TUGAS AKHIR – IS184853

PENYUSUNAN PERANGKAT CHECKLIST KEBUTUHAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS STANDAR ISO/IEC 27001:2013 DAN INDEKS KAMI 4.0

DEVELOPMENT OF REQUIREMENT CHECKLIST DEVICE FOR APPLICATION OF INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON ISO/IEC 27001:2013 STANDARDS AND INDEKS KAMI 4.0

TITUS GIGIH TRIONGGO
NRP. 05211540000107

Dosen Pembimbing
Hanim Maria Astuti, S.Kom, M.Sc., ITIL.
Anisah Herdiyanti Prabowo, S.Kom., M.Sc.

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

TUGAS AKHIR – IS184853

PENYUSUNAN PERANGKAT CHECKLIST KEBUTUHAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS STANDAR ISO/IEC 27001:2013 DAN INDEKS KAMI 4.0

TITUS GIGIH TRIONGGO
NRP 0521 1540 000 107

Dosen Pembimbing
Hanim Maria Astuti, S.Kom, M.Sc., ITIL.
Anisah Herdiyanti Prabowo, S.Kom., M.Sc.

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

UNDERGRADUATE THESES – IS184853

DEVELOPMENT OF REQUIREMENT CHECKLIST DEVICE FOR APPLICATION OF INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON ISO/IEC 27001:2013 STANDARDS AND INDEKS KAMI 4.0

TITUS GIGIH TRIONGGO
NRP 0521 1540 000 107

Supervisor
Hanim Maria Astuti, S.Kom, M.Sc., ITIL.
Anisah Herdiyanti Prabowo, S.Kom., M.Sc.

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

LEMBAR PENGESAHAN

PENYUSUNAN PERANGKAT CHECKLIST KEBUTUHAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS STANDAR ISO/IEC 27001:2013 DAN INDEKS KAMI 4.0

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:

TITUS GIGIH TRIONGGO
05211540000107

Surabaya, Januari 2020

KETUA
DEPARTEMEN SISTEM INFORMASI

Dr. Mudjahidin, S.T., M.T
NIP. 19701010 200312 1 001

LEMBAR PERSETUJUAN

PENYUSUNAN PERANGKAT CHECKLIST KEBUTUHAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS STANDAR ISO/IEC 27001:2013 DAN INDEKS KAMI 4.0

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:

TITUS GIGIH TRIONGGO
05211540000107

Disetujui Tim Penguji
Tanggal Ujian : 30 Januari 2020
Periode Wisuda : Maret 2020

Hanim Maria Astuti, S.Kom., M.Sc., ITIL.	**(Pembimbing I)**
Anisah Herdiyanti P, S.Kom., M.Sc.	**(Pembimbing II)**
Apol Pribadi S, S.T., M.T.	**(Penguji I)**
Eko Wahyu Tyas D, S.Kom., MBA.	**(Penguji II)**

PENYUSUNAN PERANGKAT CHECKLIST KEBUTUHAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS STANDAR ISO/IEC 27001:2013 DAN INDEKS KAMI VERSI 4.0

Nama Mahasiswa	**:**	**Titus Gigih Trionggo**
NRP	**:**	**05211540000107**
Departemen	**:**	**Sistem Informasi FTEIC-ITS**
Pembimbing 1	**:**	**Hanim Maria Astuti, S.Kom., M.Kom., ITIL.**
Pembimbing 2	**:**	**Anisah Herdiyanti P, S.Kom., M.Sc.**

ABSTRAK

Perkembangan teknologi informasi yang berkembang pesat membuat organisasi atau perusahaan harus menerapkan teknologi informasi untuk meningkatkan peforma organisasi atau perusahaan tersebut. Dengan dana yang besar dalam investasi teknologi informasi, organisasi atau perusahaan harus menjaga keamanan dari teknologi informasi tersebut untuk menjaga kestabilan organisasi atau perusahaan dan menjaga informasi penting yang ada. Dalam menjaga keamanan informasi perlu adanya tata kelola yang baik untuk meminimalisir risiko yang muncul. Standar keamanan informasi yang disarankan untuk diterapkan di Indonesia adalah penerapan sistem manajemen keamanan informasi. SMKI merupakan tata kelola keamanan informasi yang berbasis Indeks KAMI dan ISO/IEC 27001:2013. Permasalahan yang sering dialami organisasi atau perusahaan dalam penerapan SMKI adalah kebutuhan penerapan SMKI yang belum terdeteksi dengan baik. Belum baiknya pendeteksian tersebut membuat organisasi atau perusahaan sulit untuk menyiapkan alat kerja yang akan digunakan dalam penerapan SMKI.

Dari permasalahan yang dijabarkan menyimpulkan perlu adanya sebuah perangkat checklist yang dapat menjadi kontrol atas capaian penerapan SMKI pada sebuah organisasi

atau perusahaan. Pembuatan perangkat checklist ini berfokus pada lima area yang ada pada Indeks KAMI. Perangkat checklist kebutuhan penerapan SMKI ini dibuat berdasarkan ISO/IEC 27001:2013 dan Indeks KAMI versi 4.0.

Kata Kunci: Keamanan Informasi, SMKI, ISO/IEC 27001:2013, Indeks KAMI, Checklist.

DEVELOPMENT OF REQUIREMENT CHECKLIST DEVICE FOR APPLICATION OF INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON ISO/IEC 27001:2013 STANDARDS AND INDEKS KAMI VERSION 4.0

Student Name	**:**	**Titus Gigih Trionggo**
NRP	**:**	**05211540000107**
Department	**:**	**Sistem Informasi FTEIC-ITS**
Supervisor 1	**:**	**Hanim Maria Astuti, S.Kom., M.Kom., ITIL.**
Supervisor 2	**:**	**Anisah Herdiyanti P, S.Kom., M.Sc.**

ABSTRACT

The rapid development of information technology makes organizations or companies need to implement information technology to improve the performance of these organizations or companies. With substantial funds in the investment of information technology, the organization or the company must maintain the security of such information technology to maintain the stability of the organization or the company and safeguard the important information that exists. In maintaining the security of information need good governance to minimize the risks that arise. The recommended information security standards for implementation in Indonesia are the application of information security management systems. SMKI is an information security governance based on Indeks KAMI and ISO/IEC 27001:2013. The problem that often experienced by organizations or companies in the implementation of SMKI is the need for the implementation of SMKI that has not been detected well. It is not as good as the detection makes organizations or companies difficult to set up a work tool that will be used in implementing SMKI.

From the problems outlined in conclusion need a checklist tool that can be control of the achievement of

implementing SMKI in an organization or company. The creation of this checklist tool focuses on six areas of Indeks KAMI. Checklist device needs to implement SMKI is made based on ISO/IEC 27001:2013 and Indeks KAMI version 4.0.

Keywords: Information security, SMKI, ISO/IEC 27001:2013, Indeks KAMI version 4.0, Checklist

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertandatangan di bawah ini:

Nama	: Titus Gigih Trionggo
NRP	: 05211540000107
Tempat/Tanggal lahir	: Mempawah / 03 Desember 1996
Fakultas/Departemen	: Fakultas Teknologi Elektro dan Informatika Cerdas/ Departemen Sistem Informasi
Nomor Telp/Hp/email	: 083832628432

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

Penyusunan Perangkat Checklist Kebutuhan Penerapan Sistem Manajemen Kemanan Informasi Berbasis ISO/IEC 27001:2013 dan Indeks KAMI 4.0

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.

Titus Gigih Trionggo

NRP. 05211540000107

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala petunjuk, pertolongan dan kekuatan yang diberikan kepada peneliti sehingga dapat menyelesaikan laporan penelitian tugas akhir ini. Adapun judul dari laporan penelitian tugas akhir ini yaitu **PENYUSUNAN PERANGKAT CHECKLIST KEBUTUHAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS STANDAR ISO/IEC 27001:2013 DAN INDEKS KAMI 4.0**

Pada kesempatan kali ini, peneliti mengucapkan terima kasih sebanyak-banyaknya kepada pihak yang telah memberi bantuan, dukungan dan arahan dalam penyelesaian tugas akhir ini. Berikut penulis ucapkan terima kasih kepada:

1. Bapak dan ibu penulis yang selalu mendukung, memotivasi dan mendoakan penulis dalam menyelesaikan laporan tugas akhir ini.
2. Ibu Hanim Maria Astuti, S. Kom. dan ibu Anisah Herdiyanti Prabowo, S. Kom., M. Sc. selaku dosen pembimbing yang telah membimbing, mendukung dan memotivasi penulis untuk segera menyelesaikan tugas akhir ini.
3. Ibu Renny Pradina Kusumawardani, S.T., M. T. selaku dosen wali yang telah mengarahkan dan memotivasi penulis selama masa studi perkuliahan sampai dengan pengerjaan tugas akhir ini.
4. David Catur Kurniawan dan Wahyu Isya Wantoro yang menyediakan tempat dan wifi untuk mengerjakan tugas akhir bersama.
5. Anindya Dwi L. S. dan Ivva Rahmawati A. selaku teman baik yang selalu mendukung dan memotivasi penulis untuk menyelesaikan tugas akhir ini.

Penyusunan laporan tugas akhir yang dilakukan peneliti masih jauh dari kata sempurna, oleh karena itu peneliti sangat menerima kritik dan saran yang membangun untuk perbaikan dimasa yang akan dating. Penelitian ini

diharapkan dapat menjadi acuan atau referensi penelitian-penelitian selanjutnya yang memiliki penelitian serupa dan dapat bermanfaat bagi pembaca.

Surabaya, 30 Januari 2020

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini menjelaskan mengenai Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, Manfaat Tugas Akhir, Relevansi Tugas Akhir, dan Sistematika Penulisan dari tugas akhir.

1.1 Latar Belakang

Di zaman sekarang perkembangan TI telah meningkat pesat karena dapat membuat sebuah proses bisnis di suatu organisasi menjadi lebih efektif dan efisien. Hal ini menyebabkan perusahaan-perusahaan di seluruh dunia tidak terkecuali Indonesia sudah berbondong-bondong menerapkan TI untuk organisasi mereka. Selain perusahaan, Lembaga pemerintah di Indonesia juga sudah mulai mengembangkan teknologi informasinya secara masif. Teknologi informasi yang menjadi aset penting dalam sebuah organisasi memiliki kebutuhan yang penting yaitu pada bidang keamanan. Risiko dari keamanan informasi memiliki dampak kerugian yang tinggi pada perusahaan. The Information Systems Audit and Control Association atau yang lebih dikenal ISACA mencatat kerugian yang diakibatkan dari dampak risiko keamanan informasi secara global mencapai sebesar 600 miliar dolar amerika pada tahun 2018[1]. Dengan hal tersebut maka semakin tinggi nilai aset TI akan membuat semakin tinggi pula risiko keamanan informasi dari aset TI tersebut.

Tingginya nilai dari aset TI dan besarnya dampak kerugian dari risiko aset TI pada bidang keamanan informasi membuat organisasi atau perusahaan perlu menjaga teknologi informasi tersebut. organisasi atau perusahaan perlu menerapkan keamanan informasi sebagai bentuk memberi perlindungan pada teknologi informasi yang berisi informasi penting organisasi atau perusahaan dari berbagai ancaman keamanan informasi baik secara langsung maupun tidak langsung[2]. Keamanan informasi dapat menjamin keberlanjutan proses bisnis, mengurangi resiko bisnis dan meningkatkan peluang

bisnis organisasi sehingga keamanan informasi sangat diperlukan organisasi maupun perusahaan[3].

Demi meningkatkan keamanan informasi untuk menjamin terjaganya TI yang dimiliki organisasi, diperlukan sebuah tata kelola keamanan informasi untuk mengatur keamanan dari TI. Di Indonesia, setiap organisasi atau perusahaan yang menyelenggarakan TI wajib untuk menetapkan tata kelola keamanan informasi yang andal, aman dan bertanggung jawab sesuai pasal 15 UU Nomor 19 Tahun 2016 dan Peraturan Pemerintah Nomor 82 Tahun 2012. Berdasarkan Undang-Undang dan Peraturan Pemerintah tersebut, organisasi atau perusahaan disarankan menetapkan sebuah sistem yang bernama sistem manajemen keamanan informasi (SMKI) dalam mengelola keamanan informasi organisasi. SMKI dapat menjadi acuan dalam tata kelola keamanan informasi karena sudah berbasis Indeks KAMI yang merupakan alat evaluasi untuk melihat kematangan dari keamanan informasi di sebuah organisasi. Selain itu SMKI sudah sesuai dengan standar SNI dari best practice ISO/IEC 27000:2013. ISO/IEC 27001:2013 adalah standar yang fokus pada penggunaan teknologi informasi dan pengelolaan aset untuk membantu organisasi memastikan keamanan yang diterapkan berjalan dengan lancar. ISO/IEC 27001:2013 berfokus menyediakan standar yang membahas tentang manajemen keamanan informasi di sebuah organisasi. Standar dari best practice ini digunakan untuk membuat kontrol dari keamanan yang sudah diterapkan [4].

Permasalahan yang sering dihadapi perusahaan atau organisasi dalam merencanakan dan menerapkan SMKI adalah tidak adanya perangkat checklist yang memberikan informasi sejauh mana kontrol-kontrol pada standar ISO/IEC 27001:2013 yang telah dicapai dari SMKI yang telah diterapkan sebuah organisasi atau perusahaan. Permasalahan ini menyebabkan kurang baiknya indentifikasi kebutuhan pada organisasi atau perusahaan yang sedang menerapkan SMKI karena tidak tahu mana kontrol-kontrol pada standar dari best practice ISO/IEC 27001:2013 yang sudah dicapai dan mana yang belum dicapai.

Disamping itu juga permasalahan ini juga menyebabkan kesulitan organisasi atau perusahaan dalam menyiapkan alat kerja yang akan digunakan untuk memenuhi standar.

Berdasarkan hal tersebut, organisasi atau perusahaan yang akan menerapkan SMKI memerlukan sebuah perangkat yang dapat mencatat pencapaian standar yang sudah dicapai. Tugas akhir ini akan mengemukakan rancangan perangkat checklist penerapan SMKI yang berbasis standar dari best practice ISO/IEC 27001:2013 dan berdasarkan alat evaluasi Indeks KAMI versi 4.0.

1.2 Rumusan Masalah

Berdasarkan penjabaran latar belakang di atas, berikut rumusan masalah yang akan dibahas pada tugas akhir ini :

1. Bagaimana cara mendapatkan kebutuhan di dalam checklist kebutuhan penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001:2013 dan Indeks KAMI versi 4.0?
2. Bagaimana bentuk perangkat checklist penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001:2013 dan Indeks KAMI versi 4.0?

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas, Batasan dalam pengerjaan tugas akhir adalah sebagai berikut :

1. Perancangan sistem manajemen keamanan informasi ini diarahkan untuk fokus pada pembuatan checklist penerapan sistem keamanan manajemen keamanan informasi.
2. Perancangan checklist penerapan sistem manajemen keamanan informasi menggunakan standar dari best practice ISO/IEC 27001:2013 yang berhubungan dengan Indeks KAMI versi 4.0.
3. Perancangan checklist penerapan sistem manajemen keamanan informasi hanya menggunakan pertanyaan

Indeks KAMI yang terpetakan dengan klausul ISO/IEC 27001:2013 pada hasil pemetaan pertanyaan Indeks KAMI 4.0 dengan klausul ISO/IEC 27001:2013.

1.4 Tujuan Tugas Akhir

Berdasarkan rumusan masalah dan batasan masalah yang telah dijabarkan, tujuan dari penelitian tugas akhir ini adalah sebagai berikut :

1. Mengetahui daftar kebutuhan di dalam checklist penerapan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001:2013 dan Indeks KAMI versi 4.0.
2. Mengembangkan solusi dalam penerapan sistem manajemen keamanan informasi berupa checklist kebutuhan dari penerapan sistem manajemen keamanan informasi.

1.5 Manfaat Tugas Akhir

Manfaat yang didapatkan dari pengerjaan tugas akhir ini adalah sebagai berikut :

1. Tugas akhir ini diharapkan dapat memberi luaran berupa checklist kebutuhan penerapan SMKI yang mempermudah suatu organisasi atau perusahaan dalam menerapan sistem manajemen keamanan informasi mereka.
2. Tugas akhir ini diharapkan dapat memberikan bantuan berupa pemikiran dan referensi untuk peneliti yang sedang melakukan penelitian sejenis.

1.6 Relevansi Tugas Akhir

Tugas akhir ini tentang pembuatan perangkat checklist penerapan sistem manajemen keamanan informasi yang berkaitan dengan mata kuliah Manajemen Risiko & Kualitas TI dan Tatakelola TI.

1.7 Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini dibagi menjadi tiga bagian bab. Berikut masing-masing bab yang sudah dibagi.

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, relevansi tugas akhir, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai definisi dan penjelasan pustaka dari berbagai sumber yang berhubungan dengan penelitian serta dijadikan referensi dalam pembuatan tugas akhir ini.

BAB III METODOLOGI

Bab ini membahas mengenai gambaran langkah-langkah pekerjaan yang dilakukan selama penyusunan tugas akhir mulai awal sampai akhir penelitian.

BAB IV PERANCANGAN

Bab ini akan membahas tentang perancangan dari penggalian data, identifikasi data dan output untuk menghasilkan perangkat *checklist* kebutuhan yang *deliverables.*

BAB V IMPLEMENTASI

Bab ini akan membahas tentang proses implementasi dari rancangan penggalian data yang telah dibuat pada bab sebelumnya dimana akan dijelaskan hasil dari rancangan penggalian data yang telah didapatkan melalui studi dokumen.

BAB VI HASIL DAN PEMBAHASAN

Bab ini akan membahas mengenai proses identifikasi kebutuhan dan tingkat kepentingan kebutuhan dari hasil penggalian data yang dilakukan pada bab sebelumnya. Bab ini juga membahas tentang hasil perangkat checklist yang dibuat berdasarkan referensi penelitian sebelumnya.

BAB VII KESIMPULAN DAN SARAN

Bab ini berisi tentang simpulan dari seluruh pengerjaan tugas akhir dan adapun saran maupun rekomendasi terkait perbaikan untuk penelitian selanjutnya yang memiliki kesamaan topik.

BAB II
TINJAUAN PUSTAKA

Pada bab ini membahas mengenai definisi dan penjelasan pustaka dari berbagai sumber yang berhubungan dengan penelitian serta dijadikan referensi dalam pembuatan tugas akhir. Berikut merupakan hal yang ada pada Tinjauan Pustaka penelitian ini.

2.1 Studi Sebelumnya

Penelitian sebelumnya digunakan peneliti sebagai referensi dan acuan dalam pengerjaan tugas akhir ini. Sub bab ini dijelaskan dengan menggunakan tabel pada tabel 2.1.

Tabel 2. 1 Penelitian Sebelumnya

Judul Penelitian	Penulis	Metodologi	Hubungan dengan Penelitian
Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem	Firzah A. Basyarahil (2017)	• Standar yang digunakan adalah ISO/IEC 27001:2013. • Menggunakan Indeks KAMI versi 3.1 sebagai alat penilaian. • Melakukan penilaian kelima area Indeks KAMI pada	Pemetaan keterhubungan antara ISO/IEC 27001:2013 dengan Indeks KAMI versi 3.1 menjadi referensi studi pustaka pendukung dan acuan dalam pengerjaan penelitian ini.

Judul Penelitian	Penulis	Metodologi	Hubungan dengan Penelitian
Informasi (DPTSI) ITS Surabaya[5]		seluruh bagian di DPTSI ITS.	
Penyusunan Template Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005 dan Patuh Terhadap COBIT 5 Control Objective APO13 Manage Security[6]	Faridl Mughoffar (2014)	• Menggunakan kerangka kerja COBIT 5 pada APO13 yang membahas tentang Align, Plan dan Organize Manage Security. • Melakukan penyusunan template tata kelola keamanan informasi berdasarkan hasil pemetaan ISO 27001:2005 ke COBIT 5 APO13 untuk implementasi SMKI.	Pemetaan ISO 27001:2005 ke COBIT 5 APO13 dan metode penelitian yang digunakan narasumber menjadi referensi studi pustaka pendukung dan referensi penyusunan perangkat checklist pada pengerjaan penelitian ini.

Judul Penelitian	Penulis	Metodologi	Hubungan dengan Penelitian
Perencanaan Program Implementasi Enterprise Resource Planning (ERP) di PT. Perkebunan Nusantara XI: Pengendalian Kualitas[7]	Aprill Yozha (2016)	Melakukan pembuatan checklist pengendalian kualitas terkait perencanaan program implementasi ERP	Checklist yang dibuat oleh nara sumber dijadikan referensi studi pustaka pendukung dan referensi penyusunan perangkat checklist pada pengerjaan penelitian ini.

2.2 Dasar Teori

2.2.1 Informasi

Informasi adalah hasil pengolahan data dalam suatu bentuk yang lebih berguna dan lebih berarti bagi penerimanya. Data tersebut menggambarkan suatu kejadian – kejadian yang nyata yang digunakan untuk pengambilan keputusan. Kejadian – kejadian nyata yang dimaksud adalah Kejadian yang sering terjadi perubahan dari suatu nilai. Contoh dari kejadian ini seperti saat kita melakukan penjualan. Saat melakukan penjualan akan ada perubahan dari nilai barang menjadi nilai uang[8].

2.2.2 Keamanan Informasi

Keamanan informasi adalah upaya pengamanan atau perlindungan suatu aset informasi dari berbagai ancaman yang

mungkin timbul untuk memastikan atau menjamin keberlanjutan bisnis, meminimalisir resiko bisnis dan meningkatkan investasi dan peluang bisnis. semakin banyak informasi perusahaan yang disimpan, dikelola dan dibagikan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan [9].

Pada keamanan informasi ada tiga elemen dasar yang menjadi acuan dalam pengembangan program – program keamanan. Ketiga elemen tersebut merupakan mata rantai yang saling terhubung dalam konsep keamanan informasi. Berikut tiga aspek yang dimiliki keamanan informasi[9]:

1. Confidentiality
   Keamanan informasi mengamankan dan memastikan informasi hanya diakses oleh orang yang berhak mengakses informasi tersebut. Informasi yang diamankan biasanya berkaitan dengan data personal dan bersifat rahasia yang tidak boleh diketahui banyak orang. Data personal yang dimaksud lebih berkaitan dengan data pribadi, sendangkan data bersifat rahasia yang dimaksud adalah data yang rahasia yang dimiliki sebuah organisasi.
2. Integrity
   Keamanan informasi dapat menjamin semua data yang berisi informasi lengkap dan dalam keadaan utuh. Keamanan informasi juga menjamin data tidak dapat dimodifikasi oleh orang yang tidak berhak memodifikasinya dan data aman dari segala kerusakan dan ancaman lainnya.
3. Availability
   Keamanan informasi bisa menjamin data informasi dapat di akses oleh pengguna kapanpun, dimanapun dengan tanpa adanya delay yang menghambat serta tersampaikannya seluruh data informasi yang di akses secara utuh tanpa mengalami kerusakan sedikitpun.

Dalam keamanan informasi ada beberapa jenis fokusan keamanan yang digunakan. Berikut jenis keamanan informasi tersebut :

1. Physical security
   Keamanan informasi berfokus pada aset yang berbentuk fisik dari segala ancaman yang menyebabkan hilangnya aset fisik tersebut. Aset fisik yang dimaksud seperti individu atau anggota organisasi, aset fisik, dan tempat kerja yang dimiliki organisasi.
2. Personal security
   Keamanan informasi berfokus pada keamanan personal individu atau anggota organisasi. Jenis keamanan informasi ini biasanya berhubungan dengan jenis keamanan informasi physical security.
3. Operasional security
   Keamanan informasi berfokus pada pengamanan kemampuan yang dimiliki organisasi untuk menjamin organisasi dapat selalu beroperasi tanpa ada gangguan apapun.
4. Communication security
   Keamanan informasi berfokus pada yang pengamanan media komunikasi, teknologi komunikasi dan semua unsur komunikasi yang ada di dalam organisasi, serta kemampuan dalam pemanfaatan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. Network security
   Keamanan informasi yang berfokus pada pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan dalam menggunakan jaringan tersebut untuk memenuhi fungsi komunikasi data organisasi.

2.2.3 Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) adalah salah satu bagian dari sistem manajemen organisasi yang digunakan untuk menetapkan, menerapkan, mengoperasikan, memantau,

meninjau, memelihara dan meningkatkan keamanan informasi di sebuah organisasi. Dalam mengembangkan keamanan informasi, aspek SMKI dan teknologi keamanan informasi merupakan aspek yang sangat penting dan tidak dapat dipisahkan satu dengan lainnya. Artinya sebaiknya suatu organisasi tidak hanya menerapkan teknologi keamanan informasi saja tanpa menerapkan SMKI[10].

SMKI juga merupakan pendekatan yang sistematis untuk mengelola data informasi sensitif yang dimiliki organisasi atau perusahaan melalui kebijakan dan prosedur yang dimiliki organisasi. Standar yang digunakan dalam implementasi SMKI di Indonesia adalah ISO/IEC 27001:2013, dimana standar yang dimiliki telah bebasis manajemen resiko. Dengan standar yang berbasis manajemen resiko, penerapan SMKI di Indonesia memiliki tujuan untuk meminimalisir risiko dan memitigasi risiko tersebut secara cepat dan tepat sehingga mengurangi dampak dari risiko tersebut dan menjamin keberlangsungan bisnis organisasi atau perusahaan [11].

Dalam pengembangan SMKI standar yang ada di ISO/IEC 27001:2013 dikembangkan menjadi proses – proses yang akan menjadi sebuah model bagi pengembangan SMKI di sebuah organisasi. Model yang dimaksud adalah model PLAN – DO – CHECK – ACT atau yang lebih dikenal PDCA merupakan model yang akan diterapkan pada struktur keseluruhan pada proses pembangunan SMKI [11]. Dalam model PDCA, semua proses SMKI dapat dipetakan seperti tabel berikut :

Tabel 2. 2 Peta PDCA dalam Proses SMKI

PLAN (Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.

DO (Menerapkan dan mengoperasikan SMKI)	Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur-prosedur.
CHECK (Memantau dan melakukan tinjau ulang SMKI)	Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.
ACT (Memelihara dan meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

2.2.4 Best Practice ISO/IEC 27001:2013 sebagai Standar SMKI

ISO/IEC 27001:2013 adalah sebuah standar yang dikeluarkan oleh International Organization for Standardization. ISO/IEC 27001:2013 merupakan standar yang membahas tentang spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) pada sebuah organisasi[4]. Standar ini memiliki sifat yang independen terhadap produk teknologi informasi. Standar ini juga mensyaratkan penggunanya melakukan pendekatan manajemen berbasis risiko ketika menggunakan standar ini. Standar ini dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan yang akurat kepada pihak yang berkepentingan di organisasi[10].

ISO/IEC 27001:2013 digunakan sebagai standar acuan dalam membangun sistem keamanan informasi atau SMKI. Standar ini

dikembangkan dan di sesuaikan dengan kondisi di Indonesia dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (review), pemeliharaan dan peningkatan suatu organisasi yang sedang membangun SMKI. ISO/IEC 27001:2013 mempunyai struktur yang dibagi menjadi dua bagian besar yaitu klausul yang terdiri dari 11 klausul dan mandatory process yang berisikan kumpulan security control atau lebih dikenal dengan Annex A yang terdiri dari 14 domain area dengan 35 kontrol objektif dan 114 kontrol keamanan informasi[12].

2.2.4.1 Annex A

Annex A merupakan dokumen yang disediakan ISO untuk memberi referensi atau gambaran tentang semua kontrol yang ada pada ISO/IEC 27001:2013[12]. Dengan adanya Annex A organisasi atau perusahaan dapat mengetahui kontrol mana yang dapat diterapkan pada organisasi atau perusahaannya dan menggunakan dokumen Annex A tersebut untuk dijadikan rujukan dalam menerapkan standar yang akan di implementasikan dalam SMKI[11]. Berikut adalah 14 klausal dan 35 kontrol objektifnya:

Tabel 2. 3 Daftar klausal dan kontrol objektif di Annex A

Klausal	Kontrol Objektif
A5 Kebijakan Keamanan Informasi	A5.1 Arahan Manajemen untuk keamanan Informasi
A6 Organisasi Keamanan Informasi	A6.1 Organisasi Internal
	A6.2 perangkat bergerak dan teleworking
A7 Keamanan Sumber Daya Manusia	A7.1 Sebelum dipekerjakan
	A7.2 Selama Bekerja

Klausal	Kontrol Objektif
	A7.3 Penghentian dan perubahan kepegawaian
A8 Manajemen Aset	A8.1 Tanggung Jawab terhadap aset
	A8.2 Klasifikasi Informasi
	A8.3 Penanganan Media
A9 Kendali Akses	A9.1 Persyaratan bisnis untuk kendali akses
	A9.2 Manajemen Akses Pengguna
	A9.3 Tanggung Jawab Pengguna
	A9.4 Kendali akses sistem dan aplikasi
A10 Kriptografi	A10.1 Kendali Kriptografi
A11 Keamanan Fisik dan Lingkungan	A11.1 Daerah Aman
	A11.2 Peralatan
A12 Keamanan Operasi	A12.1 Prosedur dan tanggung jawab operasional
	A12.2 Perlindungan dari malware
	A12.3 Cadangan (back up)

Klausal	Kontrol Objektif
	A12.4 Pencatatan dan pemantauan
	A12.5Kendali perangkat lunak operasional
	A12.6 Manajemen kerentanan teknis
	A12.7 Pertimbangan ausit sistem informasi
A13 Keamanan Komunikasi	A13.1 Manajemen Keamanan jaringan
	A13.2 Perpindahan informasi
A14. Akuisisi, pengembangan dan persyaratan sistem	A14.1 Persyaratam Keamanan Informasi
	A14.2 Keamanan dalam proses pengembangan dan dukungan
	A14.3 Data Uji
A15 Hubungan Pemasok	A15.1 Keamanan Informasi dalam hubungan pemasok
	A15.2 Manajemen penyampaian layanan pemasok

Klausal	Kontrol Objektif
A16 Manajemen Insiden Keamanan Informasi	A16.1 Manajemen insiden keamanan informasi dan perbaikan
A17 Aspek keamanan informasi manajemen keberlangsungan bisnis	A17.1 Keberlangsungan Keamanan Informasi
	A17.2 Redundansi
A18 Kesesuaian	A18.1 Kesesuaian dengan persyaratan hukum dan kontraktual
	A18.2 Tinjauan Keamanan Informasi

2.2.4.2 SOA

Statement of Applicability (SoA) merupakan salah satu dokumen utama dalam membangun sebuah sistem manajemen keamanan informasi (SMKI) berdasarkan ISO/IEC 27001. Dokumen SoA secara garis besar memberikan fungsi penerapan SMKI melalui kontrol dari Annex A. salah satu fungsi dari dokumen SoA yaitu digunakan untuk mengidentifikasi kontrol yang dipilih untuk mengatasi risiko yang ditemukan dari proses penilaian risiko. Selain itu, Dokumen SoA juga digunakan untuk menjelaskan kenapa kontrol tersebut dipilih, menjelaskan apakah kontrol tersebut sudah dilaksanakan atau belum dan menjelaskan kontrol pada Annex A yang tidak digunakan atau dihilangkan [11].

Dokumen SoA digunakan karena laporan dari proses penilaian resiko yang bisa sangat banyak sampai menyentuh ribuan dan ribuan risiko itu belum tentu berdampak besar bagi organisasi sehingga dengan adanya SoA yang relatif singkat dan menggambarkan kondisi kontrol yang penting di seluruh SMKI

diperlukan. SoA secara sederhana digunakan untuk mengidentifikasi kebijakan, prosedur dan sistem yang telah diterapkan untuk mengatasi risiko yang telah teridentifikasi. SoA selalu mendapat pembaharuan secara teratur dalam penerapan SMKI. Hal ini sesuai dengan proses yang ada di ISO/IEC 27001 yaitu tentang perbaikan berkelanjutan dan disamping itu juga merupakan bukti adanya peningkatan kontrol pada SMKI yang telah diterapkan [12].

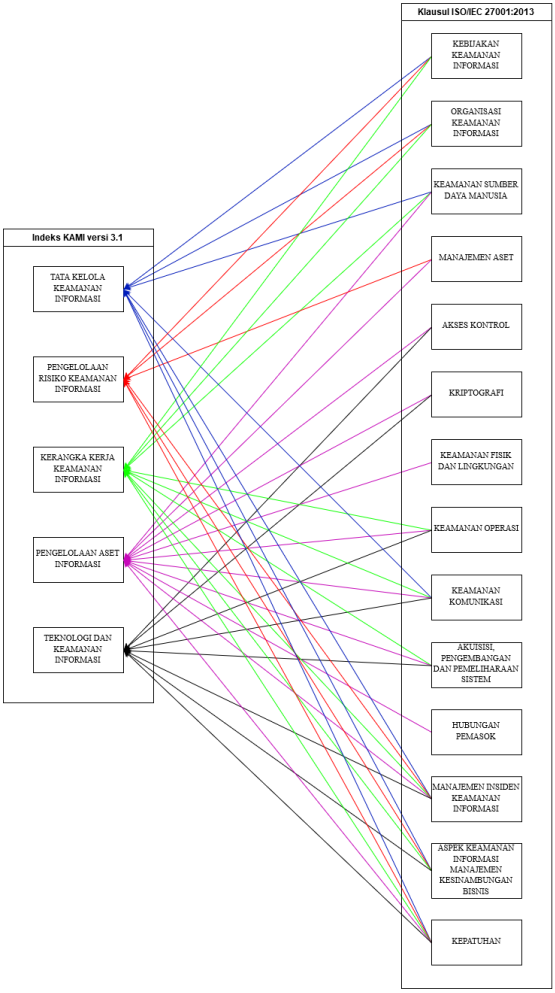
2.2.5 Indeks KAMI

Indeks KAMI merupakan suatu aplikasi untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2013 serta peta area tata kelola keamanan sistem informasi di suatu instansi pemerintah. Evaluasi dilakukan terhadap beberapa area target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2013 [10], yaitu :

Gambar 2. 1 Area Evaluasi Indeks KAMI

Lima area yang digunakan untuk mengevaluasi tingkat kematangan pada SMKI milik instansi yang dievaluasi merupakan rangkuman dari sasaran pengendalian yang ada

pada ISO/IEC 27001:2013. Sasaran pengendalian yang dimaksud merupakan 14 Klausul area yang terdapat di Annex A pada ISO/IEC 27001:2013[12]. Berikut merupakan hubungan antara Indeks KAMI dengan klausal yang dimiliki ISO/IEC 27001:2013 :



Gambar 2. 2 Pemetaan Hubungan Indeks KAMI 3.1 dengan ISO/IEC 27001:2013

Indeks KAMI sendiri merupakan alat evaluasi yang tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi[10]. Pada bulan maret 2019 Indeks KAMI mengeluarkan versi terbarunya yaitu Indeks KAMI versi 4.0 dengan penambahan satu area bernama suplemen. Area ini fokus membahas tentang hubungan dengan pihak ketiga, layanan cloud dan perlindungan data pribadi.

2.2.6 Tinjauan Perangkat *Checklist*

Tinjauan pada perangkat checklist kebutuhan penerapan sistem manajemen keamanan informasi merupakan hasil dari studi literatur dari checklist yang pernah dibuat oleh penelitian sebelumnya. Tinjauan ini memberikan gambaran konten dari output perangkat checklist checklist kebutuhan penerapan sistem manajemen keamanan informasi yang akan dibuat pada penelitian tugas akhir ini.

Berdasarkan checklist pada penelitian sebelumnya, peneliti membagi item yang akan dicek menjadi dua kategori kepentingan yaitu mandatory dan optional. Kategori kepentingan dipilih dengan melihat item mana yang mempunyai prioritas tinggi. Dalam penelitian tugas akhir ini prioritas akan ditentukan dengan melihat hasil penilaian risiko yang dimitigasi dengan kontrol pada ISO/IEC 27001:2013. Dari kontrol tersebut akan dilihat keterhubungan dengan kebutuhan yang sudah di identifikasi. Berikut ini merupakan tinjauan checklist dari penelitian sebelumnya.

Membuat *template* dari *checklist* pengendalian kualitas	Terdapat beberapa hal yang harus ada dalam pembuatan/penyusunan dokumen *checklist* pengendalian kualitas hasil *deliverables* pada program implementasi ERP, yaitu: 1) Petunjuk Perhitungan Nilai (level nilai kesiapan *key deliverables*) 2) Aktivitas Utama 3) *Key Deliverables* 4) Daftar Atribut Pemeriksaan 5) Kepentingan (mandatory/optional) 6) Keterangan Level Ketepatan 7) Level Ketepatan 8) Kesimpulan

Gambar 2. 3 Contoh checklist penelitian sebelumnya [7]

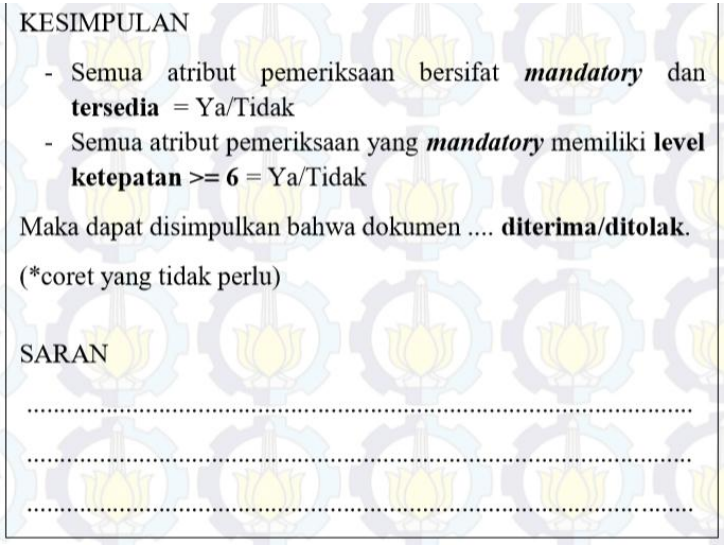
Checklist Ketepatan :		**.....**
Nama Proyek	:	**.....**
Nama Aktivitas	:	**.....**
Key Deliverables	:	**.....**

Berikut ini merupakan checklist dokumen .... . Untuk setiap atribut pemeriksaan, berilah tanda ✓ pada salah satu Level Ketepatan yang paling sesuai:

⓪ 0%-30%, ③ 31%-60%, ⑥ 61%-90%, ⑨ 91%-100%

No	Atribut Pemeriksaan	Kepentingan	Level Ketepatan
1	.....	.....	⓪ ③ ⑥ ⑨

Gambar 2. 4 Contoh checklist penelitian sebelumnya [7]



KESIMPULAN

- Semua atribut pemeriksaan bersifat ***mandatory*** dan **tersedia** = Ya/Tidak
- Semua atribut pemeriksaan yang ***mandatory*** memiliki **level ketepatan >= 6** = Ya/Tidak

Maka dapat disimpulkan bahwa dokumen .... **diterima/ditolak**.

(*coret yang tidak perlu)

SARAN

.....

.....

.....

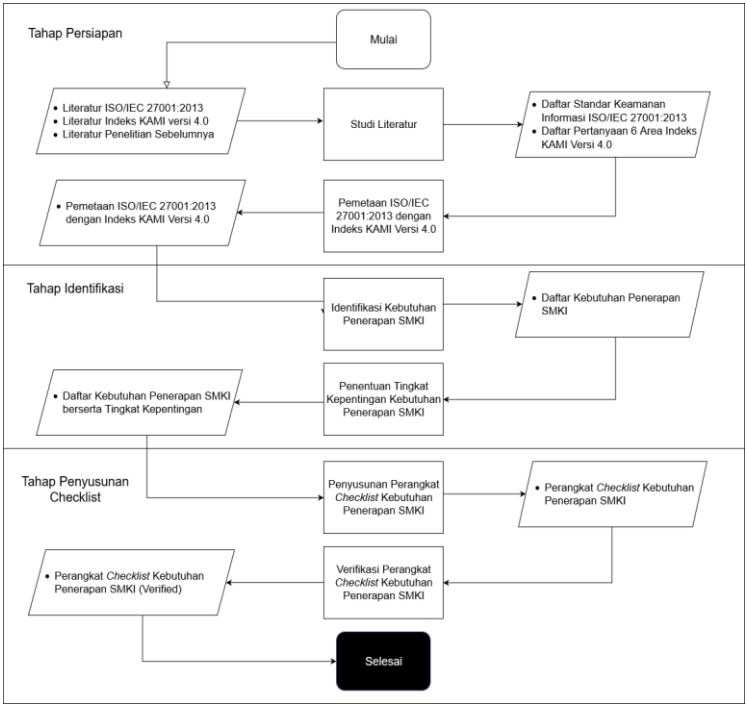
Gambar 2. 5 Contoh checklist penelitian sebelumnya [7]

BAB III
METODOLOGI

Bab ini membahas mengenai gambaran langkah-langkah pekerjaan yang dilakukan selama penyusunan tugas akhir mulai awal sampai akhir penelitian.

3.1 Tahapan Pelaksanaan Tugas Akhir

Pada tahap pengerjaan penelitian tugas akhir ini akan ada 3 tahapan. Tahapan pengerjaan dimulai dari studi literatur sampai tahap penyusunan checklist. Pengerjaan tugas akhir ini akan menghasilkan sebuah perangkat *checklist* penerapan sistem manajemen keamanan informasi.



Gambar 3. 1 Metodologi Penelitian Tugas Akhir

3.2 Uraian Metodologi

3.2.1 Tahap Persiapan

Tahapan ini merupakan tahapan awal dimana peneliti melakukan analisis literatur untuk menunjang peneliti dalam pengerjaan tugas akhir ini.

3.2.1.1 Studi Literatur

Studi literatur pada tahap ini akan membahas standar keamanan informasi yang ada pada ISO/IEC 27001:2013. Selain itu, penerapan sistem manajemen keamanan informasi yang berbasis Indeks KAMI versi 4.0 dan hubungan antara ISO/IEC 27001:2013 dengan Indeks KAMI versi 4.0 juga dibahas dalam studi literatur ini. Pada tahap ini juga dikumpulkan literatur-literatur yang berhubungan dengan penelitian tugas akhir ini seperti buku, jurnal, sumber dari internet dan penelitian-penelitian sebelumnya.

Tabel 3. 1 Studi Literatur

Input	Proses	Output
• Literatur ISO/IEC 27001:2013 • Literatur Indeks KAMI versi 4.0 • Literatur penelitian sebelumnya	Studi literatur	• Daftar standar keamanan informasi ISO/IEC 27001:2013 • Daftar Pertanyaan Indeks KAMI Versi 4.0

3.2.1.2 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0

Pemetaan Indeks KAMI versi 4.0 ke ISO/IEC 27001:2013 pada tahap ini diawali dengan memetakan pertanyaan hasil studi literatur indeks KAMI 4.0 ke klausal ISO/IEC 27001:2013 yang merupakan hasil studi literatur ISO/IEC 27001:2013. Pemetaan ini dilakukan karena terdapat hubungan antara keduanya

berdasarkan hasil literatur hubungan ISO/IEC 27001:2013 dengan Indeks KAMI. Hubungan yang dimaksud yaitu pembahasan tentang keamanan informasi yang sama antara pertanyaan pada indeks KAMI dan klausul ISO/IEC 27001:2013. Output pemetaan ini adalah terpetakannya klausal yang ada pada ISO/IEC 27001:2013 ke dalam pertanyaan-pertanyaan enam area yang ada pada Indeks KAMI 4.0. Hasil pemetaan ini akan diverifikasi pada aktivitas selanjutnya untuk mempermudah pengambilan kebutuhan pada tahap selanjutnya.

Tabel 3. 2 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI versi 4.0

Input	Proses	Output
• Daftar standar keamanan informasi ISO/IEC 27001:2013 • Daftar pertanyaan 6 area Indeks KAMI versi 4.0	Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI versi 4.0	Hasil pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0

3.2.2 Tahap Identifikasi

Tahapan ini merupakan tahapan dimana peneliti melakukan indentifikasi menggunakan literatur-literatur yang telah didapatkan pada tahap sebelumnya untuk menentukan kebutuhan penerapan sistem manajemen keamanan informasi.

3.2.2.1 Identifikasi Kebutuhan Penerapan SMKI

Pada tahapan ini dilakukan pengambilan kebutuhan untuk penerapan sistem manajemen keamanan informasi. Pengambilan kebutuhan dilakukan dengan cara menterjemahkan pertanyaan pada enam area Indeks KAMI versi 4.0 yang telah terpetakan dengan klausul ISO/IEC

27001:2013. Klausul ISO/IEC 27001:2013 yang tidak terpetakan dengan pertanyaan pada enam area Indeks KAMI 4.0 juga akan dilakukan pengambilan kebutuhan karena ISO/IEC 27001:2013 merupakan best practice dalam penerapan SMKI. Pengambilan kebutuhan dari klausul yang tidak terpetakan dilakukan dengan cara mengambil kontrol dari klausul yang tidak terpetakan terpetakan tersebut menjadi kebutuhan. Selain dari hasil pemetaan, kebutuhan penerapan sistem manajemen keamanan informasi juga akan diambil dari hasil literatur *Mandatory Document* yang disyaratkan ISO/IEC 27001:2013. Hasil dari aktivitas ini adalah sebuah daftar kebutuhan yang pada proses selanjutnya akan digunakan untuk menyusun checklist kebutuhan penerapan SMKI.

Tabel 3. 3 Identifikasi kebutuhan penerapan SMKI

Input	Proses	Output
• Hasil pemetaan hubungan klausal ISO/IEC 27001:2013 dengan pertanyaan Indeks KAMI versi 4.0 • Literatur *Mandatory Document* untuk ISO/IEC 27001:2013 • Literatur ISO/IEC 27001:2013	Identifikasi kebutuhan penerapan SMKI	Daftar kebutuhan penerapan SMKI

3.2.2.2 Penentuan Tingkat Kepentingan Kebutuhan

Pada tahap Penentuan tingkat kepentingan kebutuhan ini, pertama-tama akan dilakukan identifikasi dari klausul yang terpetakan dan yang tidak terpetakan pada hasil pemetaan

indeks KAMI 4.0 dengan ISO/IEC 27001. Dari klausul tersebut akan di identifikasi mana saja klausul yang mempunyai *Mandatory Document* berdasarkan hasil literatur *Mandatory Document* yang telah dilakukan pada tahapan sebelumnya. Hasil identifikasi tersebut akan digunakan untuk menentukan status kepentingan kebutuhan yang telah di daftar termasuk *Mandatory* atau *Optional*. Status kepentingan tersebut ditentukan berdasarkan hasil studi literatur *Mandatory Document*. Output dari tahapan ini berupa daftar kebutuhan beserta status kepentingan dari masing-masing kebutuhan tersebut.

Tabel 3. 4 Penentuan tingkat kepentingan kebutuhan penerapan SMKI

Input	Proses	Output
Daftar kebutuhan penerapan SMKI	Penentuan tingkat kepentingan kebutuhan penerapan SMKI	Daftar kebutuhan penerapan SMKI beserta tingkat kepentingan masing-masing kebutuhan

3.2.3 Tahap Penyusunan Checklist

Tahapan ini merupakan tahapan dimana peneliti menyusun checklist kebutuhan penerapan sistem manajemen keamanan informasi dari daftar kebutuhan yang merupakan hasil identifikasi pemetaan Indeks KAMI 4.0 dengan ISO/IEC 27001:2013 dan literatur *Mandatory Document* ISO/IEC 27001:2013.

3.2.3.1 Penyusunan Perangkat Checklist Kebutuhan Penerapan SMKI

Pada tahapan ini dilakukan penyusunan perangkat checklist kebutuhan untuk penerapan sistem manajemen keamanan informasi sebagai solusi dalam menerapkan sistem manajemen keamanan informasi. Penyusunan checklist mengacu pada daftar kebutuhan dari hasil penggalian kebutuhan berdasarkan

hasil Pemetaan Indeks KAMI 4.0 dan ISO/IEC 27001:2013. Output dari aktivitas ini adalah perangkat checklist kebutuhan penerapan SMKI dimana pada aktivitas selanjutnya perangkat checklist akan di verifikasi ketersesuaiannya dengan standar yang digunakan.

Tabel 3. 5 Penyusunan perangkat checklist kebutuhan penerapan SMKI

Input	Proses	Output
• Daftar kebutuhan penerapan SMKI • Hasil literatur pembuatan checklist	Penyusunan perangkat checklist kebutuhan penerapan SMKI	Perangkat checklist kebutuhan penerapan SMKI

3.2.3.2 Verifikasi Perangkat Checklist Kebutuhan Penerapan SMKI

Pada tahapan ini, setelah perangkat checklist disusun maka akan dilakukan verifikasi perangkat checklist kebutuhan penerapan SMKI. Verifikasi dilakukan dengan cara melakukan kesesuaian antara kebutuhan dengan hasil pemetaan Indeks KAMI dan ISO/IEC 27001:2013. Dari aktivitas tersebut kebutuhan akan sesuai, akurat dan tepat guna untuk membantu penerapan SMKI pada sebuah organisasi. Output dari aktivitas ini adalah perangkat checklist kebutuhan penerapan SMKI yang telah terverifikasi setelah adanya perbaikan dan perangkat checklist kebutuhan penerapan SMKI siap digunakan oleh organisasi yang akan di uji sebagai studi kasus.

Tabel 3. 6 Verifikasi kesesuaian kebutuhan dengan hasil pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013

Input	Proses	Output
Perangkat checklist	Verifikasi kesesuaian kebutuhan dengan	Perangkat checklist kebutuhan

kebutuhan penerapan SMKI	hasil pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013	penerapan SMKI (Verified)

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Tujuan tugas akhir ini adalah menghasilkan sebuah perangkat *checklist* kebutuhan penerapan sistem manajemen keamanan informasi. Untuk mencapai tujuan tersebut, maka pada bab perancangan ini akan dijelaskan tentang perancangan dari penggalian data, identifikasi data dan output untuk menghasilkan perangkat *checklist* kebutuhan yang *deliverables.*

4.1 Penggalian Data

Pada perancangan penggalian data akan dijelaskan tentang data yang dibutuhkan dan metode pengumpulan data. Pengumpulan data ini untuk mempermudah identifikasi kebutuhan bagi organisasi yang menerapkan sistem manajemen keamanan informasi pada instansi atau organisasi mereka.

4.1.1 Data yang Diperlukan

Pada bagian ini akan membahas tentang data apa saja yang diperlukan dalam penelitian tugas akhir ini. Peneliti membutuhkan data dan informasi mengenai studi kasus untuk mendukung keberhasilan pengerjaan tugas akhir ini. Berikut ini merupakan tujuan penggalian data beserta metode penggalian data yang digunakan:

Tabel 4. 1 Data yang dibutuhkan

Tujuan Penggalian data	Metode Penggalian Data
Mengetahui daftar pertanyaan Indeks KAMI versi 4.0	Studi Dokumen
Mengetahui daftar kontrol keamanan informasi yang ada pada ISO/IEC 27001:2013	Studi Dokumen
Mengetahui hubungan ISO/IEC 27001:2013 dengan Indeks KAMI 4.0	Studi Dokumen

4.1.2 Metode Penggalian Data

Pada bagian metode penggalian data ini akan dijelaskan metode yang digunakan untuk mendapatkan data yang dibutuhkan. Penggalian data yang dilakukan menggunakan metode studi dokumen dari penelitian sebelumnya, dokumen ISO/IEC 27001:2013 dan dokumen Indeks KAMI versi 4.0. Data dokumen yang digunakan yaitu tentang hubungan Indeks KAMI dengan ISO/IEC 27001:2013 pada penilaian Indeks KAMI versi 3.1 berdasarkan ISO/IEC 27001:2013 yang telah dilakukan penelitian sebelumnya. Adapun daftar klausul pada ISO/IEC 27001:2013 dan daftar pertanyaan pada 6 area Indeks KAMI versi 4.0.

Studi dokumen merupakan metode penggalian data melalui studi literatur untuk mendapatkan informasi terkait studi kasus. Dari studi dokumen yang dilakukan peneliti akan mendapatkan informasi terkait hubungan indeks KAMI dengan ISO/IEC 27001:2013 yang didapatkan pada saat penelitian sebelumnya dan peneliti juga mendapatkan cara memetakan Indeks KAMI dengan ISO/IEC 27001:2013 dari studi literatur pada penelitian sebelumnya. Informasi yang didapatkan adalah hasil pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013.

4.2 Identifikasi Data

pada perancangan ini akan dilakukan identifikasi data dari data yang telah dikumpulkan. Indentifikasi data ini bertujuan untuk mendapatkan data-data baru untuk menunjang penelitian tugas akhir ini. Data-data tersebut antara lain hasil pemetaan Indeks KAMI 4.0 dengan ISO/IEC 27001:2013, daftar kebutuhan dan status kepentingan kebutuhan. Identifikasi data dilakukan berdasarkan metodologi yang telah dibuat oleh peneliti.

4.2.1 Identifikasi Kebutuhan

Pada proses ini dilakukan identifikasi kebutuhan berdasarkan penerjemahan pertanyaan di Indeks KAMI dan literatur *Mandatory Document* yang disyaratkan penerapan ISO/IEC 27001:2013[13]. Hal ini dilakukan untuk mengetahui

kebutuhan apa saja yang terkait dengan penerapan SMKI pada sebuah instansi atau organisasi.

Tabel 4. 2 Daftar kebutuhan

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
1	A6.1.5 Information security in project management	Penerjemahan pertanyaan Indeks KAMI 4.0	Analisa aspek keamanan informasi dalam manajemen proyek yang terkait ruang lingkup

4.2.2 Idektifikasi Tingkat Kepentingan

Pada proses ini dilakukan identifikasi tingkat kepentingan untuk mengetahui kebutuhan mana saja yang termasuk *mandatory* dan kebutuhan mana saja yang termasuk *Optional*.

Tabel 4. 3 Tingkat kepentingan

Klausul ISO/IEC 27001:2013		Kebutuhan	Tingkat Kepentingan
A.8.1.1	*Inventory of assets*	Daftar inventarisasi aset	*Mandatory*

4.3 Solusi

Pada perancangan solusi ini akan dilakukan penyusunan perangkat *checklist* kebutuhan penerapan SMKI. Perangkat *checklist* yang disusun merupakan hasil dari penelitian yang

dilakukan peneliti. Perangkat *checklist* disusun berdasarkan metodologi pada bab sebelumnya dengan menggunakan data yang telah diperoleh dari tahapan sebelumnya.

4.3.1 Penyusunan *Checklist* Kebutuhan Penerapan SMKI

Setelah melakukan pemetaan dan mengidentifikasi kebutuhan serta tingkat kepentingannya maka langkah selanjutnya adalah menyusun perangkat checklist dari kebutuhan penerapan SMKI. Perangkat *checklist* yang dibuat mempunyai beberapa item di dalamnya. Item yang ada di dalamnya antara lain area, kebutuhan, kepentingan dan ketersediaan. Berikut merupakan rancangan dari checklist kebutuhan penerapan SMKI:

Tabel 4. 4 Checklist kebutuhan penerapan SMKI

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
1	Daftar inventarisasi aset	*Mandatory*	○ Y	○N

4.3.2 Verifikasi *Checklist* Kebutuhan Penerapan SMKI

Langkah selanjutnya adalah verifikasi dimana verifikasi yang dilakukan untuk *checklist* kebutuhan penerapan SMKI adalah penyesuaian isi dokumen *checklist* dengan dokumen hasil pemetaan Indeks KAMI dan ISO/IEC 27001:2013. Proses verifikasi ini disampaikan melalui lembar *checklist* yang di dalamnya berisi hasil pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013 dan isi dokumen *checklist* untuk dilihat ketersesuaiannya.

BAB V
IMPLEMENTASI

Pada bab ini akan membahas tentang proses implementasi dari rancangan penggalian data yang telah dibuat pada bab sebelumnya dimana akan dijelaskan hasil dari rancangan penggalian data yang telah didapatkan melalui studi dokumen.

1.1 Daftar Pertanyaan Indeks KAMI Versi 4.0

Berdasarkan bab perancangan dilakukan penggalian data dengan cara studi dokumen pada penelitian sebelumnya tentang penilaian Indeks KAMI pada DPTSI ITS didapatkan cara memetakan Indeks KAMI dengan ISO/IEC 27001:2013. Pemetaan dilakukan dengan cara menghubungkan pertanyaan yang ada pada Indeks KAMI versi 4.0 dengan klausul yang ada pada ISO/IEC 27001:2013. Berdasarkan cara itu dibutuhkan daftar pertanyaan Indeks KAMI dari Indeks KAMI versi terbaru yaitu versi 4.0. pertanyaan-pertanyaan tersebut akan dipetakan ke dalam control yang ada pada klausul ISO/IEC 27001:2013. Pemetaan ini bisa dilakukan karena pertanyaan pada Indeks KAMI versi 4.0 dan kontrol pada ISO/IEC 27001:2013 sama-sama membahas tentang keamanan informasi. Daftar pertanyaan Indeks KAMI versi 4.0 yang telah didapatkan dari penggalian data dengan cara studi dokumen dapat dilihat pada **LAMPIRAN A**. Dari **LAMPIRAN A** tersebut diketahui bahwa terdapatkan 184 buah pertanyaan dari 6 area pada Indeks KAMI versi 4.0.

1.2 Daftar Kontrol Keamanan Informasi pada ISO/IEC 27001:2013

Berdasarkan perancangan penggalian data pada bab sebelumnya dibutuhkan daftar kontrol keamanan informasi yang didapatkan dari studi dokumen pada ISO/IEC 27001:2013. Daftar kontrol keamanan informasi ini akan digunakan untuk melihat keterhubungan antara Indeks KAMI dengan ISO/IEC 27001:2013[12]. Daftar kontrol keamanan informasi yang didapatkan dapat dilihat pada **LAMPIRAN B**. Dari daftar kontrol keamanan informasi yang ada pada

LAMPIRAN B terdapat 114 kontrol keamanan informasi dari 35 kontrol obyektif yang ada pada 14 klausal ISO/IEC 27001:2013.

1.3 Hasil Pemetaan Indeks KAMI 4.0 dengan ISO/IEC 27001:2013

Pada bab sebelumnya yaitu perancangan telah dilakukan perancangan penggalian data tentang pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013. Pemetaan ini dilakukan karena pertanyaan Indeks KAMI 4.0 memiliki bahasan yang sama dengan klausul yang ada di ISO/IEC 27001:2013 yaitu tentang keamanan informasi. Kesamaan ini membuat adanya Indeks KAMI dapat dipetakan dengan ISO/IEC 27001:2013. Hasil dari penggalian data ini adalah pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013 dimana semua pertanyaan yang ada di Indeks KAMI memiliki kemungkinan dapat dipetakan ke dalam klausul yang ada di ISO/IEC 27001:2013. Hasil pemetaan dari Indeks KAMI 4.0 dengan ISO/IEC 27001:2013 dapat dilihat pada **LAMPIRAN C.** Dari pemetaan Indeks KAMI 4.0 dengan ISO/IEC 27001:2013 yang ada pada **LAMPIRAN C** diketahui bahwa terdapat 176 pertanyaan dari 184 pertanyaan pada enam area indeks KAMI 4.0 yang dapat dipetakan ke dalam klausul yang ada pada ISO/IEC 27001:2013. Sedangkan klausul pada ISO/IEC 27001:2013 terdapat 87 kontrol keamanan informasi dari 114 kontrol yang terpetakan pada pertanyaan Indeks KAMI versi 4.0. Dengan hal tersebut maka identifikasi kebutuhan penerapan sistem manajemen keamanan informasi dapat diambil melalui penerjemahan pertanyaan yang ada pada Indeks KAMI versi 4.0.

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan tentang hasil dan pembahasan yang didapatkan peneliti dalam penelitian tugas akhir ini. Hasil dan pembahasan tersebut akan menjawab rumusan masalah yang telah dijelaskan pada bab sebelumnya.

6.1 Pengidentifikasian Kebutuhan berdasarkan Hasil Pemetaan Indeks KAMI 4.0 dengan ISO/IEC 27001:2013

Pada tahapan ini akan dilakukan identifikasi kebutuhan penerapan SMKI. Indetifikasi dilakukan dengan cara menerjemahkan pertanyaan yang ada pada Indeks KAMI 4.0 menjadi kebutuhan dari penerapan sistem manajemen keamanan informasi. Pertanyaan yang diterjemahkan menjadi kebutuhan adalah pertanyaan yang terpetakan dengan klausul ISO/IEC 27001:2013. Selain dari penerjemahan pertanyaan, kebutuhan juga diambil dari referensi studi literatur yang dilakukan peneliti tentang *mandatory document* persyaratan ISO/IEC 27001:2013[13]. Untuk klausul yang tidak terpetakan juga akan diambil kebutuhannya karena merupakan bagian dari ISO/IEC 27001:2013 yang merupakan *best practice* dari penerapan SMKI. Berikut merupakan hasil identifikasi yang dilakukan peneliti pada penelitian tugas akhir ini dimana dari identifikasi yang dilakukan didapatkan kebutuhan sejumlah 160 buah:

Tabel 6. 1 Kebutuhan Penerapan SMKI

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
1	A6.1.5 Information security in project management	Penerjemahan pertanyaan Indeks KAMI 4.0	Analisa aspek keamanan informasi dalam manajemen proyek yang terkait ruang lingkup

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
2	A.16.1.4 Assessment of and decision on information security events	Penerjemahan pertanyaan Indeks KAMI 4.0	Analisa dampak insiden terkait pengungkapan data pribadi yang disimpan, diolah dan di pertukarkan secara ilegal
3	A.15.1.2 Addressing security within supplier agreements	Penerjemahan pertanyaan Indeks KAMI 4.0	Analisa kesesuaian pengendalian risiko pihak ketiga dengan perjanjian yang telah disepakati bersama
4	A.15.1.3 Information and communication technology supply chain	Penerjemahan pertanyaan Indeks KAMI 4.0	Analisa risiko terkait penggunaan layanan berbasis cloud dan penyesuaian kebijakan keamanan informasi terkait layanan cloud sesuai hasil analisa
5	A.17.1.1 Planning information security continuity	Literatur *mandatory document*	Analisis dampak bisnis (Business impact analysis)
6	A.8.1.1 Inventory of assets	Literatur mandatory document	Daftar inventarisasi aset (Inventory of assets)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
7	A.12.4.1 Event logging A.12.4.3 Administrator and operator logs	Literatur mandatory document	Daftar log aktivitas pengguna, pengecualian, dan peristiwa keamanan (Logs of user activities, exceptions, and security events)
8	A.12.4.1 Event logging	Penerjemahan pertanyaan Indeks KAMI 4.0	Daftar log perubahan sistem informasi yang terekam secara otomatis
9	A.12.2.1 Controls against malware	Penerjemahan pertanyaan Indeks KAMI 4.0	Daftar rekaman dan hasil analisa pemuktahiran antivirus/antimalware yang telah dikumpulkan secara rutin dan sistematis
10	A.12.4.1 Event logging	Penerjemahan pertanyaan Indeks KAMI 4.0	Daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan sesuai dengan klasifikasi keamanan informasi
11	A.16.1.1 Responsibilities and procedures	Penerjemahan pertanyaan Indeks KAMI 4.0	Definisi kebijakan dan prosedur penanganan insiden keamanan informasi terkait pelanggaran hukum

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
12	A.7.2.3 Disciplinary process	Penerjemahan pertanyaan Indeks KAMI 4.0	Definisi konsekwensi pelanggaran kebijakan keamanan informasi
13	A.6.1.5 Information security in project management	Penerjemahan pertanyaan Indeks KAMI 4.0	Definisi metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi (mencakup mekanisme, waktu pengukuran, pelaksanaan, pemantauan dan eskalasi pelaporan keamanan informasi)
14	A.6.1.1 Information security roles and responsibilities A.7.1.2 Terms and conditions of employment A.13.2.4 Confidentiality or nondisclosure agreements	Literatur mandatory document	Definisi peran dan tanggung jawab keamanan (Definition of security roles and responsibilities)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
15	A.7.3.1 Termination or change of employment responsibilities	Kontrol klausul ISO/IEC 27001:2013	Definisi tugas dan tanggung jawab keamanan informasi yang tetap berlaku setelah terjadi perubahan atau pemberhentian pekerjaan
16	A.5.1.2 Review of the policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala
17	A.12.3.1 Information backup	Literatur mandatory document	Kebijakan backup (Backup policy)
18	A.11.2.9 Clear desk and clear screen policy	Literatur mandatory document	Kebijakan clear desk dan clear screen (Clear desk and clear screen policy)
19	A.12.6.1 Management of technical vulnerabilities	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan dan prosedur operasional pengelolaan implementasi security patch (berisi tanggung jawab monitoring pembaharuan, pemasangan dan pelaporan perilisan seurity patch baru)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
20	A.18.1.3 Protection of records	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan hak pemilik data pribadi dalam mengakses data tersebut
21	A.12.6.2 Restrictions on software installation	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan instalasi piranti lunak pada aset TI milik instansi/perusahaan
22	A.18.1.3 Protection of records	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan keakuratan dan pemuktahiran data pribadi
23	A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain	Literatur mandatory document	Kebijakan keamanan pemasok (Supplier security policy)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
24	A.8.2.1 Classification of information A.8.2.2 Labelling of information A.8.2.3 Handling of assets A.16.1.4 Assessment of and decision on information security events	Literatur mandatory document	Kebijakan klasifikasi informasi (Information classification policy)
25	A.9.1.1 Access control policy	Literatur mandatory document	Kebijakan kontrol akses (Access control policy)
26	A.12.1.2 Change management A.14.2.4 Restrictions on changes to software packages	Literatur mandatory document	Kebijakan manajemen perubahan (Change management policy)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
27	A.6.2.1 Mobile device policy	Literatur mandatory document	Kebijakan membawa perangkat Anda sendiri (BYOD) (Bring your own device (BYOD) policy)
28	A.8.3.2 Disposal of media A.11.2.7 Secure disposal or reuse of equipment	Literatur mandatory document	Kebijakan pembuangan dan penghancuran (Disposal and destruction policy)
29	A.18.1.5 Regulation of cryptographic controls	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan penerapan enkripsi sebagai pelindung aset informasi penting
30	A.11.1.1 Physical security perimeter	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan pengamanan fisik sesuai zona dan klasifikasi aset di dalamnya
31	A.11.1.3 Securing offices, rooms and facilities A.11.1.6 Delivery and loading areas	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan pengamanan lokasi kerja penting

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
32	A.11.2.6 Security of equipment and assets off-premises A.11.2.8 Unattended user equipment	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan pengamanan perangkat komputasi milik instansi/perusahaan yang digunakan diluar lokasi kerja
33	A.14.2.1 Secure development policy	Kontrol klausul ISO/IEC 27001:2013	Kebijakan pengembangan perangkat lunak dan sistem harus dibuat dan diterapkan pada proses pengembangan dalam organisasi
34	A.8.1.3 Acceptable use of assets A.8.1.4 Return of assets	Literatur mandatory document	Kebijakan penggunaan aset yang dapat diterima (Acceptable use of assets)
35	A.14.1.2 Securing application services on public networks	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan penggunaan komputer, email, internet dan intranet
36	A.16.1.7 Collection of evidence	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan pengungkapan data pribadi atas permintaan resmi aparat penegak hukum

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
37	A.6.2.1 Mobile device policy A.6.2.2 Teleworking	Literatur mandatory document	kebijakan Perangkat mobile dan Teleworking (Mobile device and teleworking policy)
38	A.18.1.3 Protection of records	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku
39	A.12.2.1 Controls against malware	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan perlindungan desktop dan server dari penyerangan virus (malware)
40	A.9.2.1 User registration and de-registration A.9.2.2 User access provisioning A.9.2.3 Management of privileged access rights A.9.2.4	Literatur mandatory document	Kebijakan sandi (Password policy)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
	Management of secret authentication information of users A.9.3.1 Use of secret authentication information A.9.4.3 Password management system		
41	A.18.1.4 Privacy and protection of personally identifiable information	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan terkait perlindungan data pribadi sesuai peraturan perundangan yang berlaku
42	A.8.3.1 Management of removable media A.11.2.5 Removal of assets	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
43	A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.3 Electronic messaging	Literatur mandatory document	Kebijakan transfer informasi (Information transfer policy)
44	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan, prosedur dan rencana terkait keberlangsungan layanan pihak ketiga dalam keadaan darurat
45	A.15.1.3 Information and communication technology supply chain	Penerjemahan pertanyaan Indeks KAMI 4.0	Kebijakan, strategi dan prosedur terkait pengganti layanan cloud ketika terjadi gangguan sementara pada layanan cloud
46	A.7.2.1 Management responsibilities	Kontrol klausul ISO/IEC 27001:2013	Manajemen harus meminta semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang ditetapkan organisasi

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
47	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Perencanaan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga
48	A.6.1.1 Information security roles and responsibilities A.6.1.2 Segregation of duties	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan adanya fungsi atau bagian dari instansi/perusahaan yang spesifik memiliki tugas dan tanggung jawab mengelola keamanan informasi dan menjaga kepatuhannya
49	A.16.1.1 Responsibilities and procedures	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan adanya kerangka kerja pengelolaan risiko keamanan informasi yang secara resmi digunakan
50	A.6.1.1 Information security roles and responsibilities	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan alokasi pegawai perusahaan sesuai tanggung jawab dan wewenang yang dimiliki dalam penerapan kebijakan dan prosedur perlindungan data pribadi
51	A.12.1.3 Capacity management	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan alokasi sumber daya yang sesuai untuk pelaksana pengelolaan keamanan informasi

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
52	A.5.1.2 Review of the policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan analisa aspek finansial dan perubahan infrastruktur sebagai salah satu pertimbangan revisi kebijakan dan prosedur yang berlaku
53	A.13.1.2 Security of network services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan analisa kepatuhan penerapan konfigurasi standar secara rutin
54	A.18.2.1 Independent review of information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan analisa/evaluasi hasil audit internal untuk mengidentifikasi langkah pembenahan, pencegahan dan inisiatif peningkatan kinerja keamanan informasi
55	A.8.1.2 Ownership of assets	Kontrol klausul ISO/IEC 27001:2013	Persyaratan aset penting yang dipertahankan dalam inventaris harus dimiliki
56	A.9.1.2 Access to networks and network services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
57	A.9.4.2 Secure log-on procedures	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan bentuk pengamanan khusus yang berlapis untuk akses yang digunakan mengelola sistem (administrasi sistem)
58	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan bukti-bukti penerapan yang memadai dalam penanganan insiden keamanan informasi oleh pihak ketiga
59	A.12.7.1 Information systems audit controls	Kontrol klausul ISO/IEC 27001:2013	Persyaratan dan kegiatan audit yang melibatkan verifikasi sistem operasional harus direncanakan dan disetujui dengan cermat untuk meminimalkan gangguan pada proses bisnis
60	A.18.2.1 Independent review of information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan evaluasi audit internal mencakup tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi
61	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan evaluasi dan pemantauan secara berkala terkait SLA dan aspek keamanan informasi

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
62	A.14.2.7 Outsourced development	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan evaluasi layanan cloud terkait kelaikan keamanan dan ketersediaannya dalam pemenuhan setifikasi layanan berbasis ISO 27001
63	A.14.2.9 System acceptance testing	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan evaluasi layanan cloud terkait reputasi penyelenggara
64	A.14.2.3 Technical review of applications after operating platform changes	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan evaluasi risiko dan mitigasinya terkait rencana pembelian/implementasi sistem baru
65	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan hak audit TI secara berkala kepada pihak ketiga
66	A.18.1.1 Identification of applicable legislation and contractual requirements	Literatur mandatory document	Persyaratan hukum, regulasi, dan kontraktual (Legal, regulatory, and contractual requirements)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
67	A.15.2.2 Managing changes to supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan identifikasi risiko keamanan informasi terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan pada layanan pihak ketiga
68	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan identifikasi risiko keamanan informasi terkait kerjasama dengan pihak ketiga
69	A.7.1.1 Screening A.18.1.4 Privacy and protection of personally identifiable information	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan indetifikasi data pribadi dan kepastian perlindungan data sesuai undang-undang berlaku
70	A.6.1.5 Information security in project management	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan integrasi keperluan/persyaratan keamanan informasi ke dalam proses kerja
71	A.18.2.1 Independent review of information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan keterlibatan pihak independen dalam analisa kehandalan keamanan informasi secara rutin

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
72	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan ketersediaan laporan SLA dan aspek keamanan informasi sesuai kontrak yang disetujui bersama
73	A.16.1.4 Assessment of and decision on information security events	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan kondisi dan permasalahan keamanan informasi sebagai konsiderans atau bagian dari proses pengambilan keputusan
74	A.5.1.1 Policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan mitigasi risiko keamanan informasi dan sasaran/obyektif tertentu dari pimpinan instansi sebagai refleksi kebijakan dan prosedur keamanan informasi yang ada
75	A.18.2.1 Independent review of information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pelaporan hasil audit internal kepada pimpinan organisasi
76	A.18.2.2 Compliance with security policies and standards	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pelaporan program keamanan informasi oleh penanggung jawab pengelolaan keamanan informasi secara rutin mencakup kondisi,

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
			kinerja/efektifitas dan kepatuhan
77	A.9.4.1 Information access restriction	Kontrol klausul ISO/IEC 27001:2013	Persyaratan pembatasan akses ke informasi dan fungsi sistem aplikasi sesuai dengan kebijakan kontrol akses
78	A.9.4.5 Access control to program source code	Kontrol klausul ISO/IEC 27001:2013	Persyaratan pembatasan akses ke kode sumber program
79	A.9.2.3 Management of privileged access rights	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pembatasan waktu akses dan otomasi proses timeouts, lockout setelah gagal login dan penarikan akses
80	A.18.1.4 Privacy and protection of personally identifiable information	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pemberian ijin penggunaan data pribadi secara tertulis oleh pemilik data pribadi
81	A.13.1.2 Security of network services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pemindaian jaringan, sistem dan aplikasi secara rutin untuk indentifikasi celah

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
			kelemahan atau perubahan/keutuhan konfigurasi yang mungkin terjadi
82	A.12.1.4 Separation of development, testing and operational environments	Kontrol klausul ISO/IEC 27001:2013	Persyaratan pemisahan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko akses atau perubahan yang tidak sah terhadap lingkungan operasional
83	A.13.1.1 Network controls	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pemuktahiran konfigurasi standar keamanan sistem pada seluruh aset jaringan, sistem dan aplikasi sesuai perkembangan dan kebutuhan
84	A.12.5.1 Installation of software on operational systems	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pemuktahiran versi terkini sistem operasi perangkat desktop dan server
85	A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
	security events		
86	A.5.1.1 Policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pencantuman tanggung jawab dalam penyusunan dan penulisan kebijakan, prosedur dan dokumen yang terkait kemanan informasi
87	A.10.1.2 Key management	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan penerapan pengelolaan kunci enkripsi dan siklus penggunaannya
88	A.6.1.5 Information security in project management	Penerjemahan pertanyaan Indeks KAMI 4.0	persyaratan penerapan target dan sasaran, evaluasi pencapaian secara berkala, penerapan langkah perbaikan dan pelaporan pencapaian sasaran dalam pengelolaan keamanan informasi
89	A.15.1.3 Information and communication technology	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan penetapan data yang dapat disimpan/diolah/dipertukarkan melalui layanan cloud

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
	supply chain		
90	A.6.1.1 Information security roles and responsibilities	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan penetapan peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga pada unit organisasi tertentu
91	A.11.1.2 Physical entry controls A.11.1.6 Delivery and loading areas	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pengamanan fasilitas fisik yang sesuai kepentingan/klasifikasi aset informasi, diterapkan secara berlapis dan dapat mencegah upaya akses oleh pihak tidak bertanggung jawab
92	A.14.2.6 Secure Development Environment	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pengamanan lingkungan pengembangan dan uji coba sesuai standar platform teknologi yang digunakan untuk pembangunan sistem

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
93	A.9.1.2 Access to networks and network services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi
94	A.11.1.4 Protecting against external and environmental threats	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan penggunaan rancangan, material dan fasilitas pendukung yang dapat memitigasi risiko kebakaran pada konstruksi ruang penyimpanan perangkat pengolahan informasi penting
95	A.9.2.5 Review of user access right	Kontrol klausul ISO/IEC 27001:2013	Persyaratan peninjauan hak akses pengguna secara berkala oleh pemilik aset
96	A.18.2.3 Technical compliance review	Kontrol klausul ISO/IEC 27001:2013	Persyaratan peninjauan secara berkala sistem informasi untuk mematuhi kebijakan dan standar keamanan informasi organisasi
97	A.16.1.1 Responsibilities and procedures	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan penyusunan prosedur mitigasi risiko berdasarkan tingkat prioritas target penyelesaian dan

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
			tanggung jawab serta efektifitas penggunaan sumber daya
98	A.18.1.4 Privacy and protection of personally identifiable information	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan perlindungan data pribadi sebagai salah satu aspek kajian risiko keamanan informasi
99	A.14.1.3 Protecting application services transactions	Kontrol klausul ISO/IEC 27001:2013	Persyaratan perlindungan informasi yang terlibat dalam transaksi layanan aplikasi untuk mencegah transmisi tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah atau replay
100	A.11.1.4 Protecting against external and environmental threats A.11.2.1 Equipment siting and protection	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan perlindungan infrastruktur komputasi dari dampak lingkungan dan api serta penjagaan kondisi kelembaban dan suhu sesuai prasyarat pabrikan

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
101	A.11.1.4 Protecting against external and environmental threats A.11.2.2 Supporting utilities A.11.2.3 Cabling security	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan perlindungan infrastruktur komputasi dari gangguan pasokan listrik dan dampak dari petir
102	A.15.1.2 Addressing security within supplier agreements	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan persetujuan bersama dengan pihak ketiga terkait penghancuran data secara aman
103	A.15.1.2 Addressing security within supplier agreements	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan persetujuan kebijakan keamanan informasi bagi pihak ketiga dalam bentuk dokumen kontrak, SLA atau dokumen sejenis
104	A.15.1.2 Addressing security within supplier agreements	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan persetujuan pihak ketiga dan karyawan kontrak terhadap rencana mitigasi risiko yang telah diidentifikasi

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
105	A.6.1.1 Information security roles and responsibilities	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan pimpinan instansi/perusahaan secara resmi dan prinsip bertanggung jawab dalam pelaksanaan program keamanan informasi dan kebijakan terkait
106	A.13.1.3 Segregation in networks	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan segmentasi jaringan komunikasi sesuai dengan kepentingannya
107	A.16.1.6 Learning from information security incidents	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan strategi penerapan keamanan informasi sebagai bagian pelaksanaan program kerja
108	A.14.1.1 Information security requirements analysis and specification	Kontrol klausul ISO/IEC 27001:2013	Persyaratan terkait keamanan informasi harus disertakan dalam persyaratan untuk sistem informasi baru atau perangkat tambahan untuk sistem informasi yang ada
109	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Persyaratan uji coba, dokumentasi dan evaluasi terhadap kebijakan, prosedur dan rencana terkait keberlangsungan layanan pihak ketiga

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
110	A.14.2.5 Secure system engineering principles	Literatur mandatory document	Prinsip rekayasa sistem yang aman (Secure system engineering principles)
111	A.18.2.1 Independent review of information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Program audit internal oleh pihak independen dengan cakupan aset informasi, kebijakan dan prosedur keamanan informasi yang ada pada instansi/perusahaan
112	A.6.1.5 Information security in project management	Penerjemahan pertanyaan Indeks KAMI 4.0	Program penilaian kinerja pelaksana pengelolaan keamanan informasi
113	A.7.2.2 Information security awareness, education and training	Penerjemahan pertanyaan Indeks KAMI 4.0	Program peningkatan kompetensi dan keahlian pelaksana pengelolaan keamanan informasi
114	A.7.2.2 Information security awareness, education and training	Penerjemahan pertanyaan Indeks KAMI 4.0	Program peningkatan pemahaman terkait perlindungan data pribadi kepada semua pegawai

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
115	A.7.2.2 Information security awareness, education and training A.7.2.3 Disciplinary process	Penerjemahan pertanyaan Indeks KAMI 4.0	Program publikasi dan peningkatan pemahaman keamanan informasi kepada semua pihat terkait
116	A.8.3.1 Management of removable media	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur periode penyimpanan, penghapusan dan pemusnahan data pribadi
117	A.16.1.4 Assessment of and decision on information security events	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur identifikasi kondisi yang membahayakan keamanan informasi dan penetapan insiden keamanan informasi
118	A.11.2.4 Equipment maintenance	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur inspeksi dan pemeliharaan perangkat komputer, fasilitas dan lokasi kerja aset informasi penting
119	A.14.2.7 Outsourced development	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur keamanan teknis penggunaan layanan cloud

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
120	A.17.1.2 Implementing information security continuity	Literatur mandatory document	Prosedur kesinambungan bisnis (Business continuity procedures)
121	A.16.1.5 Response to information security incidents	Literatur mandatory document	Prosedur manajemen insiden (Incident management procedure)
122	A.6.1.3 Contact with authorities	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur mempertahankan kontak yang sesuai dengan otoritas yang relevan
123	A.6.1.4 Contact with special interest groups	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur menjaga kontak yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis dan asosiasi profesional lainnya
124	A.12.1.1 Documented operating procedures	Literatur mandatory document	Prosedur operasional manajemen TI (Operating procedures for IT management)
125	A.16.1.1 Responsibilities and procedures	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pelaporan insiden keamanan informasi ke pihak eksternal atau pihak berwajib

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
126	A.16.1.3 Reporting information security weaknesses	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pelaporan insiden terkait layanan cloud
127	A.16.1.2 Reporting information security events	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pelaporan insiden terkait terungkapnya data pribadi
128	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pelaporan, pemantauan, penanganan dan analisa insiden keamanan informasi oleh pihak ketiga
129	A.8.3.3 Physical media transfer	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan
130	A.15.1.3 Information and communication technology supply chain	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penanganan data dalam life cyclenya oleh pihak ketiga
131	A.15.2.2 Managing changes to supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penanganan hasil audit dan pelaporan rencana perbaikan beserta bukti-bukti penerapan

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
			rencana oleh pihak ketiga
132	A.15.2.2 Managing changes to supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penanganan hasil pemantauan dan evaluasi laporan atau pembahasan rapat berkala terkait pencapaian SLA dan aspek keamanan informasi oleh pihak ketiga
133	A.15.2.2 Managing changes to supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penanganan risiko dari perubahan yang terjadi terkait hubungan pihak ketiga
134	A.5.1.1 Policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penetapan kebijakan keamanan informasi secara formal dan publikasi kebijakan kepada seluruh karyawan dan pihak terkait
135	A.18.1.4 Privacy and protection of personally identifiable information	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengamanan data pribadi yang disimpan/diolah/dipertukarkan dalam layanan cloud

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
136	A.11.1.2 Physical entry controls	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengamanan lokasi kerja dari kehadiran pihak ketiga
137	A.7.1.1 Screening	Penerjemahan pertanyaan Indeks KAMI 4.0	prosedur pengecekan latar belakang SDM
138	A.11.1.3 Securing offices, rooms and facilities	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengelolaan alokasi kunci masuk ke fasilitas fisik
139	A.15.2.1 Monitoring and review of supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengelolaan dan pemantauan layanan dan aspek keamanan informasi pihak ketiga
140	A.5.1.2 Review of the policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengelolaan dokumen kebijakan dan prosedur keamanan informasi
141	A.9.4.4 Use of privileged utility programs	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengelolaan konfigurasi yang diterapkan secara konsisten
142	A.15.2.2 Managing changes to	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengelolaan perubahan layanan, kebijakan, prosedur dan kontrol risiko

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
	supplier services		terkait hubungan dengan pihak ketiga
143	A.14.2.1 Secure development policy	Kontrol klausul ISO/IEC 27001:2013	Prosedur pengendalian dengan menggunakan kontrol perubahan formal pada perubahan sistem dalam siklus pengembangan
144	A.14.3.1 Protection of test data	Kontrol klausul ISO/IEC 27001:2013	Prosedur pengendalian, perlindungan dan pemilihan secara cermat data pengujian yang akan digunakan
145	A.10.1.1 Policy on the use of cryptographic controls	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penggunaan enkripsi
146	A.18.1.2 Intellectual property rights	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor)
147	A.15.2.2 Managing changes to supplier services	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penghentian layanan cloud dan prosedur pengamanan data yang ada pada layanan cloud

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
148	A.16.1.2 Reporting information security events	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengkomunikasian dan klarifikasi risiko keamanan informasi yang ada pada pihak ketiga
149	A.5.1.1 Policies for information security	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur pengkomunikasian kebijakan keamanan informasi kepada semua pihak terkait (termasuk pihak ketiga)
150	A.12.2.1 Controls against malware	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penidaklanjutan/penyelesaian laporan penyerangan virus /malware
151	A.16.1.7 Collection of evidence	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur penyidikan/investigasi penyelesaian insiden terkait kegagalan keamanan informasi
152	A.14.2.6 Secure Development Environment	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur perilisan aset baru ke lingkungan operasional dan pembaharuan inventaris aset informasi
153	A.12.4.4 Clock synchronisation	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur sinkronasi waktu pada keseluruhan jaringan, sistem dan aplikasi sesuai standar yang ada

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
154	A.11.1.5 Working in secure areas	Literatur mandatory document	Prosedur untuk bekerja di daerah aman (Procedures for working in secure areas)
155	A.9.2.6 Removal or adjustment of access rights	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya
156	A.14.2.8 System security testing A.14.2.9 System acceptance testing	Penerjemahan pertanyaan Indeks KAMI 4.0	Prosedur verifikasi/validasi spesifikasi dan fungsi keamanan pada semua aplikasi saat proses pengembangan dan uji coba
157	A.17.1.3 Verify, review and evaluate information security continuity	Literatur mandatory document	Rencana latihan dan pengujian (Exercising and testing plan)
158	A.17.1.3 Verify, review and evaluate information security continuity	Literatur mandatory document	Rencana pemeliharaan dan peninjauan (Maintenance and review plan)

Kebutuhan Penerapan SMKI			
Asal kebutuhan			Kebutuhan
159	A.17.2.1 Availability of information processing facilities	Literatur mandatory document	Strategi keberlanjutan bisnis (Business continuity strategy)
160	A.16.1.6 Learning from information security incidents	Penerjemahan pertanyaan Indeks KAMI 4.0	Strategi penerapan keamanan informasi berdasarkan hasil analisa risiko

6.2 Penentuan Tingkat Kepentingan Kebutuhan Penerapan SMKI

Pada tahapan ini akan membahas penentuan tingkat kepentingan dimana kebutuhan yang sudah di identifikasi pada tahap sebelumnya termasuk dalam kategori *mandatory* atau *optional*. Justifikasi tingkat kepentingan pada kebutuhan didapatkan peneliti dari literatur *mandatory document* persyaratan penerapan SMKI berdasarkan ISO/IEC 27001:2013[13]. Kebutuhan yang termasuk *mandatory* adalah kebutuhan yang berhubungan dengan *mandatory document* persyaratan penerapan SMKI berdasarkan ISO/IEC 27001:2013. Penetapan tingkat kepentingan dilakukan untuk meprioritaskan pemenuhan kebutuhan yang menjadi persyaratan dalam penerapan SMKI berdasarkan ISO/IEC 27001:2013[10]. Dari hasil penentuan tingkat kepentingan yang dilakukan didapatkan kebutuhan yang memiliki tingkat kepentingan *mandatory* sebanyak 72 kebutuhan dari 160 kebutuhan yang didapatkan. Berikut merupakan penentuan tingkat kepentingan pada setiap kebutuhan yang dilakukan:

Tabel 6. 2 Penentuan tingkat kepentingan kebutuhan

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
1	Analisa aspek keamanan informasi dalam manajemen proyek yang terkait ruang lingkup	Optional
2	Analisa dampak insiden terkait pengungkapan data pribadi yang disimpan, diolah dan di pertukarkan secara ilegal	Mandatory
3	Analisa kesesuaian pengendalian risiko pihak ketiga dengan perjanjian yang telah disepakati bersama	Mandatory
4	Analisa risiko terkait penggunaan layanan berbasis cloud dan penyesuaian kebijakan keamanan informasi terkait layanan cloud sesuai hasil analisa	Mandatory
5	Analisis dampak bisnis (Business impact analysis)	Optional
6	Daftar inventarisasi aset (Inventory of assets)	Mandatory
7	Daftar log aktivitas pengguna, pengecualian, dan peristiwa keamanan (Logs of user activities, exceptions, and security events)	Mandatory
8	Daftar log perubahan sistem informasi yang terekam secara otomatis	Mandatory
9	Daftar rekaman dan hasil analisa pemuktahiran antivirus/antimalware yang telah dikumpulkan secara rutin dan sistematis	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
10	Daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan sesuai dengan klasifikasi keamanan informasi	Mandatory
11	Definisi kebijakan dan prosedur penanganan insiden keamanan informasi terkait pelanggaran hukum	Mandatory
12	Definisi konsekwensi pelanggaran kebijakan keamanan informasi	Optional
13	Definisi metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi (mencakup mekanisme, waktu pengukuran, pelaksanaan, pemantauan dan eskalasi pelaporan keamanan informasi)	Optional
14	Definisi peran dan tanggung jawab keamanan (Definition of security roles and responsibilities)	Mandatory
15	Definisi tugas dan tanggung jawab keamanan informasi yang tetap berlaku setelah terjadi perubahan atau pemberhentian pekerjaan	Mandatory
16	evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala	Mandatory
17	Kebijakan backup (Backup policy)	Optional
18	Kebijakan clear desk dan clear screen (Clear desk and clear screen policy)	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
19	Kebijakan dan prosedur operasional pengelolaan implementasi security patch (berisi tanggung jawab monitoring pembaharuan, pemasangan dan pelaporan perilisan seurity patch baru)	Optional
20	Kebijakan hak pemilik data pribadi dalam mengakses data tersebut	Mandatory
21	Kebijakan instalasi piranti lunak pada aset TI milik instansi/perusahaan	Optional
22	Kebijakan keakuratan dan pemuktahiran data pribadi	Optional
23	Kebijakan keamanan pemasok (Supplier security policy)	Mandatory
24	Kebijakan klasifikasi informasi (Information classification policy)	Optional
25	Kebijakan kontrol akses (Access control policy)	Mandatory
26	Kebijakan manajemen perubahan (Change management policy)	Optional
27	Kebijakan membawa perangkat Anda sendiri (BYOD) (Bring your own device (BYOD) policy)	Optional
28	Kebijakan pembuangan dan penghancuran (Disposal and destruction policy)	Optional
29	Kebijakan penerapan enkripsi sebagai pelindung aset informasi penting	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
30	Kebijakan pengamanan fisik sesuai zona dan klasifikasi aset di dalamnya	Optional
31	Kebijakan pengamanan lokasi kerja penting	Optional
32	Kebijakan pengamanan perangkat komputasi milik instansi/perusahaan yang digunakan diluar lokasi kerja	Optional
33	Kebijakan pengembangan perangkat lunak dan sistem harus dibuat dan diterapkan pada proses pengembangan dalam organisasi	Optional
34	Kebijakan penggunaan aset yang dapat diterima (Acceptable use of assets)	Mandatory
35	Kebijakan penggunaan komputer, email, internet dan intranet	Optional
36	Kebijakan pengungkapan data pribadi atas permintaan resmi aparat penegak hukum	Optional
37	kebijakan Perangkat mobile dan Teleworking (Mobile device and teleworking policy)	Optional
38	Kebijakan perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku	Mandatory
39	Kebijakan perlindungan desktop dan server dari penyerangan virus (malware)	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
40	Kebijakan sandi (Password policy)	Optional
41	Kebijakan terkait perlindungan data pribadi sesuai peraturan perundangan yang berlaku	Mandatory
42	Kebijakan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Optional
43	Kebijakan transfer informasi (Information transfer policy)	Optional
44	Kebijakan, prosedur dan rencana terkait keberlangsungan layanan pihak ketiga dalam keadaan darurat	Mandatory
45	Kebijakan, strategi dan prosedur terkait pengganti layanan cloud ketika terjadi gangguan sementara pada layanan cloud	Mandatory
46	Manajemen harus meminta semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang ditetapkan organisasi	Optional
47	Perencanaan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga	Mandatory
48	Persyaratan adanya fungsi atau bagian dari instansi/perusahaan yang spesifik memiliki tugas dan tanggung jawab mengelola	Mandatory

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
	keamanan informasi dan menjaga kepatuhannya	
49	Persyaratan adanya kerangka kerja pengelolaan risiko keamanan informasi yang secara resmi digunakan	Mandatory
50	Persyaratan alokasi pegawai perusahaan sesuai tanggung jawab dan wewenang yang dimiliki dalam penerapan kebijakan dan prosedur perlindungan data pribadi	Mandatory
51	Persyaratan alokasi sumber daya yang sesuai untuk pelaksana pengelolaan keamanan informasi	Optional
52	Persyaratan analisa aspek finansial dan perubahan infrastruktur sebagai salah satu pertimbangan revisi kebijakan dan prosedur yang berlaku	Optional
53	Persyaratan analisa kepatuhan penerapan konfigurasi standar secara rutin	Optional
54	Persyaratan analisa/evaluasi hasil audit internal untuk mengidentifikasi langkah pembenahan, pencegahan dan inisiatif peningkatan kinerja keamanan informasi	Optional
55	Persyaratan aset penting yang dipertahankan dalam inventaris harus dimiliki	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
56	Persyaratan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan	Mandatory
57	Persyaratan bentuk pengamanan khusus yang berlapis untuk akses yang digunakan mengelola sistem (administrasi sistem)	Mandatory
58	Persyaratan bukti-bukti penerapan yang memadai dalam penanganan insiden keamanan informasi oleh pihak ketiga	Mandatory
59	Persyaratan dan kegiatan audit yang melibatkan verifikasi sistem operasional harus direncanakan dan disetujui dengan cermat untuk meminimalkan gangguan pada proses bisnis	Optional
60	Persyaratan evaluasi audit internal mencakup tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi	Optional
61	Persyaratan evaluasi dan pemantauan secara berkala terkait SLA dan aspek keamanan informasi	Mandatory
62	Persyaratan evaluasi layanan cloud terkait kelaikan keamanan dan ketersediaannya dalam pemenuhan setifikasi layanan berbasis ISO 27001	Optional
63	Persyaratan evaluasi layanan cloud terkait reputasi penyelenggara	Optional
64	Persyaratan evaluasi risiko dan mitigasinya terkait rencana pembelian/implementasi sistem baru	Mandatory

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
65	Persyaratan hak audit TI secara berkala kepada pihak ketiga	Mandatory
66	Persyaratan hukum, regulasi, dan kontraktual (Legal, regulatory, and contractual requirements)	Mandatory
67	Persyaratan identifikasi risiko keamanan informasi terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan pada layanan pihak ketiga	Mandatory
68	Persyaratan identifikasi risiko keamanan informasi terkait kerjasama dengan pihak ketiga	Mandatory
69	Persyaratan indetifikasi data pribadi dan kepastian perlindungan data sesuai undang-undang berlaku	Mandatory
70	Persyaratan integrasi keperluan/persyaratan keamanan informasi ke dalam proses kerja	Mandatory
71	Persyaratan keterlibatan pihak independen dalam analisa kehandalan keamanan informasi secara rutin	Optional
72	Persyaratan ketersediaan laporan SLA dan aspek keamanan informasi sesuai kontrak yang disetujui bersama	Mandatory
73	Persyaratan kondisi dan permasalahan keamanan informasi sebagai konsiderans atau bagian dari proses pengambilan keputusan	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
74	Persyaratan mitigasi risiko keamanan informasi dan sasaran/obyektif tertentu dari pimpinan instansi sebagai refleksi kebijakan dan prosedur keamanan informasi yang ada	Mandatory
75	Persyaratan pelaporan hasil audit internal kepada pimpinan organisasi	Optional
76	Persyaratan pelaporan program keamanan informasi oleh penanggung jawab pengelolaan keamanan informasi secara rutin mencakup kondisi, kinerja/efektifitas dan kepatuhan	Optional
77	Persyaratan pembatasan akses ke informasi dan fungsi sistem aplikasi sesuai dengan kebijakan kontrol akses	Mandatory
78	Persyaratan pembatasan akses ke kode sumber program	Mandatory
79	Persyaratan pembatasan waktu akses dan otomasi proses timeouts, lockout setelah gagal login dan penarikan akses	Mandatory
80	Persyaratan pemberian ijin penggunaan data pribadi secara tertulis oleh pemilik data pribadi	Mandatory
81	Persyaratan pemindaian jaringan, sistem dan aplikasi secara rutin untuk indentifikasi celah kelemahan atau perubahan/keutuhan konfigurasi yang mungkin terjadi	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
82	Persyaratan pemisahan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko akses atau perubahan yang tidak sah terhadap lingkungan operasional	Mandatory
83	Persyaratan pemuktahiran konfigurasi standar keamanan sistem pada seluruh aset jaringan, sistem dan aplikasi sesuai perkembangan dan kebutuhan	Optional
84	Persyaratan pemuktahiran versi terkini sistem operasi perangkat desktop dan server	Optional
85	Persyaratan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi	Mandatory
86	Persyaratan pencantuman tanggung jawab dalam penyusunan dan penulisan kebijakan, prosedur dan dokumen yang terkait kemanan informasi	Mandatory
87	Persyaratan penerapan pengelolaan kunci enkripsi dan siklus penggunaannya	Optional
88	persyaratan penerapan target dan sasaran, evaluasi pencapaian secara berkala, penerapan langkah perbaikan dan pelaporan pencapaian sasaran dalam pengelolaan keamanan informasi	Optional
89	Persyaratan penetapan data yang dapat	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
	disimpan/diolah/dipertukarkan melalui layanan cloud	
90	Persyaratan penetapan peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga pada unit organisasi tertentu	Mandatory
91	Persyaratan pengamanan fasilitas fisik yang sesuai kepentingan/klasifikasi aset informasi, diterapkan secara berlapis dan dapat mencegah upaya akses oleh pihak tidak bertanggung jawab	Optional
92	Persyaratan pengamanan lingkungan pengembangan dan uji coba sesuai standar platform teknologi yang digunakan untuk pembangunan sistem	Optional
93	Persyaratan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi	Mandatory
94	Persyaratan penggunaan rancangan, material dan fasilitas pendukung yang dapat memitigasi risiko kebakaran pada konstruksi ruang penyimpanan perangkat pengolahan informasi penting	Optional
95	Persyaratan peninjauan hak akses pengguna secara berkala oleh pemilik aset	Mandatory

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
96	Persyaratan peninjauan secara berkala sistem informasi untuk mematuhi kebijakan dan standar keamanan informasi organisasi	Optional
97	Persyaratan penyusunan prosedur mitigasi risiko berdasarkan tingkat prioritas target penyelesaian dan tanggung jawab serta efektifitas penggunaan sumber daya	Mandatory
98	Persyaratan perlindungan data pribadi sebagai salah satu aspek kajian risiko keamanan informasi	Optional
99	Persyaratan perlindungan informasi yang terlibat dalam transaksi layanan aplikasi untuk mencegah transmisi tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah atau replay	Optional
100	Persyaratan perlindungan infrastruktur komputasi dari dampak lingkungan dan api serta penjagaan kondisi kelembaban dan suhu sesuai prasyarat pabrikan	Optional
101	Persyaratan perlindungan infrastruktur komputasi dari gangguan pasokan listrik dan dampak dari petir	Optional
102	Persyaratan persetujuan bersama dengan pihak ketiga terkait penghancuran data secara aman	Optional
103	Persyaratan persetujuan kebijakan keamanan informasi bagi pihak	Mandatory

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
	ketiga dalam bentuk dokumen kontrak, SLA atau dokumen sejenis	
104	Persyaratan persetujuan pihak ketiga dan karyawan kontrak terhadap rencana mitigasi risiko yang telah diidentifikasi	Mandatory
105	Persyaratan pimpinan instansi/perusahaan secara resmi dan prinsip bertanggung jawab dalam pelaksanaan program keamanan informasi dan kebijakan terkait	Mandatory
106	Persyaratan segmentasi jaringan komunikasi sesuai dengan kepentingannya	Optional
107	Persyaratan strategi penerapan keamanan informasi sebagai bagian pelaksanaan program kerja	Optional
108	Persyaratan terkait keamanan informasi harus disertakan dalam persyaratan untuk sistem informasi baru atau perangkat tambahan untuk sistem informasi yang ada	Optional
109	Persyaratan uji coba, dokumentasi dan evaluasi terhadap kebijakan, prosedur dan rencana terkait keberlangsungan layanan pihak ketiga	Mandatory
110	Prinsip rekayasa sistem yang aman (Secure system engineering principles)	Mandatory
111	Program audit internal oleh pihak independen dengan cakupan aset informasi, kebijakan dan prosedur	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
	keamanan informasi yang ada pada instansi/perusahaan	
112	Program penilaian kinerja pelaksana pengelolaan keamanan informasi	Optional
113	Program peningkatan kompetensi dan keahlian pelaksana pengelolaan keamanan informasi	Optional
114	Program peningkatan pemahaman terkait perlindungan data pribadi kepada semua pegawai	Optional
115	Program publikasi dan peningkatan pemahaman keamanan informasi kepada semua pihat terkait	Optional
116	Prosedur periode penyimpanan, penghapusan dan pemusnahan data pribadi	Optional
117	Prosedur identifikasi kondisi yang membahayakan keamanan informasi dan penetapan insiden keamanan informasi	Mandatory
118	Prosedur inspeksi dan pemeliharaan perangkat komputer, fasilitas dan lokasi kerja aset informasi penting	Optional
119	Prosedur keamanan teknis penggunaan layanan cloud	Optional
120	Prosedur kesinambungan bisnis (Business continuity procedures)	Mandatory
121	Prosedur manajemen insiden (Incident management procedure)	Mandatory
122	Prosedur mempertahankan kontak yang sesuai dengan otoritas yang relevan	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
123	Prosedur menjaga kontak yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis dan asosiasi profesional lainnya	Optional
124	Prosedur operasional manajemen TI (Operating procedures for IT management)	Mandatory
125	Prosedur pelaporan insiden keamanan informasi ke pihak eksternal atau pihak berwajib	Mandatory
126	Prosedur pelaporan insiden terkait layanan cloud	Mandatory
127	Prosedur pelaporan insiden terkait terungkapnya data pribadi	Mandatory
128	Prosedur pelaporan, pemantauan, penanganan dan analisa insiden keamanan informasi oleh pihak ketiga	Mandatory
129	Prosedur pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan	Mandatory
130	Prosedur penanganan data dalam life cyclenya oleh pihak ketiga	Optional
131	Prosedur penanganan hasil audit dan pelaporan rencana perbaikan beserta bukti-bukti penerapan rencana oleh pihak ketiga	Mandatory
132	Prosedur penanganan hasil pemantauan dan evaluasi laporan atau pembahasan rapat berkala	Mandatory

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
	terkait pencapaian SLA dan aspek keamanan informasi oleh pihak ketiga	
133	Prosedur penanganan risiko dari perubahan yang terjadi terkait hubungan pihak ketiga	Mandatory
134	Prosedur penetapan kebijakan keamanan informasi secara formal dan publikasi kebijakan kepada seluruh karyawan dan pihak terkait	Optional
135	Prosedur pengamanan data pribadi yang disimpan/diolah/dipertukarkan dalam layanan cloud	Optional
136	Prosedur pengamanan lokasi kerja dari kehadiran pihak ketiga	Optional
137	prosedur pengecekan latar belakang SDM	Optional
138	Prosedur pengelolaan alokasi kunci masuk ke fasilitas fisik	Optional
139	Prosedur pengelolaan dan pemantauan layanan dan aspek keamanan informasi pihak ketiga	Mandatory
140	Prosedur pengelolaan dokumen kebijakan dan prosedur keamanan informasi	Mandatory
141	Prosedur pengelolaan konfigurasi yang diterapkan secara konsisten	Optional
142	Prosedur pengelolaan perubahan layanan, kebijakan, prosedur dan kontrol risiko terkait hubungan dengan pihak ketiga	Mandatory
143	Prosedur pengendalian dengan menggunakan kontrol perubahan	Optional

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
	formal pada perubahan sistem dalam siklus pengembangan	
144	Prosedur pengendalian, perlindungan dan pemilihan secara cermat data pengujian yang akan digunakan	Optional
145	Prosedur penggunaan enkripsi	Optional
146	Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor)	Mandatory
147	Prosedur penghentian layanan cloud dan prosedur pengamanan data yang ada pada layanan cloud	Optional
148	Prosedur pengkomunikasian dan klarifikasi risiko keamanan informasi yang ada pada pihak ketiga	Optional
149	Prosedur pengkomunikasian kebijakan keamanan informasi kepada semua pihak terkait (termasuk pihak ketiga)	Optional
150	Prosedur penidaklanjutan/penyelesaian laporan penyerangan virus /malware	Mandatory
151	Prosedur penyidikan/investigasi penyelesaian insiden terkait kegagalan keamanan informasi	Mandatory
152	Prosedur perilisan aset baru ke lingkungan operasional dan pembaharuan inventaris aset informasi	Mandatory

Kebutuhan Penerapan SMKI		
Kebutuhan		Status
153	Prosedur sinkronasi waktu pada keseluruhan jaringan, sistem dan aplikasi sesuai standar yang ada	Optional
154	Prosedur untuk bekerja di daerah aman (Procedures for working in secure areas)	Optional
155	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya	Optional
156	Prosedur verifikasi/validasi spesifikasi dan fungsi keamanan pada semua aplikasi saat proses pengembangan dan uji coba	Optional
157	Rencana latihan dan pengujian (Exercising and testing plan)	Optional
158	Rencana pemeliharaan dan peninjauan (Maintenance and review plan)	Optional
159	Strategi keberlanjutan bisnis (Business continuity strategy)	Optional
160	Strategi penerapan keamanan informasi berdasarkan hasil analisa risiko	Mandatory

6.3 Penyusunan *Checklist* Kebutuhan Penerapan Sistem Manajemen Keamanan Informasi

Pada tahapan ini akan dilakukan penyusunan dokumen checklist dari kebutuhan-kebutuhan yang telah didapatkan dimana kebutuhan yang digunakan merupakan kebutuhan yang memiliki tingkat kepentingan *mandatory* dan *optional*. Referensi kerangka *checklist* didapatkan peneliti dari penelitian

sebelumnya tentang pengendalian kualitas dan pembuatan *checklist* risiko.

Perangkat *checklist* kebutuhan penerapan SMKI ditujukan untuk melakukan pemeriksaan kebutuhan apa saja yang harus dilengkapi untuk menunjang penerapan SMKI. Kesuksesan program penerapan SMKI sendiri dilihat dari kelengkapan klausul yang ada pada ISO/IEC 27001:2013. Semakin banyak klausul yang diterapkan semakin tinggi tingkat kematangan penerapan SMKI di organisasi itu.

Perangkat *checklist* kebutuhan penerapan SMKI berisi daftar dari kebutuhan penerapan SMKI dan kebutuhan tersebut memiliki tingkat kepetingan *mandatory* dan *optional.* Berikut ini merupakan deskripsi dari setiap item yang ada pada perangkat *checklist* kebutuhan penerapan SMKI:

Tabel 6. 3 Daftar item

No.	Item	Deskripsi
1	Checklist Kebutuhan Penerapan SMKI	Memberikan informasi tentang hal apa yang akan dilakukan yaitu pemeriksaan terkait kebutuhan penerapan SMKI
2	Kebutuhan	Berisi informasi kebutuhan untuk penerapan SMKI
3	Kepentingan	Memberikan informasi tentang tingkat kepentingan suatu kebutuhan. Terdapat dua tingkatan dalam tingkat kepentingan yaitu *mandatory* dan *optional*
4	Ketersediaan	Memberikan tanda centang pada setiap kebutuhan sesuai kondisi, tersedia atau tidak tersedia

Berikut ini merupakan hasil dari perangkat *checklist* kebutuhan penerapan SMKI yang dihasilkan oleh penelitian ini:

Tabel 6. 4 *Checklist* kebutuhan penerapan SMKI

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
1	Analisa aspek keamanan informasi dalam manajemen proyek yang terkait ruang lingkup	Optional	○ Y	○N
2	Analisa dampak insiden terkait pengungkapan data pribadi yang disimpan, diolah dan di pertukarkan secara ilegal	Mandatory	○ Y	○N
3	Analisa kesesuaian pengendalian risiko pihak ketiga dengan perjanjian yang telah disepakati bersama	Mandatory	○ Y	○N
4	Analisa risiko terkait penggunaan layanan berbasis cloud dan penyesuaian kebijakan keamanan informasi terkait layanan cloud sesuai hasil analisa	Mandatory	○ Y	○N
5	Analisis dampak bisnis (Business impact analysis)	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
6	Daftar inventarisasi aset (Inventory of assets)	Mandatory	○ Y	○N
7	Daftar log aktivitas pengguna, pengecualian, dan peristiwa keamanan (Logs of user activities, exceptions, and security events)	Mandatory	○ Y	○N
8	Daftar log perubahan sistem informasi yang terekam secara otomatis	Mandatory	○ Y	○N
9	Daftar rekaman dan hasil analisa pemuktahiran antivirus/antimalware yang telah dikumpulkan secara rutin dan sistematis	Optional	○ Y	○N
10	Daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan sesuai dengan klasifikasi keamanan informasi	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
11	Definisi kebijakan dan prosedur penanganan insiden keamanan informasi terkait pelanggaran hukum	Mandatory	○ Y	○N
12	Definisi konsekwensi pelanggaran kebijakan keamanan informasi	Optional	○ Y	○N
13	Definisi metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi (mencakup mekanisme, waktu pengukuran, pelaksanaan, pemantauan dan eskalasi pelaporan keamanan informasi)	Optional	○ Y	○N
14	Definisi peran dan tanggung jawab keamanan (Definition of security roles and responsibilities)	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
15	Definisi tugas dan tanggung jawab keamanan informasi yang tetap berlaku setelah terjadi perubahan atau pemberhentian pekerjaan	Mandatory	○ Y	○N
16	evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala	Mandatory	○ Y	○N
17	Kebijakan backup (Backup policy)	Optional	○ Y	○N
18	Kebijakan clear desk dan clear screen (Clear desk and clear screen policy)	Optional	○ Y	○N
19	Kebijakan dan prosedur operasional pengelolaan implementasi security patch (berisi tanggung jawab monitoring pembaharuan, pemasangan dan pelaporan perilisan seurity patch baru)	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
20	Kebijakan hak pemilik data pribadi dalam mengakses data tersebut	Mandatory	○ Y	○N
21	Kebijakan instalasi piranti lunak pada aset TI milik instansi/perusahaan	Optional	○ Y	○N
22	Kebijakan keakuratan dan pemuktahiran data pribadi	Optional	○ Y	○N
23	Kebijakan keamanan pemasok (Supplier security policy)	Mandatory	○ Y	○N
24	Kebijakan klasifikasi informasi (Information classification policy)	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
25	Kebijakan kontrol akses (Access control policy)	Mandatory	○ Y	○N
26	Kebijakan manajemen perubahan (Change management policy)	Optional	○ Y	○N
27	Kebijakan membawa perangkat Anda sendiri (BYOD) (Bring your own device (BYOD) policy)	Optional	○ Y	○N
28	Kebijakan pembuangan dan penghancuran (Disposal and destruction policy)	Optional	○ Y	○N
29	Kebijakan penerapan enkripsi sebagai pelindung aset informasi penting	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
30	Kebijakan pengamanan fisik sesuai zona dan klasifikasi aset di dalamnya	Optional	○ Y	○N
31	Kebijakan pengamanan lokasi kerja penting	Optional	○ Y	○N
32	Kebijakan pengamanan perangkat komputasi milik instansi/perusahaan yang digunakan diluar lokasi kerja	Optional	○ Y	○N
33	Kebijakan pengembangan perangkat lunak dan sistem harus dibuat dan diterapkan pada proses pengembangan dalam organisasi	Optional	○ Y	○N
34	Kebijakan penggunaan aset yang dapat diterima (Acceptable use of assets)	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
35	Kebijakan penggunaan komputer, email, internet dan intranet	Optional	○ Y	○N
36	Kebijakan pengungkapan data pribadi atas permintaan resmi aparat penegak hukum	Optional	○ Y	○N
37	kebijakan Perangkat mobile dan Teleworking (Mobile device and teleworking policy)	Optional	○ Y	○N
38	Kebijakan perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku	Mandatory	○ Y	○N
39	Kebijakan perlindungan desktop dan server dari penyerangan virus (malware)	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
40	Kebijakan sandi (Password policy)	Optional	○ Y	○N
41	Kebijakan terkait perlindungan data pribadi sesuai peraturan perundangan yang berlaku	Mandatory	○ Y	○N
42	Kebijakan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Optional	○ Y	○N
43	Kebijakan transfer informasi (Information transfer policy)	Optional	○ Y	○N
44	Kebijakan, prosedur dan rencana terkait keberlangsungan layanan pihak ketiga dalam keadaan darurat	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
45	Kebijakan, strategi dan prosedur terkait pengganti layanan cloud ketika terjadi gangguan sementara pada layanan cloud	Mandatory	○ Y	○N
46	Manajemen harus meminta semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang ditetapkan organisasi	Optional	○ Y	○N
47	Perencanaan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga	Mandatory	○ Y	○N
48	Persyaratan adanya fungsi atau bagian dari instansi/perusahaan yang spesifik memiliki tugas dan tanggung jawab mengelola keamanan informasi dan menjaga kepatuhannya	Mandatory	○ Y	○N
49	Persyaratan adanya kerangka kerja pengelolaan risiko keamanan informasi yang secara resmi digunakan	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
50	Persyaratan alokasi pegawai perusahaan sesuai tanggung jawab dan wewenang yang dimiliki dalam penerapan kebijakan dan prosedur perlindungan data pribadi	Mandatory	○ Y	○N
51	Persyaratan alokasi sumber daya yang sesuai untuk pelaksana pengelolaan keamanan informasi	Optional	○ Y	○N
52	Persyaratan analisa aspek finansial dan perubahan infrastruktur sebagai salah satu pertimbangan revisi kebijakan dan prosedur yang berlaku	Optional	○ Y	○N
53	Persyaratan analisa kepatuhan penerapan konfigurasi standar secara rutin	Optional	○ Y	○N
54	Persyaratan analisa/evaluasi hasil audit internal untuk mengidentifikasi langkah pembenahan, pencegahan dan inisiatif peningkatan kinerja keamanan informasi	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
55	Persyaratan aset penting yang dipertahankan dalam inventaris harus dimiliki	Optional	○ Y	○N
56	Persyaratan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan	Mandatory	○ Y	○N
57	Persyaratan bentuk pengamanan khusus yang berlapis untuk akses yang digunakan mengelola sistem (administrasi sistem)	Mandatory	○ Y	○N
58	Persyaratan bukti-bukti penerapan yang memadai dalam penanganan insiden keamanan informasi oleh pihak ketiga	Mandatory	○ Y	○N
59	Persyaratan dan kegiatan audit yang melibatkan verifikasi sistem operasional harus direncanakan dan disetujui dengan cermat untuk meminimalkan gangguan pada proses bisnis	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
60	Persyaratan evaluasi audit internal mencakup tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi	Optional	○ Y	○N
61	Persyaratan evaluasi dan pemantauan secara berkala terkait SLA dan aspek keamanan informasi	Mandatory	○ Y	○N
62	Persyaratan evaluasi layanan cloud terkait kelaikan keamanan dan ketersediaannya dalam pemenuhan setifikasi layanan berbasis ISO 27001	Optional	○ Y	○N
63	Persyaratan evaluasi layanan cloud terkait reputasi penyelenggara	Optional	○ Y	○N
64	Persyaratan evaluasi risiko dan mitigasinya terkait rencana pembelian/implementasi sistem baru	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
65	Persyaratan hak audit TI secara berkala kepada pihak ketiga	Mandatory	○ Y	○N
66	Persyaratan hukum, regulasi, dan kontraktual (Legal, regulatory, and contractual requirements)	Mandatory	○ Y	○N
67	Persyaratan identifikasi risiko keamanan informasi terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan pada layanan pihak ketiga	Mandatory	○ Y	○N
68	Persyaratan identifikasi risiko keamanan informasi terkait kerjasama dengan pihak ketiga	Mandatory	○ Y	○N
69	Persyaratan indetifikasi data pribadi dan kepastian perlindungan data sesuai undang-undang berlaku	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
70	Persyaratan integrasi keperluan/persyaratan keamanan informasi ke dalam proses kerja	Mandatory	○ Y	○N
71	Persyaratan keterlibatan pihak independen dalam analisa kehandalan keamanan informasi secara rutin	Optional	○ Y	○N
72	Persyaratan ketersediaan laporan SLA dan aspek keamanan informasi sesuai kontrak yang disetujui bersama	Mandatory	○ Y	○N
73	Persyaratan kondisi dan permasalahan keamanan informasi sebagai konsiderans atau bagian dari proses pengambilan keputusan	Optional	○ Y	○N
74	Persyaratan mitigasi risiko keamanan informasi dan sasaran/obyektif tertentu dari pimpinan instansi sebagai refleksi kebijakan dan prosedur keamanan informasi yang ada	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
75	Persyaratan pelaporan hasil audit internal kepada pimpinan organisasi	Optional	○ Y	○N
76	Persyaratan pelaporan program keamanan informasi oleh penanggung jawab pengelolaan keamanan informasi secara rutin mencakup kondisi, kinerja/efektifitas dan kepatuhan	Optional	○ Y	○N
77	Persyaratan pembatasan akses ke informasi dan fungsi sistem aplikasi sesuai dengan kebijakan kontrol akses	Mandatory	○ Y	○N
78	Persyaratan pembatasan akses ke kode sumber program	Mandatory	○ Y	○N
79	Persyaratan pembatasan waktu akses dan otomasi proses timeouts, lockout setelah gagal login dan penarikan akses	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
80	Persyaratan pemberian ijin penggunaan data pribadi secara tertulis oleh pemilik data pribadi	Mandatory	○ Y	○N
81	Persyaratan pemindaian jaringan, sistem dan aplikasi secara rutin untuk indentifikasi celah kelemahan atau perubahan/keutuhan konfigurasi yang mungkin terjadi	Optional	○ Y	○N
82	Persyaratan pemisahan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko akses atau perubahan yang tidak sah terhadap lingkungan operasional	Mandatory	○ Y	○N
83	Persyaratan pemuktahiran konfigurasi standar keamanan sistem pada seluruh aset jaringan, sistem dan aplikasi sesuai perkembangan dan kebutuhan	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
84	Persyaratan pemuktahiran versi terkini sistem operasi perangkat desktop dan server	Optional	○ Y	○N
85	Persyaratan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi	Mandatory	○ Y	○N
86	Persyaratan pencantuman tanggung jawab dalam penyusunan dan penulisan kebijakan, prosedur dan dokumen yang terkait kemanan informasi	Mandatory	○ Y	○N
87	Persyaratan penerapan pengelolaan kunci enkripsi dan siklus penggunaannya	Optional	○ Y	○N
88	persyaratan penerapan target dan sasaran, evaluasi pencapaian secara berkala, penerapan langkah perbaikan dan pelaporan pencapaian sasaran dalam pengelolaan keamanan informasi	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
89	Persyaratan penetapan data yang dapat disimpan/diolah/dipertukarkan melalui layanan cloud	Optional	○ Y	○N
90	Persyaratan penetapan peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga pada unit organisasi tertentu	Mandatory	○ Y	○N
91	Persyaratan pengamanan fasilitas fisik yang sesuai kepentingan/klasifikasi aset informasi, diterapkan secara berlapis dan dapat mencegah upaya akses oleh pihak tidak bertanggung jawab	Optional	○ Y	○N
92	Persyaratan pengamanan lingkungan pengembangan dan uji coba sesuai standar platform teknologi yang digunakan untuk pembangunan sistem	Optional	○ Y	○N
93	Persyaratan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
94	Persyaratan penggunaan rancangan, material dan fasilitas pendukung yang dapat memitigasi risiko kebakaran pada konstruksi ruang penyimpanan perangkat pengolahan informasi penting	Optional	○ Y	○N
95	Persyaratan peninjauan hak akses pengguna secara berkala oleh pemilik aset	Mandatory	○ Y	○N
96	Persyaratan peninjauan secara berkala sistem informasi untuk mematuhi kebijakan dan standar keamanan informasi organisasi	Optional	○ Y	○N
97	Persyaratan penyusunan prosedur mitigasi risiko berdasarkan tingkat prioritas target penyelesaian dan tanggung jawab serta efektifitas penggunaan sumber daya	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
98	Persyaratan perlindungan data pribadi sebagai salah satu aspek kajian risiko keamanan informasi	Optional	○ Y	○N
99	Persyaratan perlindungan informasi yang terlibat dalam transaksi layanan aplikasi untuk mencegah transmisi tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah atau replay	Optional	○ Y	○N
100	Persyaratan perlindungan infrastruktur komputasi dari dampak lingkungan dan api serta penjagaan kondisi kelembaban dan suhu sesuai prasyarat pabrikan	Optional	○ Y	○N
101	Persyaratan perlindungan infrastruktur komputasi dari gangguan pasokan listrik dan dampak dari petir	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
102	Persyaratan persetujuan bersama dengan pihak ketiga terkait penghancuran data secara aman	Optional	○ Y	○N
103	Persyaratan persetujuan kebijakan keamanan informasi bagi pihak ketiga dalam bentuk dokumen kontrak, SLA atau dokumen sejenis	Mandatory	○ Y	○N
104	Persyaratan persetujuan pihak ketiga dan karyawan kontrak terhadap rencana mitigasi risiko yang telah diidentifikasi	Mandatory	○ Y	○N
105	Persyaratan pimpinan instansi/perusahaan secara resmi dan prinsip bertanggung jawab dalam pelaksanaan program keamanan informasi dan kebijakan terkait	Mandatory	○ Y	○N
106	Persyaratan segmentasi jaringan komunikasi sesuai dengan kepentingannya	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
107	Persyaratan strategi penerapan keamanan informasi sebagai bagian pelaksanaan program kerja	Optional	○ Y	○N
108	Persyaratan terkait keamanan informasi harus disertakan dalam persyaratan untuk sistem informasi baru atau perangkat tambahan untuk sistem informasi yang ada	Optional	○ Y	○N
109	Persyaratan uji coba, dokumentasi dan evaluasi terhadap kebijakan, prosedur dan rencana terkait keberlangsungan layanan pihak ketiga	Mandatory	○ Y	○N
110	Prinsip rekayasa sistem yang aman (Secure system engineering principles)	Mandatory	○ Y	○N
111	Program audit internal oleh pihak independen dengan cakupan aset informasi, kebijakan dan prosedur keamanan informasi yang ada pada instansi/perusahaan	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
112	Program penilaian kinerja pelaksana pengelolaan keamanan informasi	Optional	○ Y	○N
113	Program peningkatan kompetensi dan keahlian pelaksana pengelolaan keamanan informasi	Optional	○ Y	○N
114	Program peningkatan pemahaman terkait perlindungan data pribadi kepada semua pegawai	Optional	○ Y	○N
115	Program publikasi dan peningkatan pemahaman keamanan informasi kepada semua pihat terkait	Optional	○ Y	○N
116	Prosedur periode penyimpanan, penghapusan dan pemusnahan data pribadi	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
117	Prosedur identifikasi kondisi yang membahayakan keamanan informasi dan penetapan insiden keamanan informasi	Mandatory	○ Y	○N
118	Prosedur inspeksi dan pemeliharaan perangkat komputer, fasilitas dan lokasi kerja aset informasi penting	Optional	○ Y	○N
119	Prosedur keamanan teknis penggunaan layanan cloud	Optional	○ Y	○N
120	Prosedur kesinambungan bisnis (Business continuity procedures)	Mandatory	○ Y	○N
121	Prosedur manajemen insiden (Incident management procedure)	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
122	Prosedur mempertahankan kontak yang sesuai dengan otoritas yang relevan	Optional	○ Y	○N
123	Prosedur menjaga kontak yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis dan asosiasi profesional lainnya	Optional	○ Y	○N
124	Prosedur operasional manajemen TI (Operating procedures for IT management)	Mandatory	○ Y	○N
125	Prosedur pelaporan insiden keamanan informasi ke pihak eksternal atau pihak berwajib	Mandatory	○ Y	○N
126	Prosedur pelaporan insiden terkait layanan cloud	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
127	Prosedur pelaporan insiden terkait terungkapnya data pribadi	Mandatory	○ Y	○N
128	Prosedur pelaporan, pemantauan, penanganan dan analisa insiden keamanan informasi oleh pihak ketiga	Mandatory	○ Y	○N
129	Prosedur pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan	Mandatory	○ Y	○N
130	Prosedur penanganan data dalam life cyclenya oleh pihak ketiga	Optional	○ Y	○N
131	Prosedur penanganan hasil audit dan pelaporan rencana perbaikan beserta bukti-bukti penerapan rencana oleh pihak ketiga	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
132	Prosedur penanganan hasil pemantauan dan evaluasi laporan atau pembahasan rapat berkala terkait pencapaian SLA dan aspek keamanan informasi oleh pihak ketiga	Mandatory	○ Y	○N
133	Prosedur penanganan risiko dari perubahan yang terjadi terkait hubungan pihak ketiga	Mandatory	○ Y	○N
134	Prosedur penetapan kebijakan keamanan informasi secara formal dan publikasi kebijakan kepada seluruh karyawan dan pihak terkait	Optional	○ Y	○N
135	Prosedur pengamanan data pribadi yang disimpan/diolah/dipertukarkan dalam layanan cloud	Optional	○ Y	○N
136	Prosedur pengamanan lokasi kerja dari kehadiran pihak ketiga	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
137	prosedur pengecekan latar belakang SDM	Optional	○ Y	○N
138	Prosedur pengelolaan alokasi kunci masuk ke fasilitas fisik	Optional	○ Y	○N
139	Prosedur pengelolaan dan pemantauan layanan dan aspek keamanan informasi pihak ketiga	Mandatory	○ Y	○N
140	Prosedur pengelolaan dokumen kebijakan dan prosedur keamanan informasi	Mandatory	○ Y	○N
141	Prosedur pengelolaan konfigurasi yang diterapkan secara konsisten	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
142	Prosedur pengelolaan perubahan layanan, kebijakan, prosedur dan kontrol risiko terkait hubungan dengan pihak ketiga	Mandatory	○ Y	○N
143	Prosedur pengendalian dengan menggunakan kontrol perubahan formal pada perubahan sistem dalam siklus pengembangan	Optional	○ Y	○N
144	Prosedur pengendalian, perlindungan dan pemilihan secara cermat data pengujian yang akan digunakan	Optional	○ Y	○N
145	Prosedur penggunaan enkripsi	Optional	○ Y	○N
146	Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor)	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
147	Prosedur penghentian layanan cloud dan prosedur pengamanan data yang ada pada layanan cloud	Optional	○ Y	○N
148	Prosedur pengkomunikasian dan klarifikasi risiko keamanan informasi yang ada pada pihak ketiga	Optional	○ Y	○N
149	Prosedur pengkomunikasian kebijakan keamanan informasi kepada semua pihak terkait (termasuk pihak ketiga)	Optional	○ Y	○N
150	Prosedur penidaklanjutan/penyelesaian laporan penyerangan virus /malware	Mandatory	○ Y	○N
151	Prosedur penyidikan/investigasi penyelesaian insiden terkait kegagalan keamanan informasi	Mandatory	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
152	Prosedur perilisan aset baru ke lingkungan operasional dan pembaharuan inventaris aset informasi	Mandatory	○ Y	○N
153	Prosedur sinkronasi waktu pada keseluruhan jaringan, sistem dan aplikasi sesuai standar yang ada	Optional	○ Y	○N
154	Prosedur untuk bekerja di daerah aman (Procedures for working in secure areas)	Optional	○ Y	○N
155	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya	Optional	○ Y	○N
156	Prosedur verifikasi/validasi spesifikasi dan fungsi keamanan pada semua aplikasi saat proses pengembangan dan uji coba	Optional	○ Y	○N

Checklist Kebutuhan Penerapan SMKI				
No	Kebutuhan	Kepentingan	Ketersediaan	
157	Rencana latihan dan pengujian (Exercising and testing plan)	Optional	○ Y	○N
158	Rencana pemeliharaan dan peninjauan (Maintenance and review plan)	Optional	○ Y	○N
159	Strategi keberlanjutan bisnis (Business continuity strategy)	Optional	○ Y	○N
160	Strategi penerapan keamanan informasi berdasarkan hasil analisa risiko	Mandatory	○ Y	○N

6.4 Verifikasi *Checklist* Kebutuhan Penerapan Sistem Manajemen Keamanan Informasi

Pada tahap ini akan dilakukan verifikasi dari *checklist* kebutuhan penerapan SMKI yang sudah dibuat. Verifikasi dilakukan dengan cara melakukan pengecekan isi dokumen *checklist* dengan kondisi terkini instansi/organisasi yang dibuat studi kasus. Verifikasi yang dilakukan bertujuan untuk

memenuhi kesesuaian dari kebutuhan yang ada pada *checklist* kebutuhan penerapan SMKI dengan kondisi terbaru perusahaan. Karena pada penelitian yang dilakukan peneliti tidak didapatkan studi kasus maka untuk hasil verifikasi checklist tidak ada hasilnya.

Halaman ini sengan dikosongkan

BAB VII
KESIMPULAN DAN SARAN

7.1 Kesimpulan

Berdasarkan hasil dari penelitian tugas akhir yang dilakukan peneliti, didapatkan kesimpulan sebagai berikut:

1. Dari pengerjaan tugas akhir yang dilakukan peneliti didapatkan tiga cara dalam mendapatkan kebutuhan penerapan SMKI. Cara pertama untuk mendapatkan kebutuhan adalah mengidentifikasi kebutuhan dari studi literatur *mandatory document* yang merupakan literatur yang membahas tentang dokumen persyaratan penerapan ISO/IEC 27001:2013 dimana di dalamnya disebutkan kebutuhan yang dapat diambil menjadi kebutuhan penerapan SMKI. Dari indentifikasi studi literatur *mandatory document* persyaratan ISO/IEC 27001:2013 ini didapatkan 25 kebutuhan penerapan SMKI. Cara kedua yang dilakukan adalah dengan mengidentifikasi kebutuhan penerapan SMKI dari penerjemahan pertanyaan Indeks KAMI versi 4.0 dimana pertanyaan yang diterjemahkan adalah pertanyaan yang terpetakan dengan klausul ISO/IEC 27001:2013 dari hasil pemetaan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013. Dari indentifikasi kebutuhan dari penerjemahan pertanyaan Indeks KAMI versi 4.0 ini didapatkan 121 kebutuhan penerapan SMKI. Cara terakhir yang dilakukan untuk mendapatkan kebutuhan adalah dengan indentifikasi kebutuhan dari penerjemahan kontrol klausul ISO/IEC 27001:2013 yang tidak terpetakan dengan pertanyaan Indeks KAMI versi 4.0 dan tidak didapatkan dari studi literatur *mandatory document* pesyaratan ISO/IEC 27001:2013. Dari cara ini didapatkan 14 kebutuhan penerapan SMKI.
2. Penyusunan perangkat *checklist* yang dilakukan pada pengerjaan tugas akhir ini didapatkan empat *item* yang dimasukkan dalam perangkat *checklist* kebutuhan

penerapan SMKI. Empat *item* tersebut adalah *checklist* kebutuhan SMKI, kebutuhan, kepentingan dan status. *Item checklist* kebutuhan penerapan SMKI pada perangkat *checklist* kebutuhan penerapan SMKI adalah memberikan informasi tentang hal yang dilakukan yaitu pemeriksaan terkait kebutuhan penerapan SMKI. *Item* kedua pada perangkat *checklist* adalah kebutuhan dimana *item* ini memberikan informasi terkait kebutuhan penerapan SMKI. *Item* kepentingan pada perangkat *checklist* memberikan informasi tentang status *mandatory* atau *optional* dari kebutuhan penerapan SMKI tersebut. *Item* terakhir adalah ketersediaan dimana *item* ini memberikan informasi terkait kondisi ketersediaan kebutuhan penerapan SMKI pada instansi/organisasi yang sedang menerapkan SMKI.

7.2 Saran

Dari kesimpulan pada tahap sebelumnya dan batasan masalah didapatkan hasil berupa saran dari pengerjaan tugas akhir ini. Berikut merupakan saran yang didapatkan:

1. Penelitian ini hanya menggunakan dua buah landasan dalam pengidentifikasian kebutuhan penerapan SMKI, penelitian selanjutnya dapat menambahkan landasan baru yang memiliki bahasan tentang keamanan informasi agar hasil indentifikasi kebutuhan lebih detail dan akurat untuk penerapan SMKI.
2. Penelitian selanjutnya dapat mengujikan perangkat *checklist* kebutuhan penerapan SMKI yang telah dibuat ke beberapa studi kasus yang menerapkan SMKI di level yang sama.
3. Membuat panduan cara pengisian dokumen *checklist* kebutuhan penerapan SMKI berdasarkan Indeks KAMI 4.0 dan ISO/IEC 27001:2013.

Halaman ini sengan dikosongkan

DAFTAR PUSTAKA

[1] ELE Times, "The Real Cost of Cyber Crime and how to stay Protected," 2019. [Online]. Available: https://www.eletimes.com/the-real-cost-of-cyber-crime-and-how-to-stay-protected. [Accessed: 25-Mar-2019].

[2] B. Soewito, "Pengantar Information Security," *BINUS University*, 2015. [Online]. Available: https://mti.binus.ac.id/2015/04/02/pengantar-information-security/. [Accessed: 21-Jan-2019].

[3] MMSI BINUS University, "Keamanan Informasi," *BINUS University*, 2017. [Online]. Available: https://mmsi.binus.ac.id/2017/11/17/keamanan-informasi/. [Accessed: 21-Nov-2018].

[4] P. A. Perani, "Mengapa Perlu Menerapkan ISO 27001:2013?," *ISOCENTER INDONESIA*, 2016. [Online]. Available: https://isoindonesiacenter.com/mengapa-perlu-menerapkan-iso-270012013/. [Accessed: 22-Nov-2018].

[5] F. A. Basyarahil, H. M. Astuti, and C. Hidayanto, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," vol. 6, no. 1, 2017.

[6] F. Mughoffar, "Penyusunan Template Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005 dan Patuh Terhadap COBIT 5 Control Objective APO13 Manage Security," 2014.

[7] Y. April, "Perencanaan Program Implementasi Enterprise Resource Planning (ERP) di PT. Perkebunan Nusantara XI: Pengendalian Kualitas," *POMITS*, 2016.

[8] J. HM, *Analisis & Desain Sistem Informasi: Pendekatan*

Terstruktur Teori dan Praktek Aplikasi Bisnis. Yogyakarta: Penerbit ANDI, 1989.

[9] W. M. E. and M. H. J., *Principles of Information Security Fifth Edition*, 5th ed. Boston, 2014.

[10] Kominfo, "Panduan Penerapan SMKI Berbasis Indeks KAMI," 2017.

[11] Tim Direktorat Keamanan Informasi, *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*, vol. 53, no. 9. 2011.

[12] I. S. O. Iec, "ISO/IEC 27001:2013," 2013.

[13] 27001 Academy, "White paper : Checklist of Mandatory Documentation Required by 1 . Which documents and records are required ?," 2014.

BIODATA PENULIS

Titus Gigih Trionggo, lahir 03 Desember 1996 di kota Mempawah Provinsi Kalimantan Barat. Penulis merupakan anak pertama dari dua bersaudara. Penulis pernah menempuh pendidikan formal di SDN Wotsogo II, SMPN 1 Jatirogo, SMAN 1 Tuban, dan terakhir masuk menjadi mahasiswa program sarjana jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) angkatan 2015 dan terdaftar dengan NRP 05211540000107. Pada akhir masa perkuliahan di jurusan Sistem Informasi ITS, penulis memilih untuk mengerjakan tugas akhir di Laboratorium Manajemen Sistem Informasi (MSI). Penulis mengambil topik mengenai pembuatan perangkat *checklist* untuk penerapan SMKI dibawah bimbingan Hanim Maria Astuti, S.Kom., M.Sc dan Anisah Herdiyanti Prabowo, S.Kom., M.Sc. Selama menjadi mahasiswa di jurusan Sistem Informasi, penulis aktif dalam mengikuti kegiatan organisasi institut yaitu BEM ITS dan menjabat sebagai staf kementerian sosial masyarakat. Tidak hanya itu, penulis juga aktif menjadi panitia diberbagai kegiatan kampus dan salah satunya pernah menjadi ketua panitia acara ITS Green Campaign 2017. Untuk kepentingan terkait penelitian yang dilakukan penulis dapat menghubungi melalui e-mail: titusgigih21@gmail.com

LAMPIRAN A
Daftar Pertanyaan Indeks KAMI Versi 4.0

Tabel Lampiran A. 1 Daftar pertanyaan Indeks KAMI versi 4.0

Indeks KAMI versi 4.0	
Tata Kelola	
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?
2.2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?
2.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?

Indeks KAMI versi 4.0	
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?
2.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?
2.7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?

Indeks KAMI versi 4.0	
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?
2.9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?
2.10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses

Indeks KAMI versi 4.0	
	kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?
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?
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?

Indeks KAMI versi 4.0	
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?
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?

Indeks KAMI versi 4.0	
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?
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?
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?

Indeks KAMI versi 4.0	
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?
2.21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan 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)?
Risiko	

Indeks KAMI versi 4.0	
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
3.4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?

Indeks KAMI versi 4.0	
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?
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?
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)?
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?

Indeks KAMI versi 4.0	
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?
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?

Indeks KAMI versi 4.0	
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?
Kerangka Kerja	
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?
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?
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?

Indeks KAMI versi 4.0	
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?
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?
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?

Indeks KAMI versi 4.0	
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?
4.8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?
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?

Indeks KAMI versi 4.0	
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?
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?
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?

Indeks KAMI versi 4.0	
4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?
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?

Indeks KAMI versi 4.0	
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi 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?
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?

Indeks KAMI versi 4.0	
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)?
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?

Indeks KAMI versi 4.0	
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?
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?
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?
Pengelolaan Aset	
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)

Indeks KAMI versi 4.0	
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?

Indeks KAMI versi 4.0	
Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda
5.9	Tata tertib penggunaan komputer, email, internet dan intranet
5.10	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan

Indeks KAMI versi 4.0	
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
5.13	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
5.18	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala

Indeks KAMI versi 4.0	
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
5.20	Proses pengecekan latar belakang SDM
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan
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
5.24	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.

Indeks KAMI versi 4.0	
5.25	Apakah tersedia daftar data/informasi yang harus di-*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?
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?
5.28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?

Indeks KAMI versi 4.0	
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?
5.33	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)?

Indeks KAMI versi 4.0	
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?
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)

Indeks KAMI versi 4.0	
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?
Teknologi	
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?
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?
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?

Indeks KAMI versi 4.0	
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?

Indeks KAMI versi 4.0	
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?
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?

Indeks KAMI versi 4.0	
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?
6.19	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?
6.20	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?

Indeks KAMI versi 4.0	
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?
6.25	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?

Indeks KAMI versi 4.0	
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?
Suplemen	
7.1	Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan
7.1.1	Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?

Indeks KAMI versi 4.0	
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?
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?
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?
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?

Indeks KAMI versi 4.0	
7.1.2	Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?
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?
7.1.3	Pengelolaan Layanan dan Keamanan Pihak Ketiga
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?

Indeks KAMI versi 4.0	
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?
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?
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?

Indeks KAMI versi 4.0	
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?
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?
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga
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?
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?
7.1.5	Penanganan Aset

Indeks KAMI versi 4.0	
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?
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?
7.1.7	Rencana Kelangsungan Layanan Pihak Ketiga

Indeks KAMI versi 4.0	
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?
7.2	Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?

Indeks KAMI versi 4.0	
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?

Indeks KAMI versi 4.0	
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?
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?
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?
7.3	Perlindungan Data Pribadi
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?

Indeks KAMI versi 4.0	
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?
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?
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?
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?

Indeks KAMI versi 4.0	
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?
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?
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 ?
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?

Indeks KAMI versi 4.0	
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?
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?
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?
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?

LAMPIRAN B
Daftar Klausul ISO/IEC 27001:2013

Tabel Lampiran B. 1 Daftar klausul ISO/IEC 27001:2013

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
A5. Kebijakan Keamanan Informasi	A5.1 Arahan Manajemen untuk keamanan Informasi	A5.1.1 Policies for information
		A5.1.2 Review of the policies for information security
A6. Organisasi Keamanan Informasi	A6.1 Organisasi Internal	A6.1.1 Information security roles and responsibilities
		A6.1.2 Segregation of duties
		A6.1.3 Contact with authorities
		A6.1.4 Contact with special interest groups

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A6.1.5 Information security in project management
	A6.2 perangkat bergerak dan teleworking	A6.2.1 Mobile device policy
		A6.2.2 Teleworking
A7. Keamanan Sumber Daya Manusia	A7.1 Sebelum dipekerjakan	A7.1.1 Screening
		A7.1.2 Terms and conditions of employment
	A7.2 Selama Bekerja	A7.2.1 Management responsibilities Disciplinary proces
		A7.2.2 Information security awareness, education and training

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A7.2.3 Disciplinary process
	A7.3 Penghentian dan perubahan kepegawaian	A7.3.1 Termination or change of employment responsibilities
A8 Manajemen Aset	A8.1 Tanggung Jawab terhadap aset	A8.1.1 Inventory of assets
		A8.1.2 Ownership of assets
		A8.1.3 Acceptable use of assets
		A8.1.4 Return of assets
	A8.2 Klasifikasi Informasi	A8.2.1 Classification of information

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A8.2.2 Labeling of information
		A8.2.3 Handling of assets
	A8.3 Penanganan Media	A8.3.1 Management of removable media
		A8.3.2 Disposal of media
		A8.3.3 Physical media transfer
A9. Kendali Akses	A9.1 Persyaratan bisnis untuk kendali akses	A9.1.1 Access control policy
		A9.1.2 Access to networks and network services

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
	A9.2 Manajemen Akses Pengguna	A9.2.1 User registration and de-registration
		A9.2.2 User access provisioning
		A9.2.3 Management of privileged access rights
		A9.2.4 Management of secret authentication information of users
		A9.2.5 Review of user access rights
		A9.2.6 Removal or adjustment of access rights
	A9.3 Tanggung Jawab Pengguna	A9.3.1 Use of secret authentication information

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
	A9.4 Kendali akses sistem dan aplikasi	A9.4.1 Information access restriction
		A9.4.2 Secure log-on procedures
		A9.4.3 Password management system
		A9.4.4 Use of privileged utility programs
		A9.4.5 Access control to program source code
A10 Kriptografi	A10.1 Kendali Kriptografi	A10.1.1 Policy on the use of cryptographic controls
		A10.1.2 Key management

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
A11 Keamanan Fisik dan Lingkungan	A11.1 Daerah Aman	A11.1.1 Physical security perimeter
		A11.1.2 Physical entry controls
		A11.1.3 Securing office, room and facilities
		A11.1.4 Protecting against external end environmental threats
		A11.1.5 Working in secure areas
		A11.1.6 Delivery and loading areas
	A11.2 Peralatan	A11.2.1 Equipment siting and protection

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A11.2.2 Supporting utilities
		A11.2.3 Cabling security
		A11.2.4 Equipment maintenance
		A11.2.5 Removal of assets
		A11.2.6 Security of equipment and assets off-premises
		A11.2.7 Secure disposal or re-use of equipment
		A11.2.8 Unattended user equipment

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A11.2.9 Clear desk and clear screen policy
A12 Keamanan Operasi	A12.1 Prosedur dan tanggung jawab operasional	A12.1.1 Documented operating procedures
		A12.1.2 Change management
		A12.1.3 Capacity management
		A12.1.4 Separation of development, testing and operational environments
	A12.2 Perlindungan dari malware	A12.2.1 Controls against malware
	A12.3 Cadangan (back up)	A12.3.1 Information backup

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
	A12.4 Pencatatan dan pemantauan	A12.4.1 Event logging
		A12.4.2 Protection of log information
		A12.4.3 Administrator and operator logs
		A12.4.4 Clock synchronisaton
	A12.5 Kendali perangkat lunak operasional	A12.5.1 Installation of software on operational systems
	A12.6 Manajemen kerentanan teknis	A12.6.1 Management of technical vulnerabilities
		A12.6.2 Restrictions on software installation

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
	A12.7 Pertimbangan ausit sistem informasi	A12.7.1 Information systems audit controls
A13 Keamanan Komunikasi	A13.1 Manajemen Keamanan jaringan	A13.1.1 Network controls
		A13.1.2 Security of network services
		A13.1.3 Segregation in networks
	A13.2 Perpindahan informasi	A13.2.1 Information transfer policies and procedures
		A13.2.2 Agreements on information transfer
		A13.2.3 Electronic messaging

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A13.2.4 Confidentiality or non-disclosure agreements
A14. Akuisisi, pengembangan dan persyaratan sistem	A14.1 Persyaratam Keamanan Informasi	A14.1.1 Information security requirements analysis and specification
		A14.1.2 Securing applications services on public networks
		A14.1.3 Protecting application services transactions
	A14.2 Keamanan dalam proses pengembangan dan dukungan	A14.2.1 Secure development policy
		A14.2.2 System change control procedures
		A14.2.3 Technical review of applications after operating platform changes

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A14.2.4 Restrictions on changes to software packages
		A14.2.5 Secure system engineering principles
		A14.2.6 Secure development environment
		A14.2.7 Outsourced development
		A14.2.8 System security testing
		A14.2.9 System acceptance testing
	A14.3 Data Uji	A14.3.1 Protection of test data

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
A15 Hubungan Pemasok	A15.1 Keamanan Informasi dalam hubungan pemasok	A15.1.1 Information security policy for supplier relationships
		A15.1.2 Addressing security within supplier agreements
		A15.1.3 Information and communication technology supply chain
	A15.2 Manajemen penyampaian layanan pemasok	A15.2.1 Monitoring and review of supplier services
		A15.2.2 Managing changes to supplier services
A16 Manajemen Insiden Keamanan Informasi	A16.1 Manajemen insiden keamanan informasi dan perbaikan	A16.1.1 Responsibilities and procedures
		A16.1.2 Reporting information security events

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A16.1.3 Reporting information security weaknesses
		A16.1.4 Assessment of and decision on information security events
		A16.1.5 Response to information security incidents
		A16.1.6 Learning from information security incidents
		A16.1.7 Collection of evidence
A17 Aspek keamanan informasi manajemen keberlangsungan bisnis	A17.1 Keberlangsungan Keamanan Informasi	A17.1.1 Planning information security continuity
		A17.1.2 Implementing information security continuity

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
		A17.1.3 Verify, review and evaluate information security continuity
	A17.2 Redundansi	A17.2.1 Availability of information processing facilities
A18 Kesesuaian	A18.1 Kesesuaian dengan persyaratan hukum dan kontraktual	A18.1.1 Identification of applicable legislation and contractual requirements
		A18.1.2 Intellectual property rights
		A18.1.3 Protection of records
		A18.1.4 Privacy and protection of personally identifiable information
		A18.1.5 Regulation of cryptographic controls

Klausul	Kontrol Objektif	Kontrol Keamanan Informasi
	A18.2 Tinjauan Keamanan Informasi	A18.2.1 Independent review of information security
		A18.2.2 Compliance with security policies and standards
		A18.2.3 Technical compliance review

Halaman ini sengan dikosongkan

LAMPIRAN C
Daftar Hasil Pemetaan Indeks KAMI 4.0 dengan ISO/IEC 27001:2013

C.1 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0 Area Tata Kelola

Tabel Lampiran C. 1 Pemetaan area tata kelola

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Tata Kelola					
2.1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk	A.6 Organization of information security	A.6.1 internal organization	A.6.1.1 Information security roles and responsibilities	Pertanyaan tersebut merepresentasikan tanggung jawab yang telah ditetapkan dan dialokasikan (tanggung jawab pimpinan instansi/perusahaan) pada A.6.1.1 Information security

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
	penetapan kebijakan terkait?				roles and responsibilities

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.1 Information security roles and responsibilities A.6.1.2 Segregation of duties	Pertanyaan tersebut merepresentasikan klausul A.6.1.1 Information security roles and responsibilities bahwa instansi telah mengalokasikan tanggung jawab pengelolaan keamanan informasi dan merepresentasikan klausul A.6.1.2 Segregation of duties terkait pembagian tugas secara spesifik untuk mgengurangi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
					peluang terjadinya risiko
2.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	A.7 Human resource security	A.7.1 Prior to employment	A.7.1.2 Terms and conditions of employment	Pertanyaan tersebut merepresentasikan tentang perjanjian kontraktual antara pejabat/petugas pelaksana keamanan informasi dengan instansi yang didalamnya terdapat wewenang dan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
					tanggung jawab terhadap organisasi pada klausul A.7.1.2 Terms and conditions of employment

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.3 Capacity management	pertanyaan tersebut merepresentasikan pemantauan, pengaturan dan prediksi terkait alokasi penggunaan sumberdaya untuk mengelola dan menjamin kepatuhan program keamanan informasi pada klausul A.12.1.3 Capacity management
2.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan	A.6 Organization of information security	A.6.1 internal organization	A.6.1.1 Information security roles and responsibilities	Pertanyaan tersebut merepresentasikan peran pelaksana yang telah dipetakan dalam kerangka kerja

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
	dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?				dimana setiap peran telah diberi tanggung jawab masing-masing (klausul A.6.1.1 Information security roles and responsibilities) dan dijelaskan pada perjanjian kontraktual masing-masing pelaksana (A.7.1.2 Terms and conditions of employment)

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
		A.7 Human resource security	A.7.1 Prior to employment	A.7.1.2 Terms and conditions of employment	
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	A.7 Human resource security	A.7.2 During employment	A.7.2.2 Information security awareness, education and training A.7.2.3 Disciplinary process	Pertanyaan tersebut menjelaskan bahwa karyawan menerima program sosialisasi dan peningkatan pemahaman keamanan informasi pada klausul A.7.2.2 Information security awareness, education and training dan kepentingan kepatuhan bagi semua pihak yang terkait pada klausul A.7.2.3 Disciplinary process

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	A.7 Human resource security	A.7.2 During employment	A.7.2.2 Information security awareness, education and training	Pertanyaan tersebut menjelaskan bahwa program peningkatan kompetensi dan keahlian pengelolaan keamanan informasi yang relevan sangat berguna bagi karyawan pada klausul A.7.2.2 Information security awareness, education and training

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.5 Information security in project management	Pertanyaan tersebut merepresentasikan klausul A.6.1.5 Information security in project management terkait integrasi persyaratan dilakukan melalui kerangka kerja yang dibangun untuk mengedalikan pelaksanaan dan pengoprasian keamanan informasi
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang	A.7 Human resource security	A.7.1 Prior to employment	A.7.1.1 Screening	Pertanyaan tersebut merepresentasikan klausul A.7.1.1 yang menjelaskan identifikasi data

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
	digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?				pribadi pelaksana yang akan digunakan kerja dan klausul A.18.1.4 menjelaskan perlindungan dan privasi data pribadi sesuai peraturan dan perundang-undangan yang berlaku
		A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personally identifiable information	

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
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	A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.3 Acceptable use of assets	Pertanyaan tersebut merepresentasikan tanggung jawab penggunaan aset informasi pada pihak pengguna/pengelola internal, eksternal dan pihak lain yang berkepentingan dalam mengidentifikasikan persyaratan/kebutuhan pengamanan pada klausul A.8.1.3 Acceptable use of assets

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
	permasalahan yang ada?				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
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?	A.13 Communications security	A.13.2 Information transfer	A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.13.2.4 Confidentiality or nondisclosure agreements	Pertanyaan tersebut merepresentasikan kepatuhan pengamanan informasi yang di tranfer dengan satker di dalam suatu organisasi dan organisasi dengan pihak eksternal pada klausul A.13.2.1 Information transfer policies and procedures, klausul A.13.2.2 Agreements on information transfer dan klausul A.13.2.4 Confidentiality or

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
					nondisclosure agreements

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1 Planning information security continuity A.17.1.2 Implementing information security continuity A.17.1.3 Verify, review and evaluate information security continuity	Pertanyaan ini merepresentasikan klausul A.17.1.1 Planning information security continuity klausul A.17.1.2 Implementing information security continuity dan klausul A.17.1.3 Verify, review and evaluate information security continuity terkait keberlangsungan layanan TIK telah didefinisikan dan dialokasikan keputusan,

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
					perancang, pelaksanaan dan pengelolanya pada organisasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.2 Compliance with security policies and standards	Pertanyaan ini merepresentasikan klausul A.18.2.2 Compliance with security policies and standards dimana kepastian keamanan informasi sudah diimplementasikan dan dioperasikan dengan kebijakan dan prosedur dari instansi dengan cara laporan secara rutin dan resmi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
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?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.4 Assessment of and decision on information security events	Pertanyaan tersebut merepresentasikan klausul A.16.1.4 Assessment of and decision on information security events terkait kondisi dan permasalahan keamanan informasi menjadi bagian dalam pengambilan keputusan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
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?	A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.3 Acceptable use of assets	Pertanyaan tersebut merepresentasikan klausul A.8.1.3 Acceptable use of assets terkait program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi khususnya aset informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
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?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.5 Information security in project management	Pertanyaan ini merepresentasikan klausul A.6.1.5 Information security in project management yaitu terkait manajemen proyek didalam pengelolaan keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.5 Information security in project management	Pertanyaan ini merepresentasikan klausul A.6.1.5 Information security in project management yaitu terkait manajemen proyek didalam pengelolaan keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
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?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.5 Information security in project management	Pertanyaan ini merepresentasikan klausul A.6.1.5 Information security in project management yaitu terkait manajemen proyek didalam pengelolaan keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.1 Identification of applicable legislation and contractual requirements	pertanyaan ini merepresentasikan klausul A.18.1.1 Identification of applicable legislation and contractual requirements yaitu semua legislasi, perangkat hukum dan standar lainnya yang relevan harus diindetifikasi untuk melihat tingkat kepatuhannya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
2.22	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	Pertanyaan tersebut merepresentasikan definisi kebijakan dan prosedur penanggulangan insiden keamanan informasi pada klausul A.16.1.1 Responsibilities and procedures

C.2 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0 Area Pengelolaan Risiko

Tabel Lampiran C. 2 Pemetaan area pengelolaan risiko

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1 Management of information security incidents and improvements	pertanyaan tersebut merepresentasikan klausul A.16.1 terkait program kerja yang memanajemen risiko dari pengelolaan keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information security events	pertanyaan tersebut merepresentasikan klausul A.16.1.1 Responsibilities and procedures terkait penanggung jawab manajemen risiko dan klausul A.16.1.2 Reporting information security events terkait eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	Pertanyaan tersebut merepresentasikan klausul A.16.1.1 Responsibilities and procedures terkait dokumentasi dari kerangka kerja pengelolaan risiko keamanan informasi
3.4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman	A.8 Asset management	A.8.2 information classification	A.8.2.1 Classification of information	Pertanyaan tersebut merepresentasikan klausul A.8.2.1 Classification of information terkait kerangka kerja pengelolaan risiko tentang tingkat klasifikasi aset

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
	tersebut dan dampak kerugian terhadap instansi/perusahaan anda?				informasi dan klausul A.16.1.4 terkait kerangka kerja pengelolaan risiko yang mencakup tingkat ancaman, kemungkinan terjadi ancaman dan dampak kerugian yang digunakan untuk menilai dan memutuskan suatu peristiwa termasuk risiko atau bukan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
		A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.4 Assessment of and decision on information security events	
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	A.8 Asset management	A.8.2 information classification	A.8.2.1 Classification of information	Pertanyaan tersebut merepresentasikan klausul A.8.2.1 Classification of information terkait penetapan ambang batas yang dapat diterima

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
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?	A.8 Asset management	A.8.1 Responsibility for assets	A8.1.2 Ownership of assets	Pertanyaan tersebut merepresentasikan klausul A8.1.2 terkait kepemilikan aset harus dimiliki ketika aset tersebut merupakan aset yang harus dipertahankan untuk inventarisasi
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset	A.8 Asset management	A.8.2 information classification	A8.2.3 Handling of assets	pertanyaan tersebut merepresentasikan klausul A8.2.3 Handling of assets terkait ancaman dan kelemahan aset

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
	utama sudah teridentifikasi?				informasi yang telah didefinisikan untuk pengembangan dan implementasi prosedur penanganannya
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terangguny a fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	A.8 Asset management	A.8.2 information classification	A.8.2.1 Classification of information	pertanyaan tersebut merepresentasikan klausul A.8.2.1 Classification of information menjelaskan tentang penetapan dampak dari hilang/terganggunya aset utama dari fungsi aset tersebut

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
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)?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A16.1.6 Learning from information security incidents	pertanyaan tersebut merepresentasikan klausul A16.1.6 Learning from information security incidents terkait analisa/kajian risiko keamanan informasi dari aset informasi yang menghasilkan pengetahuan untuk digunakan mengidentifikasi langkah mitigasi dari risiko tersebut

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A16.1.5 Response to information security incidents	pertanyaan tersebut merepresentasikan klausul A16.1.5 Response to information security incidents terkait langkah penanggulangan/mitigasi risiko

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	pertanyaan tersebut merepresentasikan klausul A.16.1.1 Responsibilities and procedures menjelaskan langkah mitigasi yang dibuat teratur sesuai tingkat prioritas target penyelesaiannya dan penanggung jawabnya dengan memastikan efektifitasnya dalam menurunkan tingkat risiko

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A16.1.5 Response to information security incidents	pertanyaan tersebut merepresentasikan klausul A16.1.5 Response to information security incidents terkait pemantauan penyelesaian mitigasi risiko atau kemajuan mitigasinya
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.5 Response to information security incidents	pertanyaan tersebut merepresentasikan klausul A.16.1.5 Response to information security incidents terkait penerapan dan evaluasi langkah

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
	konsistensi dan efektifitasnya?				mitigasi yang telah diterapkan untuk memastikan konsistensi dan efektifitasnya
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	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A16.1.6 Learning from information security incidents	pertanyaan tersebut merepresentasikan klausul A16.1.7 Collection of evidence terkait analisis/kajian secara berulang untuk merevisi profil risiko dan bentuk mitigasinya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
	keperluan penerapan bentuk pengamanan baru?				
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A16.1.6 Learning from information security incidents	pertanyaan tersebut merepresentasikan klausul A16.1.6 Learning from information security incidents yaitu tentang peningkatan efektifitas kerangka kerja pengelolaan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Risiko					
					risiko dari pengetahuan kajian insiden keamanan informasi yang telah diselesaikan
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?				

C.3 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0 Area Kerangka Kerja

Tabel Lampiran C. 3 Pemetaan area kerangka kerja

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
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?	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	pertanyaan tersebut merepresentasikan klausul A.5.1.1 Policies for information security tentang kebijakan, prosedur dan dokumen terkait keamanan informasi yang disusun dan ditulis dengan jelas

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	pertanyaan tersebut merepresentasikan klausul A.5.1.1 Policies for information security terkait penetapan kebijakan kemanan informasi secara formal oleh manajemen dan publikasi kebijakan kepada seluruh karyawan dan pihak terkait

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.2 Review of the policies for information security	pertanyaan tersebut merepresentasikan A.5.1.2 Review of the policies for information security dimana klausul tersebut menjelaskan tentang mekanisme pengelolaan kebijakan dan prosedur kemanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	pertanyaan tersebut merepresentasikan klausul A.5.1.1 Policies for information security terkait proses pengkomunikasian kebijakan keamanan informasi kepada semua pihak terkait
4.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi,	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	pertanyaan tersebut merepresentasikan klausul A.5.1.1 Policies for information security terkait kebijakan dan prosedur keamanan informasi yang

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
	maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?				merefleksikan mitigasi risiko 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?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.4 Assessment of and decision on information security events	pertanyaan tersebut merepresentasikan klausul A.16.1.4 Assessment of and decision on information security events terkait indentifikasi kodisi yang membahayakan keamanan informasi dan penetapan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
					kondisi tersebut sebagai insiden keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.1 Information security policy for supplier relationships A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain	pertanyaan tersebut merepresentasikan klausul A.15.1.1 Information security policy for supplier relationships, klausul A.15.1.2 Addressing security within supplier agreements dan klausul A.15.1.3 Information and communication technology supply chain terkait persyaratan yang tercantum dalam kontrak dengan pihak ketiga dimana di dalamnya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
					mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	A.7 Human resource security	A.7.2 During employment	A.7.2.3 Disciplinary process	pertanyaan tersebut merepresentasikan klausul A.7.2.3 Disciplinary process terkait pendefinisian, pengkomunikasian dan penegakan konsekwensi dari pelanggaran kebijakan keamanan informasi
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
	lanjuti konsekwensi dari kondisi ini?				
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	A.12 Operations security	A.12.6 Technical vulnerability management	A.12.6.1 Management of technical vulnerabilities	pertanyaan tersebut merepresentasikan klausul A.12.6.1 Management of technical vulnerabilities terkait penerapan kebijakan dan prosedur pengelolaan implementasi security patch dan alokasi tanggung

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
	pemasangannya dan melaporkannya?				jawab pemonitor security patch baru serta memastikan pemasangan dan pelaporannya
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.5 Information security in project management	pertanyaan tersebut merepresentasikan klausul A.6.1.5 Information security in project management terkait ruang lingkup aspek keamanan informasi dalam manajemen proyek

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.3 Technical review of applications after operating platform	pertanyaan tersebut merepresentasikan klausul A.14.2.3 Technical review of applications after operating platform terkait proses evaluasi risiko rencana implementasi sistem baru untuk memastikan tidak ada dampak buruk pada organisasi dan keamanan informasi organisasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.5 Secure system engineering principles	pertanyaan tersebut merepresentasikan klausul A.14.2.5 Secure system engineering principles terkait penggunaan prinsip atau metode yang sesuai standar platform teknologi dalam penerapan proses pengembangan sistem yang aman

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.5 Response to information security incidents	pertanyaan tersebut merepresentasikan klausul A.16.1.5 Response to information security incidents terkait prosedur atau proses penanggulangan risiko yang timbul dari penerapan sistem

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran s keamanan informasi, termasuk penjadwalan uji cobanya?	A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1 Planning information security continuity	pertanyaan tersebut merepresentasikan klausul A.17.1.1 Planning information security continuity terkait kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran,	A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1 Planning information security continuity	pertanyaan tersebut merepresentasikan klausul A.17.1.1 Planning information security continuity terkait komposisi, peran, wewenang

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
	wewenang dan tanggungjawab tim yang ditunjuk?				dan tanggung jawab dari perencanaan pemulihan bencana terhadap layanan TIK.
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.2 Implementing information security continuity	pertanyaan tersebut merepresentasikan klausul A.17.1.2 Implementing information security continuity terkait uji coba DRP layanan TIK

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.3 Verify, review and evaluate information security continuity	pertanyaan tersebut merepresentasikan klausul A.17.1.3 Verify, review and evaluate information security continuity terkait dengan evaluasi langkah perbaikan atau pembenaran yang diperlukan dari hasil dari perencanaan DRP layanan TIK

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.2 Review of the policies for information security	pertanyaan tersebut merepresentasikan klausul A.5.1.2 Review of the policies for information security menjelaskan tentang evaluasi kebijakan dan prosedur keamanan informasi secara berkala untuk memastikan kesesuaikan, kecukupan dan keefektifan yang berkelanjutan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.6 Learning from information security incidents	pertanyaan tersebut merepresentasikan klausul A.16.1.6 Learning from information security incidents terkait strategi penerapan keamanan informasi dari hasil analisa risiko
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan	A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.2 Change management	pertanyaan tersebut merepresentasikan klausul A.12.1.2 Change management terkait stratefi pemuktahiran dan penerapan keamanan informasi yang disesuaikan dengan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
	perubahan profil risiko?				perubahan dan kebutuhan profil risiko
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.5 Information security in project management	pertanyaan tersebut merepresentasikan klausul A.6.1.5 Information security in project management terkait strategi penerapan keamanan informasi yang merupakan bagian dari pelaksanaan program kerja organisasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.23	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	pertanyaan tersebut merepresentasikan klausul A.18.2.1 Independent review of information security terkait program audit internal yang dimiliki organisasi dan dilakukan oleh pihak independen

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	pertanyaan tersebut merepresentasikan klausul A.18.2.1 Independent review of information security terkait audit internal yang mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	pertanyaan tersebut merepresentasikan klausul A.18.2.1 Independent review of information security terkait hasil audit internal yang dikaji/evaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	pertanyaan tersebut merepresentasikan klausul A.18.2.1 Independent review of information security terkait pelaporan hasil audit internal kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau peningkatan kinerja keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	A.5 Information security policies	A.5.1 Management direction for information security	A.5.1.2 Review of the policies for information security	pertanyaan tersebut merepresentasikan klausul A.5.1.2 Review of the policies for information security terkait revisi kebijakan dan prosedur dengan merujuk pada aspek finalsial atau perubahan infrastruktur

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	pertanyaan tersebut merepresentasikan klausul A.18.2.1 Independent review of information security terkait evaluasi status kepatuhan untuk memastikan keseluruhan inisiatif deterapkan secara efektif

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Kerangka Kerja					
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	A.17.1.1 Planning information security continuity	pertanyaan tersebut merepresentasikan klausul A.17.1.1 Planning information security continuity terkait program peningkatan keamanan informasi dengan jangka waktu menengah/panjang

C.4 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0 Area Pengelolaan Aset

Tabel Lampiran C. 4 Pemetaan area pengelolaan aset

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.1 Inventory of assets	pertanyaan tersebut merepresentasikan klausul A.8.1.1 Inventory of assets tentang daftar inventaris aset informasi dan aset yang berhubungan dengan TI secara lengkap dan akurat

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	A.8 Asset management	A.8.2 information classification	A.8.2.1 Classification of information	pertanyaan tersebut merepresentasikan klausul A.8.2.1 Classification of information terkait definisi klasifikasi asrt informasi yang sesuai dengan peraturan perundang-undangan yang berlaku
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan	A.8 Asset management	A.8.2 information classification	A.8.2.1 Classification of information	pertanyaan tersebut merepresentasikan klausul A.8.2.1 Classification of information terkait evaluasi dan pengklasifikasian aset informasi sesuai

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
	dan keperluan pengamanannya?				tingkat kepentingan aset
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?	A.8 Asset management	A.8.2 information classification	A.8.2.1 Classification of information	pertanyaan tersebut merepresentasikan klausul A.8.2.1 Classification of information terkait tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrik alokasi akses

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	A.12 Operations security	A.12.1 Operational procedures and responsibilities	A.12.1.2 Change management	pertanyaan tersebut merepresentasikan klausul A.12.1.2 Change management terkait proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	A.9 Access control	A.9.4 System and application access control	A.9.4.4 Use of privileged utility programs	pertanyaan tersebut merepresentasikan klausul A.9.4.4 Use of privileged utility programs terkait proses pengelolaan konfigurasi yang diterapkan secara ketat dan konsisten

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.6 Secure development environment	pertanyaan tersebut merepresentasikan klausul A.14.2.6 Secure development environment terkait perilisan aset baru di lingkungan operasional secara aman dan memutakhirkan inventaris aset informasi
Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?					

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.3 Acceptable use of assets	pertanyaan tersebut merepresentasikan klausul A.8.1.3 Acceptable use of assets terkait aturan yang telah mendefinisikan tanggung jawab pengmanan informasi secara individual untuk semua personil di organisasi
5.9	Tata tertib penggunaan komputer, email, internet dan intranet	A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	A.14.1.2 Securing application services on public networks	pertanyaan tersebut merepresentasikan klausul A.14.1.2 Securing application services on public networks terkait

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					perlindungan informasi yang terlibat dalam penggunaan komputer, email, internet dan intranet
5.10	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	A.8 Asset management	A.8.1 Responsibility for assets	A.8.1.3 Acceptable use of assets A.8.1.4 Return of assets	pertanyaan tersebut merepresentasikan klausul A.8.1.3 Acceptable use of assets dan klausul A.8.1.4 Return of assets terkait tata tertib pengamanan dan penggunaan aset perusahaan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	A.12 Operations security	A.12.6 Technical vulnerability management	A.12.6.2 Restrictions on software installation	pertanyaan tersebut merepresentasikan klausul A.12.6.2 Restrictions on software installation terkait instalasi software pada aset TI perusahaan
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personally identifiable information	pertanyaan tersebut merepresentasikan klausul A.18.1.4 Privacy and protection of personally identifiable information terkait penggunaan data pribadi harus mendapat ijin tertulis

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					pemilik data guna memastikan perlindungan informasi pribadi tersebut
5.13	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	A.9 Access control	A.9.1 Business requirements of access control	A.9.1.1 Access control policy	pertanyaan tersebut merepresentasikan klausul A.9.1.1 Access control policy terkait kebijakan terhadap pelanggaran pengelolaan identitas elektronik dan proses otentifikasi serta klausul A.9.2.4 Management of

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					secret authentication information of users terkait pengelolaan identitas elektronik dan proses otentifikasi
			A.9.2 User access management	A.9.2.4 Management of secret authentication information of users	
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	A.9 Access control	A.9.2 User access management	A.9.2.2 User access provisioning	pertanyaan tersebut merepresentasikan klausul A.9.2.2 User access provisioning terkait persyaratan dan prosedur pengelolaan atau

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					pemberian akses, klausul A.9.2.3 Management of privileged access rights terkait prosedur pengelolaan atau pemberian otorisasi dan klausul A.9.2.4 Management of secret authentication information of users terkait prosedur pengelolaan atau pemberian otentifikasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
				A.9.2.3 Management of privileged access rights	
				A.9.2.4 Management of secret authentication information of users	
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	A.8 Asset management	A.8.3 Media handling	A.8.3.1 Management of removable media	pertanyaan tersebut merepresentasikan klausul A.8.3.1 Management of removable media dan A.11.2.5 Removal of assets terkait lama waktu penyimpanan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					untuk klasifikasi data dan penghacuran data
		A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.5 Removal of assets	
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	A.13 Communications security	A.13.2 Information transfer	A.13.2.2 Agreements on information transfer	pertanyaan tersebut merepresentasikan klausul A.13.2.2 Agreements on information transfer dan A.13.2.4 Confidentiality or nondisclosure agreements terkait ketetapan pertukaran dan pengamanan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					data antara organisasi dengan pihak eksternal
				A.13.2.4 Confidentiality or nondisclosure agreements	
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.7 Collection of evidence	pertanyaan tersebut merepresentasikan klausul A.16.1.7 Collection of evidence terkait proses investigasi dalam menyelesaikan insiden dari kegagalan keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.18	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	A.12 Operations security	A.12.3 Backup	A.12.3.1 Information backup	pertanyaan tersebut merepresentasikan klausul A.12.3.1 Information backup terkait prosedur back-up dan restore data secara berkala
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.1 Physical security perimeter	pertanyaan tersebut merepresentasikan klausul A.11.1.1 Physical security perimeter terkait pengamanan fisik sesuai definisi zona dan klasifikasi aset yang ada di dalamnya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.20	Proses pengecekan latar belakang SDM	A.7 Human resource security	A.7.1 Prior to employment	A.7.1.1 Screening	pertanyaan tersebut merepresentasikan klausul A.7.1.1 Screening terkait pengecekan latar belakang SDM
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	pertanyaan tersebut merepresentasikan klausul A.16.1.1 Responsibilities and procedures terkait prosedur pelaporan insiden ke pihak eksternal atau pihak berwajib

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan	A.8 Asset management	A.8.3 Media handling	A.8.3.2 Disposal of media	pertanyaan tersebut merepresentasikan klausul A.8.3.2 Disposal of media dan A.11.2.7 Secure disposal or reuse of equipment terkait penghancuran data atau aset yang sudah tidak diperlukan
		A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.7 Secure disposal or reuse of equipment	

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
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	A.9 Access control	A.9.1 Business requirements of access control	A.9.1.1 Access control policy	pertanyaan tersebut merepresentasikan klausulA.9.1.1 Access control policy terkait pengelolaan dan kajian hak akses untuk pembenahan kebijakan
5.24	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	A.9 Access control	A.9.2 User access management	A.9.2.6 Removal or adjustment of access rights	pertanyaan tersebut merepresentasikan klausul A.9.2.6 Removal or adjustment of access rights terkait penghapusan hak akses user yang

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya
5.25	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	A.12 Operations security	A.12.3 Backup	A.12.3.1 Information backup	pertanyaan tersebut merepresentasikan klausul A.12.3.1 Information backup terkait informasi daftar back-up dan kepatuhan terhadap prosedur back-up

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.1 Event logging	pertanyaan tersebut merepresentasikan klausul A.12.4.1 Event logging terkait log aktifitas pelaksanaan keamanan informasi beserta bentuk keamanan yang sesuai dengan klasifikasi
5.27	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.2 Intellectual property rights	pertanyaan tersebut merepresentasikan klausul A.18.1.2 Intellectual property rights terkait pemastian aspek HAKI dan pengamanan akses

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
	memastikan aspek HAKI dan pengamanan akses yang digunakan?				yang digunakan pada perangkat pengolahan informasi milik pihak ketiga
5.28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.2 Physical entry controls A.11.1.6 Delivery and loading areas	pertanyaan tersebut merepresentasikan klausul A.11.1.2 Physical entry controls dan A.11.1.6 Delivery and loading areas terkait pengamanan fasilitas fisik untuk mencegah upaya akses dari pihak yang tidak

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					memiliki kewenangan
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.3 Securing offices, rooms and facilities	pertanyaan tersebut merepresentasikan klausul A.11.1.3 Securing offices, rooms and facilities terkait pengamanan kantor, ruangan dan fasilitas salah satunya alokasi kunci masuk

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.4 Protecting against external and environmental threats	pertanyaan tersebut merepresentasikan klausul A.11.1.4 Protecting against external and environmental threats dan A.11.2.1 Equipment siting and protection terkait pelindungan fisik dari bencana alam serta ancaman dan bahaya lingkungan untuk mengurangi risiko

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
			A.11.2 Equipment	A.11.2.1 Equipment siting and protection	
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.4 Protecting against external and environmental threats	pertanyaan tersebut merepresentasikan klausul A.11.1.4 Protecting against external and environmental threats terkait perlindungan dari bencana alam, serangan berbahaya dan kecelakaan seperti sambaran petir dan gangguan pasokan listrik,

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					merepresentasikan juga klausul A.11.2.2 Supporting utilities terkait perlindungan infrastruktur komputasi dari gangguan-gangguan yang ada dan merepresentasikan klausul A.11.2.3 Cabling security terkait perlindungan kabel pada infrastruktur komputasi dari gangguan pasokan listrik

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
			A.11.2 Equipment	A.11.2.2 Supporting utilities A.11.2.3 Cabling security	
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.6 Security of equipment and assets off-premises A.11.2.8 Unattended user equipment	pertanyaan tersebut merepresentasikan klausul A.11.2.6 Security of equipment and assets off-premises dan klausul A.11.2.8 Unattended user equipment terkait

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
					peraturan keamanan aset perangkat komputasi diluar lokasi kerja resmi
5.33	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)?	A.8 Asset management	A.8.3 Media handling	A.8.3.3 Physical media transfer	pertanyaan tersebut merepresentasikan klausul A.8.3.3 Physical media transfer terkait proses pemindahan aset TIK dari lokasi yang sudah ditetapkan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.4 Protecting against external and environmental threats	pertanyaan tersebut merepresentasikan klausul A.11.1.4 Protecting against external and environmental threats terkait perlindungan dari bencana alam, serangan berbahaya dan kecelakaan seperti kebakaran

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	A.11 Physical and environmental security	A.11.2 Equipment	A.11.2.4 Equipment maintenance	pertanyaan tersebut merepresentasikan klausul A.11.2.4 Equipment maintenance terkait pemeliharaan perangkat komputer, fasilitas pendukung dan kelayakan keamanan lokasi kerja dari aset informasi
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang	A.13 Communications security	A.13.2 Information transfer	A.13.2.2 Agreements on information transfer	pertanyaan tersebut merepresentasikan klausul A.13.2.2 Agreements on information transfer terkait perjanjian tentang pengiriman

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
	melibatkan pihak ketiga?				aset informasi yang aman antara organisasi dengan pihak ketiga
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	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.3 Securing offices, rooms and facilities A.11.1.6 Delivery and loading areas	pertanyaan tersebut merepresentasikan klausul A.11.1.3 Securing offices, rooms and facilities terkait pengamanan ruangan kerja penting seperti ruang server dan ruang arsip dan klausul A.11.1.6 Delivery and loading areas terkait pengendalian

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
	telpon genggam di dalam ruang server, menggunakan kamera dll)				keamanan ruangan kerja penting berupa larangan atau isolasi ruangan dari perangkat atau bahan yang berisiko membahayakan aset informasi
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan	A.11 Physical and environmental security	A.11.1 Secure areas	A.11.1.2 Physical entry controls	pertanyaan tersebut merepresentasikan klausul A.11.1.2 Physical entry controls terkait proses pengamanan lokasi kerja dari pihak ketiga yang

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Pengelolaan Aset					
	instansi/perusahaan anda?				memiliki kepentingan

C.5 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0 Area Aspek Teknologi dan Keamanan

Tabel Lampiran C. 5 Pemetaan area aspek teknologi dan keamanan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
	lebih dari 1 lapis pengamanan?				
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	A.13 Communications security	A.13.1 Network security management	A.13.1.3 Segregation in networks	pertanyaan tersebut merepresentasikan klausul A.13.1.3 Segregation in networks terkait segmentasi jaringan komunikasi sesuai kepentingannya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	A.13 Communications security	A.13.1 Network security management	A.13.1.1 Network controls	pertanyaan tersebut merepresentasikan klausul A.13.1.1 Network controls terkait konfigurasi standar keamanan sistem yang mutakhirkan sesuai perkembangan dan kebutuhan untuk seluruhan aset jaringan, sistem dan aplikasi
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan	A.13 Communications security	A.13.1 Network security management	A.13.1.2 Security of network services	pertanyaan tersebut merepresentasikan klausul A.13.1.2 Security of network services terkait analisa kepatuhan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
	konfigurasi standar yang ada?				penerapan konfigurasi standar secara rutin dalam pengelolaan keamanan informasi
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	A.13 Communications security	A.13.1 Network security management	A.13.1.2 Security of network services	pertanyaan tersebut merepresentasikan klausul A.13.1.2 Security of network services terkait pemindaian jaringan, sistem dan aplikasi secara rutin untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan konfigurasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	A.17 Information security aspects of business continuity management	A.17.2 Redundancies	A.17.2.1 Availability of information processing facilities	pertanyaan tersebut merepresentasikan klausul A.17.2.1 Availability of information processing facilities terkait kepastian ketersediaan yang cukup untuk memenuhi persyaratan yang ada
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	A.17 Information security aspects of business continuity management	A.17.2 Redundancies	A.17.2.1 Availability of information processing facilities	pertanyaan tersebut merepresentasikan klausul A.17.2.1 Availability of information processing facilities terkait kepastian ketersediaan yang

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
					cukup untuk memenuhi kebutuhan yang ada
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.1 Event logging	pertanyaan tersebut merepresentasikan klausul A.12.4.1 Event logging terkait perekaman otomatis setiap perubahan sistem informasi di dalam log

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.1 Event logging	pertanyaan tersebut merepresentasikan klausul A.12.4.1 Event logging terkait perekaman peristiwa otomatis setiap aktivitas pengguna dan upaya akses pengguna yang tidak berhak di dalam log peristiwa

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.2 Protection of log information A.12.4.3 Administrator and operator logs	pertanyaan tersebut merepresentasikan klausul A.12.4.2 Protection of log information terkait kepastian kelengkapan isi log peristiwa dimana fasilitas log dan informasi log akan dilindungi untuk kepentingan audit dan forensik serta klausul A.12.4.3 Administrator and operator logs terkait analisa log secara berkala untuk kepastian akurasi,

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
					validitas dan kelengkapan isi log
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.5 Regulation of cryptographic controls	pertanyaan tersebut merepresentasikan klausul A.18.1.5 Regulation of cryptographic controls terkait kebijakan pengelolaan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
					penerapan enkripsi untuk melindungi aset informasi penting sesuai kebijakan yang ada
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	A.10 Cryptography	10.1 Cryptographic controls	A.10.1.1 Policy on the use of cryptographic controls	pertanyaan tersebut merepresentasikan klausul A.10.1.1 Policy on the use of cryptographic controls terkait standar dalam penggunaan enskripsi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	A.10 Cryptography	10.1 Cryptographic controls	A.10.1.2 Key management	pertanyaan tersebut merepresentasikan klausul A.10.1.2 Key management terkait pengelolaan kunci enkripsi yang digunakan
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur	A.9 Access control	A.9.4 System and application access control	A.9.4.3 Password management system	pertanyaan tersebut merepresentasikan klausul A.9.4.3 Password management system terkait sistem pendukung dan penerapan penggantian

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
	kompleksitas/panjangnya dan penggunaan kembali *password* lama?				password secara otomatis
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	A.9 Access control	A.9.4 System and application access control	A.9.4.2 Secure log-on procedures	pertanyaan tersebut merepresentasikan klausul A.9.4.2 Secure log-on procedures terkait penggunaan pengaman khusus pada akses pengelolaan sistem

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts, lockout* setelah kegagalan *login*,dan penarikan akses?	A.9 Access control	A.9.2 User access management	A.9.2.3 Management of privileged access rights	pertanyaan tersebut merepresentasikan klausul A.9.2.3 Management of privileged access rights terkait pembatasan waktu akses pada sistem dan aplikasi
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan	A.9 Access control	A.9.1 Business requirements of access control	A.9.1.2 Access to networks and network services	pertanyaan tersebut merepresentasikan klausul A.9.1.2 Access to networks and network services terkait pengamanan dalam bentuk pendeteksian dan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
	nirkabel) yang tidak resmi?				pencegahan pengguna akses yang tidak resmi
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	A.9 Access control	A.9.1 Business requirements of access control	A.9.1.2 Access to networks and network services	pertanyaan tersebut merepresentasikan klausul A.9.1.2 Access to networks and network services terkait pengamanan akses dari luar instansi/perusahaan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.19	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	A.12 Operations security	A.12.5 Control of operational software	A.12.5.1 Installation of software on operational systems	pertanyaan tersebut merepresentasikan klausul A.12.5.1 Installation of software on operational systems terkait pemutakhiran sistem operasi perangkat desktop dan server versi terkini
6.20	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	A.12 Operations security	A.12.2 Protection from malware	A.12.2.1 Controls against malware	pertanyaan tersebut merepresentasikan klausul A.12.2.1 Controls against malware terkait perlindungan perangkat desktop dan server dari

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
					penyerangan virus (malware)
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	A.12 Operations security	A.12.2 Protection from malware	A.12.2.1 Controls against malware	pertanyaan tersebut merepresentasikan klausul A.12.2.1 Controls against malware terkait pemuktahiran antimalware secara rutin dan sistematis
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses	A.12 Operations security	A.12.2 Protection from malware	A.12.2.1 Controls against malware	pertanyaan tersebut merepresentasikan klausul A.12.2.1 Controls against malware terkait

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
	ditindaklanjuti dan diselesaikan?				laporan penyerangan malware yang ditindaklanjuti dan diselesaikan
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	A.12 Operations security	A.12.4 Logging and monitoring	A.12.4.4 Clock synchronisation	pertanyaan tersebut merepresentasikan klausul A.12.4.4 Clock synchronisation terkait mekanisme sinkronasi waktu yang akurat pada seluruh jaringan, sistem dan aplikasi yang digunakan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.8 System security testing A.14.2.9 System acceptance testing	pertanyaan tersebut merepresentasikan klausul A.14.2.8 System security testing terkait validasi/verifikasi fungsi keamanan aplikasi pada proses pengembangan dan uji coba dan klausul A.14.2.9 System acceptance testing terkait validasi/verifikasi spesifikasi keamanan aplikasi pada proses pengembangan dan uji coba

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.25	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.6 Secure development environment	pertanyaan tersebut merepresentasikan klausul A.14.2.6 Secure development environment terkait pengamanan lingkungan pengembangan yang aman sesuai standar teknologi untuk pengembangan dan uji coba seluruh siklus hidup yang dibangun

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Teknologi					
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	A.18 Compliance	A.18.2 Information security reviews	A.18.2.1 Independent review of information security	pertanyaan tersebut merepresentasikan klausul A.18.2.1 Independent review of information security terkait pengkajian kehandalan keamanan informasi pada perusahaan secara rutin dengan melibatkan pihak independen

C.6 Pemetaan ISO/IEC 27001:2013 dengan Indeks KAMI Versi 4.0 Area Aspek Suplemen

Tabel Lampiran C. 6 Pemetaan area suplemen

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1	**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**				
7.1.1	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**				
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait identifikasi risiko keamanan informasi dari kerjasama pihak

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					ketiga atau pegawai kontrak
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.2 Reporting information security events	pertanyaan tersebut merepresentasikan klausul A.16.1.2 Reporting information security events terkait pengkomunikasian dan klarifikasi risiko keamanan informasi kepada pihak ketiga

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.1 Information security policy for supplier relationships	pertanyaan tersebut merepresentasikan klausul A.15.1.1 Information security policy for supplier relationships terkait klarifikasi persyaratan mitigasi risiko dan ekspetasi mitigasi risiko yang harus dipatuhi pihak ketiga

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.2 Addressing security within supplier agreements	pertanyaan tersebut merepresentasikan klausul A.15.1.2 Addressing security within supplier agreements terkait persetujuan rencana mitigasi risiko oleh pihak ketiga dan karyawan kontrak

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.1 Information security policy for supplier relationships	pertanyaan tersebut merepresentasikan klausul A.15.1.1 Information security policy for supplier relationships terkait kebijakan keamanan informasi untuk pihak ketiga

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.2 Addressing security within supplier agreements	pertanyaan tersebut merepresentasikan klausul A.15.1.2 Addressing security within supplier agreements terkait kebijakan keamanan informasi yang telah dikomunikasikan dan di setujui oleh pihak ketiga dan organisasi melalui dokumentasi yang dilakukan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait hak audit TI secara berkala ke pihak ketiga
7.1.2	**Pengelolaan Sub-Kontraktor/Alih**				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	Daya pada Pihak Ketiga				
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.2 Managing changes to supplier services terkait indentifikasi risiko pihak ketiga terhadap alih daya, subkontraktor dan penyediaan teknologi yang digunakan layanannya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.2 Addressing security within supplier agreements	pertanyaan tersebut merepresentasikan klausul A.15.1.2 Addressing security within supplier agreements terkait pengendalian risiko yang harus dilakukan oleh pihak ketiga sesuai perjanjian
7.1.2.3	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?				
7.1.3	**Pengelolaan Layanan dan Keamanan Pihak Ketiga**				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait proses, prosedur atau rencana terdokumentasi dalam mengelola dan memantau layanan dan aspek keamanan informasi terhadap pihak ketiga

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	A.6 Organization of information security	A.6.1 internal organization	A.6.1.1 Information security roles and responsibilities	pertanyaan tersebut merepresentasikan klausul A.6.1.1 Information security roles and responsibilities terkait alokasi peran dan tanggung jawab pemantauan, evaluasi dan audit aspek keamanan informasi pihak ketiga

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait laporan berkala tentang pencapaian sasaran tingkat layanan
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait pemantauan dan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					evaluasi pencapaian sasaran tingkat layanan dan aspek keamanan
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	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.2 Managing changes to supplier services terkait pendokumentasian, pengkomunikasian dan tindak lanjut pihak ketiga terhadap hasil pemantauan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	kemajuannya kepada instansi/perusahaan?				dan evaluasi dalam rapat berkala
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait penetapan rencana dan kegiatan audit

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	informasi oleh pihak ketiga?				terhadap pihak ketiga untuk pemenuhan persyaratan keamanan informasi
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.2 Managing changes to supplier services terkait tindaklanjut dari hasil audit berupa laporan rencana perbaikan yang terukur dan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					bukti-bukti penerapannya
7.1.3.8	Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan, dikomunikasikan,				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	dipahami dan diterapkan?				
7.1.4	**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.2 Managing changes to supplier services terkait pengelolaan perubahan dari pihak ketiga berupa perubahan layanan, kebijakan, prosedur dan kontrol risiko

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.6 Learning from information security incidents	pertanyaan tersebut merepresentasikan klausul A.16.1.6 Learning from information security incidents terkait penetapan rencana mitigasi baru dari risiko yang dikaji dan dilakukan pendokumentasianny a
7.1.5	**Penanganan Aset**				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.3 Information and communication technology supply chain	pertanyaan tersebut merepresentasikan klausul A.15.1.3 Information and communication technology supply chain terkait prosedur formal pihak ketiga untuk penanganan data selama dalam siklus hidupnya

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.2 Addressing security within supplier agreements	pertanyaan tersebut merepresentasikan klausul A.15.1.2 Addressing security within supplier agreements terkait persetujuan bersama dengan pihak ketiga untuk penghancuran data secara aman
7.1.6	**Pengelolaan Insiden oleh Pihak Ketiga**				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait prosedur pelaporan, pemantauan dan analisis insiden keamanan informasi milik pihak ketiga
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					bukti-bukti penerapan penangan insiden keamanan informasi milik pihak ketiga
7.1.7	**Rencana Kelangsungan Layanan Pihak Ketiga**				
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait kebijakan, prosedur

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	keadaan darurat/bencana?				atau rencana terdokumentasi penanganan kelangsungan layanan ketika terjadi keadaan darurat atau bencana
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.1 Monitoring and review of supplier services terkait pengujian kebijakan, prosedur atau rencana terdokumentasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					penanganan kelangsungan layanan ketika terjadi keadaan darurat atau bencana
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.2	**Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**				
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.3 Information and communication technology supply chain	pertanyaan tersebut merepresentasikan klausul A.15.1.3 Information and communication technology supply chain terkait penyesuaian kebijakan dan kajian risiko layanan cloud

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.3 Information and communication technology supply chain	pertanyaan tersebut merepresentasikan klausul A.15.1.3 Information and communication technology supply chain terkait penetapan data yang disimpan pada layanan cloud
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipert	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personally identifiable information	pertanyaan tersebut merepresentasikan klausul A.18.1.4 Privacy and protection of personally identifiable

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	ukarkan melalui layanan *cloud*?				information terkait pengamanan data pribadi yang disimpan pada cloud
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.1 Identification of applicable legislation and contractual requirements	pertanyaan tersebut merepresentasikan klausul A.18.1.1 Identification of applicable legislation and contractual requirements terkait pengkajian, penetapan kriteria dan pemastian aspek hukum pada

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					penggunaan layanan cloud
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.9 System acceptance testing	pertanyaan tersebut merepresentasikan klausul A.14.2.9 System acceptance testing terkait evaluasi penyelenggara layanan cloud

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.7 Outsourced development	pertanyaan tersebut merepresentasikan klausul A.14.2.7 Outsourced development terkait standar keamanan teknis penggunaan layanan cloud
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan	A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	A.14.2.7 Outsourced development	pertanyaan tersebut merepresentasikan klausul A.14.2.7 Outsourced development terkait evaluasi kelaikan keamanan layanan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	pemenuhan sertifikasi layanan berbasis ISO 27001?				cloud pada aspek ketersediaan dan pemenuhan sertifikasi layanan berbasis ISO 27001
7.2.8	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan	A.15 Supplier relationships	A.15.1 Information security in supplier relationships	A.15.1.3 Information and communicatio n technology supply chain	pertanyaan tersebut merepresentasikan klausul A.15.1.3 Information and communication technology supply chain terkait kebijakan, strategi dan proses pengganti

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	sementara pada layanan tersebut?				layanan cloud ketika terjadi masalah
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.3 Reporting information security weaknesses	pertanyaan tersebut merepresentasikan klausul A.16.1.3 Reporting information security weaknesses terkait proses pelaporan insiden tentang layanan cloud

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	A.15 Supplier relationships	A.15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	pertanyaan tersebut merepresentasikan klausul A.15.2.2 Managing changes to supplier services terkait penghentian layanan cloud dan proses pengamanan datanya
7.3	**Perlindungan Data Pribadi**				

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	A.13 Communications security	A.13.2 Information transfer	A.13.2.4 Confidentiality or nondisclosure agreements	pertanyaan tersebut merepresentasikan klausul A.13.2.4 Confidentiality or nondisclosure agreements terkait dokumentasi jenis dan bentuk data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.13 Communications security	A.13.2 Information transfer	A.13.2.1 Information transfer policies and procedures	pertanyaan tersebut merepresentasikan klausul A.13.2.1 Information transfer policies and procedures terkait alur pemrosesan data pribadi dengan pihak eksternal
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	A.13 Communications security	A.13.2 Information transfer	A.13.2.4 Confidentiality or nondisclosure agreements	pertanyaan tersebut merepresentasikan klausul A.13.2.4 Confidentiality or nondisclosure agreements terkait dokumentasi pada

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					proses penyimpanan, pengolahan dan pertukaran data pribadi
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personally identifiable information	pertanyaan tersebut merepresentasikan klausul A.18.1.4 Privacy and protection of personally identifiable information terkait kebijakan perlindungan data pribadi sesuai

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					peraturan dan perundangan yang berlaku
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	A.6 Organization of information security	A.6.1 internal organization	A.6.1.1 Information security roles and responsibilities	pertanyaan tersebut merepresentasikan klausul A.6.1.1 Information security roles and responsibilities terkait alokasi tanggung jawab dan wewenang penerapan kebijakan dan proses

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	Perlindungan Data Pribadi?				perlindungan data pribadi
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.4 Assessment of and decision on information security events	pertanyaan tersebut merepresentasikan klausul A.16.1.4 Assessment of and decision on information security events terkait analisa dampak penyimpanan,

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
	ilegal atau karena insiden lain?				pertukaran dan pengolahan data pribadi secara ilegal
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personally identifiable information	pertanyaan tersebut merepresentasikan klausul A.18.1.4 Privacy and protection of personally identifiable information terkait kajian risiko keamanan informasi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					tentang aspek perlindungan data pribadi
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.3 Protection of records	pertanyaan tersebut merepresentasikan klausul A.18.1.3 Protection of records terkait mekanisme perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.7 Human resource security	A.7.2 During employment	A.7.2.2 Information security awareness, education and training	pertanyaan tersebut merepresentasikan klausul A.7.2.2 Information security awareness, education and training terkait program peningkatan tentang perlindungan data pribadi kepada seluruh pegawai

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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 ?	A.7 Human resource security	A.7.1 Prior to employment	A.7.1.2 Terms and conditions of employment	pertanyaan tersebut merepresentasikan klausul A.7.1.2 Terms and conditions of employment terkait persetujuan dari pemilik data pribadi beserta penjelasan hak pemilik data dan penggunaan data pribadi tersebut

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.2 Reporting information security events	pertanyaan tersebut merepresentasikan klausul A.16.1.2 Reporting information security events terkait pelaporan insiden terungkapnya data pribadi
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.3 Protection of records	pertanyaan tersebut merepresentasikan klausul A.18.1.3 Protection of records terkait penerapan penjaminan hak pemilik data pribadi

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
					mengakses data miliknya
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	A.18.1.3 Protection of records	pertanyaan tersebut merepresentasikan klausul A.18.1.3 Protection of records terkait kepastian data pribadi akurat dan termuktahirkan

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.8 Asset management	A.8.3 Media handling	A.8.3.1 Management of removable media	pertanyaan tersebut merepresentasikan klausul A.8.3.1 Management of removable media terkait penerapan periode penyimpanan data pribadi dan penghapusan sesuai peraturan perjanjian dengan pemilik

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
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?	A.8 Asset management	A.8.3 Media handling	A.8.3.2 Disposal of media	pertanyaan tersebut merepresentasikan klausul A.8.3.2 Disposal of media terkait penghapusan atau pemusnahan data yang sudah tidak diperlukan secara sah atau menyimpan lebih lanjut sesuai permintaan pemilik data

indeks kami versi 4.0		klausul ISO 27001:2013			Justifikasi
Suplemen					
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	A.16.1.7 Collection of evidence	pertanyaan tersebut merepresentasikan klausul A.16.1.7 Collection of evidence terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum