Institut
Teknologi
Sepuluh Nopember

TUGAS AKHIR – IS184853

ANALISIS HASIL PEMETAAN KUISONER SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN DAN INDEKS KEAMANAN INFORMASI (KAMI) 4.1

ANALYSIS OF MAPPING BASED ON SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN QUESTIONNAIRE AND INDEKS KAMI 4.1

YUARDI BISATYA UTOMO
NRP 05211340000165

Dosen Pembimbing
Feby Artwodini, S.Kom., MT.
Anisah Herdiyanti, S.Kom., M.Sc.

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

TUGAS AKHIR – IS184853

ANALISIS HASIL PEMETAAN KUISONER SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN DAN INDEKS KEAMANAN INFORMASI (KAMI) 4.1.

YUARDI BISATYA UTOMO
NRP 0521 1340 0001 65

Dosen Pembimbing
Feby Artwodini, S.Kom., MT.
Anisah Herdiyanti, S.Kom., M.Sc.

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

UNDERGRADUATE THESES – IS184853

ANALYSIS OF MAPPING BASED ON SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN QUESTIONNAIRE AND INDEKS KAMI 4.1.

YUARDI BISATYA UTOMO
NRP 0521 1340 0001 65

Supervisor
Feby Artwodini, S.Kom., MT.
Anisah Herdiyanti, S.Kom., M.Sc.

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

LEMBAR PENGESAHAN

Analisis Hasil Pemetaan Kuisoner Sistem Pemerintahan Berbasis Elektronik (SPBE) BSSN dan Indeks Keamanan Informasi (KAMI) 4.1.

TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S.Kom)
pada
Departemen Sistem Informasi
Fakultas Teknologi Elektro dan Informatika Cerdas (ELECTICS)
Institut Teknologi Sepuluh Nopember

Oleh

Yuardi Bisatya Utomo
05211340000165

Surabaya, 15 Agustus 2020

Kepala Departemen Sistem Informasi

Dr. Mudjahidin, ST., MT.
NIP. 197010102003121001

LEMBAR PERSETUJUAN

ANALISIS HASIL PEMETAAN KUISONER SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN DAN INDEKS KEAMANAN INFORMASI (KAMI) 4.1.

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:

YUARDI BISATYA UTOMO
NRP 05211340000165

Disetujui Tim Penguji
Tanggal Ujian : 3 Agustus 2020
Periode Wisuda : September 2020

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

Anisah Herdiyanti P, S.Kom., M.Sc. **(Pembimbing II)**

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

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

ANALISIS HASIL PEMETAAN KUISONER SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN DAN INDEKS KEAMANAN INFORMASI (KAMI) 4.1.

Nama Mahasiswa	**:**	**Yuardi Bisatya Utomo**
NRP	**:**	**05211340000165**
Departemen	**:**	**Sistem Informasi FTEIC-ITS**
Pembimbing 1	**:**	**Feby Artwodini, S.Kom., MT.**
Pembimbing 2	**:**	**Anisah Herdiyanti P, S.Kom., M.Sc.**

ABSTRAK

Kebutuhan informasi yang akurat, cepat, serta terpercaya mengharuskan perusahaan menjaga keamanan informasi agar tidak mengganggu dan mempengaruhi peforma perusahaan, organisasi atau Institusi. Dengan adanya kebutuhan tersebut, keamanan informasi harus dapat dikelola dengan baik. Pengelolaan keamanan informasi akan memitigasi resiko yang berkaitan dengan aspek keamanan informasi seperti kerusakan perangkat TI, kehilangan data karena pencurian dan risiko lainnya. Kerugian yang diakibatkan oleh risiko keamanan di Indonesia diprediksi mencapai US$34,2 miliar atau setara Rp 478,8 triliun pada tahun 2018. Untuk itu diperlukan Sistem Manajemen Keamanan Informasi yang melindungi seluruh aspek keamanan informasi. Namun dengan padatnya aktivitas bisnis, termasuk layanan, Kementrian, Lembaga dan Pemerintah Daerah cenderung kesulitan untuk menyiapkan alat kerja dalam melakukan tata kelola keamanan informasi. Oleh karena itu, dibutuhkankan solusi dalam mempersiapkan pengelolaan sistem manajemen keamanan informasi dalam Kementrian, Lembaga dan Daerah. Analisis Pemetaan Sistem manajemen keamanan informasi akan berfokus dengan area pengamanan yang diambil dari pertanyaan Indeks KAMI 4.1 dan Kuisioner SPBE BSSN.

Kata Kunci: Analisis, Indeks KAMI, ISO 27001:2013, Sistem Manajemen Keamanan Informasi, SPBE, BSSN, Kuisioner SPBE BSSN, Kementrian, Lembaga, Pemerintah Daerah.

ANALYSIS OF MAPPING BASED ON SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN QUESTIONNAIRE AND INDEKS KAMI 4.1

Student Name	**: Yuardi Bisatya Utomo**
NRP	**: 05211340000165**
Department	**: Sistem Informasi FTEIC-ITS**
Supervisor 1	**: Feby Artwodini, S.Kom., MT.**
Supervisor 2	**: Anisah Herdiyanti P, S.Kom., M.Sc.**

ABSTRACT

The needs for accurate, fast, and reliable information requires companies to maintain information security so as not to interfere with and affect the performance of companies, organizations or institutions. Given this need, information security must be well managed. Information security management will mitigate risks related to information security aspects such as damage to IT equipment, data loss due to theft and other risks. Losses caused by security risks in Indonesia are predicted to reach US $ 34.2 billion or equivalent to Rp. 478.8 trillion in 2018. This requires the implementation of an Information Security Management System that protects all aspects of information security. However, due to the density of business activities, including services, Ministries, Institutions and Local Governments tends to meet difficulties in preparation of working tools for information security governance. Therefore, solutions are needed in preparing the management of information security management systems in Ministries, Agencies and Regions. Mapping Analysis Information security management system will focus on security areas taken from Indeks KAMI 4.1 and the BSSN SPBE Questionnaire.

Keywords: Analysis, Indeks KAMI 4.1, ISO 27001:2013, Information Security Management System, SPBE, BSSN, SPBE BSSN Questionnaire, Ministries, Institutions, Local Government

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertandatangan di bawah ini:

Nama	: Yuardi Bisatya Utomo
NRP	: 05211340000165
Tempat/Tanggal lahir	: Madiun / 28 Juli 1995
Fakultas/Departemen	: Fakultas Teknologi Elektro dan Informatika Cerdas/ Departemen Sistem Informasi
Nomor Telp/Hp/email	: 08113421828

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

Analisis Hasil Pemetaan Kuisoner Sistem Pemerintahan Berbasis Elektronik (SPBE) BSSN dan Indeks Keamanan Informasi (KAMI) 4.1.

Bebas Dari Plagiarisme Dan Bukan Hasil Karya Orang Lain.

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

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

Surabaya, 03 Agustus 2020

Yuardi Bisatya Utomo

NRP. 05211340000165

Halaman ini sengaja dikosongkan

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 **ANALISIS HASIL PEMETAAN KUISONER SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) BSSN DAN INDEKS KEAMANAN INFORMASI (KAMI) 4.1.**

Pada kesempatan kali ini, penulis 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. Orang Tua dan Keluarga Besar dari penulis yang selalu mendukung secara materiil, memotivasi dan mendoakan penulis dalam menyelesaikan laporan tugas akhir ini dan Pendidikan S1 penulis secara Umumnya.
2. Ibu Feby Artwodini, S.Kom., MT. 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. Bapak Faizal Johan Atletiko, S.Kom., M.T., Bapak Arif Wibisono, S.Kom., M.Sc. dan Bapak Ir.Achmad Holil Noor Ali, M.Kom. selaku dosen-dosen wali yang telah mengarahkan dan memotivasi penulis selama masa studi perkuliahan sampai dengan pengerjaan tugas akhir ini.
4. Sisa- sisa Angkatan 2013 yang lulus di periode wisuda September 2020 yang selalu saling menyemangati sebagai teman baik yang selalu mendukung dan memotivasi penulis untuk menyelesaikan tugas akhir ini, serta Angkatan 2012 dan 2016 yang berjuang Bersama-sama.

Penyusunan laporan tugas akhir yang dilakukan penulis masih jauh dari kata sempurna, oleh karena itu penulis sangat menerima kritik dan saran yang membangun untuk perbaikan dimasa yang akan datang. Penelitian ini diharapkan dapat menjadi acuan atau referensi penelitian-penelitian selanjutnya yang memiliki penelitian serupa dan dapat bermanfaat bagi pembaca.

Surabaya, Agustus 2020

Penulis

DAFTAR ISI

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Halaman ini sengaja dikosongkan

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

Salah satu Primadona pada abad ke-21 ini, adalah berkembangnya secara pesat implementasi Teknologi Informasi pada Perusahaan, Organisasi dan Institusi. Dengan efektifitas dan efisiensi proses bisnis yang terbantu oleh adanya Teknologi Informasi pada tiga badan badan tersebut, ada juga ancaman yang mengintai, karena Teknologi informasi yang menjadi aset penting dalam sebuah Perusahaan, Organisasi dan Institusi memiliki kebutuhan yang penting pada bidang keamanan informasi. Risiko dari keamanan informasi memiliki dampak kerugian yang tinggi pada perusahaan baik secara material, maupun secara imaterial. Menurut penelitian yang dilakukan oleh *Home Office Science Advisory Council* (HOSAC), menemukan kerugian sebesar £ 1.600.000 dalam kurun waktu antara tahun 2007 sampai dengan 2015 pada industri dan pemerintahan di Inggris [1]. Selain itu menurut penelitian penelitian dari *Frost & Sullivan* yang diprakarsai *Microsoft*, mencatat kerugian Kejahatan siber di Indonesia bisa menimbulkan kerugian mencapai US$34,2 miliar atau setara Rp 478,8 triliun pada tahun 2018 [2].

Selain Perusahaan, Organisasi, Institusi yang terdiri dari swasta dan pemerintahan. Khususnya lembaga pemerintah di Indonesia juga sudah mulai mengembangkan teknologi informasinya secara masif [3].

Sistem Manajemen Keamanan Informasi (SMKI) adalah seperangkat kebijakan dan prosedur untuk mengelola data sensitif perusahaan, organisasi atau Institusi secara sistematis. Tujuan dari SMKI adalah untuk memitigasi risiko dan memastikan kelangsungan bisnis dengan secara proaktif

membatasi dampak pelanggaran keamanan informasi. SMKI bertujuan untuk merancang, menerapkan, dan memelihara suatu rangkaian proses terpadu dan sistem untuk secara efektif mengelola keamanan informasi serta menjamin kerahasiaan, integritas, ketersediaan aset-aset informasi, meminimalkan risiko keamanan informasi. Sebab sebuah sistem manajemen yang diterapkan berisi informasi yang beredar di perusahaan, organisasi atau Institusi, agar dapat dikelola dengan benar sehingga perusahaan, organisasi atau Institusi dapat mengambil keputusan berdasarkan informasi yang ada dengan benar, dalam rangka memberikan pelayanan terbaik ke pelanggan [4].

SMKI memiliki 4 Fungsi, yaitu: Identifikasi Ancaman, Mendefinisikan Resiko dari identifikasi Ancaman, penetapan kebijakan keamanan informasi, dan penerapan kontrol pada resiko [5].

ISO 27001:2013 adalah standarisasi untuk membuat SMKI. Dimana didalamnya terdapat saran untuk dokumentasi, audit internal, peningkatan berkelanjutan, dan tindakan korektif dan preventif. Menurut Organisasi Internasional untuk Standardisasi, ISO / IEC 27001:2013 adalah standar dalam penerapan SMKI yang dibuat untuk memastikan tingkat keamanan informasi yang tinggi dalam produk, layanan, dan proses teknologi [4].

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, perusahaan atau organisasi atau institusi disarankan menetapkan sebuah sistem yang bernama sistem manajemen keamanan informasi (SMKI) dalam mengelola keamanan informasi perusahaan, organisasi atau institusi. SMKI dapat menjadi acuan dalam tata kelola

keamanan informasi. Alat Evaluasi yang berdasarkan Standard SMKI dan ISO/IEC 27001:2013 adalah Indeks KAMI 4.1. Jadi Indeks KAMI 4.1 adalah alat evaluasi pelaksanaan Keamanan Informasi untuk mengetahui tingkat kematangan Keamanan Informasi sebuah Perusahaan, Organisasi atau Institusi [6].

Karena sudah berbasis Indeks KAMI yang merupakan alat evaluasi untuk melihat kematangan keamanan informasi di sebuah Perusahaan, Organisasi atau Institusi. Maka SMKI sudah sesuai dengan standar SNI dari *best practice* ISO/IEC 27000:2013. ISO/IEC 27001:2013 menyediakan standar yang membahas tentang manajemen keamanan informasi di sebuah perusahaan, organisasi atau Institusi. Standar dari *best practice* ini digunakan untuk membuat kontrol dari keamanan yang sudah diterapkan [6].

Indeks KAMI 4.1 adalah audit keamanan sistem informasi yang merupakan salah satu alat yang diterapkan untuk memberikan gambaran sistem keamanan informasi sehingga bisa mengurangi potensi resiko kerentanan suatu sistem informasi terhadap pihak yang tidak bertanggung jawab. Standar yang digunakan untuk melakukan audit keamanan informasi yaitu dengan menggunakan indeks keamanan informasi (KAMI 4.1.) berdasarkan ISO/IEC 27001:2013, dimana dalam indeks tersebut dapat digunakan untuk melakukan analisa dan evaluasi tingkat kesiapan atau kematangan sistem informasi pada sebuah perusahaan, organisasi atau Institusi dengan kriteria SNI ISO/IEC 27001:2013. Indeks KAMI 4.1 dipublikasikan oleh Badan Siber dan Sandi Negara (BSSN) pada November 2019 [7].

Untuk Institusi Pemerintahan, berdasarkan Peraturan Presiden nomor 95 tahun 2018 yang meliputi Kementrian/Lembaga/Pemerintahan Daerah (K/L/D), mempunyai sistem informasi tersendiri yang dsebut Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE adalah sisitem penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi (TIK) untuk memberikan layanan kepada pengguna SPBE, yakni K/L/D, yang bertujuan

mewujudkan tatakelola pemerintahan yang bersih, efektif, transparan, dan akuntabel. Serta meningkatkan efisiensi dan keterpaduan penyelenggaraan SPBE [8].

Dalam penerapannya, SPBE diatur oleh Peraturan Kementrian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PERMENPANRB) nomor 5 tahun 2018, dalam melaksanakan SPBE, Kementrian PanRB yang ditunjuk sebagai ketua tim koordinasi SPBE Nasional dibantu oleh 6 kementrian dan Badan tinggi negara, yaitu Kominfo, Kementrian Dalam Negeri, Kementrian Keuangan, Kementrian PPN/Bappenas, BPPT dan yang terakhir BSSN. BSSN memiliki tanggung jawab dalam pelaksanaan SPBE nasional, yaitu sebagai Penyusun Arsitektur Keamanan SPBE Nasional, Memberikan pertimbangan dalam kelayakan Infrastruktur SPBE Nasional, Menerapkan Keamanan SPBE, Manajemen Keamanan SPBE dan Melakukan Fungsi Audit Keamanan SPBE Nasional. [9].

Sebagai bentuk nyata pelaksanaan tupoksi dalam pelaksana keamanan SPBE, BSSN mengeluarkan sebuah kuisioner evaluasi keamanan yang menghitung tingkat kematangan pelaksanaan SPBE dari segi tatakelola dan manajemen keamanan informasi. Selanjutnya Kuisioner ini disebut sebagai Kuisioner SPBE-BSSN [10].

Jadi BSSN telah merilis dua form evaluasi Keamanan Informasi, Indeks KAMI 4.1 dan Kuisioner SPBE-BSSN. Indeks KAMI 4.1 diimplementasikan pada Perusahaan, Organisasi atau Institusi baik Swasta maupun Pemerintahan. Sedangkan Kuisioner SPBE-BSSN, hanya diimplementasikan pada Institusi Pemerintahan, baik untuk Kementrian, Lembaga dan Pemerintah Daerah (K/L/D) [7].

Indeks KAMI 4.1 Terdiri dari 1 Kategori SE (Sistem Elektronik) dan 6 area penilaian sedangkan Kuisioner SPBE-BSSN terdiri dari 4 Domain. Dari 6 Area penilaian dan 4 domain tersebut, yang akan menjadi objek penelitian penulis, dengan cara membuat sebuah analisis pemetaan dari hasil pemetaan antara area dan domain diatas. [7].

Pemetaan Indeks Kami 4.1 dan Kuisioner SPBE-BSSN ini diharapkan dapat memberi bantuan terhadap K/L/D dalam mengisi kuisioner SPBE BSSN pada umumnya, dan membantu K/L/D yang belum menerapkan Indeks KAMI agar dapat menerapkannya dan memenuhi syarat SMKI sesuai ISO IEC 27001:2013.

1.2 Rumusan Masalah

Rumusan masalah berdasarkan uraian latar belakang diatas, maka rumusan permasalahan yang menjadi fokus yang akan diselesaikan dalam tugas akhir ini adalah sebagai berikut:

1. Seperti apa hasil pemetaan Indeks KAMI versi 4.1 dan Kuisioner SPBE BSSN ?
2. Bagaimana bentuk analisa pemetaan Indeks KAMI versi 4.1 dan Kuisioner SPBE BSSN dalam memberikan bantuan terhadap K/L/D dalam mengisi Kuisioner SPBE BSSN?

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 pemetaan Indeks KAMI versi 4.1 dan Kuisioner SPBE BSSN **edisi Agustus 2019**.
2. Analisa pemetaan hanya menggunakan pertanyaan dari Indeks KAMI versi 4.1 yang terpetakan dan teridentifikasi dengan Kuisioner SPBE BSSN.
3. Pada hasil pemetaan yang tidak dipetakan, tetap digunakan sebagai alat bantu bagi K/L/D yang belum mengimplementasikan Indeks KAMI sebagai alat evaluasi.
4. Perancangan Analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1 ini **hanya sebatas studi literatur**, **belum diimplementasikan** pada objek studi kasus pada Kementrian, Lembaga atau Pemerintah

Daerah. Sehingga Verifikasi maupun Validasi, bukan merupakan *scope* penelitian TA ini. Hal ini dikarenakan keterbatasan mobilitas penulis di masa pandemik Covid-19 saat ini.

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 hasil pemetaan Indeks KAMI versi 4.1 dan Kuisioner SPBE BSSN.
2. Mengembangkan solusi berupa analisa pemetaan dari Indeks KAMI versi 4.1 dan Kuisioner SPBE BSSN sebagai acuan penerapan SMKI.
3. Memberikan bantuan pengisian Kuisioner SPBE BSSN, bagi K/L/D dari analisis hasil pemetaannya dengan Indeks KAMI versi 4.1.

1.5 Manfaat Tugas Akhir

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

1. Tugas akhir ini diharapkan dapat memberi luaran (*output*) berupa analisis pemetaan penerapan SMKI yang mempermudah K/L/D mengisi kuisioner SPBE BSSN dalam menerapkan sistem manajemen keamanan informasi mereka.
2. Tugas akhir ini diharapkan dapat memberikan bantuan berupa referensi untuk peneliti yang sedang maupun akan melakukan penelitian sejenis, terlebih bila mereka mau melanjutkannya dengan studi kasus pada Kementrian, Lembaga atau Pemerintah Daerah.

1.6 Relevansi Tugas Akhir

Tugas akhir ini tentang analisis hasil pemetaan penerapan sistem manajemen keamanan informasi yang berkaitan dengan

mata kuliah Manajemen Risiko dan Kualitas TI dan Tata kelola TI.

1.7 Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini dibagi menjadi tujuh bab. Berikut masing-masing bab:

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 Analisa Pemetaan 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 pada kebutuhan dari hasil penggalian

data yang dilakukan pada bab sebelumnya. Bab ini juga membahas tentang hasil Analisa pemetaan yang dibuat berdasarkan referensi penelitian sebelumnya. Dimana penulis hanya **mengambil** metode pemetaan.

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 Tabel Penelitian Radhifan Hidayat

Judul	**Evaluasi Keamanan Informasi Menggunakan Metode Indeks Keamanan Informasi (Kami) (Studi Kasus: Stie Perbanas Surabaya)**
Nama, Tahun	Hidayat, Radhifan (2016)
Gambaran umum penelitian	Makalah ini mengevaluasi Keamanan Manajemen Informasi STIE PERBANAS Surabaya menggunakan indeks KAMI Versi 2.2 yang berdasarkan pada ISO/IEC 27001:2005 , 19 April 2012 dari Kementerian Kominfo. Hasil penilaian tingkat ketergantungan TIK adalah sebesar 30 dari total keseluruhan 48, dan termasuk dalam kategori tinggi. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 252 dari total keseluruhan 588. Dengan ketergantungan TIK yang tinggi tersebut penilaian kelima area masih termasuk ke dalam kategori tidak layak. Dan untuk mencapai status kesiapan baik minimal membutuhkan skor sebesar 393. Untuk itu akan dibuatkan suatu rekomendasi perbaikan pada

	bagian-bagian yang masih kurang dari hasil penilaian indeks KAMI yang telah dilakukan.
Keterkaitan penelitian	Penelitian ini menggunakan Indeks KAMI. Dengan mengacu penelitian ini penulis dapat mempelajari dasar dasar metode Indeks KAMI yang lebih dalam karena banyak informasi informasi yang tidak tersedia di website BSSN. Perbedaan objek penelitian antara penulis dengan penelitian ini, adalah penulis meneliti tanpa studi kasus, sedangkan penelitian ini di sektor Pendidikan.

Tabel 2.2 Tabel Penelitian Firzah Abdullah Basyarahil, Hanim Maria Astuti, and Bekti Cahyo Hidayanto

Judul	**Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (DPTSI) ITS Surabaya**
Nama, Tahun	Basyarahil, Firzah Abdullah, Hanim Maria Astuti, and Bekti Cahyo Hidayanto (2017)
Gambaran umum penelitian	DPTSI merupakan sebuah direktorat untuk menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki oleh ITS. Semua kegiatan

	teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di DPTSI ITS. Salah satu upaya yang dapat dilakukan untuk meningkatkan kualitas dari keamanan informasi, kementrian Kominfo membuat alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Penggunaan Indeks KAMI ini juga diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Hasil penilaian tingkat ketergantungan TIK adalah sebesar 30 dari total keseluruhan 48, dan termasuk dalam kategori tinggi. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 252 dari total keseluruhan 588. Dengan ketergantungan TIK yang tinggi tersebut penilaian kelima area masih termasuk ke dalam kategori tidak layak. Untuk itu

	dibuatkan suatu rekomendasi perbaikan pada bagian-bagian yang masih kurang dari hasil penilaian indeks KAMI yang telah dilakukan.
Keterkaitan penelitian	Penelitian ini menggunakan Indeks KAMI versi 3.1. Dengan mengacu penelitian ini penulis dapat mempelajari buku buku yang menjadi referensi penulisan tugas akhir ini. Sedangkan Penulis menggunakan Indeks KAMI versi 4.1. Penelitian ini menggunakan objek penelitian di sector Pendidikan, Penulis meneliti tanpa studi kasus.

Tabel 2.3 Tabel Penelitian T. G. Trionggo

Judul	**T. G. Trionggo, Penyusunan Perangkat Checklist Kebutuhan Penerapan Sistem Manajemen Keamanan Informasi berbasis Standar ISO/IEC 27001:2013 dan Indeks KAMI 4.0**
Nama, Tahun	T. G. Trionggo (2020)
Gambaran umum penelitian	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.
Keterkaitan penelitian	Melakukan pembuatan checklist terkait tata kelola keamanan informasi dengan melakukan pemetaan ISO 27001:2013 ke Indeks KAMI 4.0. untuk implementasi SMKI. Pemetaan keterhubungan antara ISO 27001:2013 ke Indeks KAMI 4.0 dan metode penelitian yang digunakan menjadi referensi studi pustaka pendukung dan referensi pemetaan antara Kuisioner SPBE BSSN dan Indeks KAMI 4.1 pada pengerjaan penelitian ini.

Tabel 2.4 Tabel Penelitian Faridl Mughoffar

Judul	**Penyusunan Template Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005 dan Patuh Terhadap COBIT 5 Control Objective APO13 Manage Security**
Nama, Tahun	Faridl Mughoffar (2014)
Gambaran umum penelitian	Kebutuhan informasi yang akurat, cepat, serta reliable mengharuskan perusahaan menjaga keamanan informasi agar tidak mengganggu dan mempengaruhi peforma organisasi atau perusahaan. Dengan adanya kebutuhan tersebut, keamanan informasi harus dapat dikelola dengan baik. Pengelolaan keamanan informasi akan memperkecil munculnya risiko yang berkaitan dengan aspek keamanan informasi seperti kerusakan perangkat TI, kehilangan data karena pencurian dan risiko lainnya. Data kerugian yang diakibatkan oleh risiko keamanan informasi pun telah mencapai 1 miliar dollar US [1]. Untuk itu diperlukan tata kelola keamanan informasi yang melingkupi seluruh aspek

	keamanan informasi. Namun dengan padatnya aktivitas bisnis, organisasi atau perusahaan cenderung kesulitan untuk menyiapkan alat kerja dalam melakukan tata kelola keamanan informasi. Oleh karena itu jika melihat permasalahan tersebut maka diperlukan template dokumen yang diharapkan menjadi solusi dalam mempersiapkan tata kelola keamanan informasi dalam organisasi atau perusahaan. Pembuatan template tata kelola keamanan informasi akan berfokus dengan area pengamanan yang diambil dari standar COBIT 5 dan ISO/IEC 27001:2005, serta standar lain yang terkait.
Keterkaitan penelitian	Pemetaan ISO 27001:2005 ke COBIT 5 APO13 dan metode penelitian yang digunakan narasumber menjadi referensi studi pustaka pendukung dan referensi pemetaan pada pengerjaan Tugas Akhir Penulis.

`2.1.1 Kesimpulan dari penelitian-penelitian sebelumnya

Dengan membaca penelitian-penelitian sebelumnya, penulis dapat mengambil kesimpulan bahwa Pemetaan ISO 27001 dengan Indeks KAMI pernah dilakukan. Pemetaan Indeks KAMI dengan Kuisioner SPBE BSSN bukanlah hal yang mustahil karena persamaan dari badan pembuat dan salah satu domain pada kuisioner SPBE BSSN menggunakan pertanyaan yang tercantum dalam Indeks KAMI sebagai alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang digunakan sebagai gambaran keamanan informasi terkini sebuah Kementrian, Lembaga dan Pemda.

2.1.2 Posisi Penelitian Tugas Akhir Ini

Dari studi literatur yang telah penulis kumpulkan, **masih belum ada penelitian** tentang Pemetaan penerapan SMKI dengan Indeks KAMI versi terbaru, yaitu Indeks KAMI 4.1. yang diluncurkan bulan November 2019 **dengan** Kuisioner SPBE buatan BSSN edisi Agustus 2019.

Metode Pemetaan dan analisa pemetaan penerapan Sistem Manajemen Keamanan Informasi pada penelitian ini akan dilakukan dengan studi literatur.

2.2 Dasar Teori

Pada sub-bab ini berisikan dasar teori atas istilah-istilah ilmiah dan teori ilmiah dalam pengerjaan tugas akhir oleh penulis yang akan dijelaskan lebih lanjut.

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 proses produksi. Saat melakukan proses produksi akan ada perubahan dari nilai bahan baku menjadi nilai barang jadi[11].

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 [12].

Keamanan informasi terbagi menjadi 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[12]:

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 diakses oleh pengguna kapanpun, dimanapun dengan tanpa adanya hambatan serta tersampaikannya seluruh data informasi yang di akses secara utuh tanpa mengalami kerusakan sedikitpun.

Dalam keamanan informasi ada beberapa jenis fokus keamanan yang digunakan. Berikut jenis keamanan informasi:

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 Perusahaan, Organisasi atau Institusi harus menerapkan teknologi keamanan informasi, dengan menerapkan SMKI[13].

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 [14].

SMKI biasanya membahas perilaku dan proses karyawan serta data dan teknologi. Ini dapat ditargetkan pada tipe data tertentu, seperti data pelanggan, atau dapat diimplementasikan secara komprehensif yang menjadi bagian dari budaya Perusahaan, Organisasi atau Institusi [5].

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 [13]. Dalam model PDCA, semua proses SMKI dapat dipetakan seperti tabel berikut :

Tabel 2.5 Tabel 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 ISO/IEC 27001:2013 sebagai Standar SMKI

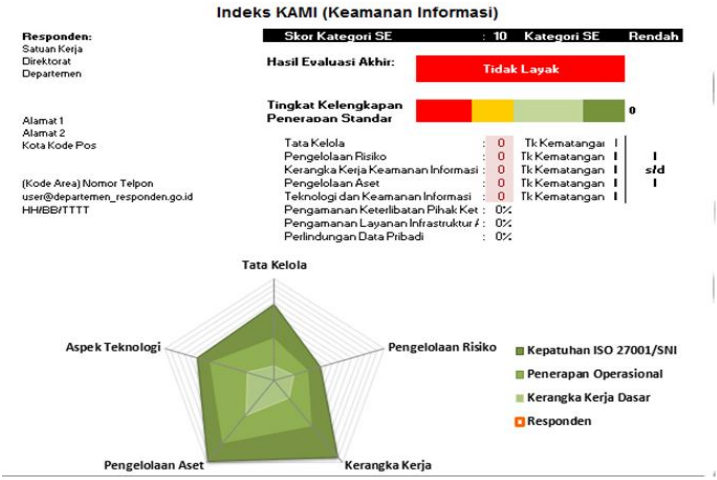
ISO/IEC 27001:2013 adalah sebuah standar yang dikeluarkan oleh *International Organization for Standardization*. ISO/IEC 27001:2013 merupakan standar yang membahas tentang spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) pada sebuah Perusahaan, Organisasi atau Institusi [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[12].

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[15].

2.2.5 Indeks KAMI 4.1

Indeks KAMI 4.1 yang diluncurkan November 2019 oleh BSSN, merupakan **suatu alat evaluasi tingkat kematangan dan tingkat kelengkapan** dalam penerapan SNI ISO/IEC 27001:2013 serta peta area tata kelola keamanan sistem informasi di suatu institusi pemerintah, namun bisa diterapkan pada Perusahaan, Organisasi dan Institusi baik Swasta maupun

Pemerintahan. 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 [7], yaitu :



Gambar 2.1 Dasboard Indeks KAMI 4.1 yang berisi diagram Area Evaluasi Indeks KAMI

Lima area yang digunakan untuk mengevaluasi tingkat kematangan pada SMKI milik Perusahaan, Organisasi atau Institusi 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[15].

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 Perusahaan, Organisasi atau Intitusi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi [7]. Pada bulan

Maret 2019 BSSN mengeluarkan 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, lalu pada November 2019 BSSN mengeluarkan Indeks KAMI versi terbarunya yaitu versi 4.1 dengan penambahan tabel nama dan nomor dokumen yang membedakannya [7].

Indeks KAMI 4.1 terdiri dari 7 modul yang berisi daftar pertanyaan-pertanyaan yang memberikan gambaran kondisi kerangka kerja keamanan informasi pada satu Perusahaan, Organisasi atau Intitusi yang diaudit [7].

I.Kategori Sistem Elektronik (SE) merupakan modul pertama pada dokumen evaluasi indeks KAMI 4.1. Kategori ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan. Terdapat tiga kategori hasil evaluasi yaitu rendah, tinggi, dan strategis.

II.Tata Kelola Keamanan Informasi pada modul kedua ini merupakan evaluasi tata kelola keamanan informasi yang dapat mempengaruhi data di Perusahaan, Organisasi atau Intitusi yang diaudit. Maka evaluasi pada kategori ini lebih menekankan pada **rencana** yang dipersiapkan untuk menanggulangi resiko terhadap ancaman keamanan informasi.

III.Pengelolaan Risiko Keamanan Informasi pada modul ketiga dilakukan evaluasi terhadap pengelolaan risiko keamanan informasi yang mencakup berbagai **risiko yang dapat tejadi dan berpengaruh** terhadap data informasi pada di Perusahaan, Organisasi atau Intitusi yang diaudit. Terdapat 4 kategori dalam evaluasi ini, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan/ penerapan sebagian dan diterapkan secara menyeluruh. Masing-masing kategori tersebut memilki skor 0, 1, 2, 3, 4, 6 yang terbagi sesuai dengan tingkat

kematangan yang telah ditentukan oleh indeks keamanan informasi KAMI 4.1.

IV.Kerangka Kerja Pengelolaan Keamanan Informasi pada modul ke empat yaitu evaluasi terhadap kerangka pengelolaan keamanan informasi yang menekankan pada persiapan dan kelengkapan kerangka kerja. Pada tahapan ini merupakan **tahapan realisasi dan evaluasi** dari tahap sebelumnya. Terdapat 29 pertanyaan yang memiliki empat kompnen penilaian, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, diterapkan secara menyeluruh dan dibagi menjadi 4 kategori kesiapan.

V.Pengelolaan Aset Informasi pada modul kelima ini dilakukan **evaluasi kelengkapan pengamanan aset informasi**, termasuk keseluruhan siklus penggunaan aset yang digunakan. Evaluasi pengelolaan asset informasi beberapa bagian memiliki pertanyaan mengenai aset inventaris yang akan dilaksanakan oleh Perusahaan, Organisasi atau Intitusi yang diaudit.

VI.Teknologi dan Keamanan Informasi **Evaluasi terhadap teknologi dan keamanan informasi** menekankan kepada bagian kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Beberapa elemen yang dievaluasi meliputi keamanan data pengguna informasi, jenis pengamanan, jenis sistem operasi yang digunakan pada Perusahaan, Organisasi atau Intitusi yang diaudit, keamanan jaringan komputer dan lain-lain yang terkait dengan mobilisasi data.

VII.Suplemen merupakan tahap tambahan yang dikembangkan oleh BSSN yang ditambahkan pertama kali di Indeks KAMI 4.1. Pada tahap ini terdapat **tiga golongan aspek** pendukung penilaian, yaitu evaluasi kesiapan pengamanan pihak ketiga, pengamanan

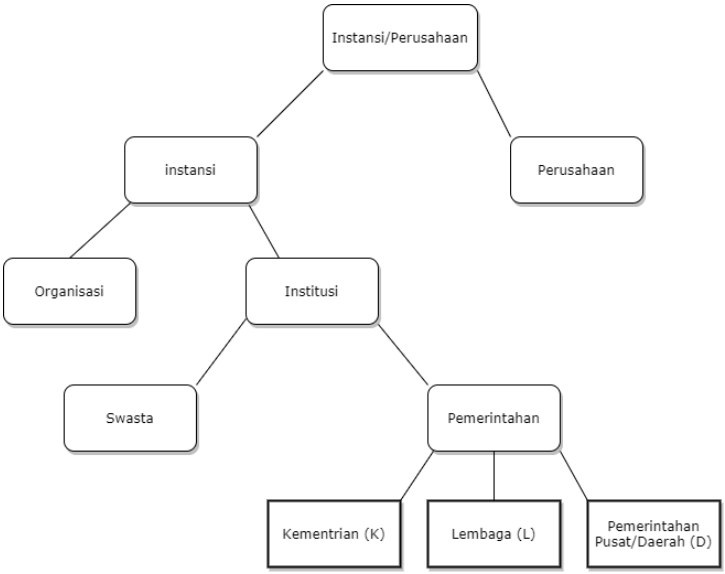
layanan infrastruktur awan/*cloud*, dan perlindungan data pribadi yang dinotasikan dalam persentase.

2.2.6 Kuisioner SPBE oleh BSSN

Berdasarkan Peraturan Presiden nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang akan **dilaksanakan oleh Kementrian/Lembaga/Pemerintahan Daerah (K/L/D),** Pemerintah Daerah yang dimaksud adalah Pemerintah Pusat dan Pemerintah Daerah. Jadi Pemerintah RI mempunyai **sistem informasi tersendiri** yang disebut Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE adalah sisitem penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi (TIK) untuk memberikan layanan kepada pengguna SPBE, yakni K/L/D, yang bertujuan mewujudkan tatakelola pemerintahan yang bersih, efektif, transparan, dan akuntabel. Serta meningkatkan efisiensi dan keterpaduan penyelenggaraan SPBE [8].

Dalam pelaksanaannya, SPBE diatur oleh Peraturan Kementrian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PERMENPANRB) nomor 5 tahun 2018, dalam melaksanakan SPBE, Kementrian PANRB yang ditunjuk sebagai ketua tim koordinasi SPBE Nasional dibantu oleh 6 Kementrian dan Badan tinggi negara, yaitu Kominfo, Kementrian Dalam Negeri, Kementrian Keuangan, Kementrian PPN/Bappenas, BPPT dan yang terakhir Badan Siber dan Sandi Negara (BSSN) [9].

BSSN sebagai anggota tim koordinasi SPBE Nasional, memiliki peran dalam melaksanakan SPBE Nasional, yaitu bertanggung jawab dalam penyusunan domain Arsitektur Keamanan SPBE, Memberikan pertimbangan dalam kelayakan Infrastruktur SPBE Nasional, Menerapkan Keamanan SPBE, Manajemen Keamanan SPBE dan Melakukan Fungsi Audit Keamanan SPBE Nasional [9].



Gambar 2.2 Diagram Pembagian Instansi/ Perusahaan di Indonesia

BSSN yang merupakan anggota Tim koordinasi SPBE Nasional dan dalam melaksanakan perannya dalam tim telah menyusun sebuah formulir berupa Kuisioner SPBE yang berfungsi sebagai alat batu dalam penyusunan pedoman tata kelola dan manajemen keamanan informasi penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE). Untuk selanjutnya Penulis akan menyebutnya sebagai **"Kuisioner SPBE BSSN"** Edisi Agustus 2019 [16].

Kuisioner SPBE BSSN terdiri dari 4 (Empat) Domain, yaitu :

1. Proses Bisnis Teknologi Informasi dan Komunikasi (TIK)

2. Data Center

3. Arsitektur Keamanan TIK

4. Audit TIK

Atas 4 Domain di atas terdiri dari 106 pertanyaan [16].

Berikut merupakan hubungan antara Kuisioner SPBE BSSN dengan Pertanyaan yang sesuai dengan Indeks KAMI 4.1 [7]:

Kuisioner SPBE BSSN yang penulis petakan dan verifikasi adalah Domain Nomor 1, 3 dan 4 sedangkan Indeks KAMI 4.1 yang penulis petakan dan verifikasi adalah Area penilaian Nomor II, III, IV, V, VI dan Suplemen.

Dari hasil pemetaan dan verifikasi penulis, 3 domain Kuisioner SPBE BSSN dan 6 area penilaian inilah yang dipakai dalam Analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1 Tugas Akhir ini.

Penulis mengesampingkan Domain ke 2 (Data Center) SPBE BSSN dan Area penilaian Indeks KAMI 4.1 ke-I (Kategori SE) karena jenis pertanyaan yang diajukan terlalu teknis, subjektif dan tidak terstandar.

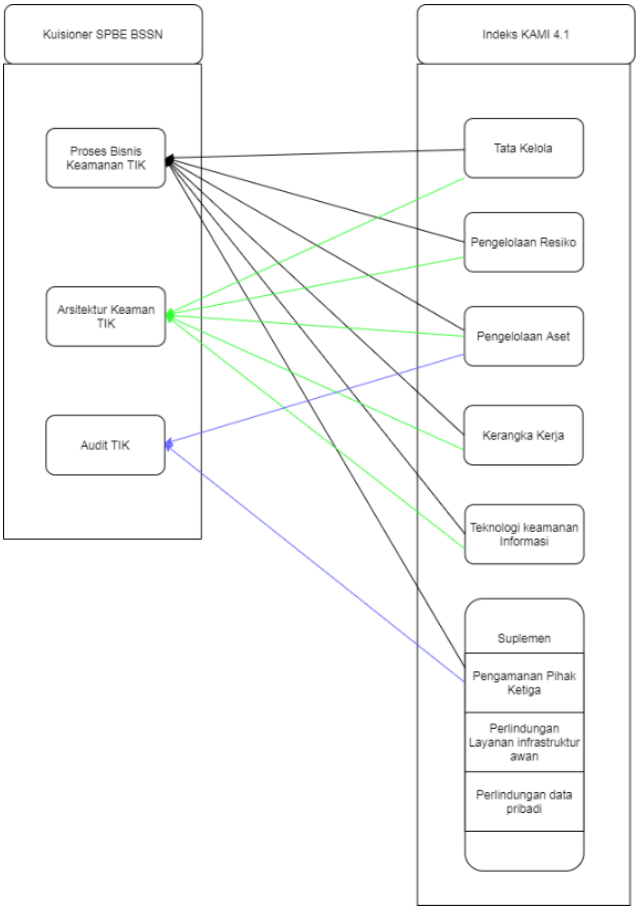
2.2.7 Tinjauan Analisa Pemetaan

Tinjauan pada Analisa Pemetaan, ini digunakan sebagai alat bantu penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang merupakan hasil dari studi literatur dari hasil pemetaan yang dibuat sebelumnya yang pernah dibuat oleh penelitian sebelumnya. Tinjauan ini memberikan gambaran konten dari *output* analisis pemetaan penerapan sistem manajemen keamanan informasi yang akan dibuat pada penelitian Tugas Akhir ini [3].

Berdasarkan pemetaan pada penelitian sebelumnya, peneliti tersebut memetakan ISO/IEC 27001: 2013 dengan Indeks KAMI 4.0 dengan menilai seberapa dekatnya hubungan pertanyaan Indeks KAMI dengan Kontrol ISO 27001:2013 [3].

Dalam penelitian tugas akhir ini pemetaan akan terlihat dari pertanyaan mana yang dipakai oleh Kuisioner SPBE BSSN dan merupakan pertanyaan Indeks KAMI, serta pertanyaan yang paling mendekati dari segi keterikatan inti pertanyaan.

Pada gambar berikut, Penulis membuat diagram pemetaan antara 3 domain Kuisioner SPBE BSSN dan 6 area penilaian Indeks KAMI 4.1



Gambar 2.3 Pemetaan Kuisioner SPBE-BSSN dengan Indeks KAMI 4.1

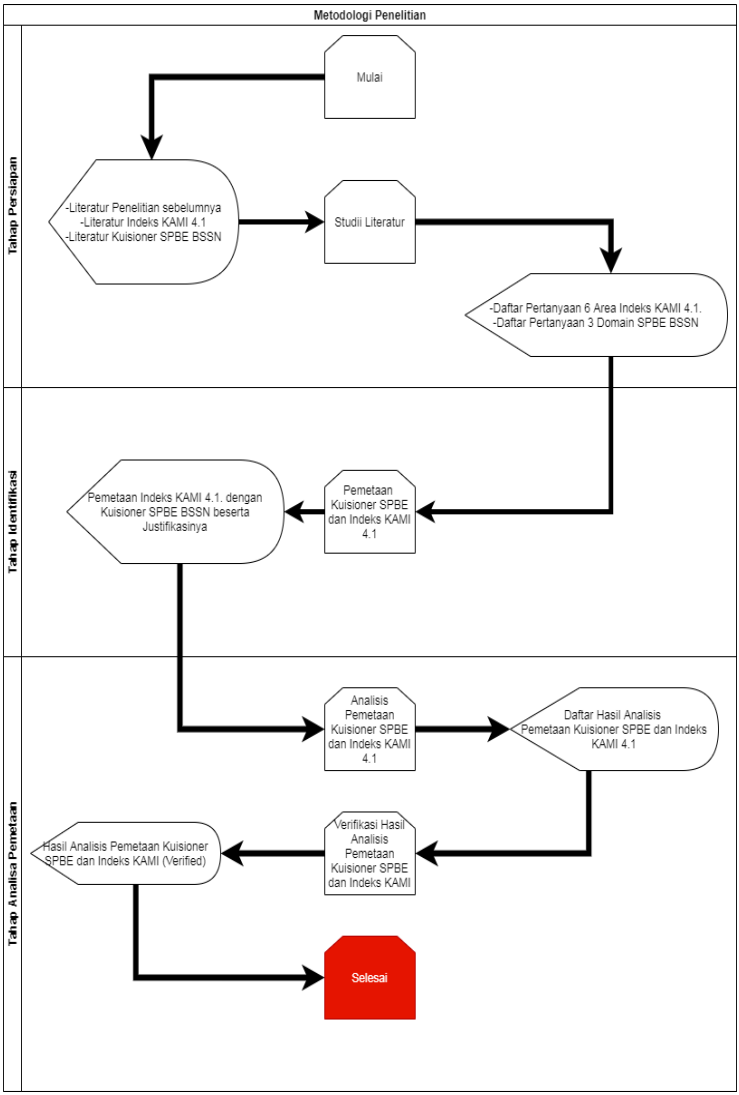
Halaman ini sengaja dikosongkan

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 bab ini menggambarkan metodologi yang akan digunakan sekaligus berisi gambaran rencana pengerjaan dan uraian. Berikut ada 3 tahapan. Tahapan pengerjaan dimulai dari studi literatur sampai tahap Analisis Pemetaan. Pengerjaan tugas akhir ini akan menghasilkan sebuah Daftar analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI untuk membantu K/L/D menerapkan Sistem Manajemen Keamanan Informasi (SMKI) atau mempersiapkan pengisian Kuisioner SPBE BSSN.



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 4.1 dan hubungan Indeks KAMI versi 4.1 dengan Kuisioner SPBE BSSN edisi Agustus 2019 juga dibahas dalam studi literatur ini. Pada tahap ini juga dikumpulkan literatur-literatur yang berhubungan dengan penelitian tugas akhir ini seperti buku, jurnal, sumber data dari internet dan penelitian-penelitian sebelumnya.

Tabel 3. 1 Studi Literatur

Input	Proses	Output
• Literatur penelitian sebelumnya • Literatur Indeks KAMI versi 4.1 • Literatur Kuisioner SPBE BSSN edisi Agustus 2019	Studi literatur	• Daftar Pertanyaan Indeks KAMI Versi 4.1 • Daftar Pertanyaan Kuisioner SPBE BSSN

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 Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1

Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1 pada tahap ini diawali dengan memetakan pertanyaan hasil studi literatur Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1 yang merupakan hasil studi literatur Kuisioner SPBE BSSN dan Indeks KAMI 4.1. Pemetaan ini dilakukan karena terdapat hubungan antara keduanya berdasarkan hasil studi literatur hubungan Indeks KAMI dan Kuisioner SPBE BSSN. Hubungan yang dimaksud yaitu pembahasan tentang keamanan informasi yang sama antara pertanyaan pada indeks KAMI dan Kuisioner tersebut. Output pemetaan ini adalah terpetakannya 184 pertanyaan-pertanyaan dari 6 (enam) area penilaian yang ada pada Indeks KAMI 4.1 ke dalam 69 pertanyaan-pertanyaan dalam 3 (tiga) domain yang ada pada Kuisioner SPBE BSSN. Hasil pemetaan ini akan diverifikasi pada aktivitas selanjutnya untuk mempermudah analisis pada tahap selanjutnya.

Tabel 3.2 Pemetaan Indeks KAMI versi 4.1 dengan Indeks Kuisioner SPBE BSSN

Input	Proses	Output
• Daftar pertanyaan 6 area Indeks KAMI versi 4.1 • Daftar pertanyaan 3 Domain Kuisioner SPBE BSSN edisi Agustus 2019	Pemetaan Indeks KAMI versi 4.1 dengan Indeks Kuisioner SPBE BSSN	Hasil Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1

3.2.3 Tahap Analisis Pemetaan

Tahapan ini merupakan tahapan dimana penulis menyusun Analisis pemetaan yang merupakan hasil identifikasi pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1.

3.2.3.1 Penyusunan Analisis Pemetaan dengan Indeks Kuisioner SPBE dan Indeks KAMI versi 4.1

Pada tahapan ini dilakukan penyusunan Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 untuk penerapan Sistem Manajemen Keamanan Informasi (SMKI) sebagai solusi dalam menerapkan Sistem Manajemen Keamanan Informasi (SMKI). Penyusunan Analisis Pemetaan mengacu pada hasil Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1 beserta justifikasi dari pemetaan diatas. Output dari aktivitas ini adalah daftar analisis Pemetaan yang berisi hasil dan manfaat dari setiap pemetaan penerapan SMKI

dimana pada aktivitas selanjutnya daftar ini akan di verifikasi ke objek studi kasus K/L/D untuk membantu pengisian Kuisioner.

Tabel 3.3 Hasil Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1

Input	Proses	Output
• Daftar Hasil Pemetaan Indeks KAMI versi 4.1 dengan Indeks Kuisioner SPBE BSSN edisi Agustus 2019 • Hasil literatur Analisis Pemetaan	Penyusunan Analisis Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1	Daftar Analisis Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1

3.2.3.2 Verifikasi Hasil Analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1

Pada tahapan ini, setelah daftar analisis pemetaan disusun maka akan dilakukan verifikasi pada perangkat tersebut.

Verifikasi dilakukan dengan melakukan kesesuaian antara kebutuhan dan hasil pemetaan Kuisioner SPBE-BSSN dan Indeks KAMI 4.1. Output dari aktivitas ini adalah Hasil Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI yang telah terverifikasi dan siap digunakan oleh K/LD sebagai alat bantu pengisian Kuisioner yang akan diuji sebagai objek studi kasusnya.

Tapi hasil verifikasi analisis pemetaan ini TA ini tidak ada hasilnya. Hal ini dikarenakan penulis melakukan penyusunan Tugas Akhir dalam keadaan dan kondisi Pandemi Covid-19 yang melanda Dunia, khususnya di Indonesia, yang tidak memungkinkan penulis melakukannya dengan objek studi kasus.

Tabel 3. 4 Verifikasi Hasil Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI

Input	Proses	Output
Daftar Analisis Pemetaan Kuisioner SPBE BSSN ke Indeks KAMI Versi 4.1	Verifikasi Hasil Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI	Hasil Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI 4.1 (Verified)

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Tujuan tugas akhir ini adalah menghasilkan Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI 4.1. Untuk mencapai tujuan tersebut, maka pada bab perancangan ini akan dijelaskan tentang perancangan dari penggalian data, identifikasi data dan output untuk menghasilkan Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI 4.1. yang berguna dalam membantu pengisian kuisioner SPBE BSSN bagi K/L/D.

4.1 Penggalian Data

Pada perancangan penggalian data akan dijelaskan tentang data yang dibutuhkan dan metode pengumpulan data. Pengumpulan data ini untuk mengidentifikasi kebutuhan bagi organisasi yang menerapkan sistem manajemen keamanan informasi pada Perusahaan, Organisasi atau Institusi 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 diperlukan

Tujuan Penggalian data	Metode Penggalian Data
Mengetahui daftar pertanyaan Indeks KAMI versi 4.1	Studi Dokumen
Mengetahui daftar Pertanyaan Kuisioner SPBE BSSN edisi Agustus 2019	Studi Dokumen
Mengetahui hubungan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1, hasilnya	Studi Dokumen

Tujuan Penggalian data	Metode Penggalian Data
adalah Pemetaan hubungan antara keduanya.	

4.2 Identifikasi Data

Pada perancangan ini akan dilakukan identifikasi data dari data yang telah dikumpulkan. Identifikasi data ini bertujuan untuk mendapatkan data-data baru untuk menunjang penelitian tugas akhir ini. Data-data tersebut antara lain hasil identifikasi pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1,. Identifikasi data dilakukan berdasarkan metode penggalian data.

4.2.1 Identifikasi Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1

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 4.0 berdasarkan ISO/IEC 27001:2013 yang telah dilakukan penelitian sebelumnya. Adapun daftar klausul pada ISO/IEC 27001:2013 dan daftar pertanyaan di 6 area Indeks KAMI versi 4.0 [3].

Studi dokumen merupakan metode penggalian data melalui studi literatur untuk mendapatkan informasi terkait penelitian. Dari studi dokumen yang dilakukan penulis akan mendapatkan informasi terkait hubungan Indeks KAMI 4.1 dengan Kuisioner SPBE BSSN yang didapatkan berdasarkan metodologi penelitian sebelumnya. Informasi yang didapatkan adalah hasil pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1 beserta justifikasi yang menghubungkan antara dua faktor tersebut.

Tabel 4. 2 Hasil Pemetaan

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi
ARSITEKTUR TIK			
9	Apakah dikantor Bapak sudah ada pedoman untuk proses management keamanan aplikasi, proses keseluruhan dalam mengelola keamanan pada setiap aplikasi spesifik ?	6.3	pertanyaan tersebut merepresentasikan kebutuhan terkait konfigurasi standar keamanan sistem yang mutakhirkan sesuai perkembangan dan kebutuhan untuk seluruhan aset jaringan, sistem dan aplikasi

4.3 Solusi

Pada perancangan solusi ini akan dilakukan Analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1. Perangkat yang disusun merupakan hasil dari penelitian yang dilakukan penulis. Analisa Pemetaan ini disususn berdasarkan metodologi pada bab sebelumnya dengan menggunakan data yang telah diperoleh dari tahapan sebelumnya.

4.3.1 Hasil Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1

Setelah melakukan pemetaan langkah selanjutnya adalah menyusun Hasil analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1. yang dibuat mempunyai beberapa item di dalamnya. Tiga (3) item yang ada di dalamnya antara lain Nomor, Kebutuhan dan Manfaat. Berikut merupakan rancangan dari daftar analisis pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1:

Tabel 4. 3 Daftar hasil analisis pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1

Hasil Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
1	Definisi peran dan tanggung jawab keamanan	Menunjukan peran apa saja yang dibutuhkan dalam tupoksi kerja keamanan Informasi.

4.3.2 Verifikasi Hasil Analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1

Langkah selanjutnya adalah verifikasi, dimana verifikasi yang dilakukan untuk Hasil Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI 4.1 adalah penyesuaian isi Hasil Analisa dengan kegiatan lapangan untuk membantu K/L/D mengisi Kuisioner SPBE BSSN maupun mempersiapkan penerapan SMKI. Proses verifikasi ini dilakukan melalui daftar Analisis hasil pemetaan Indeks KAMI versi 4.1 dengan Kuisioner SPBE BSSN. Pada hasil analisis tersebut akan terlihat ketersesuaian penerapan SMKI di K/LD yang menjadi objek studi kasus sebagai alat bantu pengisian Kuisioner SPBE BSSN.

Namun untuk hasil verifikasi Analisis Pemetaan dalam TA ini tidak ada hasilnya. Hal ini dikarenakan penulis melakukan penyusunan Tugas Akhir dalam keadaan dan kondisi Pandemi Covid-19 yang melanda Dunia, khususnya di Indonesia, yang tidak memungkinkan penulis melakukannya dengan objek studi kasus.

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.

5.1 Daftar Pertanyaan Kuisioner SPBE BSSN edisi Agustus 2019

Berdasarkan bab perancangan dilakukan penggalian data dengan cara studi dokumen pada salah satu penelitian sebelumnya tentang penilaian Indeks KAMI pada DPTSI ITS didapatkan cara memetakan Indeks KAMI dengan ISO/IEC 27001:2013 [16]. Namun Pemetaan yang akan penulis buat adalah Identifikasi pemetaan dari Kuisioner SPBE BSSN edisi Agustus 2019 dan Indeks KAMI 4.1. Pemetaan ini bisa dilakukan karena pertanyaan pada Kuisioner SPBE BSSN dan Indeks KAMI versi 4.1 **sama-sama membahas tentang keamanan informasi** dan pembuatnya adalah badan negara yang sama, yaitu BSSN. Daftar pertanyaan Kuisioner SPBE BSSN yang telah didapatkan dari penggalian data dengan cara studi dokumen dapat dilihat pada **LAMPIRAN A**. Dari **LAMPIRAN A** tersebut diketahui bahwa terdapat 69 buah pertanyaan dari 3 Domain penilaian.

5.2 Daftar Pertanyaan Indeks KAMI Versi 4.1

Berdasarkan perancangan penggalian data pada bab sebelumnya daftar pertanyaan Indeks KAMI 4.1 terdapat 184 buah pertanyaan dari 6 area pada Indeks KAMI versi 4.1. Daftar Pertanyaan ini akan digunakan untuk melihat keterhubungan antara Indeks KAMI 4.1 dan Kuisioner SPBE BSSN. Dimana dapat dilihat pada **LAMPIRAN B**.

5.3 Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1

Pada bab sebelumnya yaitu perancangan telah dilakukan penggalian data tentang hubungan pemetaan Kuisioner SPBE

BSSN dengan Indeks KAMI versi 4.1. Pemetaan ini dilakukan karena pertanyaan Kuisioner SPBE BSSN memiliki bahasan yang sama dengan Indeks KAMI versi 4.1. yaitu tentang keamanan informasi dan pempunyai kesamaan yang lain, yaitu sama-sama dibuat oleh BSSN. Kesamaan inilah membuat Indeks KAMI 4.1 dapat dipetakan dengan Kuisioner SPBE BSSN. Hasil dari penggalian data ini adalah Pemetaan antara Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1, dimana semua pertanyaan yang ada di dalam Kuisioner SPBE BSSN memiliki potensi dapat dipetakan ke dalam pertanyaan yang ada pada Indeks KAMI versi 4.1. Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1 dapat dilihat pada **LAMPIRAN C.**

Dari **Pemetaan** Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1 yang ada pada **LAMPIRAN C**, diketahui bahwa semua pertanyaan dari 69 pertanyaan pada tiga (3) Domain Kuisioner SPBE BSSN dapat terpetakan pada enam (6) area Indeks KAMI 4.1. Sedangkan pada Indeks KAMI versi 4.1. terdapat 48 pertanyaan sebagai irisan dari total 184 pertanyaan Indeks KAMI versi 4.1 yang terpetakan pada pertanyaan Kuisioner SPBE BSSN. Berdasarkan hasil pemetaan maka identifikasi kebutuhan penerapan sistem manajemen keamanan informasi dapat diambil melalui penerjemahan pertanyaan yang ada pada Indeks KAMI versi 4.1.

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 Hasil Analisa Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1

Pada tahapan ini akan dilakukan identifikasi kebutuhan penerapan SMKI. Indentifikasi dilakukan dengan cara menerjemahkan pertanyaan yang ada pada Indeks KAMI 4.1 menjadi kebutuhan dari penerapan sistem manajemen keamanan informasi. Pertanyaan yang diterjemahkan menjadi kebutuhan adalah pertanyaan yang terpetakan dengan Kuisioner SPBE BSSN. Untuk pertanyaan yang tidak terpetakan juga akan diambil kebutuhannya karena Indeks KAMI 4.1 sendiri harus diisi semua pertanyaannya untuk mengetahui hasil evaluasi penerapan dan tingkat kematangan SMKI agar sesuai dengan implementasi kontrol ISO/IEC 27001:2013. Berikut merupakan hasil identifikasi yang dilakukan penulis pada penelitian tugas akhir ini dimana dari identifikasi yang dilakukan, terdapat Hasil pemetaan dari **69 Pertanyaan Kuisioner SPBE BSSN dengan 184 Pertanyaan Indeks KAMI 4.1.**

Pada identifikasi pemetaan Kuisioner SPBE BSSN terdapat 48 kebutuhan yang terpetakan dengan Indeks KAMI 4.1 ditandai dengan **warna Hijau** dan 21 kebutuhan sisanya adalah pertanyaan kuisioner SPBE BSSN yang terpetakan dengan Indeks KAMI 4.1 yang muncul lebih dari satu kali pemetaannya, ditandai dengan **warna Kuning**. Sedangkan 136 kebutuhan berasal dari pertanyaan Indeks KAMI 4.1 yang tidak terpetakan pada kuisioner SPBE BSSN ditandai dengan **warna Biru**. Jadi, **total keseluruhan Kebutuhan** untuk penyusunan **Analisis pemetaan adalah 205 Kebutuhan**, yang diagramnya dapat dilihat pada **LAMPIRAN D.** Berikut adalah detail 205 kebutuhan penerapan SMKI dalam bentuk tabel:

Pada tahapan ini akan dilakukan analisa dari hasil pemetaan yang telah didapatkan sebelumnya, sejumlah 205 kebutuhan yang terbagi atas 48 Indeks KAMI 4.1 yang terpetakan (Hijau) dan 21 adalah sisa yang terpetakan lebih dari satu kali (Kuning) dan bila tergabung sejumlah 69, seperti jumlah hasil pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1. Sedangkan 136 adalah pertanyaan Indeks KAMI 4.1 yang tidak terpetakan pada kuisioner SPBE BSSN (Biru) dimana 136 hasil tersebut dipakai sebagai alat bantu penerapan SMKI bagi K/L/D yang mau menerapkan SMKI.

Analisa Pemetaan 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 yang mendasari pembuatan Indeks KAMI dan Kuisioner SPBE BSSN. Semakin banyak klausul, dalam hal ini diterapkan kedalam bentuk *list* kebutuhan, yang diterapkan semakin tinggi tingkat kematangan penerapan SMKI pada sebuah K/L/D.

Analisis Hasil Pemetaan ini berisi daftar dari kebutuhan penerapan SMKI. Berikut adalah deskripsi dari setiap item yang ada pada daftar Analisis Pemetaan:

Tabel 6. 1 Daftar Item

No.	Item	Deskripsi
1	Nomor	Memberikan informasi tentang hal apa yang akan dilakukan yaitu pemeriksaan terkait kebutuhan penerapan SMKI
2	Kebutuhan	Berisi informasi kebutuhan hasil dari pemetaan dan Justifikasi Kuisioner SPBE BSSN dan Indeks KAMI untuk penerapan SMKI
3	Manfaat	Manfaat dengan adanya hasil Analisis Pemetaan

Berikut ini merupakan Hasil Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 yang dihasilkan dari penelitian ini:

Tabel 6. 2 Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
1	Definisi peran dan tanggung jawab keamanan	Menunjukan peran apa saja yang dibutuhkan dalam tupoksi kerja keamanan Informasi.
2	Definisi peran dalam pengelolaan keamanan informasi	Menunjukan peran pengelolaan dalam tupoksi kerja keamanan Informasi.
3	Perjanjian kontraktual antara pejabat/petugas pelaksana keamanan informasi terhadap peran yang ditentukan	Membuat sebuah kontrak yang mampu mengikat pekerja dalam peran yang di alokasikan pada pekerja terpilih.
4	Pemantauan, pengaturan dan prediksi terkait alokasi penggunaan sumber daya untuk pengelolaan dan jaminan kepatuhan program keamanan informasi	Melihat hasil Pemantauan, pengaturan dan prediksi penggunaan sumber daya pengelolaan dan jaminan Keamanan Informasi.
5	Penerapan program Sosialisasi dalam peningkatan pemahaman Keamanan Informasi termasuk kepatuhan bagi pihak terkait	Meningkatkan pemahaman Keamanan Informasi bagi Pegawai K/L/D.

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
6	Penerapan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi	Training untuk peningkatan kemampuan Pejabat dan pelaksana pengelola keamanan informasi.
7	Persyaratan keamanan informasi melalui kerangka kerja yang dibangun untuk mengendalikan pelaksanaan dan pengoperasian keamanan informasi	Kebijakan ini mampu memberikan syarat-syarat yang membantu pengoperasian dan pelaksanaan Keamanan Informasi sehingga berjalan dengan baik.
8	Daftar Log Aktifitas Pengguna	Mencatat segala aktivitas pengguna yang masuk maupun keluar dalam sistem secara aktual.
9	Analisis Dampak Bisnis (*Business Impact Analysis*)	Memberikan analisis terkait penggunaan Keamanan Informasi yang terkait dengan proses bisnis Instansi.
10	Definisi kebijakan dan prosedur penanggulangan insiden keamanan informasi	Memberikan kamus definisi terhadap Kebijakan dan prosedur penanggulangan insiden Keamanan Informasi.
11	Analisis aspek keamanan informasi dalam manajemen proyek yang terkait	Memberikan Analisis dampak Keamanan Informasi terhadap Manajemen Proyek

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	ruang lingkup Perusahaan	
12	Definisi Klasifikasi Resiko Informasi	Kamus Definisi hal-hal yang menjelaskan hubungan Klasifikasi Resiko dari Informasi yang dimiliki K/L/D.
13	Definisi peran dalam kepemilikan dan pihak pengelola aset informasi	Kamus Definisi yang memperjelas Peran Pemilik dan Pengelola Aset Keamanan Informasi terkait K/L/D
14	Daftar klasifikasi dampak kerugian hilangnya sebuah aset	Memberikan daftar klasifikasi dampak kerugian hilangnya aset perusahaan dari yang paling tinggi sampai yang paling rendah
15	Daftar analisa resiko Aset informasi	Menampilkan Daftar hasil analisa Resiko tiap Aset Informasi, untuk mengetahui perbedaan resiko antar aset.
16	Daftar prosedural dalam analisa resiko Aset informasi	Menampilkan Daftar prosedur analisa Resiko tiap Aset Informasi, untuk menganalisa resiko yang dimiliki tiap aset.
17	Revisi Analisis Profil resiko secara berkala	Daftar revisi ini merupakan dokumen hasil Revisi Profil resiko keamanan Informasi yang di revisi berkala, sehinggan mampu

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
		menunjukan perubahan periodik Resiko K/L/D.
18	Daftar Kebijakan, Prosedur dan Dokumen terkait Keamanan Informasi Perusahaan, Organisasi dan Institusi	Dokumen ini mendaftarkan semua Kebijakan, Prosedur, dan Dokumen terkait Keamanan Informasi K/L/D
19	Definisi dan penegakan konsekuensi pelanggaran kebijakan	Konsekuensi/Hukuman/Denda yang berlaku pada para pelanggar kebijakan Keamanan informasi sebagai efek jera
20	Kerangka rencana berjangka pengelolaan keberlangsungan layanan IT	Rangka perancanaan tujuan pengelolaan layanan IT SPBE pada K/L/D dalam waktu tertentu sebagai arah tujuan SPBE
21	Prosedur proses evaluasi resiko terkait pengadaan barang	Prosedur ini membantu penyusunan Proses evaluasi Resiko pengadaan barang terkait Keamanan Informasi
22	Prosedur Audit Internal Keamanan Informasi	Prosedur ini memberikan tata cara mengaudit internal Keamanan Informasi K/L/D
23	Kerangka rencana berjangka peningkatan keamanan informasi secara berkala	Rangka perancanaan peningkatan Keamanan IT SPBE pada K/L/D dalam waktu tertentu sebagai cara pengamanan Aset informasi K/L/D

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
24	Daftar Inventori aset	Mampu membuat dokumen daftar semua aset IT yang dimiliki oleh K/L/D agar tidak hilang/ tercecer
25	Prosedur proses perubahan sistem proses bisnis dan proses teknologi	Prosedur ini membantu penyusunan Proses sistem proses bisnis dan proses teknologi agar dapat menyelaraskan dengan Keamanan informasi yang terimplemetasi
26	Prosedur proses pelaporan insiden keamanan terhadap pihak berwenang	Prosedur ini membantu penyusunan Proses pelaporan insiden secara sistematis
27	Prosedur pengamanan fasilitas fisik	Prosedur ini membantu pelaksanaan tata cara pengamanan fasilitas fisik
28	Perjanjian pengamanan pengiriman aset informasi pada pihak ke tiga	Perjanjian ini adalah perjanjian dengan pihak ketiga yang membatu kita mebuat pengamanan pengiriman aset informasi.
29	Prosedur peraturan dan larangan dalam pengamanan fasilitas fisik	Memberikan tata cara dan pengamanan fasilitas fisik
30	Konfigurasi Standar keamanan sistem keseluruhan aset jaringan, sistem dan aplikasi	Dokumen ini memberikan Konfigurasi Standar keamanan sistem keseluruhan aset jaringan, sistem dan aplikasi yang dipakai oleh K/L/D

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
31	Analisa kepatuhan penerapan pengelolaan sistem informasi	Dokumen ini memberikan Hasil Analisa dari kepatuhan penerapan pengelolaan sistem informasi oleh pengelola.
32	Prosedur pengamanan lingkungan pengembangan uji coba siklus sistem	Prosedur ini memberikan pengamanan terhadap *environtment* sebelum menjadi tempat uji coba siklus sistem terbaru
33	Prosedur Audit keamanan informasi dengan pihak independen	Memberikan informasi terkait hal-hal yang harus dilakukan oleh K/L/D sebelum Audit dilakukan dengan ppihak independen
34	Analisa identifikasi resiko dengan pihak ketiga	Dokumen ini berisi hasil analisis Identifikasi resiko yang disusun dengan pihak ketiga sebagai pihak pembantu
35	Persyaratan Mitigasi Resiko dan ekspektasi oleh pihak ke-tiga	Dokumen ini memberikan persyaratan kepada pihak ketiga sebelum melakukan mitigasi resiko dan hal hal terkait dengan K/L/D agar pihak ke-tiga bisa mempersiapkan semua yang di persyaratkan oleh K/L/D
36	Kebijakan keamanan informasi untuk pihak ketiga	Kebijakan ini mampu memberikan arahan terhadap pihak ketiga untuk hak-hak yang mereka dapatkan dalam

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
		melakukan keamanan informasi terhadap K/L/D
37	Prosedur monitoring dan review pengelolaan layanan dan keamanan informasi oleh pihak ketiga	Prosedur ini memberikan arahan tata cara Montitoring dan review Pihak ke-tiga terhadap pengelolaan layanan dan keamanan informasi K/L/D
38	Prosedur pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi	Prosedur ini merangkum tata cara terkait pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi yang dibutuhkan oleh K/L/D
39	Prosedur Audit berkala oleh pihak ketiga	Prosedur ini memberikan ketentuan dan tata cara Audit berkala dengan pihak ketiga yang dikontrak.
40	Pedoman Keamanan Organisasi/Infrastruktur	Pedoman Arahan Keamanan Organisasi/Infrastruktur yang membantu KLD menentukan bentuk keamanan organisasi terkait infrastrukur
41	Pedoman Arsitektur Keamanan Informasi	Memberikan Arahan terhadap K/L/D terkait arsitektur yang dimiliki oleh Keamanan Informasi yang terimplementasi/ akan di integrasi

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
42	Pedoman Keamanan baseline dan Pengukuran Risiko	Memberikan Arahan terhadap keamanan mendasar dan indikator pengukuran resiko keamanan informasi
43	Pedoman Kepedulian Pengguna dan Training Keamanan	Menunjukan Arahan dan training bagi pengguna SPBE
44	Pedoman Kontrol Internal dan alokasi akses	Memberikan Arahan pada K/L/D untuk mengontrol internal sistem dan alokasi akses pada pengguna yang dituju
45	Pedoman untuk *overview* dan konsep keamanan aplikasi	Memberikan Arahan pada K/L/D tentang cakupan konsep keamanan SPBE
46	Pedoman untuk *framework* normative organisasi	Memberikan Arahan pada K/L/D dalam penyusunan rangka mormatif organisasi dalam lingkup K/L/D sebagai pengguna Keamanan Informasi.
47	Pedoman peran dalam pengelolaan keamanan informasi	Memberikan Arahan pada K/L/D terhadap Peran yang dialokasikan pada pegawainya dalam linkgkup keamanan informasi.
48	Pedoman untuk proses management keamanan aplikasi	Memberikan Arahan pada K/L/D dalam melakukan proses manajemen keamanan aplikasi SPBE

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
49	Pedoman untuk validasi dan sertifikasi keamanan aplikasi	Memberikan Arahan pada K/L/D dalam proses Validasi dan sertifikasi keamanan Aplikasi yang digunakan oleh pegawai
50	Pedoman untuk protokol dan struktur pengendalian data keamanan aplikasi	Memberikan Arahan pada K/L/D menyusun protokol dan struktur pengendalian data keamanan Aplikasi
51	Pedoman untuk keamanan aplikasi spesifik	Memberikan Arahan pada K/L/D untuk melakukan keamanan pada aplikasi yang tingkat resikonya tinggi
52	Pedoman untuk tinjauan dan konsep keamanan jaringan	Memberikan Arahan pada K/L/D berupa tinjauan dari keamanan Jaringan yang dipakai
53	Pedoman untuk Desain dan Implementasi Keamanan Jaringan	Memberikan Arahan pada K/L/D untuk Desain Implementasi Kemanan Jaringan yang sesuai dengan keadaan K/L/D
54	Pedoman referensi skenario jaringan untuk ancaman	Memberikan Arahan pada K/L/D untuk penyusunan scenario ancaman terhadap keamanan jaringan
55	Pedoman untuk keamanan komunikasi antar jaringan menggunakan keamanan gateway	Memberikan Arahan pada K/L/D untuk mengamankan jaringan komunikasi dengan keamanan gateway yang disetujui

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
56	Pedoman untuk keamanan komunikasi lintas jaringan menggunakan VPN	Memberikan Arahan pada K/L/D untuk memakai VPN sebagai bentuk pengamanan lintas jaringan VPN
57	Pedoman untuk keamanan akses *wireless IP network*	Memberikan Arahan pada K/L/D untuk memngimplementasikan keamanan pada *wireless IP Network.*
58	Pedoman Keamanan sistem penghubung konstituen/User	Memberikan Arahan pada K/L/D pada keamanan sistem penghubung antar user
59	Pedoman Keamanan sistem penghubung *service provider*	Memberikan Arahan pada K/L/D untuk mengamankan jaringan layanan
60	Pedoman Keamanan sistem penghubung *data owners*	Memberikan Arahan pada K/L/D untuki mengamankan hubungan data dengan pemiiliknya
61	Pedoman Keamanan sistem penghubung data *storage* (penyimpanan data)	Memberikan Arahan pada K/L/D untuk mengimplementasikan skema pengamanan penyimpanan data.
62	Prosedur Audit TIK internal secara berkala	Memberikan tata cara pada K/L/D dalam pelaksanaan Audit TIK Internal dalam waktu berkala.

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
63	Prosedur Audit TIK eksternal secara berkala	Memberikan tata cara pada K/L/D dalam pelaksanaan Audit TIK Eksternal dalam waktu berkala.
64	Pedoman pelaksanaan Audit TIK	Memberikan arahan pada K/L/D dalam penlaksanaan Audit
65	Manajemen program audit	Meberikan gambaran terhadap K/L/D dalam menerapkan manajemen program audit secara keseluruhan
66	Menerapkan standard hasil pelaksanaan tindak lanjut Audit	Membuat K/L/D menerapkan hasil Tindak Lanjut dari Audit TIK sesuai Standard.
67	Unit kerja khusus yang mengelola hasil temuan Audit TIK	K/LD membuat unit khusus terkait dengan hasil temuan Audit
68	Evaluasi auditor dan kompetensi	KLD mengevaluasi Auditor yang melaksanakan Audit Internal maupun External agar Audit mampu meningkatkan Kinerja SPBE
69	Sertifikasi manajemen sistem	K/L/D membekali dengan sertifikasi SMKI yaitu pemenuhan syarat ISO/IEC 27001:2013 sebagai standard SMKI.
70	Verifikasi Sertifikasi kompetensi bagi	K/L/D mendapatkan SDM yang benar-benar mampu

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	pelaksana pengamanan informasi	melaksanakan pengamanan informasi dalam jajaran pegawainya
71	Persyaratan integrasi keamanan informasi kedalam proses kerja	K/L/D dapat dengan mudah mengintegrasi keamanan informasi kedalam proses kerja
72	Prosedur koordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan	K/L/D mendapat arahan untuk mebangun koordinasi Satker (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan, bila terjadi pelanggaran/pembobolan.
73	Prosedur melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara berkala	pimpinan K/L/D secara berkala mendapatkan hasil dari kondisi kerja efektifitas dan kepatuhan program keamanan informasi
74	Prosedur proses pengambilan keputusan strategis berdasarkan keadaan keamanan informasi	Pimpinan K/L/D memiliki cara proses pengambilan keputusan strategis yang selaras dengan Keadaan Keamanan informasi terkini
75	Kebijakan program aturan tujuan dan sasaran kepatuhan	K/L/D memiliki kebijakan peyusunan aturan tujuan dan sasaran demi

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	pengamanan aset informasi	kepatuhan pengamanan aset informasi
76	Definisi metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi	K/L/D memiliki definisi metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi
77	Kebijakan program penilaian kinerja pengelolaan keamanan informasi bagi individu	K/L/D memiliki kebijakan yang mampu menilai kinerja individual terkait pengelolaan keamanan informasi yang dilakukan oleh individual tersebut sebagai bahan introspeksi.
78	Identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi	K/L/D memiliki hal-hal yang terkait dengan legalitas perangkat keamanan informasinya
79	Dokumentasi program kerja pengelolaan risiko keamanan informasi	K/L/D memiliki Dokumentasi program kerja yang pernah atau akan dilakukan demi pengelolaan risiko keamanan informasi
80	Struktur penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi	K/L/D memiliki Struktur penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi
81	Dokumentasi kerangka kerja pengelolaan risiko keamanan informasi	K/L/D memiliki Dokumentasi Kerangka kerja yang digunakan sebagai pengelolaa resiko

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
82	Kebijakan penetapan ambang batas tingkat risiko	K/L/D memiliki Peraturan terkait Batasan tingkat resiko
83	Dokumen ancaman dan kelemahan aset informasi terkait	K/L/D memiliki Dokumentasi Ancaman dan kelamahan Aset yang dimiliki untuk memitigasi resiko.
84	Prosedur mitigasi dan penanggulangan risiko	K/L/D memiliki tatacara memitikgasi dan menaggulangi resiko
85	Dokumentasi status penyelesaian langkah mitigasi risiko	K/L/D memiliki dokumentasi status penyelesaian langkah mitigasi.
86	Kebijakan evaluasi objektif prosedur mitigasi resiko	K/L/D memiliki memiliki aturan yang mengevaluasi hasil dari tiap resiko yang dikerjakan
87	Kebijakan pengkajian berkala efektifitas kerangka kerja pengelolaan risiko	K/L/D memiliki peraturan pengkajian efektifitas pengelolaan resiko secara berkala.
88	Kebijakan memasukan pengelolaan risiko menjadi bagian dari kriteria proses penilaian objektif kinerja efektifitas pengamanan	K/L/D memiliki peraturan untuk memasukan pengelolaan risiko menjadi bagian dari kriteria proses penilaian objektif kinerja efektifitas pengamanan
89	Kebijakan publikasi formalitas keamanan informasi	K/L/D mampu mempublikasikan fkeamanan informasi yang dimiliki secara formal

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
		demi penelitian atapun publisitas.
90	Mekanisme pengelolaan dokumen kebijakan dan prosedur keamanan informasi	K/L/D memiliki mekanisme dalam mengelola dokumen kebijakan dan prosedu untuk dapat di telaah sesuaikeadaan mendatang.
91	Prosedur komunikasi kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait	K/L/D memiliki tatacara mengkomunikasikan kebijakan keamanan informasi kepada semua pihak
92	Dokumentasi pelaksanaan kebijakan dan prosedur keamanan informasi berdasarkan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi	K/L/D memiliki dokumentasi pelaksanaan kebijakan dan prosedur keamanan informasi berdasarkan kebutuhan mitigasi kajian resiko yang ditelaah.
93	Prosedur identifikasi kondisi insiden keamanan informasi	K/L/D memiliki mekanisme dalam mengidentifikasi kondisi insiden keamanan informasi
94	Kebijakan pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK pada kontrak pihak ketiga	K/L/D memiliki kontrak dengan pihak ketiga teerkait pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK.

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
95	Prosedur pengelolaan suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi	K/L/D memiliki Prosedur pengelolaan sebuah hal yang dapat dikecualikan terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi
96	Kebijakan dan prosedur operasional implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan pelaporan	K/L/D mampu menerapkan monitoring security patch terbaru untuk aplikasi sebagai bentuk tanggung jawab terhadap K/L/D.
97	Definsi aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup	K/L/D mampu mendefinisikan aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkupnya
98	Kebijakan pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan	K/L/D mampu mengembangkan Secure SDLC dengan dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
99	Kebijakan penanganan konflik penerapan sistem baru terhadap kebijakan yang berlaku dan jadwal penyelesaiannya	K/L/D menangani konflik penerapan sistem baru terhadap kebijakan lama dan penyelesaiannya
100	Kebijakan definisi komposisi, peran, wewenang dan tanggungjawab tim perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*)	K/L/D mampu menunjuk pegawai sebagai komposisi, peran, wewenang dan tanggungjawab tim perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan)
101	Dokumentasi uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*)	K/L/D memiliki dokumentasi uji coba perencanaan pemulihan bencana IT yang di simulasikan.
102	kebijakan evaluasi prosedur perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) yang gagal	K/L/D punya rencana evaluasi evaluasi prosedur perencanaan pemulihan bencana terhadap layanan TIK.
103	Kebijakan Evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala	K/L/D memiliki Evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala
104	Kebijakan penyusunan strategi penerapan	K/L/D menerapkan aturan dalam penyusunan strategi

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	keamanan informasi sesuai hasil analisa risiko sebagai bagian dari rencana kerja organisasi	penerapan keamanan informasi sesuai hasil analisa risiko sebagai bagian dari rencana kerja organisasi
105	Persyaratan strategi penggunaan teknologi keamanan informasi	K/L/D memenuhi persyaratan strategi penggunaan teknologi keamanan informasi
106	Prosedur strategi penerapan keamanan informasi sebagai bagian dari pelaksanaan program kerja organisasi anda	K/L/D memiliki strategi penerapan keamanan informasi sebagai bagian dari pelaksanaan program kerja organisasi anda
107	Kebijakan audit internal keamanan informasi	K/L/D mengaudit internal Keamanan informasinya sendiri
108	Kebijakan hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan program peningkatan kinerja keamanan informasi	K/L/D melaporkan hasil aaudit internal kepada pimpinan K/L/D untuk menetapkan program peningkatan kinerja keamanan informasi
109	Prasyarat analisa aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya	K/L/D memenuhi Prasyarat analisa aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
110	Kebijakan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya)	K/L/D menguji dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya)
111	Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku	K/L/D mengklasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku
112	Prosedur mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset	K/L/D mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset
113	Definisi tingkatan akses klasifikasi aset informasi dan matriks	K/L/D mengklasifikasi tingkatan akses klasifikasi aset informasi dan matriks
114	Prosedur pengelolaan konfigurasi	K/L/D memiliki Prosedur pengelolaan konfigurasi aset IT
115	Prosedur perilisan aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi	K/L/D bisa mengatur perilisan aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi
116	Definisi tanggungjawab pengamanan informasi	K/L/D menerapkan tanggungjawab pengamanan informasi

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	secara individual untuk semua personil di instansi/perusahaan anda	secara individual untuk semua pegawai.
117	Kebijakan Tata tertib penggunaan komputer, email, internet dan intranet	K/L/D menerapkan Kebijakan Tata tertib penggunaan komputer, email, internet dan intranet
118	Kebijakan Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	K/L/D menerapkan Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI
119	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	K/L/D menerapkan Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan
120	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	K/L/D menerapkan Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
121	Prosedur Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya	K/L/D menerapkan Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya
122	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan	K/L/D menerapkan persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	otorisasi untuk menggunakan aset informasi	otorisasi untuk menggunakan aset informasi
123	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	K/L/D bisa menetapkan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
124	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	K/L/D K/L/D bisa menetapkan pertukaran data dengan pihak eksternal dan pengamanannya
125	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	K/L/D mampu melakukan penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
126	Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	K/L/D memiliki back-up dan uji coba pengembalian data (restore) secara berkala
127	Kebijakan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	K/L/D dapat melakukan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
128	Proses pengecekan latar belakang SDM	K/L/D mampu meng investigasi latar belakang SDM.

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
129	Prosedur penghancuran data/aset yang sudah tidak diperlukan	K/L/D mempunyai tata cara penghancuran data/aset yang sudah tidak diperlukan
130	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	K/L/D dapat mengkaji penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku
131	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.	K/L/D dapat melakukan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
132	Daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*	K/L/D memiliki Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup
133	Daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasi	K/L/D memiliki Daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasi
134	Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk	K/L/D melakukan Prosedur penggunaan perangkat pengolah informasi milik pihak

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	perangkat milik pribadi dan mitra kerja/ *vendor*) dengan memastikan aspek HAKI dan pengamanan akses	ketiga (termasuk perangkat milik pribadi dan mitra kerja/ vendor) dengan memastikan aspek HAKI dan pengamanan akses
135	Prosedur pengelolaan alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik	K/L/D melaksanakan Prosedur pengelolaan alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
136	Kebijakan perlindungan infrastruktur komputasi dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikan	K/L/D menerapkan perlindungan infrastruktur komputasi dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikan.
137	Kebijakan perlindungan infrastruktur komputasi dari gangguan pasokan listrik atau dampak dari petir	K/L/D memiliki back-up sebagai upaya perlindungan infrastruktur komputasi dari gangguan pasokan listrik atau dampak dari petir
138	Peraturan pengamanan perangkat komputasi milik instansi/perusahaan apabila digunakan di luar lokasi kerja resmi (kantor)	K/L/D menerapkan Peraturan pengamanan perangkat komputasi milik instansi/perusahaan apabila digunakan di luar lokasi kerja resmi (kantor)

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
139	Prosedur pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)	K/L/D memiliki tata cara pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)
140	Kebijakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) pada konstruksi ruang penyimpanan perangkat pengolah informasi	K/L/D merancang dan menentukan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) pada konstruksi ruang penyimpanan perangkat pengolah informasi
141	Proses inspeksi dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting	K/L/D menginspeksi dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting
142	Proses untuk mengamankan lokasi kerja dari	K/L/D memiliki Proses untuk mengamankan lokasi kerja dari

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan	keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan
143	Prosedur perlindungan dengan lebih dari 1 lapis pengamanan pada layanan TIK (sistem komputer) yang terhubung internet	K/L/D mebuat tata cara perlindungan dengan lebih dari 1 lapis pengamanan pada layanan TIK (sistem komputer) yang terhubung internet
144	Persyaratan ketersediaan keseluruhan infrastruktur jaringan, sistem dan aplikasi	K/L/Dmampu memenuhi Persyaratan ketersediaan keseluruhan infrastruktur jaringan, sistem dan aplikasi
145	Daftar log perubahan dalam sistem informasi	K/L/D memiliki Daftar log perubahan dalam sistem informasi
146	Daftar Log akses Sistem berdasarkan ID Pengguna	K/L/D memiliki Daftar Log akses Sistem berdasarkan ID Pengguna
147	Analisa Daftar Rekaman log secara berkala	K/L/D memiliki hasil analisis Daftar Rekaman log secara berkala
148	Kebijakan enkripsi perlindungan aset informasi	K/L/D mengimplementasikan enkripsi perlindungan aset informasi
149	Kebijakan standarisasi enkripsi	K/L/D menjalankan standarisasi enkripsi sesuai dengan standard yang digunakan

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
150	Kebijakan pengamanan untuk penggelolaan kunci enkripsi (termasuk sertifikat elektronik) dan siklus penggunaan	K/L/D memiliki pengamanan untuk penggelolaan kunci enkripsi (termasuk sertifikat elektronik) dan siklus penggunaan
151	Prosedur penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/ panjangnya dan penggunaan kembali password lama pada semua sistem dan aplikasi	K/L/D dapat penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/ panjangnya dan penggunaan kembali password lama pada semua sistem dan aplikasi
152	Kebijakan bentuk pengamanan berlapis pada pengelolaan sistem (administrasi sistem)	K/L/D bentuk pengamanan berlapis pada pengelolaan sistem (administrasi sistem)
153	Proses pembatasan waktu akses termasuk otomatisasi proses *timeouts, lockout* setelah kegagalan login,dan penarikan akses	K/L/D membatasi waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses
154	Kebijakan mendeteksi dan mencegah penggunaan akses jaringan (termasuk	K/L/D dapat mendeteksi dan mencegah penggunaan akses jaringan (termasuk

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	jaringan nirkabel) yang tidak resmi	jaringan nirkabel) yang tidak resmi
155	Kebijakan pembaharuan sistem operasi untuk setiap perangkat desktop dan server dengan versi terkini	K/L/D mengadakan pembaharuan sistem operasi untuk setiap perangkat desktop dan server dengan versi terkini
156	Prosedur perlindungan desktop dan server dari penyerangan virus (*malware*)	K/L/D memiliki Prosedur perlindungan desktop dan server dari penyerangan virus (malware)
157	Daftar Log rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa *antivirus/ antimalware* telah dimutakhirkan secara rutin dan sistematis	K/L/D menyimpan Daftar Log rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/ antimalware telah dimutakhirkan secara rutin dan sistematis
158	Prosedur penindaklanjutan dan penyelesaian laporan penyerangan virus/ *malware* yang gagal/sukses.	K/L/D memiliki tata cara penindaklanjutan dan penyelesaian laporan penyerangan virus/ malware yang gagal/sukses.
159	Prosedur mekanisme sinkronisasi waktu jaringan, sistem dan aplikasi	K/L/D memiliki mekanisme sinkronisasi waktu jaringan, sistem dan aplikasi
160	Kebijakan komunikasi dan klarifikasi risiko keamanan informasi yang ada pada pihak	K/L/D berkomunikasi dan klarifikasi risiko keamanan informasi yang ada pada pihak ketiga

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	ketiga kepada Perusahaan/Organisasi /Institusi	
161	Kebijakan persetujuan rencana mitigasi terhadap risiko yang diidentifikasi oleh manajemen pihak ketiga atau karyawan kontrak	K/L/D menyetujui rencana mitigasi terhadap risiko yang diidentifikasi oleh manajemen pihak ketiga atau karyawan kontrak
162	Kebijakan identifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan oleh Pihak ketiga	K/L/D mengatur identifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan oleh Pihak ketiga
163	Dokumen Perjanjian/Kontrak pihak ketiga dalam penerapan pengendalian risiko	K/L/D memiliki Kontrak pihak ketiga dalam penerapan pengendalian risiko
164	Kebijakan pemantauan dan evaluasi persyaratan keamanan terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur oleh pihak ketiga	K/L/D bisa memantau dan evaluasi persyaratan keamanan terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur oleh pihak ketiga
165	Kebijakan penetapan peran dan tanggung jawab pemantauan,	K/L/D menetapkan penetapan peran dan tanggung jawab

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	evaluasi dan/atau audit aspek keamanan informasi pada pihak ketiga dalam unit organisasi tertentu	pemantauan, evaluasi dan/atau audit aspek keamanan informasi pada pihak ketiga dalam unit organisasi tertentu
166	Dokumen laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)	K/L/D menyimpan Dokumen laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)
167	Kebijakan pengadaan rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan	K/L/D mengadakan rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan
168	Dokumentasi hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala oleh pihak ketiga untuk dilaporkan kemajuannya kepada Perusahaan/Organisasi /Institusi	K/L/D memiliki Dokumentasi hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala oleh pihak ketiga untuk dilaporkan kemajuannya kepada Pejabat K/L/D.
169	Kebijakan pemenuhan persyaratan	K/L/D memenuhi persyaratan perencanaan

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	perencanaan dan melakukan audit terhadap keamanan informasi oleh pihak ketiga	dan melakukan audit terhadap keamanan informasi oleh pihak ketiga
170	Prosedur tindaklanjut hasil audit oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana	K/L/D bisa menindaklanjuti hasil audit oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana
171	Kebijakan terhadap prosedur dokumentasi, komunikasi, pemahaman dan penerapan terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan	K/L/D membuat peraturan yang terkait terhadap prosedur dokumentasi, komunikasi, pemahaman dan penerapan terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan
172	Kebijakan pengelolaan perubahan yang terjadi dalam hubungan dengan pihak ketiga	K/L/D mampu mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga
173	Analisa risiko yang menyertai perubahan hubungan dengan pihak ketiga	K/L/D mempunyai hasil analisis risiko yang menyertai perubahan hubungan dengan pihak ketiga
174	Prosedur formal untuk menangani data selama dalam siklus hidupnya	K/L/D memiliki Prosedur formal untuk menangani data selama dalam siklus

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/penghancuran aset oleh pihak ketiga	hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/penghancuran aset oleh pihak ketiga
175	Kebijakan kesepakatan penghancuran (*disposal*) data secara aman bersama pihak ketiga (pihak ketiga)	K/L/D membuat kesepakatan penghancuran (disposal) data secara aman bersama pihak ketiga (pihak ketiga)
176	Dokumentasi bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi oleh pihak ketiga	K/L/D memiliki dokumentasi bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi oleh pihak ketiga
177	Dokumentasi kebijakan, prosedur atau rencana untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana	K/L/D memiliki dokumentasi kebijakan, prosedur atau rencana untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana
178	Dokumentasi ujicoba dan evaluasi efektifitasnya kebijakan, prosedur atau rencana kelangsungan layanan pihak ketiga.	K/L/D memiliki dokumentasi simulasi dan evaluasi efektifitasnya kebijakan, prosedur atau rencana kelangsungan layanan pihak ketiga.
179	Kebijakan pembentukan	K/L/D memiliki organisasi atau tim khusus

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanan pihak ketiga	yang ditugaskan untuk mengelola proses kelangsungan layanan oleh pihak ketiga
180	Analisa kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan	K/L/D menganalisa kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan
181	Kebijakan klasifikasi data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*	K/L/D memiliki klasifikasi data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud
182	Kebijakan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*	K/L/D memiliki langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud
183	Analisa kajian, kriteria dan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*	K/L/D dapat menganalisis kajian, kriteria dan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud
184	Prosedur evaluasi penyelenggara layanan	K/L/D memiliki tata cara evaluasi penyelenggara

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	cloud terkait reputasi penyelenggara	layanan cloud terkait reputasi penyelenggara
185	Kebijakan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal	K/L/D menerapkan Kebijakan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal.
186	Prosedur evaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001	K/L/D mampu mengevaluasi kelayakan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001
187	Analisa kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan	K/L/D dapan menganalisa kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan.
188	Prosedur proses pelaporan insiden terkait layanan *cloud*	K/L/D memiliki tata cara proses pelaporan insiden terkait layanan cloud.
189	Prosedur untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang	K/L/D memiliki Prosedur untuk menghentikan layanan cloud, termasuk proses pengamanan data

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	ada (memindahkan dan menghapus data)	yang ada (memindahkan dan menghapus data)
190	Dokumentasi jenis dan bentuk (dokumen kertas/ elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal	K/L/D menyimpan dokumentasi jenis dan bentuk (dokumen kertas/ elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal
191	Kebijakan pemetaan alur proses data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh	K/L/D memetakan alur proses data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh
192	Dokumentasi proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/ perusahaan	K/L/D dapat menyimpan dokumentasi proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/ perusahaan
193	Kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku	K/L/D melindungi Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku
194	Kebijakan penunjukan pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang	K/L/D dapat mengangkat pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi	bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi
195	Analisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain	K/L/D mampu menganalisis dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain.
196	Analisa kajian risiko keamanan pada instansi/perusahaan pada aspek Perlindungan Data Pribadi	K/L/D mampu menganalisis kajian risiko keamanan pada instansi/perusahaan pada aspek Perlindungan Data Pribadi.
197	Prosedur perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku	K/L/D memiliki tata cara perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku.
198	Kebijakan implementasi program peningkatan pemahaman/ kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan	K/L/D menerapkan implementasi program peningkatan pemahaman/ kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, terkait dengan undang undang yang berlaku.

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	Perundangan yang berlaku	
199	Perjanjian persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data dan perlakuan pada data pribadi	K/L/D membuat perjanjian dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data dan perlakuan pada data pribadi
200	Prosedur melaporkan insiden terkait terungkapnya data pribadi	K/L/D dapat mngetahui cara melaporkan insiden terkait terungkapnya data pribadi
201	Kebijakan pemberian jaminan hak pemilik data pribadi untuk mengakses data tersebut	K/L/D memberikan jaminan hak pemilik data pribadi untuk mengakses data tersebut
202	Prosedur proses evaluasi akurasi dan pemutakhirkan data pribadi secara rutin	K/L/D mampu mengevaluasi akuasi dan pemuktahiran data pribadi
203	Prosedur proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data	K/L/D memiliki periode waktu penyimpanan data sesuai perjanjian dengan pemilik data.
204	Prosedur proses terkait penghapusan/pemusnahan data apabila sudah	K/L/D memiliki prosedur yang sistematis mengenai penghapusan data yang

Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1		
No	Kebutuhan	Manfaat
	tidak ada keperluan yang sah untuk menyimpan/mengolah nya lebih lanjut atau atas permintaan pemilik data dan daftar log catatan proses tersebut	tidak diperlukan atau atas permintaan pemilik.
205	Pedoman pengungkapan data pribadi atas permintaan resmi aparat penegak hukum	K/L/D memiliki pedoman untuk tatacara pengungkapan data pribadi atas permintaan aparat hukum.

6.2 Verifikasi Hasil Analisis Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1

Pada tahap ini akan dilakukan verifikasi dari Daftar Hasil Analisis Pemetaan Kuisioner SPBE dan Indeks KAMI 4.1 yang dibuat. Verifikasi dilakukan dengan cara melakukan pengecekan isi Hasil Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 dengan kondisi terkini sebuah Kementrian, Lembaga, dan Pemerintah Daerah sebagai objek studi kasus. Verifikasi yang dilakukan bertujuan untuk membantu K/L/D dalam pengisian Kuisioner SPBE BSSN dan memenuhi kesesuaian dari kebutuhan yang ada dalam penerapan SMKI dengan kondisi terbaru K/L/D.

Karena pada penelitian yang dilakukan penulis tidak menggunakan studi kasus sebagai objek penelitiannya, maka untuk hasil verifikasi Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 tidak ada hasilnya. Hal ini dikarenakan penulis melakukan penyusunan Tugas Akhir

dalam keadaan dan kondisi Pandemi Covid-19 yang melanda Dunia, khususnya di Indonesia.

BAB VII
KESIMPULAN DAN SARAN

7.1 Kesimpulan

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

1. Dari pengerjaan tugas akhir yang dilakukan penulis menemukan 2 (dua) hasil identifikasi untuk mendapatkan kebutuhan penerapan SMKI berdasarkan pemetaan Kuisioner SPBE BSSN dan Indeks KAMI 4.1. Hasil pertama adalah mengidentifikasi kebutuhan dari penerjemahan pertanyaan Kuisioner SPBE BSSN yang terpetakan dengan Indeks KAMI 4.1, dimana **di dalam pemetaan** terdapat kebutuhan yang dapat diambil menjadi kebutuhan penerapan SMKI. Didapatkan 69 kebutuhan penerapan SMKI yang terbagi menjadi **48 kebutuhan yang berasal dari pemetaan yang merupakan irisan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1** dan sisanya 21 kebutuhan berasal dari pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 yang terpetakan lebih dari satu kali. Hasil kedua dilakukan dengan mengidentifikasi kebutuhan dari penerjemahan Pertanyaan Indeks KAMI 4.1 yang **tidak terpetakan** dengan pertanyaan Kuisioner SPBE BSSN. Dari hasil identifikasi ini didapatkan **136 kebutuhan** penerapan SMKI.
2. Penyusunan Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 yang dilakukan pada pengerjaan tugas akhir ini menemukan **205 kebutuhan** penerapan SMKI yang memberikan informasi terkait kondisi ketersediaan kebutuhan penerapan SMKI pada Kementrian, Lembaga dan Pemerintah Daerah yang sedang menerapkan SMKI maupun akan menerapkan SMKI.

7.2 Saran

Dari kesimpulan pada tahap sebelumnya dan batasan masalah maka penulis memberikan saran-saran sebagai berikut:

1. Analisis Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 yang dibuat oleh penulis menyajikan kebutuhan penerapan SMKI, apabila penelitian berikutnya menggunakan Analisis Pemetaan ini, maka dapat dibantu dalam pengisian kuisioner SPBE BSSN dan Indeks KAMI 4.1 untuk mengetahui progress penerapan SMKI sesuai kebutuhan pada Kementrian, Lembaga dan Pemerintah Daerah.
2. Penelitian selanjutnya dapat mengujikan Analisis Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI 4.1 untuk penerapan SMKI yang telah dibuat oleh penulis, ke studi kasus pada Kementrian, Lembaga dan Pemerintah Daerah setelah pandemi usai.
3. Mampu memberikan gambaran dan kebutuhan bagi K/L/D yang belum pernah memakai Indeks KAMI sebagai alat Evaluasi SMKI, dalam mempersiapkan penerapan SMKI sesuat kaidah kontrol ISO/IEC 27001:2013 yang mendasari penyusunan Indeks KAMI 4.1.

DAFTAR PUSTAKA

[1] Home Office, "Understanding the costs of cybercrime A report of key findings from the Costs of Cyber Crime Working Group," 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf

[2] Roy Franedya, "Kejahatan Siber Merebak, RI Rugi Rp 478,8 Triliun," 2018. [Online]. Available: https://www.cnbcindonesia.com/tech/20180524190150-37-16463/kejahatan-siber-merebak-ri-rugi-rp-4788-triliun

[3] T. G. Trionggo, Penyusunan Perangkat Checklist Kebutuhan Penerapan Sistem Manajemen Keamanan Informasi berbasis Standar ISO/IEC 27001:2013 dan Indeks KAMI 4.0. 2020.

[4] Ikhsan Hidayat, "Information Security Management System (ISMS) : ISO 27001," ITGID, 2019, Nov 4 2019. [Online]. Available: https://itgid.org/information-security-management-system-isms-iso-27001

[5] Riandi, "Manajemen Keamanan Informasi Di Perusahaan," ITGID, 2019, Sep 2019. [Online]. Available: https://itgid.org/manajemen-keamanan-informasi-perusahaan/

[6]P. A. Perani, "Mengapa Perlu Menerapkan ISO 27001:2013?," ISOCENTER INDONESIA, 2016. [Online]. Available: <https://isoindonesiacenter.com/mengapa-perlu-menerapkan-iso-270012013/>

[7] BSSN, INDEKS KEAMANAN INFORMASI (KAMI). 2019. [Online]. Available: <https://bssn.go.id/indeks-kami/>

[8] Peraturan Presiden Nomor 95 tahun 2018. 2018.

[9] Peraturan Mentri PANRB Nomor 5 tahun 2018.2018

[10] MENPANRB, Evaluasi SPBE. 2019. [Online]. Available: <https://spbe.go.id/dokumen/>

[11] J. HM, Analisis & Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis. Yogyakarta: Penerbit ANDI, 1989.

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

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

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

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

[16] BSSN, Form Kuesioner SPBE BSSN. 2019. 19 Agustus 2019 [Online]. Available: < https://www.menlhk.go.id/site/post/241>

BIODATA PENULIS

Penulis bernama lengkap Yuardi Bisatya Utomo, dilahirkan di kota Madiun, 28 Juli 1995, merupakan anak tunggal. Penulis telah menempuh pendidikan formal di SDN Taman, Madiun, SDN Margorejo IV, Surabaya, SMPN 13 Surabaya, dan SMA Trimurti Surabaya. Penulis meneruskan pendidikan tinggi negeri di Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya dan terdaftar dengan NRP 05211340000165. Pengalaman selama menjadi mahasiswa di ITS, penulis aktif sebagai desainer seni *freelancer*. Penulis juga pernah melaksanakan kerja praktik selama satu bulan pada tahun 2017 di PT GEPSI (General Electric Power Systems Indonesia), Surabaya.

Penulis mengambil bidang minat Manajemen Sistem Informasi (MSI) dengan mengambil topik Analisa Pemetaan Kuisioner SPBE BSSN dan Indeks KAMI untuk penerapan SMKI dibawah bimbingan Ibu Feby Artwodini, S.Kom., M.T. dan Ibu Anisah Herdiyanti, S.Kom., M.Sc..
Untuk menghubungi penulis, dapat melalui e-mail : arsyautomo@gmail.com.

Halaman ini sengaja dikosongkan

LAMPIRAN A
Daftar Pertanyaan Kuisioner SPBE BSSN Edisi Agustus 2019

Tabel Lampiran A. 1 Daftar Pertanyaan Kuisioner SPBE BSSN Edisi Agustus 2019

Kuisioner SPBE BSSN	
PROSES BISNIS KEAMANAN TIK	
1	Apakah pimpinan instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi termasuk penetapan kebijakan terkait?
2	Apakah instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?
3	Apakah penanggungjawab pelaksanaan pengamanan informasi memiliki wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?

Kuisioner SPBE BSSN	
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?
5	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhan bagi semua pihak yang terkait ?
6	Apakah instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?
7	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?

Kuisioner SPBE BSSN	
8	Apakah tanggungjawab pengelola keamanan informasi mencangkup koordinasi dengan pikah pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan untuk mengidentifikasi persyaratan /kebutuhan pengamanan dan penyelesaian permasalahan yang ada ?
9	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (Business continuity dan disaster recovery plans) sudah di definisikan dan dialokasikan ?
10	Apakah instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?

Kuisioner SPBE BSSN	
11	Apakah instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi?)
12	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi anda?
13	Apakah instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?
14	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?

Kuisioner SPBE BSSN	
15	Apakah instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?
16	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?

Kuisioner SPBE BSSN	
17	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?
18	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?
19	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?

Kuisioner SPBE BSSN	
20	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?
21	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?
22	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)?

Kuisioner SPBE BSSN	
23	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?
24	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)
25	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?
26	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
27	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?

Kuisioner SPBE BSSN	
28	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?
29	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)
30	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?
31	Apakah instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?

Kuisioner SPBE BSSN	
32	Apakah instansi ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?
33	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?
34	Apakah instansi mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?
35	Apakah instansi mengklarifikasi persyaratan mitigasi risiko instansi dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?
36	Apakah instansi 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?

Kuisioner SPBE BSSN	
37	Apakah instansi 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?
38	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?
39	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?
ARSITEKTUR KEAMANAN TIK	
1	Apakah dikantor Bapak sudah ada Pedoman Keamanan Organisasi/Infrastruktur, Kontrol keamanan data organisasi dengan menjaga informasi sensitif agar tetap aman dan melakukan proteksi sebagai penanggulangan terhadap akses tidak sah ?

Kuisioner SPBE BSSN	
2	Apakah dikantor Bapak sudah ada Pedoman Arsitektur Keamanan Informasi, mewakili bagian dari arsitektur organisasi/perusahaan yang secara khusus membahas ketahanan sistem informasi dan menyediakan informasi arsitektur untuk implementasi kemampuan dalam memenuhi persyaratan keamanan ?
3	Apakah dikantor Bapak sudah ada Pedoman Kebijakan Keamanan, Standard dan Prosedur, Standar keamanan memainkan peran penting dalam organisasi dan relevansinya yang tidak perlu dipertanyakan lagi terlihat ketika kebijakan tidak memiliki pendorong teknologi ?
4	Apakah dikantor Bapak sudah ada Pedoman Keamanan baseline dan Pengukuran Risiko, Mengenali pentingnya manajemen keamanan informasi, menjelaskan implementasi kebijakan keamanan, menjelaskan manajemen risiko Informasi

Kuisioner SPBE BSSN	
5	Apakah dikantor Bapak sudah ada Pedoman Kepedulian Pengguna dan Training Keamanan, pelatihan kesadaran keamanan berkala adalah untuk mengembangkan kompetensi esensial, teknik dan metode baru yang sangat penting dalam menghadapi kemungkinan masalah keamanan ?
6	Apakah dikantor Bapak sudah ada Pedoman Compliance, Untuk memperkuat kontrol internal dan mencegah akses yang tidak sah dan tidak patut ke data, dengan demikian memastikan perlindungan aset informasi yang sesuai ?
7	Apakah dikantor Bapak sudah ada pedoman untuk overview dan konsep keamanan aplikasi, didukung dengan metode dan standard yang lebih rinci ?
8	Apakah dikantor Bapak sudah ada pedoman untuk framework normative organisasi, yang menjelaskan tentang struktur, hubungan dan saling ketergantungan antara proses dalam kerangka kerja normative organisasi ?

Kuisioner SPBE BSSN	
9	Apakah dikantor Bapak sudah ada pedoman untuk proses management keamanan aplikasi, proses keseluruhan dalam mengelola keamanan pada setiap aplikasi spesifik ?
10	Apakah dikantor Bapak sudah ada pedoman untuk validasi keamanan aplikasi dan sertifikasi untuk menilai dan membandingkan tingkat kepercayaan sistem aplikasi ?
11	Apakah dikantor Bapak sudah ada pedoman untuk protocol dan struktur pengendalian data keamanan aplikasi dalam pembentukan perpustakaan fungsi keamanan aplikasi ?
12	Apakah dikantor Bapak sudah ada pedoman untuk keamanan aplikasi spesifik dalam memberikan jaminan yang diperlukan untuk menaruh kepercayaan pada pengaturan keamanan aplikasi computer ?

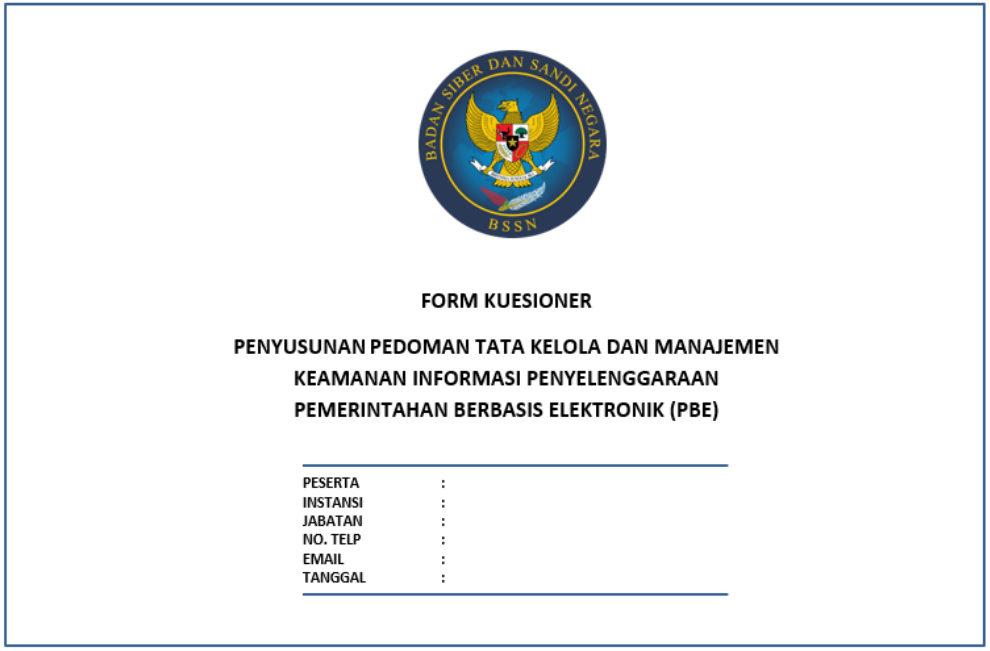
Kuisioner SPBE BSSN	
13	Apakah dikantor Bapak sudah ada pedoman untuk tinjauan dan konsep keamanan jaringan, panduan tentang cara mengidentifikasi dan menganalisis risiko keamanan jaringan ?
14	Apakah dikantor Bapak sudah ada pedoman untuk Desain dan Implementasi Keamanan Jaringan menggunakan pendekatan yang konsisten sesuai perencanaan ?
15	Apakah dikantor Bapak sudah ada pedoman untuk referensi scenario jaringan untuk ancaman, teknis desain termasuk isu-isu pengendalian ?
16	Apakah dikantor Bapak sudah ada pedoman untuk keamanan komunikasi antar jaringan menggunakan keamanan gateway termasuk mengidentifikasi dan menganalisis ancaman keamanan jaringan ?

Kuisioner SPBE BSSN	
17	Apakah dikantor Bapak sudah ada pedoman untuk keamanan komunikasi lintas jaringan menggunakan VPN, menghubungkan jaringan dan menghubungkan jarak jauh ke jaringan ?
18	Apakah dikantor Bapak sudah ada pedoman untuk keamanan akses wireless IP network untuk menentukan risiko spesifik, Teknik desain dan masalah control ?
19	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung konstituen, kostituen disini adalah berbagai pihak yang menggunakan h/w, s/w yang terhubung dengan layanan pemerintah ?
20	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung service provider (penyedia layanan), penyedia layanan dari eksternal dan sebagai penghubung layanan pemerintah ?

Kuisioner SPBE BSSN	
21	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung data owners (pemilik data), pemilik data merupakan penyedia layanan pemerintah ?
22	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung data storage (penyimpanan data), merupakan penyimpanan data layanan pemerintah dan penghubung pemerintah ?
AUDIT TIK	
1	Apakah Instansi anda sudah melaksanakan Audit TIK internal secara berkala?
2	Apakah Instansi anda sudah melaksanakan Audit TIK eksternal secara berkala?
3	Apakah di Instansi anda sudah memiliki pedoman pelaksanaan Audit TIK?

Kuisioner SPBE BSSN	
4	Apakah instansi anda sudah melakukan manajemen program audit?
5	Apakah di Instansi anda sudah menerapkan standart pelaksanaan Apakah di Instansi anda sudah melaksanakan tindak lanjut dan perbaikan hasil temuan Audit TIK berdasarkan rekomendasi yang diberikan?
6	Apakah di Instansi anda sudah memiliki unit kerja khusus yang mengelola hasil temuan Audit TIK?
7	Apakah di instansi anda sudah dilakukan evaluasi auditor dan kompetensinya?
8	Apakah instansi anda sudah memiliki sertifikasi manajemen sistem yang membutuhkan proses audit?

Di halaman berikutnya adalah cover kuisioner SPBE BSSN Edisi Agustus 2019, yang disusun oleh BSSN dalam versi aslinya.



Gambar A.1 Cover Kuisioner SPBE BSSN Edisi Agustus 2019

Halaman ini sengaja dikosongkan

LAMPIRAN B
Daftar Pertanyaan Indeks KAMI versi 4.1.

Tabel Lampiran B. 1 LAMPIRAN B Daftar Pertanyaan Indeks KAMI versi 4.1.

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?

Indeks KAMI versi 4.1	
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 4.1	
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses 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?

Indeks KAMI versi 4.1	
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 4.1	
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang objektif/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 4.1	
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 objektif kinerja efektifitas pengamanan?
Kerangka Kerja	

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?
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?

Indeks KAMI versi 4.1	
4.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/objektif 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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
4.13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
4.27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?
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?

Indeks KAMI versi 4.1	
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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

Indeks KAMI versi 4.1	
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
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi

Indeks KAMI versi 4.1	
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

Indeks KAMI versi 4.1	
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
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
5.20	Proses pengecekan latar belakang SDM

Indeks KAMI versi 4.1	
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

Indeks KAMI versi 4.1	
5.24	Prosedur untuk *user* yang 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?
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?

Indeks KAMI versi 4.1	
5.27	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?
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?

Indeks KAMI versi 4.1	
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?

Indeks KAMI versi 4.1	
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 4.1	
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?

Indeks KAMI versi 4.1	
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 4.1	
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)?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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?
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
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?
7.1.2	Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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

Indeks KAMI versi 4.1	
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 4.1	
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

Indeks KAMI versi 4.1	
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 4.1	
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?

Indeks KAMI versi 4.1	
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 4.1	
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*?

Indeks KAMI versi 4.1	
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?
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?

Indeks KAMI versi 4.1	
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)?

Indeks KAMI versi 4.1	
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?
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?

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?
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?

Indeks KAMI versi 4.1	
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 ?

Indeks KAMI versi 4.1	
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?
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?

Indeks KAMI versi 4.1	
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?

Indeks KAMI versi 4.1	
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?

LAMPIRAN C
Daftar Hasil Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1

C.1 Pemetaan Indeks KAMI Versi 4.1 dengan Kuisioner SPBE BSSN Domain Proses Bisnis TIK

Tabel Lampiran C. 1 Pemetaan Domain Proses Bisnis TIK

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
1	Apakah pimpinan instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi termasuk penetapan kebijakan terkait?	2.1	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Definisi peran dan tanggung jawab keamanan

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
2	Apakah instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	2.2	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Definisi peran dalam pengelolaan keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
3	Apakah penanggungjawab pelaksanaan pengamanan informasi memiliki wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	2.3	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Perjanjian kontraktual antara pejabat/petugas pelaksana keamanan informasi terhadap peran yang ditentukan

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	2.4	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Pemantauan, pengaturan dan prediksi terkait alokasi penggunaan sumber daya untuk penngelolaan dan jaminan kepatuhan program keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
5	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhan bagi semua pihak yang terkait ?	2.8	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Penerapan program Sosialisasi dalam peningkatan pemahaman Keamanan Informasi termasuk kepatuhan bagi pihak terkait

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
6	Apakah instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	2.9	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Penerapan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
7	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	2.10	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Persyaratan keamanan informasi melalui kerangka kerja yang dibangun untuk mengendalikan pelaksanaan dan pengoprasian keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
8	Apakah tanggungjawab pengelola keamanan informasi mencangkup koordinasi dengan pikah pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan untuk mengidentifikasi persyaratan /kebutuhan pengamanan dan penyelesaian permasalahan yang ada ?	2.12	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Daftar Log Aktifitas Pengguna

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
9	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (Business continuity dan disaster recovery plans) sudah di definisikan dan dialokasikan ?	2.14	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Analisis dampak Bisnis (*Business Impact Analysis*)

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
10	Apakah instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	2.22	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Definisi kebijakan dan prosedur penanggulangan insiden keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
11	Apakah instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi?)	2.20	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Analisis aspek keamanan informasi dalam manajemen proyek yang terkait ruang lingkup Perusahaan

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
12	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi anda?	3.4	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Definisi Klasifikasi Resiko Informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
13	Apakah instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	3.6	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Definisi peran dalam kepemilikan dan pihak pengelola aset informasi
14	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	3.8	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Daftar klasifikasi dampak kerugian hilangnya sebuah aset

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
15	Apakah instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	3.9	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Daftar analisa resiko Aset informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
16	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?	3.11	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Daftar prosedural dalam analisa resiko Aset informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
17	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	3.14	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Revisi Analisis Profil resiko secara berkala

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
18	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?	4.1	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Daftar Kebijakan, Prosedur dan Dokumen terkait Keamanan Informasi Perusahaan, Organisasi dan Institusi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
19	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	4.8	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Definisi dan penegakan konsekuensi pelanggaran kebijakan
20	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran s keamanan informasi,	4.15	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Kerangka rencana berjangka pengelolaan keberlangsungan layanan IT

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	termasuk penjadwalan uji cobanya?			
21	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	4.12	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur proses evaluasi resiko terkait pengadaan barang

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
22	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)?	4.23	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur Audit Internal Keamanan Informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
23	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	4.29	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Kerangka rencana berjangka peningkatan keamanan informasi secara berkala
24	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ?	5.1	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Daftar Inventori aset

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	(termasuk kepemilikan aset)			
25	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang	5.5	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur proses perubahan sistem proses bisnis dan proses teknologi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	diterapkan secara konsisten?			
26	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	5.21	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur proses pelaporan insiden keamanan terhadap pihak berwenang

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
27	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?	5.28	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur pengamanan fasilitas fisik

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
28	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	5.36	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Perjanjian pengamanan pengiriman aset informasi pada pihak ke tiga
29	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk	5.37	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur peraturan dan larangan dalam pengamanan fasilitas fisik

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)			
30	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan	6.3	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Konfigurasi Standar keamanan sistem keseluruhan aset jaringan, sistem dan aplikasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	(standar industri yang berlaku) dan kebutuhan?			
31	Apakah instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	6.4	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Analisa kepatuhan penerapan pengelolaan sistem informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
32	Apakah instansi ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	6.25	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur pengamanan lingkungan pengembangan uji coba siklus sistem

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
33	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	6.26	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur Audit keamanan informasi dengan pihak independen
34	Apakah instansi mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	7.1.1.1	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Analisa identifikasi resiko dengan pihak ketiga

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
35	Apakah instansi mengklarifikasi persyaratan mitigasi risiko instansi dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	7.1.1.3	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Persyaratan Mitigasi Resiko dan ekspektasi oleh pihak ke-tiga
36	Apakah instansi telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen	7.1.1.5	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Kebijakan keamanan informasi untuk pihak ketiga

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?			
37	Apakah instansi telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset	7.1.3.1	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur monitoring dan review pengelolaan layanan dan keamanan informasi oleh pihak ketiga

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
	informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?			
38	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	7.1.6.1	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
PROSES BISNIS KEAMANAN TIK				
39	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	7.1.1.7	Memakai Pertanyaan yang sama dengan indeks KAMI 4.1	Prosedur Audit berkala oleh pihak ketiga

C.2 Pemetaan Indeks KAMI 4.1 Versi 4.1 dengan Kuisioner SPBE BSSN Domain Arsitektur TIK

Tabel Lampiran C. 2 Pemetaan Domain Arsitektur TIK

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
1	Apakah dikantor Bapak sudah ada Pedoman Keamanan Organisasi/Infrastruktur, Kontrol keamanan data organisasi dengan menjaga informasi sensitif agar tetap aman dan melakukan proteksi sebagai penanggulangan terhadap akses tidak sah ?	5.28	pertanyaan tersebut merepresentasikan kebutuhan terkait pengamanan fasilitas fisik untuk mencegah upaya akses dari pihak yang tidak memiliki kewenangan	Pedoman Keamanan Organisasi/Infrastruktur

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
2	Apakah dikantor Bapak sudah ada Pedoman Arsitektur Keamanan Informasi, mewakili bagian dari arsitektur organisasi/perusahaan yang secara khusus membahas ketahanan sistem informasi dan menyediakan informasi arsitektur untuk implementasi kemampuan dalam memenuhi persyaratan keamanan ?	2.2	Pertanyaan tersebut merepresentasikan kebutuhan instansi telah mengalokasikan tanggung jawab pengelolaan keamanan informasi dan pembagian tugas untuk kemampuan terspesifik dalam penanganan keamanan	Pedoman Arsitektur Keamanan Informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
3	Apakah dikantor Bapak sudah ada Pedoman Kebijakan Keamanan, Standard dan Prosedur, Standar keamanan memainkan peran penting dalam organisasi dan relevansinya yang tidak perlu dipertanyakan lagi terlihat ketika kebijakan tidak memiliki pendorong teknologi ?	2.5	Pertanyaan tersebut merepresentasikan kebutuhan peran pelaksana yang telah dipetakan dalam kerangka kerja dimana setiap aktor telah diberi tanggung jawab masing-masing dan dijelaskan pada perjanjian kontraktual masing-masing pelaksana	Pedoman Keamanan baseline dan Pengukuran Risiko

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
4	Apakah dikantor Bapak sudah ada Pedoman Keamanan baseline dan Pengukuran Risiko, Mengenali pentingnya manajemen keamanan informasi, menjelaskan implementasi kebijakan keamanan, menjelaskan manajemen risiko Informasi	3.4	Pertanyaan tersebut merepresentasikan kebutuhan terkait kerangka kerja pengelolaan risiko yang mencakup tingkat ancaman, kemungkinan terjadi ancaman dan dampak kerugian yang digunakan penilaian suatu peristiwa termasuk risiko atau bukan.	Pedoman Kepedulian Pengguna dan Training Keamanan

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
5	Apakah dikantor Bapak sudah ada Pedoman Kepedulian Pengguna dan Training Keamanan, pelatihan kesadaran keamanan berkala adalah untuk mengembangkan kompetensi esensial, teknik dan metode baru yang sangat penting dalam menghadapi kemungkinan masalah keamanan ?	2.9	Pertanyaan tersebut menjelaskan bahwa program peningkatan kompetensi dan keahlian pengelolaan keamanan informasi yang relevan sangat berguna bagi karyawan adalah sebuah kebutuhan.	Pedoman Kontrol Internal dan alokasi akses

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
6	Apakah dikantor Bapak sudah ada Pedoman Compliance, Untuk memperkuat kontrol internal dan mencegah akses yang tidak sah dan tidak patut ke data, dengan demikian memastikan perlindungan aset informasi yang sesuai ?	2.8	Pertanyaan tersebut menjelaskan bahwa karyawan menerima program sosialisasi dan peningkatan pemahaman keamanan informasi sebagai salah satu kontrol informasi internal.	Pedoman untuk *overview* dan konsep keamanan aplikasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
7	Apakah dikantor Bapak sudah ada pedoman untuk overview dan konsep keamanan aplikasi, didukung dengan metode dan standard yang lebih rinci ?	2.6	Pertanyaan tersebut menjustifikasikan hububgan antara persamaan/standar dalam sebuah perusahaan dalam penyusunan pedoman keamanan informasi	Pedoman untuk *framework* normative organisasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
8	Apakah dikantor Bapak sudah ada pedoman untuk framework normative organisasi, yang menjelaskan tentang struktur, hubungan dan saling ketergantungan antara proses dalam kerangka kerja normative organisasi ?	4.15	pertanyaan tersebut kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK dalam proses bisnis Perusahaan, Organisasi, Institusi	Definisi peran dalam pengelolaan keamanan informasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
9	Apakah dikantor Bapak sudah ada pedoman untuk proses management keamanan aplikasi, proses keseluruhan dalam mengelola keamanan pada setiap aplikasi spesifik ?	6.3	pertanyaan tersebut merepresentasikan kebutuhan terkait konfigurasi standar keamanan sistem yang mutakhirkan sesuai perkembangan dan kebutuhan untuk seluruhan aset jaringan, sistem dan aplikasi	Pedoman untuk proses management keamanan aplikasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
10	Apakah dikantor Bapak sudah ada pedoman untuk validasi keamanan aplikasi dan sertifikasi untuk menilai dan membandingkan tingkat kepercayaan sistem aplikasi ?	6.24	pertanyaan tersebut merepresentasikan kebutuhan terkait validasi/verifikasi fungsi keamanan aplikasi pada proses pengembangan dan uji coba	Pedoman untuk validasi dan sertifikasi keamanan aplikasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
11	Apakah dikantor Bapak sudah ada pedoman untuk protocol dan struktur pengendalian data keamanan aplikasi dalam pembentukan perpustakaan fungsi keamanan aplikasi ?	6.5	pertanyaan tersebut merepresentasikan pemindaian jaringan, sistem dan aplikasi secara rutin untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan konfigurasi	Pedoman untuk protokol dan struktur pengendalian data keamanan aplikasi

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
12	Apakah dikantor Bapak sudah ada pedoman untuk keamanan aplikasi spesifik dalam memberikan jaminan yang diperlukan untuk menaruh kepercayaan pada pengaturan keamanan aplikasi computer ?	6.7	pertanyaan tersebut merepresentasikan kepastian ketersediaan yang cukup untuk memenuhi kebutuhan yang ada, salah satunyanya berupa jaminan dalam pengaturan aplikasi.	Pedoman untuk keamanan aplikasi spesifik
13	Apakah dikantor Bapak sudah ada pedoman untuk tinjauan dan konsep keamanan jaringan, panduan tentang cara mengidentifikasi dan menganalisis risiko keamanan jaringan ?	3.9	analisa/kajian risiko keamanan informasi dari aset informasi yang menghasilkan pengetahuan untuk digunakan mengidentifikasi	Pedoman untuk tinjauan dan konsep keamanan jaringan

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
			langkah mitigasi dari risiko tersebut	
14	Apakah dikantor Bapak sudah ada pedoman untuk Desain dan Implementasi Keamanan Jaringan menggunakan pendekatan yang konsisten sesuai perencanaan ?	4.29	pertanyaan tersebut menunjukan kebutuhan berupa program peningkatan keamanan informasi dengan jangka waktu menengah/panjang	Pedoman untuk Desain dan Implementasi Keamanan Jaringan
15	Apakah dikantor Bapak sudah ada pedoman untuk referensi scenario jaringan untuk ancaman, teknis	3.4	Pertanyaan tersebut terkait kerangka kerja pengelolaan risiko tentang tingkat klasifikasi aset	Pedoman referensi skenario jaringan untuk ancaman

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
	desain termasuk isu-isu pengendalian ?		informasi dan kerangka kerja pengelolaan risiko yang mencakup tingkat ancaman, kemungkinan terjadi ancaman dan dampak kerugian yang digunakan untuk memutuskan suatu peristiwa termasuk risiko atau bukan.	

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
16	Apakah dikantor Bapak sudah ada pedoman untuk keamanan komunikasi antar jaringan menggunakan keamanan gateway termasuk mengidentifikasi dan menganalisis ancaman keamanan jaringan ?	6.2	pertanyaan tersebut merepresentasikan kebutuhan terkait segmentasi jaringan komunikasi sesuai kepentingannya.	Pedoman untuk keamanan komunikasi antar jaringan menggunakan keamanan gateway
17	Apakah dikantor Bapak sudah ada pedoman untuk keamanan komunikasi lintas jaringan menggunakan VPN, menghubungkan jaringan dan menghubungkan jarak jauh ke jaringan ?	6.2	pertanyaan tersebut merepresentasikan kebutuhan terkait segmentasi jaringan komunikasi sesuai kepentingannya.	Pedoman untuk keamanan komunikasi lintas jaringan menggunakan VPN

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
18	Apakah dikantor Bapak sudah ada pedoman untuk keamanan akses wireless IP network untuk menentukan risiko spesifik, Teknik desain dan masalah control ?	3.9	pertanyaan tersebut merepresentasikan kebutuhan terkait analisa/kajian risiko keamanan informasi dari aset informasi yang menghasilkan pengetahuan untuk digunakan mengidentifikasi langkah mitigasi dari risiko tersebut	Pedoman untuk keamanan akses *wireless IP network*

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
19	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung konstituen, kostituen disini adalah berbagai pihak yang menggunakan h/w, s/w yang terhubung dengan layanan pemerintah ?	6.2	pertanyaan tersebut merepresentasikan kebutuhan segmentasi jaringan komunikasi sesuai kepentingannya, dalam hal ini Pemerintah sebagai penyedia Layanan	Pedoman Keamanan sistem penghubung konstituen/User
20	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung service provider (penyedia layanan), penyedia layanan dari eksternal dan sebagai penghubung layanan pemerintah ?	2.14	Pertanyaan ini terkait kebutuhan keberlangsungan layanan TIK telah didefinisikan dan dialokasikan keputusan, perancang, pelaksanaan dan	Pedoman Keamanan sistem penghubung *service provider*

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
			pengelolanya pada organisasi	
21	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung data owners (pemilik data), pemilik data merupakan penyedia layanan pemerintah ?	2.11	Pertanyaan tersebut merepresentasikan kebutuhan yang menjelaskan identifikasi data pribadi pelaksana yang akan digunakan kerja dan menjelaskan	Pedoman Keamanan sistem penghubung *data owners*

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
			perlindungan dan privasi data pribadi sesuai peraturan dan perundang-undangan yang berlaku, dalam hal ini merupakan data pribadi/ data milik pemerintah	
22	Apakah dikantor Bapak sudah ada pedoman Keamanan sistem penghubung data storage (penyimpanan data), merupakan penyimpanan data layanan pemerintah dan penghubung pemerintah ?	2.11	Pertanyaan tersebut merepresentasikan kebutuhan yang menjelaskan identifikasi data pribadi pelaksana yang akan digunakan kerja dan menjelaskan perlindungan dan	Pedoman Keamanan Organisasi/Infrastruktur

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
ARSITEKTUR TIK				
			privasi data pribadi sesuai peraturan dan perundang-undangan yang berlaku, dalam hal ini merupakan penyimpanan data pribadi/ data milik pemerintah	

C.3 Pemetaan Indeks KAMI 4.1 Versi 4.1 dengan Kuisioner SPBE BSSN Domain Audit TIK

Tabel Lampiran C. 3 Pemetaan Domain Audit TIK

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
AUDIT TIK				
1	Apakah Instansi anda sudah melaksanakan Audit TIK internal secara berkala?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait pelaksanaan program audit internal yang dimiliki organisasi dan dilakukan oleh pihak independen	Prosedur Audit TIK internal secara berkala
2	Apakah Instansi anda sudah melaksanakan Audit TIK eksternal secara berkala?	7.1.1.7	pertanyaan tersebut merepresentasikan kebutuhan terkait hak audit TI secara berkala ke pihak ketiga	Prosedur Audit TIK eksternal secara berkala

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
AUDIT TIK				
3	Apakah di Instansi anda sudah memiliki pedoman pelaksanaan Audit TIK?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait pedoman program audit internal yang dimiliki organisasi dan dilakukan oleh pihak independen	Pedoman pelaksanaan Audit TIK
4	Apakah instansi anda sudah melakukan manajemen program audit?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait manajemen program audit internal yang dimiliki organisasi dan dilakukan oleh pihak independen	Manajemen program audit

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
AUDIT TIK				
5	Apakah di Instansi anda sudah menerapkan standart pelaksanaan Apakah di Instansi anda sudah melaksanakan tindak lanjut dan perbaikan hasil temuan Audit TIK berdasarkan rekomendasi yang diberikan?	4.25	pertanyaan tersebut merepresentasikan kebutuhan terkait hasil audit internal yang dikaji/evaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi	Menerapkan standard hasil pelaksanaan tindak lanjut Audit
6	Apakah di Instansi anda sudah memiliki unit kerja khusus yang mengelola hasil temuan Audit TIK?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait unit program audit internal yang dimiliki organisasi dan	Unit kerja khusus yang mengelola hasil temuan Audit TIK

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
AUDIT TIK				
			dilakukan oleh pihak independen	
7	Apakah di instansi anda sudah dilakukan evaluasi auditor dan kompetensinya?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait program audit internal yang dimiliki organisasi dan dilakukan oleh Auditor independen	Evaluasi auditor dan kompetensi
8	Apakah instansi anda sudah memiliki sertifikasi manajemen sistem yang membutuhkan proses audit?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait program audit internal yang dimiliki organisasi dan	Sertifikasi manajemen sistem

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
AUDIT TIK				
			dilakukan oleh pihak independent dengan alat evaluasi yang berdasarkan standard yang diakui.	

C.4 Sisa Indeks KAMI 4.1 Versi 4.1 yang Tidak Dapat Terpetakan

Tabel Lampiran C. 3 Pemetaan Domain Audit TIK

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
1	-	2.7		Verifikasi Sertifikasi kompetensi bagi pelaksana pengamanan informasi
2		2.10		Persyaratan integrasi keamanan informasi kedalam proses kerja
3		2.13		Prosedur koordinasi dengan satker terkait (SDM, Legal/Hukum,

				Umum, Keuangan dll) dan pihak eksternal yang berkepentingan
4		2.15		Prosedur melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara berkala
5		2.16		Prosedur proses pengambilan keputusan strategis berdasarkan keadaan keamanan informasi

6		2.17		Kebijakan program aturan tujuan dan sasaran kepatuhan pengamanan aset informasi
7		2.18		Definisi metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi
8		2.19		Kebijakan program penilaian kinerja pengelolaan keamanan informasi bagi individu
9		2.21		Identifikasi legislasi, perangkat hukum dan standar lainnya terkait

				keamanan informasi
10		3.1		Dokumentasi program kerja pengelolaan risiko keamanan informasi
11		3.2		Struktur penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi
12		3.3		Dokumentasi kerangka kerja pengelolaan risiko

				keamanan informasi
13		3.5		Kebijakan penetapan ambang batas tingkat risiko
14		3.7		Dokumen ancaman dan kelemahan aset informasi terkait
15		3.10		Prosedur mitigasi dan penanggulangan risiko
16		3.12		Dokumentasi status penyelesaian langkah mitigasi risiko

17		3.13		Kebijakan evaluasi objektif prosedur mitigasi resiko
18		3.15		Kebijakan pengkajian berkala efektifitas kerangka kerja pengelolaan risiko
19		3.16		Kebijakan memasukan pengelolaan risiko menjadi bagian dari kriteria proses penilaian objektif kinerja efektifitas pengamanan
20		4.2		Kebijakan publikasi formalitas keamanan informasi

21		4.3		Mekanisme pengelolaan dokumen kebijakan dan prosedur keamanan informasi
22		4.4		Prosedur komunikasi kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait
23		4.5		Dokumentasi pelaksanaan kebijakan dan prosedur keamanan informasi berdasarkan kebutuhan mitigasi

				dari hasil kajian risiko keamanan informasi
24		4.6		Prosedur identifikasi kondisi insiden keamanan informasi
25		4.7		Kebijakan pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK pada kontrak pihak ketiga

26		4.9		Prosedur pengelolaan suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi
27		4.10		Kebijakan dan prosedur operasional implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan pelaporan

28		4.11		Definsi aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup
29		4.13		Kebijakan pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan
30		4.14		Kebijakan penanganan konflik penerapan sistem baru terhadap kebijakan yang

				berlaku dan jadwal penyelesaiannya
31		4.16		Kebijakan definisi komposisi, peran, wewenang dan tanggungjawab tim perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*)
32		4.17		Dokumentasi uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*)

33		4.18		kebijakan evaluasi prosedur perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) yang gagal
34		4.19		Kebijakan Evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala
35		4.20		Kebijakan penyusunan strategi penerapan keamanan informasi sesuai hasil analisa risiko sebagai bagian dari

				rencana kerja organisasi
36		4.21		Persyaratan strategi penggunaan teknologi keamanan informasi
37		4.22		Prosedur strategi penerapan keamanan informasi sebagai bagian dari pelaksanaan program kerja organisasi anda
38		4.24		Kebijakan audit internal keamanan informasi

39		4.26		Kebijakan hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan program peningkatan kinerja keamanan informasi
40		4.27		Prasyarat analisa aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya

41		4.28		Kebijakan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya)
42		5.2		Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku

43		5.3		Prosedur mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset
44		5.4		Definisi tingkatan akses klasifikasi aset informasi dan matriks
45		5.6		Prosedur pengelolaan konfigurasi
46		5.7		Prosedur perilisan aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi

47		5.8		Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda
48		5.9		Kebijakan Tata tertib penggunaan komputer, email, internet dan intranet
49		5.10		Kebijakan Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI

50		5.11		Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan
51		5.12		Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
52		5.13		Prosedur Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya

53		5.14		Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
54		5.15		Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
55		5.16		Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya

56		5.17		Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
57		5.18		Prosedur back-up dan uji coba pengembalian data (restore) secara berkala
58		5.19		Kebijakan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya

59		5.20		Proses pengecekan latar belakang SDM
60		5.22		Prosedur penghancuran data/aset yang sudah tidak diperlukan
61		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
62		5.24		Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
63		5.25		Daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*
64		5.26		Daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan

				yang sesuai dengan klasifikasi
65		5.27		Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/ *vendor*) dengan memastikan aspek HAKI dan pengamanan akses
66		5.29		Prosedur penglolaan alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik

67		5.30		Kebijakan perlindungan infrastruktur komputasi dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikan
68		5.31		Kebijakan Perlindungan infrastruktur komputasi dari gangguan pasokan listrik atau dampak dari petir

69		5.32		Peraturan pengamanan perangkat komputasi milik instansi/perusahaan apabila digunakan di luar lokasi kerja resmi (kantor)
70		5.33		Prosedur pemindahan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)

71		5.34		Kebijakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) pada konstruksi ruang penyimpanan perangkat pengolah informasi
72		5.35		Proses inspeksi dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan

				keamanan lokasi kerja untuk menempatkan aset informasi penting
73		5.38		Proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan
74		6.1		Prosedur perlindungan dengan lebih dari 1 lapis pengamanan pada layanan TIK (sistem komputer) yang terhubung internet

75		6.6		Persyaratan ketersediaan keseluruhan infrastruktur jaringan, sistem dan aplikasi
76		6.8		Daftar log perubahan dalam sistem informasi
77		6.9		Daftar Log akses Sistem berdasarkan ID Pengguna
78		,6.10		Analisa Daftar Rekaman log secara berkala

79		6.11		Kebijakan enkripsi perlindungan aset informasi
80		6.12		Kebijakan standarisasi enkripsi
81		6.13		Kebijakan pengamanan untuk penggelolaan kunci enkripsi (termasuk sertifikat elektronik) dan siklus penggunaan
82		6.14		Prosedur penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur

				kompleksitas/ panjangnya dan penggunaan kembali password lama pada semua sistem dan aplikasi
83		6.15		Kebijakan bentuk pengamanan berlapis pada pengelolaan sistem (administrasi sistem)
84		6.16		Proses pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan login,dan penarikan akses

85		6.17		Kebijakan mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi
86		6.19		Kebijakan pembaharuan sistem operasi untuk setiap perangkat desktop dan server dengan versi terkini
87		6.20		Prosedur perlindungan desktop dan server dari penyerangan virus (*malware*)

88		6.21		Daftar Log rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa *antivirus/ antimalware* telah dimutakhirkan secara rutin dan sistematis
89		6.22		Prosedur penindaklanjutan dan penyelesaian laporan penyerangan virus/ *malware* yang gagal/sukses.
90		6.23		Prosedur mekanisme sinkronisasi waktu

				jaringan, sistem dan aplikasi
91		7.1.1.2		Kebijakan komunikasi dan klarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada Perusahaan/Organisasi/Institusi
92		7.1.1.4		Kebijakan persetujuan rencana mitigasi terhadap risiko yang diidentifikasi oleh manajemen pihak ketiga atau karyawan kontrak

93		7.1.2.1		Kebijakan identifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan oleh Pihak ketiga
94		7.1.2.2		Dokumen Perjanjian/Kontrak pihak ketiga dalam penerapan pengendalian risiko
95		7.1.2.3		Kebijakan pemantauan dan evaluasi persyaratan keamanan terhadap kepatuhan alih daya, subkontraktor atau penyedia

				teknologi/infrastruktur oleh pihak ketiga
96		7.1.3.2		Kebijakan penetapan peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pada pihak ketiga dalam unit organisasi tertentu
97		7.1.3.3		Dokumen laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang

				disyaratkan dalam perjanjian komersil (kontrak)
98		7.1.3.4		Kebijakan pengadaan rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan
99		7.1.3.5		Dokumentasi hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala oleh pihak ketiga untuk dilaporkan

				kemajuannya kepada Perusahaan/Organisasi/Institusi
100		7.1.3.6		Kebijakan pemenuhan persyaratan perencanaan dan melakukan audit terhadap keamanan informasi oleh pihak ketiga
101		7.1.3.7		Prosedur tindaklanjut hasil audit oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana

102		7.1.3.8		Kebijakan terhadap prosedur dokumentasi, komunikasi, pemahaman dan penerapan terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan
103		7.1.4.1		Kebijakan pengelolaan perubahan yang terjadi dalam hubungan dengan pihak ketiga

104		7.1.4.2		Analisa risiko yang menyertai perubahan hubungan dengan pihak ketiga
105		7.1.5.1		Prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/penghancuran aset oleh pihak ketiga
106		7.1.5.2		Kebijakan kesepakatan penghancuran (*disposal*) data secara aman

				bersama pihak ketiga (pihak ketiga)
107		7.1.6.2		Dokumentasi bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi oleh pihak ketiga
108		7.1.7.1		Dokumentasi kebijakan, prosedur atau rencana untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana

109		7.1.7.2		Dokumentasi ujicoba dan evaluasi efektifitasnya kebijakan, prosedur atau rencana kelangsungan layanan pihak ketiga.
110		7.1.7.3		Kebijakan pembentukan organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanan pihak ketiga oleh pihak ketiga

111		7.2.1		Analisa kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan
112		7.2.2		Kebijakan klasifikasi data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*
113		7.2.3		Kebijakan langkah pengamanan data pribadi yang disimpan/diolah/dip

				ertukarkan melalui layanan *cloud*
114		7.2.4		Analisa kajian, kriteria dan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*
115		7.2.5		Prosedur evaluasi penyelenggara layanan cloud terkait reputasi penyelenggara
116		7.2.6		Kebijakan standar keamanan teknis penggunaan layanan *cloud*,

				termasuk aspek penggunaannya oleh pengguna di internal
117		7.2.7		Prosedur evaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001
118		7.2.8		Analisa kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan

				sementara pada layanan
119		7.2.9		Prosedur proses pelaporan insiden terkait layanan *cloud*
120		7.2.10		Prosedur untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)
121		7.3.1		Dokumentasi jenis dan bentuk (dokumen kertas/ elektronik) data pribadi yang

				disimpan, diolah dan dipertukarkan dengan pihak eksternal
122		7.3.2		Kebijakan pemetaan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh
123		7.3.3		Dokumentasi proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/ perusahaan

124		7.3.4		Kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku
125		7.3.5		Kebijakan penunjukan pejabat-pejabat (*Data Protection Officer*, *Data Controller*, *Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi

126		7.3.6		Analisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain
127		7.3.7		Analisa kajian risiko keamanan pada instansi/perusahaan pada aspek Perlindungan Data Pribadi
128		7.3.8		Prosedur perlindungan data pribadi sesuai keperluan mitigasi risiko dan peraturan

				perundangan yang berlaku
129		7.3.9		Kebijakan implementasi program peningkatan pemahaman/ kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku

130		7.3.10		Perjanjian persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data dan perlakuan pada data pribadi
131		7.3.11		Prosedur melaporkan insiden terkait terungkapnya data pribadi
132		7.3.12		Kebijakan pemberian jaminan hak pemilik data pribadi untuk mengakses data tersebut

133		7.3.13		Prosedur proses evaluasi akurasi dan pemutakhirkan data pribadi secara rutin
134		7.3.14		Prosedur proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data
135		7.3.15		Prosedur proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengol

				ahnya lebih lanjut atau atas permintaan pemilik data dan daftar log catatan proses tersebut
136		7.3.16		Pedoman pengungkapan data pribadi atas permintaan resmi aparat penegak hukum

Catatan:

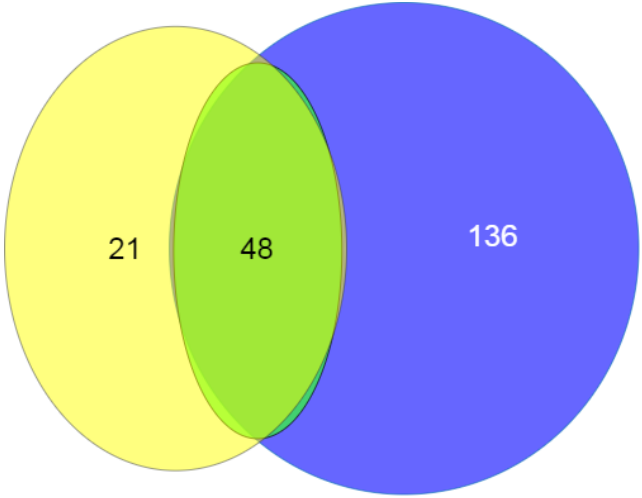
Cara membaca tabel Lampiran C dengan contoh seperti pertanyaan dibawah:

Kolom ke satu: adalah nomor pertanyaan.
Kolom ke dua: adalah pertanyaan Kuisioner SPBE BSSN.
Kolom ke tiga: adalah 4.23 Nomor 4 adalah area Indeks KAMI, Nomor 23 adalah nomor pertanyaan dari area Indeks KAMI di depan.
Kolom ke empat: adalah justifikasi hubungan pemetaan antara Kuisioner SPBE dan Indeks KAMI terkait.
Kolom ke lima: adalah kebutuhan hasil penerjemahan pemetaan Kuisioner SPBE BSSN dan Indeks KAMI.

Tabel Lampiran C. 5 Contoh Tabel

Kuisioner SPBE BSSN		Indeks KAMI versi 4.1	Justifikasi	Kebutuhan
8	Apakah instansi anda sudah memiliki sertifikasi manajemen sistem yang membutuhkan proses audit?	4.23	pertanyaan tersebut merepresentasikan kebutuhan terkait program audit internal yang dimiliki organisasi dan dilakukan oleh pihak independent dengan alat evaluasi yang berdasarkan standard yang diakui.	Sertifikasi manajemen sistem

LAMPIRAN D
Diagram Venn Hasil Identifikasi Pemetaan Kuisioner SPBE BSSN dengan Indeks KAMI versi 4.1 dan Indeks KAMI yang tidak terpetakan untuk Analisa Pemetaan

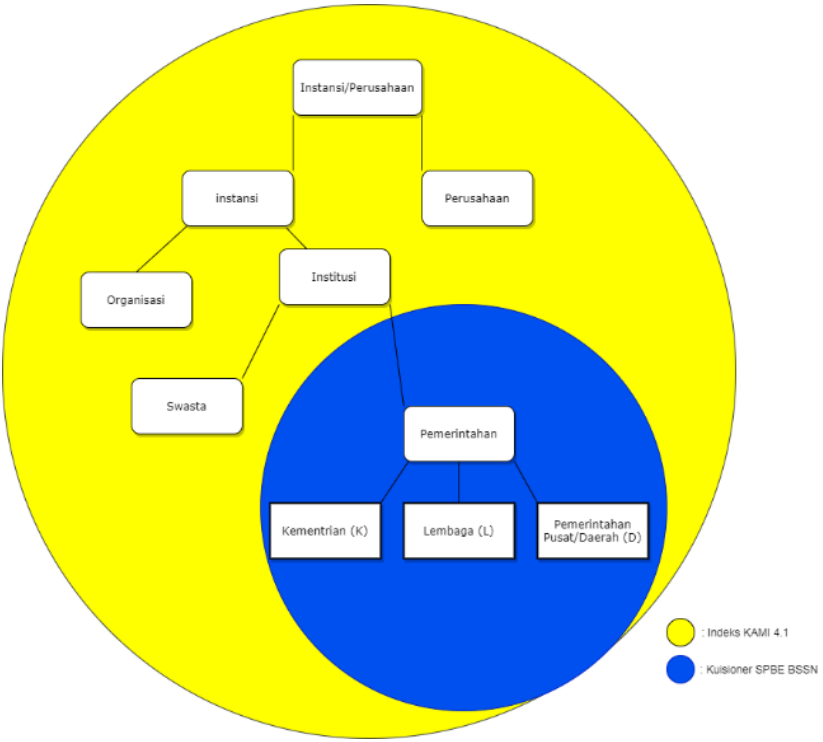


Gambar Lampiran D.1 Diagram Venn Hasil Identifikasi Pemetaan

Diagram Venn di samping untuk menjelaskan perihal klasifikasi warna yang ada pada Bab 6. Hasil pemetaan dari 69 Pertanyaan Kuisioner SPBE BSSN dengan 184 Pertanyaan Indeks KAMI 4.1. Terdiri dari 48 Kebutuhan dari pemetaan kuisioner SPBE BSSN dengan Indeks KAMI 4.1 **didalam irisan** (berwarna Hijau) dan 21 kebutuhan adalah sisa Kuisioner SPBE BSSN yang terpetakan dengan Indeks KAMI lebih dari satu kali (berwarna Kuning). Sedangkan 136 Kebutuhan adalah pertanyaan Indeks KAMI 4.1 yang tidak terpetakan pada kuisioner SPBE BSSN (berwarna Biru). Jadi, total keseluruhan **kebutuhan tercatat adalah 205**.

Halaman ini sengaja dikosongkan

LAMPIRAN E
Diagram Venn Penerapan SMKI di Indonesia, yang diklasifikasikan oleh BSSN



Gambar E.1 Diagram Venn Penerapan SMKI di Indonesia, yang diklasifikasikan oleh BSSN