dan prosedur manajemen harus disusun untuk memastikan respon insiden keamanan informasi yang cepat dan efektif. Berikut adalah yang perlu dipersiapkan, yaitu prosedur perencanaan dan persiapan respon insiden, prosedur untuk memonitor, mendeteksi, menganalisis, dan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			melaporkan kejadian insiden keamanan informasi, prosedur untuk mencatat aktivitas manajemen insiden, prosedur untuk mengelola bukti forensic, prosedur untuk menilai dan memutuskan kejadian dan kelemahan keamanan informasi, serta prsedur untuk merespon, termasuk mengeskalasi, mengontrol serta mengkomunikasikan kepada pihak internal dan eksternal dari organisasi.
	3.1 Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	N	***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. Dalam prosedur juga harus memastikan bahwa pelaksana harus

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			berkompeten dalam menangani masalah terkait insiden keamanan informasi. Tujuan dari pengelolaan insiden keamanan informasi harus disepakati dengan manajemen. ***Control 16.1.2 Reporting information security events & 16.1.3 Reporting information security weaknesses*** Harus dilakukan juga pelaporan terhadap kejadian dan kelemahan yang menyangkut keamanan informasi. Kejadian yang dapat dilaporkan sebagai insiden adalah kontrol keamanan yang tidak efektif, pelanggaran integritas informasi, kesalahan manusia, dsb. ***Control 16.1.4 Assessment of and decision on information***

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			security events Selanjutnya harus dilakukan penilaian dan 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.
	3.3 Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	N	***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

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			keamanan informasi. Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk mengidentifikasi dampak dari insiden yang terjadi.
	7.3.2 Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	QY	***Control 16.1.1 Responsibilities and procedures*** Tanggung jawab dan prosedur manajemen risiko di DPTSI termasuk eskalasi pelaporan status pengelolaan pada pimpinan harus ditetapkan untuk memastikan proses yang cepat, efektif dan tanggapan tertib terhadap insiden keamanan informasi. ***Control 16.1.5 Response to information security incidents*** Dilakukan penentuan bagian khusus dalam menangani insiden keamanan informasi. Bagian penanganan insiden

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			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
	3.8 Apakah dampak kerugian yang terkait dengan hilangnya/terangguny a fungsi aset utama sudah ditetapkan	N	***Control 16.1.6 Learning from Information Security Incidents*** Sebaiknya terdapat evaluasi insiden keamanan informasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	sesuai dengan definisi yang ada?		untuk membantu membuat penyusunan mekanisme pengukuran dan monitoring biaya insiden keamanan informasi, sehingga kerugian dapat dicegah
	3.9 Apakah instansi/perusahaan 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)?	N	***Control 16.1.6 Learning from Information Security Incidents*** Perlunya DPTSI membuat suatu prosedur untuk mengukur dan memonitor setiap risiko yang terjadi dan akan terjadi pada asset informasi yang dimiliki agar dapat mengidentifikasi mitigasi risiko-risiko tersebut. Tindakan memonitor risiko misalnya adalah melakukan rapat rutin dengan bahasan mengkaji ulang penanganan-penanganan dari tiap risiko, yang sekaligus perlu untuk didokumentasikan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			sebagai bagian awal dari mitigasi risiko.
	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?	N	***Control 16.1.6 Learning from Information Security Incidents 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 suatu insiden yang terjadi maka dapat diukur apakah langkah tersebut berjalan dengan baik dan efektif untuk menangguangi insiden yang terjadi. Kemudian apabila ditemukan ketidak efektifan suatu mitigasi dalam menangani insiden maka perlu untuk dibuat suatu forum tersendiri yang membahas mengenai permasalahan tersebut.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	3.15 Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	N	***Control 16.1.6 Learning from information security incidents*** DPTSI seharusnya membuat suatu mekanisme untuk memastikan efektifitas dan meningkatkan kinerja dari kerangka kerja yang digunakan saat ini. Kinerja dari kerangka kerja ini bisa dilihat dari seberapa besar pengaruh kerangka kerja dalam menangani insiden yang sedang terjadi. Dari sini kita juga bisa melihat efektifitas dari kerangka kerja yang digunakan.
	2.18 Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya,	N	***Control 16.1.1 Responsibilities and procedures*** DPTSI seharusnya membuat pengukuran kinerja pengelolaan keamanan informasi dan prosedur yang berkaitan dengan keamanan informasi. Prosedur dan kebijakan ini

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	pemantauannya dan eskalasi pelaporannya?		harus memuat hal – hal berikut ini: • Prosedur untuk pemantauan, pendeteksian, analisis dan pelaporan kejadian kemanan informasi. • Prosedur untuk mengelola bukti forensik • Prosedur untuk pengambilan keputusan setiap kejadian keamanan informasi dan penilaian kelemahan keamanan informasi. • Prosedur untuk eskalasi dan pemulihan dari sebuah insiden.
	3.13 Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	N	***Control 16.1.6 Learning from Information Security Incidents*** Harus ada mekanisme yang dilakukan DPTSI untuk memastikan dan meningkatkan efektivitas dari langkah mitigasi yang telah diterapkan. Hal ini dapat dilihat dari seberapa besar pengaruh mitigasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			yang telah diterapkan dalam menangani risko yang terjadi. Jika efek yang diberikan masih belum terlalu signifikan maka mitigasi tersebut perlu dikaji ulang.
	3.16 Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	N	***Control 16.1.1 Responsibilities and Procedures*** DPTSI seharusnya menyertakan pengelolaan risiko tersebut menjadi bagian dari kriteria proses penialian kinerja efektifitas pengamanan. Hal ini bertujuan untuk memastikan bahwa insiden yang terjadi bisa ditangani dengan respon yang cepat dan efektif. Manajemen isiden ini setidaknya memuat hal – hal dibawah ini : • Prosedur penanganan bukti forensik • Prosedur insiden logging Prosedur untuk eskalasi dan pemulihan dari insiden

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
A.17 Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis	7.1.7.2 Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	N	***Control 17.1.3 Verify, Review and Evaluate Information Security Continuity*** Organisasi harus memverifikasi keberlangsungan kontrol keamanan informasi yang telah dibuat dan diimplementasikan pada interval waktu yang telah ditentukan untuk memastikan kontrol tersebut valid dan efektif meski dalam keadaan merugikan. Bentuk verifikasi yang bisa dilakukan yaitu menguji fungsionalitas keberlangsungan proses keamanan informasi, prosedur, dan kontrolnya.
	4.15 Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsidera ns keamanan informasi, termasuk	N	***Control 17.1.1 Planning Information Security Continuity*** Organisasi harus menentukan persyaratan keamanan informasi dan keberlangsungan dari manajemen keamanan informasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	penjadwalan uji cobanya?		dalam kondisi yang merugikan, seperti adanya bencana.
	2.14 Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?	N	***Control 17.1.1 Planning information security continuity Control 17.1.2 Implementing information security continuity*** DPTSI harus menentukan, mengembangkan, mendokumentasikan, mengalokasikan, dan mengimplementasikan manajemen keberlangsungan bisnis untuk memastikan DPTSI memiliki aspek keberlangsungan bisnis dalam keadaan yang tidak menguntungkan sekalipun. DPTSI dalam hal ini juga harus memastikan : • Struktur manajemen yang sepadan dan mumpuni untuk menanggapi dan memitigasi suatu kejadian yang

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			bersifat mengganggu. • Keahlian dan wewenang yang dimiliki oleh pihak terkait untuk mengelola kejadian tersebut • Merencanakan dan mendokumentasi prosedur respon dan recovery secara detail bagaimana DPTSI harus mengelola insiden dan tetap menjaga kemanan informasi.
	4.16 Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	N	***Control 17.1.2 Implementing Information Security Continuity*** Organisasi harus melakukan perencanaan keberlangsungan keamanan informasi, termasuk mendefinisikan peran dan tanggungjawab dalam mengelola insiden keamanan informasi, serta melakukan dokumentasi perencanaan, respon, serta pemulihan proses tersebut.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
A.18 Kepatuhan	7.3.14 Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/ pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	QY	***Control 18.1.3 Protection of Records*** Pencatatan informasi harus terlindungi dari kehilangan, kehancuran, pemalsuan, akses tidak sah, peraturan kontrak, dan bisnis. Sistem penyimpanan data dan periode penyimpananannya harus disesuaikan dengan regulasi regional maupun nasional. Agar ogranisasi bisa memenuhi tujuan keamanan pencatatan data, langkah yang harus dilakukan yaitu mengeluarkan pedoman tentang penyimpanan dan pembuangan informasi, membuat jadwal periode data yang disimpan, dan menginventarisasi sumber informasi.
	7.3.15 Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah	N	***Control 18.1.3 Protection of Records*** Pencatatan informasi harus terlindungi dari

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	tidak ada keperluan yang sah untuk menyimpan/mengolah nya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?		kehilangan, kehancuran, pemalsuan, akses tidak sah, peraturan kontrak, dan bisnis. Sistem penyimpanan data dan periode penyimoananannya harus disesuaikan dengan regulasi regional maupun nasional. Agar ogranisasi bisa memenuhi tujuan keamanan pencatatan data, langkah yang harus dilakukan yaitu mengeluarkan pedoman tentang penyimpanan dan pembuangan informasi, membuat jadwal periode data yang disimpan, dan menginventarisasi sumber informasi.
	7.3.16 Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	QY	***Control 18.1.3 Protection of Records*** Pencatatan informasi harus terlindungi dari kehilangan, kehancuran, pemalsuan, akses tidak sah, peraturan kontrak, dan bisnis. Beberapa informasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			mungkin perlu disimpan dengan aman untuk memenuhi persyaratan hokum, peraturan, atau kontrak, seperti catatan yang diperlukan sebagai bukti bahwa organisasi beroperasi sesuai Undang-Undang atau untuk memastikan adanya tindakan pidana suatu organisasi.
	2.11 Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	N	***Control 18.1.4 Privacy and protection*** of personally identifiable information DPTSI harus mengidentifikasi perlindungan privasi dan data pribadi yang sesuai dengan legislasi dan regulasi yang berlaku. DPTSI harus mengembangakan dan mengimplementasikan kebijakan yang berkaitan dengan perlindungan privasi

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			dan data pribadi. Kebijakan ini juga harus dikomunikasikan kepada semua pihak yang terkait dalam pemrosesan data dan informasi.
	2.21 Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	N	***Control 18.2.2 Compliance with security policies and standards*** Pihak manajemen DPTSI seharusnya melakukan ulasan dan mengidentifikasi kepatuhan prosedur dan kebijakan yang ada dengan hukum dan peraturan yang berlaku. Ketika ada ketidakpatuhan atau penyimpangan terhadap aturan yang berlaku, pihak manajemen harus melakukan hal – hal dibawah ini: • Mengidentifikasi penyebab dari penyimpangan • Mengevaluasi tindakan untuk mencapai kepatuhan • Mengimplementasik

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			an tindakan perbaikan yang tepat • Mengulas tindakan perbaikan tersebut apakah sudah efektif.
	2.22 Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	N	***Control 18.2.2 Compliance with security policies and standards*** Pihak manajemen DPTSI seharusnya melakukan ulasan dan mengidentifikasi kepatuhan prosedur dan kebijakan yang ada dengan hukum dan peraturan yang berlaku. Selain itu juga harus didefinisikan langkah penanggulangan yang sesuai. Ketika ada ketidakpatuhan atau penyimpangan terhadap aturan yang berlaku, pihak manajemen harus melakukan hal – hal dibawah ini: • Mengidentifikasi penyebab dari penyimpangan • Mengevaluasi tindakan untuk

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			mencapai kepatuhan • Mengimplementasikan tindakan perbaikan yang tepat. Mengulas tindakan perbaikan tersebut apakah sudah efektif.
	5.15 Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	N	***Control 18.1.3 Protection of Records*** Pencatatan informasi harus terlindungi dari kehilangan, kehancuran, pemalsuan, akses tidak sah, peraturan kontrak, dan bisnis. Sistem penyimpanan data dan periode penyimoananannya harus disesuaikan dengan regulasi regional maupun nasional. Agar ogranisasi bisa memenuhi tujuan keamanan pencatatan data, langkah yang harus dilakukan yaitu mengeluarkan pedoman tentang penyimpanan dan pembuangan informasi, membuat

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			jadwal periode data yang disimpan, dan menginventarisasi sumber informasi.
	7.2.3 Apakah instansi/ perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/ diolah/ dipertukarkan melalui layanan cloud?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.
	7.3.6 Apakah instansi/ perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	QY	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.
	7.3.7 Apakah kajian risiko keamanan pada instansi/ perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	7.3.8 Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.
	7.3.9 Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.
	4.3 Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	N	***Control 18.2.1 Independent Review of Information Security*** ***Control 18.2.2 Compliance with Security Policies and Standards*** Organisasi harus melakukan pengelolaan dokumen kebiajakan dan prosedur keamanan informasi yang ditinjau secara independent pada interval waktu yang telah ditetapkan. Organisasi juga harus melakukan peninjauan terkait kepatuhan pengelolaan keamanan informasi. Apabila terjadi ketidakpatuhan, maka harus dilakukan identifikasi penyebabnya dan mengevaluasinya

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			agar organisasi menjadi patuh.
	4.9 Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	N	***Control 18.2.3 Technical Compliance Review*** Organisasi harus membuat prosedur resmi untuk meninjau kepatuhan teknis dan menindaklanjuti penerapan keamanan informasi. Peninjauan harus dilakukan oleh pihak yang berkompeten atau berwenang.
	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?	N	***Control 18.1.2 Intellectual Property Rights*** Organisasi harus membuat prosedur untuk memastikan kepatuhan dengan persyaratan legislative, peraturan, dan kontrak terkait HAKI dan penggunaan perangkat lunak.
	7.1.5.1 Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information***

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	pembuatan, pendaftaran, perubahan, dan penghapusan/ penghancuran aset?		Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.
	7.3.1 Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			terkait prinsip-prinsip privasi.
	7.3.3 Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Organisasi harus mengembangkan kebijakan privasi dan perlindungan terhadap data pribadi yang sesuai dengan Undang-Undang perlindungan privasi. Hal tersebut dapat diterapkan dengan memberikan panduan kepada manajer, user, dan penyedia layanan terkait prinsip-prinsip privasi.
	7.1.5.2 Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	N	***Control 18.1.3 Protection of Records*** ***Control 15.1.2 Addressing Security within Supplier Agreements*** Organisasi harus membuat panduan terkait isu penyimpanan dan pembuangan data/ informasi. Panduan tersebut harus

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
			disetujui oleh kedua belah pihak dengan mencantumkan perjanjian skema klasifikasi informasi organisasi dan supplier.
	7.3.10 Apakah instansi/ perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?	N	***Control 18.1.4 Privacy and Protection of Personally Identifiable Information*** Kebijakan privasi dan perlindungan data yang berkaitan dengan data pribadi harus dikembangkan, diimplementasikan, dan dikomunikasikan kepada seluruh pihak yang terlibat dalam proses dari data pribadi.
	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	N	***Control 18.2.1 Independent Review of Information Security*** Pendekatan organisasi dalam melakukan pengamanan keamanan informasi dan implementasinya (termasuk control objective, kontrol,

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	(atau sesuai dengan standar yang berlaku)?		kenijakan, proses, dan prosedur harus ditinjau secara independent pada interval waktu yang telah ditentukan. Peninjauan independent ini harus diinisiasi oleh manajemen, oleh internal auditor, manajer independent, atau pihak eksternal yang memiliki spesialisasi untuk melakukan hal tersebut.
	4.24 Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	N	***Control 18.2.1 Independent Review of Information Security*** Hasil audit internal harus disimpan dan dilaporkan kepada manajemen yang menginisiasi aktivitas review, dan laporan tersebut juga harus dipelihara/dievaluasi, terutama apabila teridentifikasi pendekatan implementasi keamanan informasi organisasi masih belum sesuai, maka harus dilakukan tindakan perbaikan.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	2.20 Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	N	***Control 18.2.1 Independent review of information security*** DPTSI seharusnya melakukan pendekatan untuk berbagai area yang berkaitan dengan kemanan informasi. Pendekatan(yakni berupa kontrol, sasaran, kebijakan, proses, dan prosedur untuk keamanan informasi) ini seharusnya juga diulas secara berkala. Ulasan tersebut seharusnya diaudit oleh tiap individu sesuai dengan area yang relevan. Individu yang melakukan audit ini juga harus memiliki kemampuan dan pengalaman yang sesuai. Lalu, hasil dari audit ini didokumentasikan dan dieskalasi ke pihak manajemen untuk nantinya dikelola lebih lanjut.

Annex A	Pertanyaan Indeks KAMI	*Check-list*	Rekomendasi
	6.26 Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	N	***Control 18.2.1 Independent review of information security*** ***Control 18.2.2 Compliance with security policies and standards*** DPTSI seharusnya menetapkan mekanisme untuk mengelola dokumen kebijakan dan harus diulas dalam jangka waktu tertentu. Selain itu, jika pada saat mengulas ditemukan ketidakpatuhan pihak manajemen bisa melakukan: • Identifikasi penyebab ketidakpatuhan • Evaluasi tindakan untuk mencapai kepatuhan • Menerapkan tindakan korektif yang tepat Mengevaluasi tindakan korektif apakah sudah efektif atau belum.