Arsitektur Keamanan SPBE

Arsitektur dan Peta Rencana SPBE
Kabupaten Deli Serdang
Tahun 2021 – 2026

Dinas Komunikasi dan Informatika
Pemerintah Kabupaten Deli Serdang
tahun 2021

Buku 5

Buku 5

Arsitektur Keamanan SPBE

Dinas Komunikasi dan Informatika
Kabupaten Deli Serdang
tahun 2021

Kerjasama
Dinas Komunikasi dan Informatika
Pemerintah Kabupaten Deli Serdang

dengan
Institut Teknologi Sepuluh
Nopember

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
Pendahuluan

Pada bab 1 dijelaskan mengenai penyusunan arsitektur Keamanan SPBE, dasar acuan atau referensi SPBE serta Taksonomi dan Metadata sesuai dengan mengacu pada Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Draf Arsitektur SPBE Nasional.

1.1 Keamanan SPBE

Berdasarkan Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, **Keamanan SPBE** mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE. **Penjaminan kerahasiaan** dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan lainnya. **Penjaminan keutuhan** dilakukan melalui pendeteksian modifikasi. **Penjaminan ketersediaan** dilakukan melalui penyediaan cadangan dan pemulihan. **Penjaminan keaslian** dilakukan melalui penyediaan mekanisme verifikasi dan validasi. **Penjaminan kenirsangkalan (*nonrepudiation*)** dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.

1.2 Referensi Keamanan SPBE

Berdasarkan Draf Arsitektur SPBE Nasional, Referensi Keamanan SPBE (RK) pada SPBE disusun dengan maksud sebagai kerangka dasar dalam mendeskripsikan pengendalian keamanan data dan informasi, infrastruktur, serta aplikasi yang terpadu dalam SPBE nasional dan menjadi acuan bagi Pemerintah Daerah. Kerangka dasar ini menjadi panduan dalam pengintegrasian keamanan data dan informasi, aplikasi SPBE, dan infrastruktur SPBE nasional dan juga menjadi acuan bagi Pemerintah Daerah, sehingga dapat dilakukan pengendalian melalui identifikasi program keamanan, pengujian kelaikan keamanan serta regulasi keamanan yang komprehensif. Secara tidak langsung, RK akan turut mengawal pelaksanaan pembangunan di Indonesia dan pada umumnya akan turut melancarkan pelaksanaan pemerataan infrastruktur TIK.

1.3 Struktur Referensi Keamanan SPBE

Struktur dari RK SPBE Nasional terdiri atas 2 (dua) tingkat, yaitu:

1) Domain keamanan, yang mengelompokkan keamanan SPBE ke dalam domain keamanan terdiri dari standar keamanan, penerapan keamanan dan uji kelaikan keamanan, sebagai RK tingkat 1 (pertama); dan
2) Area keamanan, yang mengelompokkan keamanan SPBE ke dalam area keamanan terhadap data dan informasi, aplikasi, serta infrastruktur SPBE sebagai RK tingkat 2 (kedua).

Selanjutnya untuk mendefinisikan elemen didalamnya, akan dijelaskan dalam pedoman penyusunan Arsitektur SPBE.

1.4 Taksonomi Referensi Keamanan SPBE

Referensi Keamanan(RK) terdiri dari 3 (tiga) domain keamanan di tingkat 1 dan 9 (sembilan) area keamanan di tingkat 2. Referensi Keamanan menjadi acuan bagi penyusunan domain arsitektur keamanan SPBE baik secara nasional maupun untuk IPPD. Rincian mengenai taksonomi RK akan dijelaskan pada **Tabel 1.1.** Atribut Keamanan SPBE dijabarkan pada **Tabel 1.2.**

Tabel 1.1 Taksonomi Referensi Keamanan SPBE

Kode	Referensi Arsitektur	Deskripsi Referensi Arsitektur
Standar Keamanan (01)		
01.01	Standar Teknis dan Prosedur Keamanan SPBE	Standar atau Peraturan Pemerintah yang digunakan untuk penerapan Keamanan SPBE.
01.02	Standar Keamanan Internasional	Standar internasional yang digunakan sebagai pendukung dan untuk meningkatkan penerapan Keamanan SPBE.
01.03	Regulasi Lainnya	Peraturan Pemerintah lainnya selain dari peraturan terkait standar teknis dan prosedur Keamanan SPBE, yang saat ini menjadi acuan dalam penerapan Keamanan SPBE.
Penerapan Keamanan (02)		

Kode	Referensi Arsitektur	Deskripsi Referensi Arsitektur
02.01	Kesadaran Keamanan SPBE	Bentuk kegiatan di IPPD untuk meningkatkan kesadaran keamanan SPBE.
02.02	Kerentanan Keamanan SPBE	Bentuk kegiatan di IPPD untuk mengidentifikasi kerentanan dan risiko keamanan SPBE.
02.03	Peningkatan Keamanan SPBE	Bentuk kegiatan di IPPD untuk meningkatkan keamanan SPBE.
02.04	Penanganan insiden Keamanan SPBE	Bentuk kegiatan di IPPD untuk menanggulangi, memulihkan dan memitigasi risiko insiden keamanan SPBE.
Kelaikan Keamanan (03)		
03.01	Kelaikan Keamanan Aplikasi Umum	Uji kelaikan keamanan terhadap aplikasi umum yang dilakukan melalui penilaian kerentanan secara mandiri di IPPD dan verifikasi di tingkat nasional. Output dari kegiatan ini adalah daftar aplikasi umum yang telah mendapatkan rekomendasi kelaikan keamanan
03.02	Kelaikan Keamanan Infrastruktur SPBE Nasional	Uji kelaikan keamanan terhadap Infrastruktur SPBE nasional yang dilakukan melalui penilaian kerentanan secara mandiri di IPPD dan verifikasi di tingkat nasional. Output dari kegiatan ini adalah daftar Infrastruktur SPBE Nasional yang telah mendapatkan rekomendasi kelaikan keamanan

Tabel 1.2 Atribut Keamanan SPBE

No.	Nama Atribut	Keterangan
1	Jenis Standar Keamanan	Jenis standar keamanan yang diacu dan menjadi prioritas oleh setiap IPPD diantaranya: 1. standar dan/atau Peraturan terkait teknis dan prosedur keamanan SPBE; 2. standar internasional terkait keamanan informasi; atau 3. regulasi lainnya.
2	Keterangan Nama Standar	Nama dari jenis standar keamanan yang diacu dan menjadi prioritas oleh setiap IPPD
3	Hasil Audit Keamanan SPBE	Hasil dari pelaksanaan Audit Keamanan SPBE untuk Aplikasi dan Infrastruktur SPBE yang terdiri dari: 1. Belum/tidak dilaksakan 2. Memadai 3. Perlu peningkatan 4. Tidak memadai (Ket: Untuk data dan informasi tidak dilakukan Audit Keamanan)
4	Tanggal Pelaksanaan Audit	Tanggal penyerahan laporan Audit Keamanan SPBE terbaru untuk Aplikasi dan Infrastruktur SPBE yang bersesuaian (Ket: Untuk data dan informasi tidak dilakukan Audit Keamanan, atribut ini tidak terbuka bila Atribut Audit Keamanan SPBE dijawab dengan "Belum/tidak dilaksanakan")
5	Penerapan Keamanan	Program kerja atau kegiatan Keamanan SPBE yang dilaksanakan oleh setiap IPPD sebagai upaya dalam meminimalkan dampak risiko Keamanan SPBE. Program kerja atau kegiatan Keamanan SPBE sebagaimana dimaksud paling sedikit meliputi: 1. edukasi kesadaran Keamanan SPBE; 2. penilaian kerentanan Keamanan SPBE; 3. peningkatan Keamanan SPBE; dan 4. penanganan insiden Keamanan SPBE

No.	Nama Atribut	Keterangan
6	Pengujian Kelaikan Keamanan	Pengujian kelaikan keamanan yang telah dilaksanakan terhadap pengendalian data dan informasi, persyaratan keamanan Aplikasi Umum SPBE, dan persyaratan keamanan Infrastruktur SPBE Nasional
7	ID metadata terkait	Mengacu kepada metadata SPBE terkait.

BAB 2
Metodologi

Bab 2 menjabarkan metodologi dalam penyusunan Buku 5 Arsitektur Keamanan SPBE. Metodologi yang digunakan terdiri dari 3 (tiga) tahapan yaitu analisa kondisi eksisting, analisis kesenjangan dan analisis usulan keamanan SPBE. Masing-masing tahapan akan dijabarkan pada subbab berikut.

2.1 Analisis Kondisi Eksisting

Analisis kondisi eksisting didapatkan dari hasil analisa data survei yang sudah dilakukan sebelumnya. Terkait dengan keamanan

2.2 Analisis Kesenjangan

Analisis kesenjangan merupakan analisis yang dilakukan untuk mengidentifikasi tindakan-tindakan apa saja yang diperlukan untuk mengurangi kesenjangan atau mencapai kinerja yang diharapkan pada masa datang dari kondisi eksisting yang dibandingkan dengan kondisi ideal untuk Keamanan SPBE. Hasil Kesenjangan sudah disajikan pada buku 1. Proses analisis kesenjangan terdiri dari:

- **Input**

  Input dari tahapan ini yaitu hasil dari tahapan sebelumnya, yaitu analisa kondisi eksisting keamanan infrastruktur saat ini dan hasil analisa penentuan ekspektasi atau target yang ingin dituju terkait Keamanan SPBE.
- **Proses**

  Proses dalam tahapan ini dilakukan dengan membandingkan antara kondisi eksisting keamanan infrastruktur saat ini dengan target atau tujuan Kondisi keamanan infrastruktur yang ingin dituju.
- **Output**

  Output yang dihasilkan berupa list Kesenjangan dari ketidaksesuaian antara kondisi eksisting keamanan infrastruktur saat ini dengan kondisi yang ingin dituju pada setiap indikatornya.

2.2 Analisis Usulan Keamanan

Analisis Keamanan SPBE ini melakukan analisis terkait kebutuhan yang mendukung penerapan Keamanan SPBE. Proses analisis usulan Keamanan SPBE terdiri dari:

- **Input**

  Pada analisis kesenjangangan, berdasarkan dengan Kondisi Eksisting yang didapat sebelumnya akan digunakan sebagai input data pada tahapan awal.

- **Proses**

  Setiap indikator yang ada diperoleh dari Kesenjangan, kemudian Proses selanjutnya dilakukan pencarian terkait solusi berupa usulan untuk memenuhi kondisi yang ingin dicapai dari setiap indikator Keamanan SPBE.

- **Output**

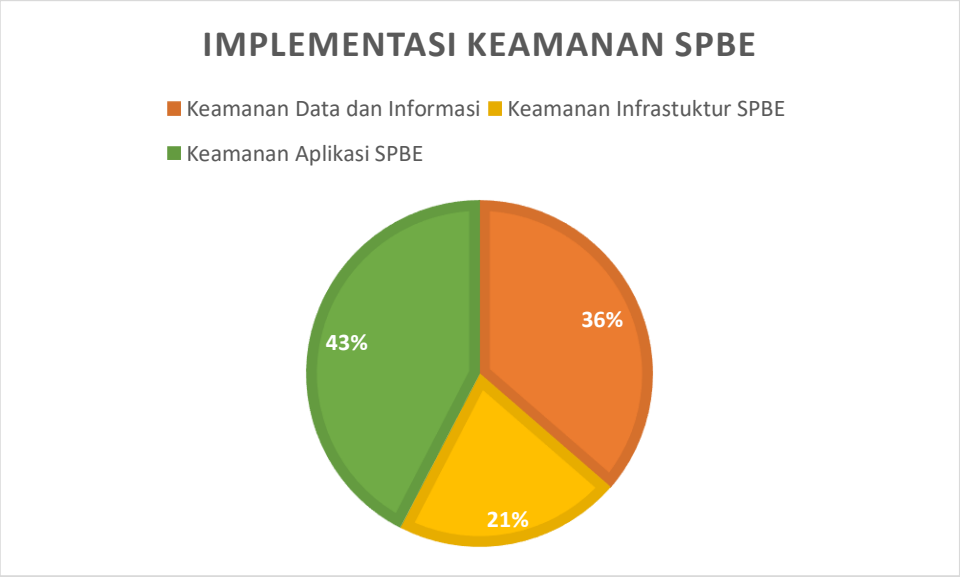
  Hasil dari tahapan ini adalah daftar berupa rekomendasi kebutuhan Keamanan SPBE yang ditujukan kepada Pemerintah Kabupaten Deli Serdang.

BAB 3
Arsitektur Keamanan SPBE

Pada bab ini dijelaskan mengenai kondisi eksisting keamanan SPBE, kesenjangan keamanan SPBE, dan usulan terkait dengan pelaksanaan keamanan SPBE.

3.1 Kondisi Eksisting Keamanan SPBE

Implementasi keamanan SPBE yang meliputi keamanan data dan informasi memiliki persentase **36%**, dimana bentuk keamanan data dan informasi yang diterapkan meliputi penggunaan kunci, standar user name dan password, dan juga framework dalam penulisan program. Selanjutnya keamanan infrastruktur SPBE sebesar **21%** dalam bentuk penerapan finger lock, dan yang terakhir **43%** untuk keamanan aplikasi juga sebatas penerapan password dan juga framework pemrograman. Secara umum, Pemerintah Kabupaten Deli Serdang **belum** menerapkan keamanan SPBE



Gambar 3.1 Implementasi Keamanan SPBE

3.2 Kondisi Kesenjangan SPBE

Berdasarkan hasil analisa yang sudah dilakukan terkait dengan kondisi kesenjangan keamanan SPBE pada Pemerintah Kabupaten Deli Serdang, terdapat beberapa kesenjangan seperti yang dapat dilihat pada **Tabel 3.1.**

Tabel 3.1 Kondisi Kesenjangan Keamanan SPBE

Parameter	Kondisi Eksisting	Kondisi yang ingin dicapai	Gap Analisis
Tata Kelola dan Manajemen Keamanan	Penerapan manajemen keamanan yang dilakukan masih sebatas SOP	Melakukan manajemen keamanan mengacu pada BSSN 10/2019 dan BSSN 4/2021	Penerapan manajemen keamanan yang dilakukan belum maksimal
	Minimnya implementasi dan pemahaman keamanan	Implementasi keamanan SPBE sesuai dengan standar/framework	Minimnya implementasi dan pemahaman keamanan
Audit Keamanan	Belum dilakukannya audit (keamanan, infrastruktur, dan aplikasi, secara berkala	Audit idealnya dilakukan secara rutin dalam 2 tahun sekali	Belum dilakukannya audit secara berkala
	Masih banyak permasalahan keamanan yang terjadi	Meminimalisir terjadinya permasalahan keamanan dengan implementasi audit keamanan	Masih banyak permasalahan keamanan yang terjadi

3.3 Usulan Keamanan SPBE

Usulan Keamanan SPBE dibagi ke dalam 2 kategori yaitu keamanan tata kelola dan keamanan teknis. Keamanan tata kelola mengarah pada sisi manajemen, dimana bentuk keamanan pada kategori tata kelola dapat berupa standar, prosedur atau SOP, kontrol, formulir aktivitas atau kegiatan, dan list dari formulir yang ada.

Kelima hal tersebut saling berkaitan satu sama lain dalam bentuk hierarki. Selanjutnya pada kategori keamanan teknis lebih berfokus pada hal yang lebih teknis, misalnya saja detail dari topologi jaringan yang tersedia, backup terhadap perangkat yang digunakan, hingga dalam hal firewall. Dalam penggunaan peraturan BSSN No.10 Tahun 2019 yang secara konteks lebih mengarah pada persandian, untuk melengkapi pembahasan terkait keamanan dapat digunakan Peraturan BSSN no.4 Tahun 2021 yang secara konteks sudah membahas keamanan SPBE secara spesifik. Sebagai contoh pada BSSN 10 terkait dengan keamanan elektronik dan keamanan komunikasi dapat dikombinasikan dengan BSSN No.4 Tahun 2021 pada poin keamanan sistem penghubung layanan.

3.3.1 Usulan Keamanan Tata Kelola

Usulan terkait keamanan SPBE mengacu pada Peraturan BSSN No.10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan informasi. dan Peraturan BSSN No.4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Sistem Pemerintahan Berbasis Elektronik. Tata Kelola Keamanan Informasi dapat dikategorikan menjadi 9 Kategori yang akan dijelaskan sebagai berikut :

a. Keamanan Sumber Daya Teknologi Informasi

Pada Keamanan Sumber Daya teknologi informasi atau kebijakan Keamanan IT merupakan fondasi dari keamanan infrastruktur yang mana pada kebijakan tersebut dapat mempengaruhi terhadap keberlangsungan sistem kedepannya. Kebijakan keamanan diperlukan untuk melindungi dan mengamankan teknologi informasi.

Tahapan yang dilakukan dapat dimulai dari tahap perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi yang sebelumnya telah disesuaikan dengan ketentuan peraturan perundang-undangan. Aset keamanan teknologi informasi yang dimaksud merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Tabel 3.2 Usulan Kegiatan Keamanan Sumber Daya Teknologi Informasi

NO	Kegiatan	OPD Pelaksana
1	Pengadaan antivirus terpusat	Dinas Komunikasi dan Informatika
2	Pembuatan standar antivirus	Dinas Komunikasi dan Informatika
3	Pembuatan standar pemindaian komputer (daily scanning)	Dinas Komunikasi dan Informatika
4	Pengadaan CCTV di ruang publik	Dinas Komunikasi dan Informatika
5	Pembuatan Prosedur Pengawasan CCTV	Dinas Komunikasi dan Informatika

b. Keamanan Akses Kontrol

Pada standar SNI ISO 27002:2013 membahas mengenai keamanan informasi yang dimana didalamnya terdapat Keamanan Akses Kontrol. Dimana tujuan dari penerapan Keamanan Akses Kontrol yaitu sebagai pembatas terhadap hak akses informasi dari orang atau jaringan yang dianggap dapat berpengaruh dalam suatu instansi. Tahapan yang dapat dilakukan dalam pembatasan akses kontrol dengan membuat Kebijakan Akses Kontrol (*Access Kontrol Policy*) dan Kebijakan Kata Sandi.

Tabel 3.3 Usulan Kegiatan Keamanan Akses Kontrol

No.	Kegiatan	OPD Pelaksana
1	Pembuatan Daftar DNS atau IP yang diperbolehkan	Dinas Komunikasi dan Informatika
2	Pembuatan Standar Hak User (User acces right)	Dinas Komunikasi dan Informatika
3	Pembuatan Pembagian Hak User	Dinas Komunikasi dan Informatika
4	Pembuatan Standar Kata Sandi	Dinas Komunikasi dan Informatika
5	Pembuatan Frekuensi Pengubahan Kata Sandi	Dinas Komunikasi dan Informatika
6	Prosedur penambahan/pergantian/penghapusan Hak Akses	Dinas Komunikasi dan Informatika

c. Keamanan Data dan Informasi

Pada Standar SNI ISO 27001:2013 membahas mengenai Standar Manajemen Keamanan Informasi yang dimana didalamnya terdapat standar mengenai data dan informasi. Dimana tujuannya sebagai penjaminan keamanan data dan informasi untuk memastikan tingkat data dan informasi menerima tingkat perlindungan yang sesuai dengan kepentingan instansi.

Kondisi tingkat keamanan data dan informasi dilihat dari beberapa aspek antara lain:

a. *Confidentiality* (kerahasiaan) dilihat dari adanya klasifikasi keamanan, dan pembatasan akses pada data dan informasi.
b. *Integrity* (keutuhan) dapat dilihat melalui adanya enkripsi/dekripsi terhadap data dan informasi yang disimpan.
c. *Availability* (ketersediaan akses) dapat dilihat dengan adanya backup dan recovery pada sistem yang digunakan.
d. *Authentication* (keaslian) dilihat melalui adanya mekanisme verifikasi dan validasi untuk mengakses data dan informasi.
e. *Non*-Repudation (kenirsangkalan) dapat dilihat melalui tersedianya fasilitas untuk adanya tandatangan atau sertifikat yang bersifat digital.

Tabel 3.4 Usulan Kegiatan Keamanan Data dan Informasi

NO	Kegiatan	OPD Pelaksana
1	Pembuatan Standar Klasifikasi Data dan Informasi	Dinas Komunikasi dan Informatika
2	Pembuatan Pelabelan Data dan Informasi	Dinas Komunikasi dan Informatika
3	Pembuatan Kebijakan Keamanan Informasi	Dinas Komunikasi dan Informatika

d. Keamanan Sumber Daya Manusia

Keamanan Sumber Daya Manusia harus memiliki kontrak yang berisi bahwa tiap pegawai tanggung jawab, peran, dan hukuman yang diberikan jika melanggar yang bertujuan untuk memastikan bahwa Sumber Daya Manusia tersebut mengerti akan tanggung jawab dan tupoksi yang sesuai guna menunjang keamanan sumber

daya manusia. Pada Standar SNI ISO 27001:2013 Memiliki 3 sasaran terkait keamanan sumber daya manusia antara lain:

a. Sebelum dipekerjakan, yang dimana sasarannya untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka sesuai dengan peran yang sudah ditetapkan bagi mereka. Terdiri dari Penyaringan, dan syarat dan ketentuan pegawai.
b. Selama Bekerja, yang dimana sasarannya untuk memastikan bahwa pegawai dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka. Terdiri dari Tanggung jawab manajemen, Kepedulian, Pendidikan dan pelatihan Keamanan Informasi, dan Proses pendisiplinan.
c. Penghentian dan Perubahan Pegawai, yang dimana sasarannya untuk melindungi kepentingan organisasi sebagai bagian dari proses pengubahan atau penghentian pegawai. Terdiri dari penghentian atau perubahan tanggung jawab kepegawaian.

Berdasarkan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, pengelolaan sumber daya manusia mencakup 3 (tiga) hal yaitu: Pengembangan Kompetensi Pengembangan kompetensi dilakukan melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop*, seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi. Mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau pemerintah daerah masing-masing. Memenuhi jumlah waktu minimal sebagai seorang pegawai untuk meningkatkan kompetensi dibidangnya.

Tabel 3.5 Usulan Kegiatan Sumber Daya Manusia

NO	Kegiatan	OPD Pelaksana
1	Pendayagunaan SDM untuk bidang keamanan informasi	Dinas Komunikasi dan Informatika
2	Peningkatan kompetensi SDM bidang keamanan informasi	Dinas Komunikasi dan Informatika
3	Pembuatan Prosedur Rekrut pegawai Baru	Dinas Komunikasi dan Informatika
4	Pembuatan Standar Pegawai Baru	Dinas Komunikasi dan Informatika

e. Keamanan Jaringan

Pada Peraturan Presiden No.95 Tahun 2018 menjelaskan bahwa dalam Infrastruktur SPBE terdiri atas 2 Jaringan yaitu Jaringan Intra Pemerintah dan jaringan Internet. Jaringan Intra Pemerintah meliputi Jaringan Intra Instansi Pusat dan Pemerintah daerah. Jaringan intra pemerintah yang dimaksud yaitu jaringan interkoneksi tertutup dimana menghubungkan antar Jaringan Intra Instansi Pusat dan Pemerintah Daerah. Sedangkan jaringan internet adalah jaringan umum yang dapat digunakan secara bebas.

Dalam penerapan keamanan dapat menerapkan Standar SNI ISO 27001:2013, terkait keamanan jaringan dengan cara mengimplementasikan pembatasan pengguna terhadap akses jaringan yang dianggap perlu diamankan oleh Kabupaten Deli Serdang, untuk menjaga keamanan perlu dibuatkan kebijakan terkait jaringan (*Network Policy*) yang dapat dijadikan acuan bagi seluruh pengguna jaringan yang ada di Kabupaten Deli Serdang. Untuk memantau Keamanan Jaringan perlu dilaksanakan monitoring jaringan atau *network administration* agar dapat mengetahui kondisi jaringan yang digunakan oleh keseluruhan sistem yang ada pada Kabupaten Deli Serdang dengan melihat daftar (Domain Name Server) DNS dan (Internet Protokol Address) IP Address yang terdaftar dan yang diperbolehkan untuk mengakses jaringan.

Tabel 3.6 Usulan Kegiatan Keamanan Jaringan

NO	Kegiatan	OPD Pelaksana
1	Pembuatan Kebijakan Jaringan (*Network Policy*)	Dinas Komunikasi dan Informatika
2	Pembuatan Kebijakan Pengiriman Informasi	Dinas Komunikasi dan Informatika
3	Pembuatan Prosedur Pengiriman Informasi	Dinas Komunikasi dan Informatika

f. Keamanan Surat Elektronik

Pada Standar SNI ISO 27001:2013 terkait dengan Keamanan Surat Elektronik, dijelaskan bahwa diperlukannya pembuatan kebijakan terkait pengiriman informasi dan prosedur pengiriman informasi untuk menjamin keamanan surat elektronik baik secara elektronik maupun non elektronik. Didalam

kebijakan tersebut menjelaskan mengenai penggunaan yang digunakan untuk mengamankan pesat dari surat elektronik dapat menggunakan teknik *Blockchain*, *Cryptographic*, dan beberapa teknik lainnya serta tata cara pengirimannya yang harus disesuaikan dengan prosedur pengiriman informasi.

Tabel 3.7 Usulan Kegiatan Keamanan Surat Elektronik

NO	Kegiatan	OPD Pelaksana
1	Pengadaan Digital Signature	Dinas Komunikasi dan Informatika
2	Pembuatan Prosedur *digital signature*	Dinas Komunikasi dan Informatika

g. Keamanan Komunikasi

Pada Standar SNI ISO 27001:2013 Terkait dengan Keamanan Komunikasi memiliki tujuan untuk memastikan informasi yang dibagikan pada jaringan internal tetap aman dan dapat diakses oleh orang yang memiliki wewenang saja. Penerapan Keamanan Komunikasi harus dilaksanakan dengan secara teknis dan Non-Teknis.

Tabel 3.8 Usulan Kegiatan Keamanan Komunikasi

NO	Kegiatan	OPD Pelaksana
1	Implementasi *encryption techniques*	Dinas Komunikasi dan Informatika
2	Kebijakan Komunikasi	Dinas Komunikasi dan Informatika
3	Prosedur Berkomunikasi yang aman	Dinas Komunikasi dan Informatika
4	Prosedur Teleworking	Dinas Komunikasi dan Informatika

h. Keamanan Perangkat Informasi

Keamanan informasi merupakan hal penting dalam penyelenggaraan layanan. Dengan semakin meningkatnya risiko dan insiden keamanan informasi dalam penyelenggaraan sistem elektronik, upaya pengamanan terhadap sistem elektronik yang memiliki data dan informasi strategis dan penting wajib segera dilakukan. Keamanan informasi yang handal, akan meningkatkan kepercayaan masyarakat terhadap penyelenggaraan sistem elektronik untuk pelayanan publik.

Tabel 3.9 Usulan Kegiatan Keamanan Perangkat Informasi

NO	Kegiatan	OPD Pelaksana
1	Penerapan *Public Key Infrastructure* (PKI)	Dinas Komunikasi dan Informatika
2	Pembuatan Standart *Public Key Infrastructure* (PKI)	Dinas Komunikasi dan Informatika
3	Prosedur Pemadaman/memutus/ mengaktifkan/ meyalakan Aplikasi	Dinas Komunikasi dan Informatika

i. Keamanan Pusat Data

Data center atau pusat data merupakan jaringan server dan perangkat komputer yang memproses, mendistrubusi, dan menyimpan data berharga, dan menjadi komponen penting bagi infrastruktur digital perusahaan. Pusat data menggabungkan kebijakan, proses, prosedur, dan teknologi yang melindung data dari serangan maupun ancaman siber. Dengan banyaknya informasi yang tersimpan dalam pusat data, tentunya keamanan menjadi faktor yang sangat diperhatikan. Berbicara keamanan tentunya tidak lepas dengan standar atau sertifikasi yang berkaitan dengan keamanan. Beberapa standar keamanan yang berkaitan dengan pusat data adalah TIA-942 untuk standar fisik pusat data, SSL/TLS yang berkaitan protokol keamanan jaringan dalam bentuk enkripsi. Bentuk keamanan fisik pusat data yang perlu ada setidaknya meliputi:

- Lokasi: Lokasi pusat data idealnya terpisah dari kantor pusat dengan tetap memperhatikan keadaan lingkungan sekitar, misalnya dari potensi bencana alam dan ketersediaan infrastruktur pendukung seperti sumber listrik
- Konstruksi Bangunan: Bangunan pusat data harus memiliki sirkulasi udara yang baik dan cukup. Hal ini berkaitan dengan suhu yang dapat mempengaruhi kinerja dari server. Penerapan yang umum digunakan dalam konstruksi pusat data diantaranya, raised floor, penggunaan pendingin ruangan, pemisahan ruang administratif dan ruang server, peletakan kabel dan tentunya akses masuk.

Tabel 3.10 Usulan Kegiatan Keamanan Pusat Data

NO	Kegiatan	OPD Pelaksana
1	Penyewaan DRC (*Disaster Recovery Center*)	Dinas Komunikasi dan Informatika
2	Penerapan Demilitarized Zone (DMZ)	Dinas Komunikasi dan Informatika
3	Penerapan firewall pada ruang server Diskominfo	Dinas Komunikasi dan Informatika
4	Pembuatan standar perangkat firewall	Dinas Komunikasi dan Informatika
5	Pembuatan standar perangkat UPS	Dinas Komunikasi dan Informatika
6	Pembuatan Prosedur Perawatan Rutin Perangkat UPS	Dinas Komunikasi dan Informatika
7	Penerapan Teknologi *Face regconize*	Dinas Komunikasi dan Informatika
8	Implementasi ruang situs dan tata letak (*site spave and layout*)	Dinas Komunikasi dan Informatika
9	Implementasi Infrastruktur Pengkabelan	Dinas Komunikasi dan Informatika
10	Implementasi *Tired Realibility*	Dinas Komunikasi dan Informatika
11	Prosedur Akses Pusat Data	Dinas Komunikasi dan Informatika
12	Prosedur menambah/mengurangi perangkat pada server di ruang server	Dinas Komunikasi dan Informatika
13	Prosedur Remote server	Dinas Komunikasi dan Informatika
14	Prosedur Perawatan Server	Dinas Komunikasi dan Informatika
15	Prosedur insiden menejemen	Dinas Komunikasi dan Informatika

3.3.2 Usulan Keamanan Teknis

Keamanan teknis lebih mengarah pada hal teknis dalam infrastruktur SPBE. Hal teknis yang dibahas pada infrastruktur meliputi kebutuhan **topologi jaringan hingga aset fisik yang berkaitan dengan IT.** Beberapa hal teknis yang perlu dilakukan persiapan terkait dengan keamanan diantaranya adalah sebagai berikut:

a) **Pengaturan Role Permission untuk IP Address** tertentu sesuai dengan kebutuhan masing masing role. Biasanya juga melihat berdasarkan jabatan dan ranah kerja.

b) Pada penerapan teknis dalam pengamanan keamanan komunikasi harus menggunakan **encryption techniques** tertentu agar tidak mudah diakses dan diketahui oleh pihak luar terkait data infomasi maupun hal lainnya yang berhubungan dengan Pemerintah Kabupaten Deli Serdang.

c) **Kondisi konstruksi bangunan.** Kondisi fisik bangunan perlu dilakukan pemeriksaan dan perbaikan secara berkala. Salah satu bangunan yang

memerlukan perhatian khusus adalah ruang server. Dimana ruang server merupakan lokasi penyimpanan data dengan kompleksitas bangunan yang cukup rumit jika dibangun mengikuti standar yang berlaku.

d) **Penggunaan lisensi terbaru.** Untuk perangkat lunak yang menggunakan lisensi perlu dilakukan pengecekan dan *update* secara berkala agar fitur yang digunakan selalu dalam kondisi terbaru.
e) **Monitoring kondisi fisik perangkat TI**. Sebagai contoh untuk perangkat yang perlu dilakukan pengecekan secara rutin diantaranya adalah UPS, CCTV, router, switch, dan lainnya.
f) **Melakukan reviu secara berkala pada setiap SOP yang berlaku.** Hal ini bertujuan untuk memastikan SOP yang berlaku masih relevan dengan kondisi eksisting di lapangan.
g) **Melakukan pelatihan, bimbingan teknis, atau bahkan sertifikasi** untuk meningkatkan kualitas SDM terutama dalam pemenuhan SDM dengan kemampuan TIK.

Dari **sisi teknis penerapan keamanan** dalam hal aplikasi dapat dilakukan, sebagai berikut:

a) Menerapkan fungsi validasi input pada sisi server
b) Menerapkan mekanisme penolakan input jika terjadi kesalahan validasi
c) Memastikan runtime environment aplikasi tidak rentan terhadap serangan
d) Melakukan validasi dan filter terhadap data yang masuk, termasuk untuk data yang tidak terpercaya
e) Menerapkan kode yang dinamis untuk mengakomodir perubahan
f) Menerapkan fungsi kriptografi

Usulan keamanan teknis yang telah dijabarkan sebelumnya, dapat disimpulkan pada **Tabel 3.11**

Tabel 3.11 Usulan Keamanan Teknis

Kegiatan	Pelaksanaan
Pengaturan Role Permission untuk IP Address	Dinkominfo
Pengamanan keamanan komunikasi menggunakan encryption techniques	Dinkominfo

Kegiatan	Pelaksanaan
Pemeriksaan dan perbaikan secara berkala Kondisi konstruksi bangunan	Dinkominfo
Penggunaan lisensi terbaru	Dinkominfo
Monitoring kondisi fisik perangkat TI	Dinkominfo
Melakukan reviu secara berkala pada setiap SOP yang berlaku	Dinkominfo
Melakukan pelatihan, bimbingan teknis, atau bahkan sertifikasi	Dinkominfo

3.4 Penerapan Keamanan SPBE

Berdasarkan Draf Arsitektur Sistem Pemerintah Berbasis Elektronik Nasional, penerapan keamanan harus memenuhi standar teknis dan prosedur keamanan. Penerapan keamanan merupakan serangkaian proses dalam bentuk program kerja keamanan SPBE yang harus dilakukan oleh setiap OPD sebagai upaya dalam meminimalkan dampak risiko keamanan SPBE. Program kerja keamanan SPBE disusun berdasarkan kategori risiko terhadap aplikasi, data dan informasi, serta infrastruktur dari setiap OPD. Target pelaksanaan program kerja keamanan SPBE ditetapkan berdasarkan kebutuhan setiap OPD. Program kerja keamanan SPBE sebagaimana dimaksud setidaknya meliputi:

3.4.1 Kesadaran Keamanan SPBE

Dalam meningkatkan kesadaran keamanan SPBE, salah satu yang dapat dilakukan adalah dengan memperbanyak literasi terkait dengan keamanan dalam lingkungan Pemerintah Kabupaten Deli Serdang. Kegiatan peningkatan kesadaran keamanan dapat mengacu pada **BSSN 4 Tahun 2021, ISO 27001:2013** dan **kebijakan internal terkait keamanan SPBE**. Bentuk kegiatan peningkatan kesadaran keamanan dapat dilakukan dengan melakukan reminder dalam bentuk email blast secara berkala kepada OPD. Salah satu contoh peningkatan kesadaran keamanan adalah **mengingatkan dan mengedukasi setiap pengguna** pada Pemerintah Kabupaten Deli Serdang untuk secara rutin **mengganti kata sandi serta menerapkan tingkat kompleksitas kata sandi yang digunakan**.

3.4.2 Kerentanan Keamanan SPBE

Kerentanan keamanan dapat dilakukan dengan melakukan uji penetrasi terhadap aplikasi ataupun dengan menganalisis aset yang dimiliki. Berdasarkan dengan Peraturan BSSN No.4 Tahun 2021 terkait Penilaian Kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf b dilaksanakan setidaknya dengan melakukan:

a) **Menginventarisasi seluruh aset SPBE** meliputi data dan informasi, aplikasi, dan infrastruktur yang ada pada Pemerintah Kabupaten Deli Serdang.
b) **Mengidentifikasi kerentanan dan ancaman terhadap aset SPBE** dengan cara melakukan **penetration testing dan vulnerability assessment** pada data dan informasi, aplikasi dan infrastruktur yang ada pada lingkup Pemerintah Kabupaten Deli Serdang.
c) **Melakukan pengukuran tingkat risiko keamanan SPBE** pada lingkup Pemerintah Kabupaten Deli Serdang.
d) **Melakukan analisis dan evaluasi kerentanan keamanan SPBE** lingkup Pemerintah Kabupaten Deli Serdang.

3.4.3 Peningkatan Keamanan SPBE

Pada Peraturan BSSN No.4 Tahun 2021 Pasal 11 (1) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 terkait Peningkatan Keamanan SPBE dilaksanakan paling sedikit melalui:

a) Menerapkan standar teknis dan prosedur Keamanan SPBE
b) Menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE

Berdasarkan pada pasal 14 Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (3), Instansi Pusat dan Pemerintah Daerah paling sedikit melakukan kegiatan:

a) **Pelatihan dan/atau sertifikasi kompetensi** keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi.
b) **Melakukan bimbingan teknis** mengenai standar Keamanan SPBE.

Dalam rangka meningkatkan keamanan SPBE pada lingkup Pemerintah Kabupaten Deli Serdang, Dinas Komunikasi dan Informatika dapat memberikan rekomendasi untuk **peningkatan keamanan kepada OPD yang memiliki server**. Peningkatan yang diberikan setidaknya dapat mengacu pada standar yang sudah diterapkan oleh Dinas Komunikasi dan Informatika. Salah satu contoh bentuk peningkatan yang dapat dilakukan adalah dengan merekomendasikan kepada OPD yang memiliki server untuk menerapkan ruang tertutup atau DMZ.

3.4.4 Penanganan Insiden Keamanan SPBE

Pada Peraturan BSSN No.4 Tahun 2021 terkait Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf d dilaksanakan paling sedikit melalui:

a) Mengidentifikasi sumber serangan
b) Menganalisis informasi yang berkaitan dengan insiden selanjutnya
c) Memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi.
d) Mendokumentasi bukti insiden yang terjadi.
e) Memitigasi atau mengurangi dampak risiko Keamanan SPBE.

Kegiatan yang dapat dilakukan dalam penanganan insiden keamanan SPBE dengan melalui **kegiatan peningkatan kesadaran keamanan TI**, baik dilakukan dalam bentuk **sosialisasi** ataupun peningkatan kompetensi melalui **sertifikasi**. Selain itu penanganan insiden dapat dibuatkan **standar operasional prosedur (SOP).** SOP merupakan panduan oleh pelaksana lapangan baik ketika terjadi insiden keamanan maupun sebagai bentuk panduan yang perlu dilakukan secara berkala. Wujud nyata yang umum ditemukan dalam kegiatan penanganan insiden juga dapat dituangkan dalam **bentuk catatan atau laporan penanganan insiden, check list dan *log book* yang dilakukan secara berkala.**

Tabel 3.12 Usulan Penerapan Keamanan SPBE

Aspek	Kegiatan	Penanggung Jawab	Pelaksana
Kesadaran Keamanan SPBE	Melakukan Pengingat menggunakan *email blast* kepada setiap OPD	Dinkominfo	Seluruh OPD
Kerentanan Keamanan SPBE	Menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur	Dinkominfo	Badan Perencanaan Pembangunan Daerah
	penetration testing dan vulnerability assessment	Dinkominfo	DINKOMINFO
	Melakukan pengukuran tingkat risiko keamanan SPBE	Dinkominfo	Inspektorat
	Melakukan analisis dan evaluasi kerentanan keamanan SPBE	Dinkominfo	Dinkominfo
Peningkatan Keamanan SPBE	Menerapkan standar teknis dan prosedur Keamanan SPBE	Dinkominfo	Seluruh OPD
	Menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE	Dinkominfo	Dinkominfo
	Pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi	Dinkominfo	Badan Kepegawaian dan Pengembangan SDM
	Melakukan bimbingan teknis mengenai standar Keamanan SPBE	Dinkominfo	Dinkominfo

Aspek	Kegiatan	Penanggung Jawab	Pelaksana
	peningkatan keamanan kepada OPD yang memiliki server untuk menerapkan ruang tertutup	Dinkominfo	OPD pemilik server
Penanganan Insiden Keamanan SPBE	Sosialisasi kegiatan peningkatan kesadaran keamanan TI	Dinkominfo	Dinkominfo
	Peningkatan kompetensi melalui sertifikasi keamanan TI	Dinkominfo	Badan Kepegawaian dan Pengembangan SDM
	Standar operasional prosedur Penanganan Insiden	Dinkominfo	Dinkominfo
	Pembuatan catatan atau laporan penanganan insiden, check list dan *logbook* yang dilakukan secara berkala	Dinkominfo	Seluruh OPD

3.5 Audit

Audit merupakan penilaian atau evaluasi teknis yang sistematis dan terukur mengenai keamanan data dan informasi, audit dilakukan secara berkala untuk meminimalisir terjadinya permasalahan keamanan informasi pada Pemerintahan Kabupaten Deli Serdang seperti kebocoran data dan informasi, mengamankan aset serta memastikan bahwa tahapan yang digunakan telah sesuai dengan SOP/Prosedur. Standar internasional yang paling umum digunakan dalam membahas sistem manajemen keamanan informasi adalah ISO 27001 yang secara kerangka sudah memenuhi keseluruhan aspek organisasi. ISO 27001:2013 memiliki 114 kontrol keamanan informasi yang pada pelaksanaannya dapat dipilih kontrol mana yang paling relevan dengan kondisi eksisting Pemerintahan Kabupaten Deli Serdang atau dapat membuat standar tersendiri dengan mengacu pada ISO

27001:2013 dengan mengadopsi kontrol mana yang sesuai dengan kebutuhan masing masing OPD. Pada tahapan awal penilaian ISO 27001:2013 mengacu pada penilaian risiko dan aset yang nantinya dapat dikembangkan lebih lanjut sebagai bentuk kontrol keamanan informasi. Penerapan ISO 27001:2013 dibagi menjadi beberapa tahapan dan dapat dikembangkan dikemudian hari sesuai dengan kebutuhan. Di dalam ISO 27001:2013 terdapat tahapan PDCA (*Plan-Do-Check-Act*) yang masing-masing akan dijelaskan pada **Tabel 3.13**,

Tabel 3.13 Tahapan PDCA

A. Tahapan Plan	
1.	Menentukan Ruang lingkup
	- Mempelajari Karakteristik Pemerintahan Kabupaten Deli Serdang mulai dari profil, visi, misi, serta tujuan yang ingin dicapai serta mempelajari tugas pokok serta struktur organisasi pada Pemerintahan Kabupaten Deli Serdang - Mengumpulkan informasi tentang seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur pada Pemerintahan Kabupaten Deli Serdang, Hal ini berguna untuk mengumpulkan informasi yang dapat digunakan ketika penilaian terhadap aset
2.	Membuat Kebijakan SMKI
	- Kebijakan sistem manajemen keamanan informasi yang mendefinisikan tanggung jawab, tugas umum dan khusus sehingga kebijakan tersebut dapat dipahami dan dijalankan pada OPD
B. Tahapan DO	
1.	Melakukan Identifikasi Risiko
	- Melakukan identifikasi aset yang telah dikumpulkan pada tahap *plan*, Kemudian dinilai berdasarkan tiga aspek keamanan informasi yaitu kerahasiaan (*confidentiality)*, keutuhan (*integrity*), dan ketersediaan *(Availability)* - Melakukan identifikasi terhadap ancaman dan kelemahan aset yang berpotensi dapat mengganggu proses bisnis

2.	Analisis dan Evaluasi Risiko
	- Melakukan analisis terhadap (*Busines Impact Analysis*) yang ditimbulkan - Melakukan identifikasi risiko diterima atau perlu pengelolaan risiko oleh OPD penanggung jawab
C. Tahapan Check	
1.	- Pemilihan objektif kontrol dan kontrol keamanan berdasarkan hasil penilaian terhadap risiko, aset utama/pendukung dan dampak terhadap pemerintahan
2.	Penilaian Maturity Level Menggunakan SSE-CCCM
	- Membuat pernyataan berdasarkan kontrol keamanan yang dipilih sesuai dengan kebutuhan untuk diterapkan pada pemerintahan kabupaten Deli Serdang dan disesuaikan berdasarkan standar ISO 27001:2013 - Menentukan nilai tingkat kemampuan pada tiap pernyataan digunakan *sysem security engineering capability maturity level* (SSE-CMM) - Perhitungan *maturity level*
B. Tahapan Act	
1.	Penelusuran Bukti
	- Penelusuran bukti berdasarkan hasil penilaian *maturity level* agar sesuai dengan kondisi eksisting keamanan dan untuk mengetahui apakah terdapat GAP antara kondisi saat ini dengan panduan implementasi keamanan yang ada pada ISO 27001:2013
2.	Rekomendasi
1	- Memberikan usulan perbaikan serta pengembangan terhadap sistem manajemen keamanan pada pemerintahan Kabupaten Deli Serdang dengan memberikan rekomendasi sesuai dengan GAP yang didapatkan

	serta berisi panduan implementasi tiap kontrol keamanan yang ada pada ISO 27001:2013

Pada **Tabel 3.14** diuraikan mengenai beberapa aktivitas terkait dengan audit dimulai sejak tahapan awal yaitu penyiapan pembentukan tim audit hingga proses evaluasi. Idealnya proses audit dilakukan setiap **dua tahun sekali** dan dilakukan oleh **Auditor Eksternal Bersertifikasi** atau minimal dilakukan oleh auditor internal.

Tabel 3.14 Aktivitas Audit

Audit SPBE	Aktivitas	Standar / Framework
Audit Infrastruktur SPBE	a. Penyiapan tim audit	ISO/IEC 19770-1:2017
	b. *Quick assessment*	
	c. Penyiapan rencana audit	
	d. Penyepakatan rencana audit	
	e. Penyiapan protokol audit	
	f. Penetapan parameter acuan	
	g. Pertemuan pembukaan	
	h. Pelaksanaan lapangan	
	i. Pertemuan penutupan	
	j. Analisa data	
	k. Pengelolaan data	
	l. Penyusunan laporan	
	m. *Proof-read* laporan	
	n. Penyerahan laporan	
	o. Evaluasi aktivitas	
Audit Aplikasi SPBE	a. Penyiapan tim audit	ISO 9001:2015, ISO/IEC/IEEE 90003:2018
	b. *Quick assessment*	
	c. Penyiapan rencana audit	

Audit SPBE	Aktivitas	Standar / Framework
	d. Penyepakatan rencana audit	
	e. Penyiapan protokol audit	
	f. Penetapan parameter acuan	
	g. Pertemuan pembukaan	
	h. Pelaksanaan lapangan	
	i. Pertemuan penutupan	
	j. Analisa data	
	k. Pengelolaan data	
	l. Penyusunan laporan	
	m. Proof-read laporan	
	n. Penyerahan laporan	
	o. Evaluasi aktivitas	
Audit Keamanan SPBE	a. Permintaan	Indeks KAMI, ISO 27001
	b. Penugasan	
	c. Perencanaa	
	d. Pelaksanaan