



PERATURAN KEPALA BADAN SIBER DAN SANDI NEGARA

NOMOR 15 TAHUN 2024

TENTANG

PENGGUNAAN INSTRUMEN AUDIT KEAMANAN  
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA

Menimbang : a. bahwa Badan Siber dan Sandi Negara berkewajiban untuk melaksanakan audit keamanan sistem pemerintahan berbasis elektronik terhadap aplikasi umum dan infrastruktur sistem pemerintahan berbasis elektronik nasional;

b. bahwa untuk menjamin keseragaman penyelenggaraan pelaksanaan audit keamanan sistem pemerintahan berbasis elektronik diperlukan instrumen audit keamanan sistem pemerintahan berbasis elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b perlu menetapkan Peraturan Kepala Badan Siber dan Sandi Negara tentang penggunaan instrumen audit keamanan sistem pemerintahan berbasis elektronik;

Mengingat : Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas

Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN SIBER DAN SANDI NEGARA TENTANG PENGGUNAAN INSTRUMEN AUDIT KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

Pasal 1

Dalam Peraturan Kepala Badan ini yang dimaksud dengan :

1. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana/media.
2. Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset Teknologi Informasi dan Komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara Teknologi Informasi dan Komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
3. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk memberikan layanan kepada pengguna SPBE.
4. Audit Keamanan SPBE adalah Audit TIK cakupan keamanan SPBE.
5. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
6. Instansi Pusat adalah kementerian, lembaga pemerintah non kementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
7. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin

pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.

8. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
9. Infrastruktur SPBE Nasional adalah Infrastruktur SPBE yang terhubung dengan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah dan digunakan secara pakai oleh Instansi Pusat dan Pemerintah Daerah.
10. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar dan digunakan secara pakai oleh Instansi Pusat dan/ atau Pemerintah Daerah.
11. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh Instansi Pusat atau Pemerintah Daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan Instansi Pusat dan Pemerintah Daerah lain.

## Pasal 2

Instrumen Audit Keamanan SPBE digunakan untuk memberikan panduan kepada tim auditor Keamanan SPBE dalam melaksanakan Audit Keamanan SPBE.

## Pasal 3

- (1) Instrumen Audit Keamanan SPBE terdiri atas:
  - a. rencana Audit Keamanan SPBE;
  - b. area pemeriksaan Audit Keamanan SPBE ; dan
  - c. konklusi Audit Keamanan SPBE.
- (2) Rencana Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf a paling sedikit memuat informasi:
  - a. objek audit;
  - b. kriteria audit;
  - c. informasi auditan;
  - d. ruang lingkup audit;
  - e. waktu pelaksanaan audit; dan

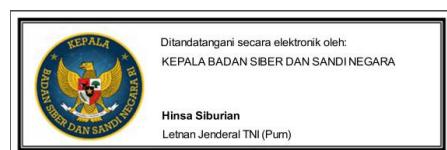
- f. tim auditor Keamanan SPBE.
- (3) Area pemeriksaan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf b terdiri atas:
- Manajemen keamanan informasi SPBE; dan
  - Standar teknis dan prosedur Keamanan SPBE.
- (4) Konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf c merupakan penilaian atas hasil audit Keamanan SPBE berdasarkan pemeriksaan terhadap:
- desain kontrol Keamanan SPBE;
  - implementasi kontrol Keamanan SPBE; dan
  - efektivitas kontrol Keamanan SPBE.
- (5) Tata cara penggunaan instrumen Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Kepala Badan ini.

#### Pasal 4

Peraturan Kepala Badan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta  
pada tanggal 27 Desember 2024

KEPALA BADAN SIBER DAN SANDI NEGARA,



HINSA SIBURIAN

LAMPIRAN

PERATURAN KEPALA BADAN SIBER DAN SANDI NEGARA

NOMOR 15 TAHUN 2024

TENTANG

PENGGUNAAN INSTRUMEN AUDIT KEAMANAN SISTEM  
PEMERINTAHAN BERBASIS ELEKTRONIK

TATA CARA PENGGUNAAN INSTRUMEN AUDIT KEAMANAN

SPBE

BAB I

KERANGKA KERJA AUDIT KEAMANAN SPBE

A. Kebijakan Umum Audit Keamanan SPBE

Audit Keamanan SPBE merupakan salah satu Proses Bisnis dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan salah satu dari 7 (tujuh) hal yang tertuang dalam Peta Rencana SPBE Nasional dan disusun dalam program dan/atau kegiatan SPBE Nasional.

Badan Siber dan Sandi Negara yang kemudian dinyatakan sebagai lembaga pelaksana audit TIK Pemerintah cakupan Keamanan SPBE melaksanakan audit keamanan terhadap objek audit yaitu Aplikasi Umum dan Infrastruktur Nasional setiap tahunnya.

B. Klasifikasi Prosedur Audit dan Instrumen Audit Keamanan SPBE

Instrumen Audit Keamanan SPBE merupakan alat bantu untuk Auditor Keamanan SPBE melakukan pemeriksaan keamanan pada kegiatan Audit Keamanan SPBE. Instrumen ini bersifat terbatas dan hanya digunakan oleh Auditor Keamanan SPBE pada lembaga pelaksana audit TIK Pemerintah Cakupan Keamanan SPBE.

### C. Kriteria Audit Keamanan SPBE

Kriteria Audit Keamanan SPBE adalah peraturan perundang-undangan dan/atau kebijakan, prosedur, dan instruksi kerja, serta standar dan praktik-praktik terbaik, yang digunakan oleh Auditor Keamanan SPBE untuk melakukan evaluasi dan pengujian atas implementasi yang dilaksanakan oleh Instansi Pusat dan Pemerintah Daerah. Kriteria Audit Keamanan SPBE meliputi hal pokok teknis pada tata kelola keamanan SPBE, manajemen keamanan SPBE, fungsionalitas dan kinerja keamanan SPBE, aspek keamanan lainnya. Empat hal pokok teknis yang disebut diatas, diselaraskan pada pengaturan kebijakan makro dan meso terkait Keamanan SPBE dan perlindungan data pribadi. Kebijakan makro dan meso yang ditetapkan dalam peraturan perundang-undangan.

Dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik yang menjadi kebijakan makro telah diatur terkait substansi Keamanan SPBE yang harus diterapkan oleh Instansi Pusat dan Pemerintah Daerah. Penerapan Keamanan SPBE meliputi 2 (dua) hal yaitu Manajemen Keamanan Informasi dan Standar Teknis dan Prosedur Keamanan SPBE yang diatur oleh Peraturan Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber. Badan Siber dan Sandi Negara kemudian mengatur 2 (dua) hal tersebut melalui Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.

Peraturan tersebut menjadi kriteria pokok dalam pemeriksaan audit keamanan. Auditor Keamanan SPBE dapat menambahkan kriteria audit berdasarkan peraturan internal, prosedur dan instruksi kerja pada Instansi Pusat dan Pemerintah Daerah yang diterapkan dan dijalankan terkait Keamanan SPBE.

### D. Kontrol Keamanan SPBE

Kontrol Keamanan merupakan sekumpulan aktivitas keamanan yang harus didefinisikan dan dilaksanakan. Kontrol keamanan diturunkan dari kriteria audit keamanan.

Dalam Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, kontrol keamanan diambil dari pasal, ayat dan poin yang terkandung dalam penjelasan peraturannya tersebut. Kontrol keamanan akan diuraikan pada Bab II dan Bab III.

#### E. Area dan Sasaran Pemeriksaan

##### 1. Area Pemeriksaan

Penggunaan Instrumen Audit Keamanan SPBE pada peraturan ini memiliki 2 (dua) area pemeriksaan, yaitu:

- a) Manajemen Keamanan Informasi SPBE; dan
- b) Standar Teknis dan Prosedur Keamanan Aplikasi.

##### 2. Sasaran Pemeriksaan

Sasaran Pemeriksaan pada area Manajemen Keamanan Informasi SPBE yaitu:

- a) penetapan ruang lingkup;
- b) penetapan penanggung jawab;
- c) perencanaan;
- d) dukungan pengoperasian;
- e) evaluasi kinerja; dan
- f) perbaikan berkelanjutan

##### 3) Sasaran Pemeriksaan pada area Standar Teknis dan Prosedur Keamanan Aplikasi yaitu:

- a) autentikasi;
- b) manajemen sesi;
- c) persyaratan kontrol akses;
- d) validasi input;
- e) kriptografi pada verifikasi statis;
- f) penanganan eror dan pencatatan log;
- g) proteksi data;
- h) keamanan komunikasi;
- i) pengendalian kode berbahaya;
- j) logika bisnis;
- k) file;
- l) keamanan *Application programming interface* dan *web service*; dan
- m) keamanan konfigurasi.

#### F. Tahapan Audit Keamanan SPBE

Tahapan Audit Keamanan SPBE terdiri dari 4 (empat) tahapan pelaksanaan, yaitu terdiri dari Pemahaman Desain Kontrol Keamanan, Evaluasi Desain Kontrol Keamanan, Evaluasi Implementasi Kontrol Keamanan, dan Evaluasi Efektivitas Kontrol Keamanan. Penjelasan untuk masing-masing tahapan dalam Audit Keamanan SPBE sebagai berikut :

1. Pemahaman Desain Kontrol Keamanan SPBE, yaitu prosedur yang dilakukan Auditor Keamanan SPBE dalam mengidentifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol Keamanan SPBE terhadap lingkup Audit Keamanan SPBE. Dalam tahapan ini, auditor Keamanan SPBE melakukan pengumpulan data dan informasi untuk mendapatkan pemahaman atas lingkungan desain kontrol keamanan aplikasi dan atau infrastruktur, berupa peraturan atau kebijakan yang ditetapkan oleh pihak auditan tentang pengaturan yang berhubungan dengan penerapan kontrol keamanan dalam rangka pengembangan suatu aplikasi. Pengumpulan data ini dapat dilakukan secara mandiri atau independen dan kemudian dimintakan konfirmasinya kepada auditan, maupun dengan meminta data awal kepada auditan terkait informasi atas lingkungan desain kontrol keamanan. Tahapan Pemahaman Desain Kontrol Keamanan dapat dilakukan sebelum pelaksanaan Audit dilaksanakan (Pra kegiatan Audit) atau dilakukan pada saat pelaksanaan kegiatan Audit Keamanan.
2. Evaluasi Desain Kontrol Keamanan SPBE, yaitu prosedur yang dilakukan auditor Keamanan SPBE untuk memperoleh keyakinan yang memadai bahwa desain kontrol Keamanan SPBE telah sesuai dengan kriteria kontrol Keamanan SPBE yang digunakan. Dalam tahapan ini, auditor Keamanan SPBE melakukan evaluasi atas kelaikan desain kontrol keamanan aplikasi dan atau infrastruktur dibandingkan dengan kriteria keamanan yang diprasyaratkan sesuai ketentuan perundang-undangan yang berlaku.
3. Evaluasi Implementasi Kontrol Keamanan SPBE, yaitu prosedur yang dilakukan auditor Keamanan SPBE untuk memperoleh keyakinan yang memadai bahwa implementasi kontrol telah sesuai dengan desain kontrol yang ada. Dalam tahapan ini, auditor Keamanan SPBE

- melakukan evaluasi atas kesesuaian implementasi kontrol keamanan aplikasi dibandingkan dengan desain kontrol keamanan aplikasi.
4. Evaluasi Efektivitas Kontrol Keamanan SPBE, yaitu prosedur yang dilakukan auditor Keamanan SPBE untuk:
    - a. memperoleh keyakinan yang memadai bahwa kontrol Keamanan SPBE yang berjalan telah dapat mencapai tujuannya dengan efektif; atau
    - b. mengidentifikasi risiko yang terjadi karena adanya kelemahan desain dan/atau implementasi kontrol Keamanan SPBE.

#### G. Status Pemeriksaan Audit Keamanan

Matriks Konklusi Audit Keamanan SPBE

<b>Hasil Evaluasi Desain Kontrol</b>	<b>Hasil Evaluasi Implementasi Kontrol</b>	<b>Hasil Evaluasi Efektivitas Kontrol</b>	<b>Konklusi Hasil Audit</b>
Memadai	Sesuai Desain Kontrol	Efektif	Memadai
		Perlu Peningkatan	Memadai
		Belum Efektif	Perlu Peningkatan
	Tidak Sesuai Desain Kontrol	Efektif	Perlu Peningkatan
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai
Perlu Peningkatan	Sesuai Desain Kontrol	Efektif	Memadai
		Perlu Peningkatan	Perlu Peningkatan
		Belum Efektif	Tidak Memadai
	Tidak Sesuai Desain Kontrol	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai
Tidak Memadai	-	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai

Dalam pelaksanaan audit keamanan, terdapat 2 (dua) area keamanan yang harus diperiksa, yaitu Manajemen Keamanan Informasi dan Standar Teknis

dan Prosedur Keamanan. Kedua area tersebut menjadi kontrol Keamanan SPBE yang harus dipatuhi dan dilaksanakan oleh Instansi Pusat dan Pemerintah Daerah. Kontrol Keamanan tersebut didefinisikan dan dijelaskan lebih lanjut pada Bab II dan Bab III.

Untuk mencapai konklusi Audit Keamanan SPBE, terdapat 3 (tiga) model evaluasi keamanan yang dilaksanakan secara berurutan yaitu: Evaluasi Desain Kontrol, Evaluasi Implementasi Kontrol, dan Evaluasi Efektivitas Kontrol Keamanan.

Evaluasi pertama dalam tahapan Audit Keamanan SPBE adalah Evaluasi Desain Kontrol. Pada tahapan tersebut akan menyimpulkan kondisi desain kontrol keamanan yang digunakan dalam 3 (tiga) kondisi yaitu **Memadai**, **Perlu Peningkatan**, atau **Tidak Memadai**.

Pada kasus tertentu, jika hasil pemeriksaan pada Evaluasi Desain Kontrol memberikan konklusi Tidak Memadai, maka tidak diperlukan lagi evaluasi terhadap implementasi desain kontrol. Pemeriksaan langsung mengarah pada Evaluasi Efektivitas Kontrol keamanan yang ditujukan untuk menilai kontrol keamanan yang ada di instansi, tanpa adanya Desain Kontrol Keamanan masih berkinerja dengan efektif atau tidak.

Evaluasi selanjutnya dalam tahapan Audit Keamanan SPBE adalah Evaluasi Implementasi Kontrol yang merupakan tahap lanjut dari Evaluasi Desain Kontrol. Pada tahapan tersebut akan menyimpulkan kondisi implementasi kontrol keamanan yang digunakan dalam 2 (dua) kondisi yaitu **Sesuai dengan Desain Kontrol**, atau **Tidak Sesuai dengan Desain Kontrol**.

Evaluasi terakhir dalam tahapan Audit Keamanan SPBE adalah Evaluasi Efektivitas Kontrol. Pada tahapan tersebut akan menyimpulkan kondisi efektivitas kontrol keamanan yang digunakan dalam 3 (tiga) kondisi yaitu **Efektif**, **Perlu Peningkatan**, atau **Belum Efektif**.

## H. Pengembangan Prosedur Audit dan Instrumen

Prosedur audit dan Instrumen Audit akan direviu atau dievaluasi secara berkala. Hal ini dilakukan untuk menjamin proses pemeriksaan yang handal dan tersedianya alat ukur yang sesuai dengan perkembangan dan kebutuhan terkini. Hasil reviu selanjutnya akan ditetapkan menjadi pengembangan versi dari prosedur audit dan instrumen yang telah ditetapkan sebelumnya. Jika perubahan yang dilakukan masih dinilai minor (kecil), maka versi Prosedur Audit dan instrumen akan dinaikkan dari versi x.0 menjadi x.1 dan seterusnya, namun jika perubahan dinilai bersifat mayor (besar), maka versi instrumen akan dinaikkan dari versi x.1 menjadi versi x+1.0 dan seterusnya.

## I. Bukti Audit

Bukti Audit yang dimaksud pada pedoman ini adalah semua media informasi yang digunakan oleh personel pelaksana untuk mendukung argumentasi, pendapat atau simpulan dan rekomendasinya dalam meyakinkan tingkat kesesuaian antara kondisi dengan kriteria. Pedoman pemilihan informasi yang akan digunakan sebagai bukti audit adalah informasi tersebut yang harus memenuhi syarat aspek bukti Audit. Terdapat 2 (dua) syarat bukti audit:

- 1) Kecukupan; dan
- 2) Ketepatan.

Bukti Audit yang cukup merupakan ukuran kuantitas bukti Audit Keamanan SPBE yang dipengaruhi oleh penilaian auditor Keamanan SPBE atas risiko Audit Keamanan SPBE dan kualitas bukti Audit Keamanan SPBE. Bukti Audit yang tepat merupakan ukuran kualitas bukti Audit Keamanan SPBE yaitu relevan, valid, dan andal untuk mendukung hasil Audit Keamanan SPBE.

## BAB II

### MANAJEMEN KEAMANAN INFORMASI

Petunjuk Teknis, Penjelasan dan Pengujian setiap fungsi kontrol keamanan Manajemen Keamanan Informasi merupakan prosedur yang dapat dilakukan oleh auditor Keamanan SPBE untuk mendapatkan bukti data dukung pengujian kontrol keamanan.

#### A. Kontrol Keamanan pada area Manajemen Keamanan Informasi

Kontrol Keamanan pada area Manajemen Keamanan Informasi berjumlah 14 kontrol keamanan, yaitu sebagai berikut :

- K1. Manajemen Keamanan Informasi SPBE ditetapkan oleh pimpinan Instansi Pusat dan Pemerintah Daerah dikomunikasikan, dilaksanakan, dan didokumentasikan berdasarkan pedoman manajemen keamanan informasi SPBE.

Deskripsi/ Tujuan	Dokumen atau pedoman Manajemen Keamanan Informasi (MKI) telah ditetapkan oleh pimpinan Instansi Pusat dan Pemerintah Daerah, dikomunikasikan kepada pihak internal Organisasi dan pihak eksternal yang terkait, dilaksanakan dan didokumentasikan berdasarkan pengaturan pada pedoman Manajemen Keamanan Informasi SPBE.
Referensi Kontrol Keamanan	Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 2, Pasal 3 ayat 2, dan Pasal 3 ayat 3.

- K2. Ruang lingkup Manajemen Keamanan Informasi mendefinisikan isu Internal keamanan informasi SPBE dalam Organisasi dan Isu Eksternal keamanan Informasi SPBE. Isu internal keamanan Informasi SPBE didefinisikan berdasarkan area yang menjadi prioritas organisasi yang paling sedikit meliputi data dan informasi SPBE, Aplikasi SPBE, Aset Infrastruktur SPBE, dan kebijakan keamanan informasi SPBE yang telah dimiliki. Sedangkan Isu

eksternal keamanan informasi SPBE didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

Deskripsi/ Tujuan	Ruang lingkup dan batasan implementasi Manajemen Keamanan Informasi telah ditetapkan secara tepat pada dokumen atau pedoman Manajemen Keamanan Informasi sesuai pengaturan pada pedoman Manajemen Keamanan Informasi SPBE.
Referensi Kontrol Keamanan	Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 4 ayat 2, Pasal 4 ayat 3, Pasal 4 ayat 4 dan Pasal 4 ayat 5.

- K3. Penanggung jawab keamanan dalam SPBE sesuai dengan pedoman manajemen keamanan informasi SPBE dalam organisasi adalah Sekretaris pada Instansi Pusat dan Pemerintah Daerah dan disebut Koordinator SPBE.

Tugas penanggung jawab Keamanan SPBE antara lain:

- menetapkan pelaksana teknis Keamanan SPBE;
- mendukung operasional Keamanan SPBE; dan
- melaksanakan evaluasi kinerja pelaksanaan Keamanan SPBE.

Deskripsi/ Tujuan	Penanggung jawab Keamanan SPBE telah dinyatakan dan ditetapkan, selain itu tugas dan tanggung jawabnya telah didefinisikan sesuai dengan pedoman Manajemen Keamanan Informasi SPBE.
Referensi Kontrol Keamanan	Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 5 ayat 2, Pasal 5 ayat 3, Pasal 6 ayat 1, Pasal 14 ayat 1 dan Pasal 15 ayat 1.

- K4. Pejabat pimpinan tinggi pratama pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah sebagai pelaksana teknis keamanan mempunyai tugas:

- a. memastikan penerapan Standar Teknis dan Prosedur Keamanan SPBE;
- b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
- c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE kepada Koordinator SPBE; dan
- d. melakukan perbaikan berkelanjutan.

Deskripsi/ Tujuan	: Pelaksana teknis keamanan pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah telah dinyatakan dan ditetapkan, selain itu tugas dan tanggung jawabnya telah didefinisikan sesuai dengan pedoman Manajemen Keamanan Informasi SPBE.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE  Pasal 7 ayat 1 dan Pasal 16 ayat 1.

- K5. Pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE sebagai pelaksana teknis Keamanan SPBE mempunyai tugas:
- a. menerapkan Standar Teknis dan Prosedur Keamanan Aplikasi di unit kerja masing-masing;
  - b. memastikan seluruh pembangunan atau pengembangan aplikasi dan Infrastruktur SPBE yang telah ditetapkan;
  - c. memastikan keberlangsungan Proses Bisnis SPBE;
  - d. berkoordinasi dengan pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan TIK Instansi Pusat dan Pemerintah Daerah terkait perumusan program kerja dan anggaran Keamanan SPBE; dan
  - e. melakukan perbaikan berkelanjutan.

Deskripsi/ Tujuan	: Pelaksana teknis Keamanan SPBE yang membawahi, membangun, memelihara,
----------------------	---

		dan/atau mengembangkan Aplikasi SPBE telah dinyatakan dan ditetapkan, selain itu tugas dan tanggung jawabnya telah didefinisikan sesuai dengan pedoman Manajemen Keamanan Informasi SPBE.
Referensi Kontrol Keamanan	:	Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE  Pasal 7 ayat 2 dan Pasal 16 ayat 1.

K6. Perencanaan dilakukan oleh pelaksana teknis Keamanan SPBE. Perencanaan dilakukan dengan merumuskan program kerja Keamanan SPBE yang disusun berdasarkan kategorisasi risiko Keamanan SPBE dan target realisasi program kerja Keamanan SPBE. Program kerja Keamanan SPBE paling sedikit meliputi edukasi kesadaran Keamanan SPBE, penilaian kerentanan Keamanan SPBE, peningkatan Keamanan SPBE, penanganan insiden Keamanan SPBE, dan Audit Keamanan SPBE. Kategorisasi risiko ditentukan sesuai dengan peraturan perundang-undangan. Target realisasi program kerja Keamanan SPBE ditetapkan berdasarkan kebutuhan setiap Instansi Pusat dan Pemerintah Daerah.

Deskripsi/ Tujuan	:	Pelaksana teknis Keamanan SPBE telah merumuskan program kerja Keamanan SPBE berdasarkan kategorisasi risiko Keamanan SPBE dan target realisasinya. Dalam merumuskan program kerja Keamanan SPBE harus memenuhi minimal 5 program kerja keamanan yang telah disebutkan dan target realisasinya sesuai kebutuhan Instansi Pusat dan Pemerintah Daerah.
Referensi Kontrol Keamanan	:	Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE

Pasal 8.

- K7. Edukasi kesadaran Keamanan SPBE dilaksanakan melalui kegiatan sosialisasi dan pelatihan.

Deskripsi/ Tujuan	: Program kerja kesadaran Keamanan SPBE dilaksanakan melalui kegiatan sosialisasi dan pelatihan untuk Internal Organisasi dan pihak eksternal terkait dan didokumentasikan.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 9.

- K8. Penilaian kerentanan Keamanan SPBE dilaksanakan melalui:
- a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
  - b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
  - c. mengukur tingkat risiko Keamanan SPBE.

Deskripsi/ Tujuan	: Penilaian kerentanan Keamanan SPBE dilaksanakan melalui Inventarisasi seluruh aset SPBE, mengidentifikasi kerentanan dan ancaman serta melakukan pengukuran tingkat risiko keamanan pada aset SPBE.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 10.

- K9. Peningkatan Keamanan SPBE dilaksanakan berdasarkan hasil penilaian kerentanan Keamanan SPBE dan dilaksanakan melalui:
- a. menerapkan Standar Teknis dan Prosedur Keamanan SPBE; dan
  - b. menguji fungsi Keamanan terhadap aplikasi SPBE dan Infrastruktur SPBE.

Deskripsi/ Tujuan	: Peningkatan Keamanan SPBE dilaksanakan berdasarkan penilaian kerentanan Keamanan SPBE yang dilakukan dan dilaksanakan melalui penerapan Standar Teknis dan Prosedur Keamanan SPBE serta pengujian fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 11.

K10. Penanganan insiden Keamanan SPBE dilaksanakan melalui:

- a. mengidentifikasi sumber serangan;
- b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
- c. mengukur tingkat risiko Keamanan SPBE; dan
- d. memitigasi atau mengurangi dampak risiko Keamanan SPBE.

Deskripsi/ Tujuan	: Penanganan insiden Keamanan SPBE dilaksanakan melalui prosedur yang telah disebutkan dalam upaya mengidentifikasi sumber serangan, dan menganalisis insiden keamanan, mengukur kembali Tingkat risiko keamanan, dan memitigasi dampak insiden dapat diminimalisir dan mencegah insiden serupa terulang kembali.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 12.

K11. Audit Keamanan SPBE dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Deskripsi/ Tujuan	: Pelaksanaan Audit Keamanan SPBE dilakukan sesuai ketentuan peraturan perundang-undangan yang berlaku khususnya yang merupakan amanat dari Peraturan Presiden 95 tahun 2018 tentang SPBE dan turunannya.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 13.

K12. Dukungan pengoperasian dilakukan dengan meningkatkan kapasitas terhadap SDM Keamanan SPBE dan Anggaran Keamanan SPBE.

SDM Keamanan SPBE harus memiliki kompetensi Keamanan Infrastruktur TIK dan Keamanan Aplikasi.

Pemenuhan kompetensi dilakukan dengan melakukan kegiatan pelatihan dan/atau sertifikasi kompetensi Keamanan Infrastruktur TIK dan Keamanan Aplikasi serta bimbingan teknis standar Keamanan SPBE.

Deskripsi/ Tujuan	: Koordinator SPBE harus mendukung melaksanakan pengoperasian Keamanan SPBE dalam hal peningkatan kapasitas terhadap SDM dan Anggaran Keamanan. Pemenuhan kapasitas SDM Keamanan untuk meningkatkan kompetensi dalam hal pengelolaan keamanan pada Aplikasi dan Infrastruktur TIK SPBE yang dilakukan melalui bimbingan teknis.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE Pasal 14 ayat 2, Pasal 14 ayat 3 dan Pasal 14 ayat 4

K13. Evaluasi kinerja dilakukan oleh Koordinator SPBE. Evaluasi kinerja dilaksanakan paling sedikit satu kali dalam satu tahun dengan:

- a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
- b. menetapkan indikator kinerja pada setiap area proses;
- c. memformulasikan pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
- d. menganalisis efektivitas pelaksanaan Keamanan SPBE; dan
- e. mendukung dan merealisasikan program Audit Keamanan SPBE.

Deskripsi/ Tujuan	: Koordinator SPBE melaksanakan evaluasi kinerja terhadap pelaksanaan Keamanan SPBE minimal 1 (satu) kali dalam 1 (satu) tahunnya. Evaluasi kinerja yang dilaksanakan harus membahas 5 (lima) hal substansi yang telah dinyatakan dalam pedoman Manajemen Keamanan Informasi SPBE.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE  Pasal 15 ayat 1, Pasal 15 ayat 2 dan Pasal 15 ayat 3.

K14. Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja. Perbaikan berkelanjutan dilakukan dengan:

- a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
- b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

Deskripsi/ Tujuan	: Pelaksanaan perbaikan berkelanjutan yang merupakan tindak lanjut hasil evaluasi kinerja dilakukan dengan mengatasi permasalahan dan memperbaiki pelaksanaan Keamanan SPBE secara periodik.
Referensi Kontrol Keamanan	: Peraturan Badan Siber dan Sandi Negara Nomor 4 tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE  Pasal 16 ayat 2 dan Pasal 16 ayat 3.



## B. Prosedur Audit Keamanan SPBE

Dalam pelaksanaan audit, auditor Keamanan SPBE melakukan pemeriksaan dengan menjalankan prosedur audit yang meliputi: observasi, wawancara, verifikasi dokumen, dan melakukan survei.

1. Observasi dilakukan dengan menggunakan panca indera terutama mata atas suatu objek. Observasi akan membantu auditor Keamanan SPBE melihat kondisi mengenai kegiatan yang diperiksa khususnya yang terkait kontrol pengamanan fisik.
2. Wawancara bertujuan untuk memperoleh informasi dan meminta klarifikasi dalam rangka melakukan pembuktian atas pelaksanaan kegiatan keamanan oleh pihak terkait dimana sebagian besar bukti dalam bentuk kesaksian.
3. Verifikasi dokumen merupakan kegiatan yang dilakukan oleh auditor Keamanan SPBE untuk menghimpun, mempelajari data dan dokumen auditan yang menjelaskan desain kontrol keamanan dan implementasi pengamanan yang dilaksanakan sesuai yang ditetapkan dalam peraturan perundangan yang berlaku.

Dokumen yang diverifikasi dapat diperoleh dari permintaan data oleh auditor Keamanan SPBE, hasil tindak lanjut dari observasi yang dilakukan oleh auditor Keamanan SPBE dan hasil tindak lanjut dari wawancara dengan auditan.

Dalam pemeriksaan verifikasi dokumen, dapat dilakukan dengan menganalisis, memperbandingkan satu dokumen dengan dokumen lainnya untuk membuktikan kebenaran substansial, konsistensi implementasi pelaksanaan keamanan informasi.

Dalam pemeriksaan substansial, verifikasi dokumen-dokumen tersebut dapat dianalisis dengan hasil pemeriksaan wawancara untuk menghasilkan kondisi yang lebih komprehensif.

4. Survei merupakan metode yang dilakukan auditor Keamanan SPBE untuk mencari kebenaran terhadap substansi kontrol keamanan dengan melibatkan secara langsung subjek pemeriksaan dalam ruang lingkup pemeriksaan secara langsung. Pemeriksaan dengan metode survei ini dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada subjek pemeriksaan untuk dijawab, dan jawabannya dianalisis dan diakumulasi untuk mendapat konklusi dari hasil survei.

Dalam melakukan survei, auditor Keamanan SPBE memiliki pilihan untuk menentukan subjek survei adalah populasi atau sampel yang mewakili populasi. Dengan sampel yang tepat, hasil yang diperoleh dapat mewakili populasi. Oleh karena itu metode pengambilan sampel (*sampling method*) oleh auditor Keamanan SPBE memegang peranan yang sangat penting. Metode pengambilan sampling dalam pemeriksaan audit dapat diklasifikasikan menjadi 2 (dua) jenis yaitu :

a) *Probability Sampling*

Merupakan teknik pengambilan sampel secara acak. Dimana setiap entitas dalam suatu populasi memiliki probabilitas yang sama untuk terpilih sebagai data sampel. Teknik pengambilan sampel ini dapat dibedakan menjadi 5 (lima) model yaitu :

- 1) *Simple random sampling*
- 2) *Systematic sampling*
- 3) *Stratified sampling*
- 4) *Cluster sampling*
- 5) *Multistage sampling*

Teknik pengambilan sampel ini diurutkan mulai dari yang paling simplifikasi sampai dengan pengaturan yang lebih kompleks dalam model *Multistage sampling*. Semakin kompleks model sampling yang diambil semakin beragam model data dan karakteristik subjek sampel yang diuraikan, namun hasil samplingnya juga akan menjelaskan banyak hal serta semakin spesifik informasi yang dapat disimpulkan dalam pemeriksaan yang sifatnya lebih spesifik juga.

b) *Non-probability Sampling*

Merupakan teknik pengambilan sampel tidak secara acak, Dimana kemungkinan entitas terpilih sebagai sampel berbeda satu sama lainnya. Pada prosedur audit, model sampel yang digunakan hanya *Purposive / Judgemental Sampling*. Metode ini menggunakan pendekatan *expert judgement* dari auditor Keamanan SPBE dalam memilih entitas dalam populasi untuk menjadi subjek sampel baik karena faktor kerahasiaan, kondisi pelaksanaan audit maupun sumber daya audit.

Petunjuk Teknis pemeriksaan kontrol keamanan merupakan prosedur audit yang dilakukan oleh Auditor Keamanan SPBE untuk menguji kontrol keamanan dan mendapatkan bukti kontrol keamanan telah dilaksanakan.

14 (empat belas) Kontrol keamanan yang diperiksa pada tahap evaluasi desain kontrol dikodefikasi ulang menyesuaikan tahap evaluasi desain kontrol sehingga kodefikasinya ditambahkan ED (Evaluasi Desain). Contoh Kontrol keamanan pertama yang dikodefikasikan K1 menjadi KED.1 dalam tahapan evaluasi desain.

Hasil pemeriksaan tiap kontrol keamanan pada tahapan evaluasi desain akan menghasilkan status pemeriksaan yaitu Sesuai atau Tidak Sesuai dengan Desain Kontrol Keamanan.

#### KED.1

Teknik pemeriksaan	:	Verifikasi dokumen untuk: <ul style="list-style-type: none"><li>- Memastikan bahwa Dokumen SMKI Instansi Pusat dan Pemerintah Daerah telah ditetapkan Pimpinan Instansi Pusat dan Pemerintah Daerah; dan</li><li>- Memastikan bahwa Dokumen SMKI Instansi Pusat dan Pemerintah Daerah disusun berdasarkan 100% substansi pedoman Manajemen Keamanan Informasi SPBE.</li></ul>
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang pedoman Manajemen Keamanan Informasi (MKI) telah sesuai dengan pedoman Manajemen Keamanan Informasi SPBE dan telah dilakukan penetapan hukum.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

#### KED.2

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa ruang lingkup dan isu internal dan eksternal keamanan Informasi dinyatakan
--------------------	---	--

		dalam pengaturan Manajemen Keamanan Informasi Instansi Pusat dan Pemerintah Daerah, serta sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah yang memuat tentang SMKI dan telah dilakukan penetapan hukum yang memuat tentang ruang isu Internal dan eksternal Keamanan informasi SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.3

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa Penanggung Jawab keamanan beserta tugas dan tanggung jawabnya dalam SPBE dinyatakan sesuai dengan pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang SMKI atau dokumen lain yang relevan dalam pelaksanaan implementasi SPBE dan telah dilakukan penetapan hukum memuat: <ol style="list-style-type: none"><li>1. Sekretaris Instansi Pusat dan Pemerintah Daerah sebagai penanggung jawab Keamanan SPBE; dan</li><li>2. Penjelasan tugas dan tanggung jawab Penanggung Jawab Keamanan SPBE.</li></ol>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.4

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan pelaksana teknis keamanan yang dijabat oleh Pejabat pimpinan tinggi pratama pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah ditetapkan oleh koordinator SPBE dan menjalankan tugas dan tanggung jawabnya sesuai pedoman Manajemen keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang SMKI dan atau dokumen lain yang relevan dalam pelaksanaan implementasi SPBE beserta aturan turunannya dan telah dilakukan penetapan hukum memuat: <ol style="list-style-type: none"><li>1. Penetapan Pelaksana teknis keamanan yang dijabat oleh Pejabat pimpinan tinggi pratama pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah oleh Koordinator SPBE; dan</li><li>2. Tugas dan tanggung jawab Pelaksana teknis keamanan Pejabat pimpinan tinggi pratama pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah.</li></ol>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.5

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan Pelaksana teknis keamanan yang dijabat oleh Pejabat Pimpinan tinggi atau pejabat
--------------------	---	--

		administrator ditetapkan oleh Koordinator SPBE dan menjalankan tugas dan tanggung jawabnya sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	<p>Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang SMKI dan atau dokumen lain yang relevan dalam pelaksanaan implementasi SPBE beserta aturan turunannya dan telah dilakukan penetapan hukum memuat:</p> <ol style="list-style-type: none"><li>1. Penetapan Pelaksana teknis keamanan yang dijabat oleh pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE oleh Koordinator SPBE;</li><li>2. Tugas dan tanggung jawab Pejabat Pimpinan Tinggi atau Pejabat Administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE sesuai dengan pedoman Manajemen Keamanan Informasi (MKI) SPBE.</li></ol>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

#### KED.6

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi : <ol style="list-style-type: none"><li>1) Perencanaan dilakukan oleh pelaksana teknis Keamanan SPBE;</li><li>2) Perencanaan dilakukan untuk merumuskan program kerja dan target realisasi program kerja Keamanan SPBE;</li></ol>
--------------------	---	---

		<p>3) Program kerja keamanan minimal meliputi: edukasi kesadaran keamanan, penilaian kerentanan keamanan, peningkatan keamanan, penanganan insiden keamanan, dan Audit Keamanan SPBE;</p> <p>4) Program kerja keamanan disusun berdasarkan kategorisasi risiko sesuai dengan ketentuan peraturan perundang-undangan (Peraturan Menpan RB nomor 5 tahun 2020 tentang Manajemen Risiko SPBE); dan</p> <p>5) Target realisasi program kerja Keamanan SPBE ditetapkan dan berdasarkan kebutuhan Instansi Pusat dan Pemerintah Daerah.</p>
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah yang memuat tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang perencanaan program kerja Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.7

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi Program Kerja Edukasi Kesadaran Keamanan SPBE yang meliputi Sosialisasi dan Pelatihan didefinisikan dalam Dokumen Manajemen Keamanan Informasi dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah

		dilakukan penetapan hukum yang memuat tentang program Edukasi Kesadaran Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.8

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi Penilaian Kerentanan Keamanan didefinisikan dalam Dokumen SMKI dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang program penilaian kerentanan keamanan.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.9

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi Peningkatan Keamanan SPBE tercantum dalam Dokumen SMKI dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang program peningkatan Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.10

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi penanganan insiden Keamanan SPBE diatur dalam Dokumen SMKI dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang penanganan insiden Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.11

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi Audit Keamanan SPBE diatur dalam Dokumen SMKI dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang program Audit Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.12

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa dukungan pengoperasian SPBE diatur dalam Dokumen SMKI dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
--------------------	---	---

Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang dukungan pengoperasian Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.13

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi evaluasi kinerja diatur dalam Dokumen Manajemen Keamanan Informasi Instansi Pusat dan Pemerintah Daerah dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang memuat tentang evaluasi kinerja Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KED.14

Teknik pemeriksaan	:	Verifikasi dokumen untuk memastikan bahwa substansi perbaikan berkelanjutan diatur dalam Dokumen SMKI dan sesuai pedoman Manajemen Keamanan Informasi SPBE.
Bukti	:	Peraturan / Keputusan Kepala Instansi Pusat dan Pemerintah Daerah tentang Manajemen Keamanan Informasi dan telah dilakukan penetapan hukum yang

		memuat tentang perbaikan berkelanjutan Keamanan SPBE.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

#### D. Petunjuk Teknis Pemeriksaan Kontrol Keamanan pada Evaluasi Implementasi Kontrol

Petunjuk Teknis pemeriksaan kontrol keamanan merupakan prosedur audit yang dilakukan oleh auditor Keamanan SPBE untuk menguji kontrol keamanan dan mendapatkan bukti kontrol keamanan telah dilaksanakan.

14 (empat belas) Kontrol keamanan yang diperiksa pada tahap evaluasi implementasi kontrol dikodefikasi ulang menyesuaikan tahap evaluasi implementasi kontrol sehingga kodefikasinya ditambahkan EI (Evaluasi Implementasi). Contoh Kontrol keamanan pertama yang dikodefikasikan K1 menjadi KEI.1 dalam tahapan evaluasi Implementasi.

Hasil pemeriksaan tiap kontrol keamanan pada tahapan evaluasi implementasi akan menghasilkan status pemeriksaan yaitu Sesuai dengan Desain Kontrol atau Tidak Sesuai dengan Desain Kontrol Keamanan.

##### KEI.1

Teknik pemeriksaan	:	Wawancara dan verifikasi dokumen untuk memastikan bahwa dokumen Manajemen Keamanan (MKI) Informasi Instansi Pusat dan Pemerintah Daerah telah dikomunikasikan kepada pihak-pihak terkait.
Bukti	:	1) Bukti implementasi dokumen Manajemen Keamanan Informasi telah dikomunikasikan kepada Internal Organisasi dan Eksternal terkait. Contoh: a. Bukti kegiatan sosialisasi Peraturan Manajemen Keamanan Informasi Instansi antara lain proposal kegiatan, daftar undangan, daftar

		<p>hadir, materi sosialisasi, dan laporan kegiatan;</p> <p>b. <i>Email Blast, banner, publikasi regulasi dalam website JDIH Instansi; dan</i></p> <p>c. <i>Bukti-bukti lain yang menggambarkan kondisi komunikasi telah dilaksanakan dan diyakini oleh auditor Keamanan SPBE bahwa peraturan Manajemen Keamanan Informasi telah dikomunikasikan kepada internal Organisasi dan Eksternal terkait.</i></p>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.2

Teknik pemeriksaan	:	<p>Wawancara dan Verifikasi dokumen untuk memastikan bahwa Isu Internal yang menjadi prioritas organisasi meliputi :</p> <ul style="list-style-type: none"><li>a. data dan informasi;</li><li>b. aplikasi SPBE;</li><li>c. aset Infrastruktur SPBE; dan</li><li>d. kebijakan keamanan; serta</li><li>e. Isu Eksternal keamanan informasi yang sesuai dengan ketentuan perundang-undangan telah dilaksanakan.</li></ul>
Bukti	:	<p>Bukti implementasi Isu Internal dan Eksternal telah dilaksanakan oleh organisasi. Contoh:</p> <p>(1) Bukti dokumentasi pelaksanaan program atau kegiatan keamanan informasi terkait identifikasi isu internal yang didefinisikan pada poin a</p>

		s.d d pada ruang lingkup pemeriksaan / pengujian; (2) Bukti dokumentasi pelaksanaan program atau kegiatan keamanan informasi terkait identifikasi isu eksternal keamanan informasi.
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.3

Teknik pemeriksaan	:	Wawancara dan Verifikasi dokumen untuk memastikan bahwa : 1) Terdapat surat penugasan penanggung jawab Keamanan SPBE yang dijabat oleh Sekretaris Instansi Pusat dan Pemerintah Daerah; 2) Penanggung jawab Keamanan telah ditetapkan sesuai peraturan internal yang berlaku, dan dijabat oleh Sekretaris Instansi Pusat dan Pemerintah Daerah dan mempunyai tanggung jawab sesuai pedoman Manajemen Keamanan Informasi Internal dan pedoman Manajemen Keamanan Informasi SPBE; 3) Koordinator SPBE atau Penanggung jawab Keamanan melaksanakan tugas: a. menetapkan pelaksana Teknis Keamanan SPBE; b. mendukung operasional Keamanan SPBE; dan c. melaksanakan evaluasi kinerja.
Bukti	:	1) Surat Penugasan yang mencantumkan nama Sekretaris sebagai penanggung jawab Keamanan SPBE pada periode tahun tersebut;

		<p>2) Substansi tugas dan tanggung jawabnya yang tertuang dalam Surat Penugasan atau cukup didefinisikan pada Dokumen Manajemen Keamanan Informasi Instansi Pusat dan Pemerintah Daerah tentang peran dan tanggung jawab;</p> <p>3) Penetapan Pelaksana Teknis Keamanan SPBE oleh Koordinator pada periode tahun tersebut;</p> <p>4) Pernyataan dukungan operasional Keamanan SPBE oleh Koordinator SPBE;</p> <p>5) Dokumen KAK dan RAB terkait Program Kerja Keamanan yang disetujui oleh koordinator SPBE; dan</p> <p>6) Pelaksanaan Evaluasi Kinerja yang diinisiasi dan dipimpin oleh Koordinator SPBE dan dapat ditunjukkan dengan dokumen berupa Notula dan Laporan Evaluasi Kinerja.</p>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.4

Teknik pemeriksaan	:	<p>Wawancara dan Verifikasi dokumen untuk memastikan bahwa pejabat pimpinan tinggi pratama pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah:</p> <p>1) Mengkoordinasikan pelaksanaan penerapan Standar Teknis dan Prosedur Keamanan SPBE di lingkungan organisasi sesuai dengan Manajemen Keamanan Informasi</p>
--------------------	---	---

		<p>Internal dan pedoman Manajemen Keamanan SPBE;</p> <p>2) Merumuskan, mengkoordinasikan dan melaksanakan Program kerja dan anggaran Keamanan SPBE;</p> <p>3) Pelaksanaan keamanan informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE dilaporkan kepada Koordinator SPBE atau Penanggung jawab Keamanan SPBE; dan</p> <p>4) Pelaksanaan Perbaikan berkelanjutan dilaksanakan.</p>
Bukti	:	<p>Bukti Poin 1) dapat berupa :</p> <ul style="list-style-type: none"><li>- Dokumen Standar Teknis dan Prosedur Keamanan SPBE yang telah ditetapkan oleh Instansi;</li><li>- Pelaksanaan rapat pembahasan Penerapan Standar Teknis dan Prosedur Keamanan SPBE yang akan dan sedang dilaksanakan oleh unit kerja pengelola aplikasi SPBE. Dokumentasi kegiatan dapat berupa undangan kegiatan, materi, daftar hadir dan notula rapat.</li></ul> <p>Bukti Poin 2) dapat berupa :</p> <ul style="list-style-type: none"><li>- Rekapitulasi usulan rencana program kerja keamanan;</li><li>- Nota dinas usulan rekapitulasi rencana program kerja keamanan;</li><li>- KAK dan RAB Program kerja Keamanan;</li><li>- Laporan pelaksanaan Program Kerja Keamanan (sampling data).</li></ul> <p>Bukti Poin 3) berupa laporan pelaksanaan Manajemen Keamanan Informasi dan</p>

		<p>Standar Teknis dan Prosedur Keamanan, serta kegiatan program kerja keamanan kepada koordinator SPBE dan Nota dinas Laporan tersebut kepada koordinator SPBE.</p> <p>Bukti Poin 4) berupa Laporan perbaikan berkelanjutan (dapat menggunakan referensi bukti KEI.9).</p>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.5

Teknik pemeriksaan	:	<p>Wawancara dan verifikasi dokumen untuk memastikan tugas pejabat pimpinan tinggi / pejabat yang membawahi, membangun, memelihara dan atau mengembangkan Aplikasi SPBE sebagai pelaksana teknis Keamanan SPBE :</p> <ol style="list-style-type: none"><li>1) Melaksanakan penerapan Standar Teknis dan Prosedur Keamanan terhadap Aplikasi baik yang dikelola secara mandiri maupun oleh pihak ketiga yang ditunjuk sesuai dengan Manajemen Keamanan Informasi Internal dan pedoman Manajemen keamanan Informasi (MKI) SPBE;</li><li>2) Melaksanakan koordinasi dengan pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi Instansinya terkait perumusan program kerja dan anggaran Keamanan SPBE.</li></ol>
Bukti	:	<p>Bukti Poin 1) dapat berupa:</p> <ul style="list-style-type: none"><li>- Dokumentasi pelaksanaan rapat pembahasan Penerapan Standar</li></ul>

		<p>Teknis dan Prosedur Keamanan SPBE yang akan dan sedang dilaksanakan. Dokumentasi kegiatan dapat berupa undangan kegiatan, materi, daftar hadir dan notula rapat;</p> <ul style="list-style-type: none"><li>- Dokumen pembangunan / pengembangan aplikasi dan Infrastruktur SPBE yang telah dilegalisasi;</li><li>- Dokumen yang berisi rencana keberlangsungan Proses Bisnis SPBE, contoh bukti adalah dokumen BIA;</li><li>- Hasil evaluasi penerapan Standar Teknis dan Prosedur Keamanan SPBE pada aplikasi yang dikelola;</li><li>- Laporan kegiatan program kerja unit kerja kepada Pimpinan Tinggi Pratama;</li><li>- Laporan Perbaikan berkelanjutan terhadap pengelolaan Aplikasi (merujuk pada kontrol KEI.9);</li></ul> <p>Bukti Poin 2) dapat berupa pelaksanaan rapat pembahasan Penerapan Standar Teknis dan Prosedur Keamanan SPBE yang telah dilaksanakan dan akan dilakukan kepada berupa pejabat pimpinan tinggi pratama pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah. Dokumentasi kegiatan dapat berupa undangan kegiatan, materi, daftar hadir dan notula rapat.</p>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

**KEI.6**

Teknik pemeriksaan	:	<p>Wawancara dan Verifikasi dokumen untuk memastikan :</p> <ol style="list-style-type: none"> <li>1) Perencanaan yang mencakup perumusan program kerja keamanan dan target realisasinya dilaksanakan;</li> <li>2) Program kerja Keamanan SPBE yang dirumuskan minimal mencakup 5 program keamanan seperti desain kontrolnya; dan</li> <li>3) Dalam penyusunan program kerja Keamanan SPBE berdasarkan kategorisasi risiko Keamanan SPBE sesuai dengan ketentuan perundang-undangan.</li> </ol>
Bukti	:	<p>Bukti yang mendukung implementasi didapatkan pada substansi dokumen berikut ini :</p> <ul style="list-style-type: none"> <li>- Dokumen Manajemen Risiko Instansi Pusat dan Pemerintah Daerah;</li> <li>- <i>Risk Register</i> pengelola aplikasi dan atau Infrastruktur SPBE; dan</li> <li>- Dokumen rencana Program Kerja Keamanan SPBE pengelola aplikasi dan atau Infrastruktur SPBE dan target realisasinya yang telah dilegalisasi.</li> </ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

**KEI.7**

Teknik pemeriksaan	:	<p>Wawancara dan verifikasi dokumen untuk memastikan berjalannya kegiatan edukasi kesadaran keamanan berupa sosialisasi dan pelatihan.</p>
Bukti	:	<ul style="list-style-type: none"> <li>- Bukti Kegiatan Sosialisasi. Contoh : Dokumentasi kegiatan Sosialisasi</li> </ul>

		<p><i>Security</i> antara lain sosialisasi SMKI dalam bentuk daftar hadir, materi sosialisasi dan laporan sosialisasi</p> <ul style="list-style-type: none"><li>- Bukti Kegiatan Pelatihan. Contoh: Dokumentasi kegiatan Pelatihan Keamanan SPBE dalam bentuk daftar hadir, materi pelatihan, laporan pelatihan, dan sertifikat pelatihan.</li></ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.8

Teknik pemeriksaan	:	<p>Wawancara dan Verifikasi dokumen untuk memastikan penilaian kerentanan Keamanan SPBE dilaksanakan melalui kegiatan:</p> <ol style="list-style-type: none"><li>1) Inventarisasi aset SPBE meliputi data, dan informasi, aplikasi dan infrastruktur;</li><li>2) Identifikasi kerentanan dan ancaman terhadap aset SPBE; dan</li><li>3) Pengukuran tingkat risiko Keamanan SPBE.</li></ol>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti poin 1) berupa Daftar Aset SPBE;</li><li>- Bukti poin 2) berupa Risk Register;</li><li>- Bukti poin 3) berupa Analisis Risiko yang dilakukan untuk mengukur tingkat risiko keamanan terhadap Aset SPBE.</li></ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.9

Teknik pemeriksaan	:	<p>Wawancara dan verifikasi dokumen untuk memastikan peningkatan keamanan dilaksanakan berdasarkan:</p>
--------------------	---	---

		<ol style="list-style-type: none"><li>1) Penilaian kerentanan Keamanan SPBE;</li><li>2) Penerapan standar teknis dan prosedur Keamanan SPBE;</li><li>3) Pelaksanaan uji fungsi keamanan terhadap aplikasi SPSE dan atau infrastruktur.</li></ol>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti untuk poin 1) berupa hasil atau laporan Penilaian kerentanan Keamanan SPBE ( merujuk pada bukti KEI.8) dan mitigasi risiko yang dipilih untuk dilaksanakan.</li><li>- Bukti untuk poin 2) dapat berupa :<ul style="list-style-type: none"><li>✓ Dokumen Standar Teknis dan Prosedur Keamanan SPBE yang telah dilegalisasi;</li><li>✓ Laporan pelaksanaan Penerapan Standar Teknis dan Prosedur Keamanan SPBE;</li><li>✓ Laporan evaluasi Penerapan Standar Teknis dan Prosedur Keamanan SPBE.</li></ul></li><li>- Bukti untuk poin 3) berupa bukti pelaksanaan uji fungsi keamanan pada aplikasi dan atau Infrastruktur SPBE. Misal Laporan <i>Vulnerability Assessment</i> (VA), dan Laporan <i>Pentest</i>.</li></ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

#### KEI.10

Teknik pemeriksaan	:	Verifikasi dokumen dan wawancara untuk memastikan penanganan insiden Keamanan SPBE dilaksanakan sesuai pedoman Manajemen Keamanan Informasi SPBE.
--------------------	---	---

Bukti	:	<ul style="list-style-type: none"><li>- Dokumen Prosedur penanganan insiden yang telah dilegalisasi;</li><li>- SOP yang berlaku dan diakui terkait model pelaporan insiden Keamanan SPBE;</li><li>- Rekapitulasi insiden Keamanan SPBE per tahun yang diakui;</li><li>- Laporan penanganan insiden yang telah dilegalisasi;</li><li>- Laporan penanganan insiden yang menyatakan insiden tersebut telah ditangani dan diselesaikan secara formal.</li></ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.11

Teknik pemeriksaan	:	<p>Verifikasi dokumen dan wawancara untuk memastikan program Audit Keamanan SPBE dilaksanakan sesuai norma dan ketentuan peraturan perundungan sebagai berikut :</p> <ol style="list-style-type: none"><li>1) Periode waktu audit keamanan eksternal (minimal 1x dalam 2 tahun);</li><li>2) Pelaksanaan Audit keamanan masuk dalam program audit Instansi Pusat dan Pemerintah Daerah;</li><li>3) Ruang lingkup audit sesuai dengan pedoman Manajemen Keamanan Informasi SPBE;</li><li>4) Hasil Audit dilaporkan kepada penanggungjawab keamanan / koordinator SPBE.</li></ol>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti untuk poin 1) adalah Laporan Hasil Audit Keamanan (LHAK);</li></ul>

		<ul style="list-style-type: none"><li>- Bukti Untuk poin 2) adalah Laporan Pelaksanaan audit Internal Keamanan SPBE;</li><li>- Bukti untuk poin 3) dapat melihat dari Laporan Pelaksanaan Audit Internal dan Audit Eksternal pada bagian ruang lingkup audit;</li><li>- Bukti untuk poin 4) dapat berupa nota dinas penyampaian hasil audit kepada penanggung jawab keamanan / koordinator SPBE.</li></ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

KEI.12

Teknik pemeriksaan	:	<p>Verifikasi dokumen dan wawancara untuk memastikan dukungan pengoperasian Keamanan SPBE dilaksanakan. Dukungan pengoperasian dilakukan pada :</p> <ol style="list-style-type: none"><li>1) Anggaran Keamanan SPBE (baik dalam bentuk kegiatan maupun pengadaan); dan</li><li>2) Kapasitas SDM pengelola Keamanan Aplikasi dan atau Infrastruktur TIK.</li></ol>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti untuk poin 1) dapat berupa :<ul style="list-style-type: none"><li>✓ Dokumen pengajuan anggaran keamanan (baik berupa bentuk kegiatan maupun pengadaan) dari unit kerja pengelola aplikasi dan atau infrastruktur dan atau unit kerja yang mempunyai fungsi keamanan Aplikasi dan Infrastruktur Instansi Pusat dan Pemerintah Daerah tahun sebelumnya.</li></ul></li></ul>

		<ul style="list-style-type: none"><li>✓ KAK dan RAN yang terkait program kerja yang telah disetujui.</li><li>- Bukti untuk poin 2) dapat berupa :<ul style="list-style-type: none"><li>✓ Pengajuan anggaran pelaksanaan pelatihan dan bimtek bagi pengelola keamanan aplikasi dan atau infrastruktur tahun sebelumnya;</li><li>✓ KAK dan RAN yang terkait program kerja pelatihan dan Bimtek Keamanan SPBE yang telah disetujui POK tahun berjalan;</li><li>✓ Bukti pelaksanaan pelatihan dan Bimtek Keamanan SPBE;</li><li>✓ Dokumen Matriks kompetensi SDM;</li><li>✓ Dokumen rencana peningkatan kapasitas SDM Keamanan SPBE.</li></ul></li></ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

#### KEI.13

Teknik pemeriksaan	:	<p>Verifikasi dokumen dan wawancara untuk memastikan Instansi Pusat dan Pemerintah Daerah melaksanakan evaluasi kinerja minimal 1x dalam 1 tahun yang mencakup:</p> <ol style="list-style-type: none"><li>1) Identifikasi area proses yang memiliki risiko tinggi terhadap pelaksanaan Keamanan SPBE;</li><li>2) Penetapan Indikator Kinerja pada setiap area proses;</li><li>3) Formulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;</li><li>4) Analisa efektivitas pelaksanaan Keamanan SPBE;</li></ol>
--------------------	---	--

		5) Dukungan dan realisasi program audit Keamanan SPBE.
Bukti	:	<ul style="list-style-type: none"> <li>- Laporan Evaluasi Kinerja;</li> <li>- Notula Rapat Evaluasi Pelaksanaan Kegiatan Keamanan;</li> <li>- Laporan kegiatan pelaksanaan evaluasi kinerja yang mencakup substansi poin 1) s.d 5);</li> <li>- Undangan Evaluasi Kinerja dari Koordinator SPBE;</li> <li>- Risalah rapat evaluasi kinerja;</li> <li>- Laporan <i>Risk Register</i> dari setiap area proses;</li> <li>- Bukti pelaksanaan audit keamanan baik internal maupun eksternal. Contoh: bukti program audit;</li> <li>- Program Audit Keamanan Instansi;</li> <li>- Dokumen realisasi anggaran.</li> </ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

#### KEI.14

Teknik pemeriksaan	:	Verifikasi dokumen dan wawancara untuk memastikan : <ul style="list-style-type: none"> <li>- Instansi Pusat dan Pemerintah Daerah telah mempunyai rencana perbaikan berkelanjutan terhadap hasil evaluasi kinerja;</li> <li>- Rencana perbaikan berkelanjutan telah dilaksanakan.</li> </ul>
Bukti	:	<ul style="list-style-type: none"> <li>- Dokumen Rencana Perbaikan Berkelanjutan;</li> <li>- Laporan Pelaksanaan Perbaikan Berkelanjutan.</li> </ul>
Status Pemeriksaan	:	Sesuai / Tidak Sesuai dengan Desain Kontrol keamanan

## E. Petunjuk Teknis Pemeriksaan Kontrol Keamanan pada Evaluasi Efektivitas Kontrol

Petunjuk Teknis pemeriksaan kontrol keamanan merupakan prosedur audit yang dilakukan oleh Auditor Keamanan SPBE untuk menguji kontrol keamanan dan mendapatkan bukti kontrol keamanan telah dilaksanakan.

14 (empat belas) Kontrol keamanan yang diperiksa pada tahap evaluasi efektivitas kontrol dikodefikasi ulang menyesuaikan tahap evaluasi efektivitas kontrol sehingga kodefikasinya ditambahkan EF (Evaluasi Efektivitas). Contoh Kontrol keamanan pertama yang dikodefikasikan K1 menjadi KEF.1 dalam tahapan evaluasi Efektivitas.

Hasil pemeriksaan tiap kontrol keamanan pada tahapan evaluasi efektivitas akan menghasilkan status pemeriksaan yaitu Efektif, atau Perlu Peningkatan atau Belum efektif.

Pada Teknik pemeriksaan substansial yang melibatkan analisis survei dan dokumen-dokumen untuk menguji konsistensi pencapaian tujuan kontrol keamanan, auditor Keamanan SPBE dapat menerapkan norma *passing grade* atau persentase penerimaan hasil. Norma yang dapat menjadi referensi bagi auditor Keamanan SPBE adalah pada keberlanjutan dari pemeriksaan sebagai berikut :

Pemeriksaan	:	<i>Passing grade</i> atau persentase hasil
Audit Pertama	:	75% - 80%
Audit Kedua	:	80% - 85%
Audit Ketiga	:	85% - 100%

### KEF.1

Teknik pemeriksaan	:	1) Pemeriksaan substansial untuk Memastikan Internal Instansi dan pihak eksternal terkait telah mengetahui dan memahami dokumen / peraturan SMKI dilakukan sebagai berikut : - Pemeriksaan dilakukan dengan metode Survei (uji sampling) terhadap personel Internal
--------------------	---	--

		<p>Organisasi dan pihak eksternal dilakukan.</p> <ul style="list-style-type: none"><li>- Personel yang menjadi subjek sampling adalah yang hadir dalam kegiatan sosialisasi dan atau populasi internal organisasi dan pihak eksternal terkait jika bukti komunikasi yang dilakukan menggunakan metode bukan kegiatan Sosialisasi peraturan.</li><li>- Penggunaan metode uji sampling disampaikan kepada auditan, dan melihat kondisi dan waktu yang tersedia.</li></ul> <p>2) Pemeriksaan substansial untuk Memastikan Manajemen Keamanan informasi dilaksanakan dan didokumentasikan berdasarkan pemeriksaan pada kontrol 2 sampai dengan 14.</p>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti poin 1) berupa Hasil Survei internal organisasi dan pihak terkait pengetahuan dan pemahaman dokumen / peraturan SMKI</li><li>- Bukti poin 2) berupa hasil pemeriksaan substansial pada kontrol 2 sampai dengan 14.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

#### KEF.2

Teknik pemeriksaan	:	Pemeriksaan substansial untuk memastikan isu internal dan isu eksternal ditindaklanjuti sehingga mencegah eksplorasi yang dilakukan oleh pihak-pihak tidak berkepentingan.
--------------------	---	--

		<p>Pemeriksaan pada K2 ini erat kaitannya dengan pemeriksaan pada kontrol keamanan lainnya baik pada tahapan implementasi dan tahapan efektivitas yang relevan terhadap isu internal dan eksternal.</p> <p>Pemeriksaan pada K2 ini erat kaitannya dengan pemeriksaan pada kontrol-kontrol baik pada tahapan implementasi dan tahapan efektivitas lain yang didefinisikan sebagai isu internal dan eksternal.</p> <p>Indikator dalam pemeriksaan substansial ini adalah memastikan tidak ada bukti kejadian / insiden keamanan dalam kurun waktu pemeriksaan audit.</p>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti pemeriksaan kontrol keamanan lain yang relevan dengan isu Internal dan eksternal</li><li>- Rekapitulasi Insiden Tahunan</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

### KEF.3

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan Penanggung Jawab Keamanan SPBE menjalankan tugas dan tanggung jawabnya.</p> <p>Pemeriksaan pada K3 ini erat kaitannya dengan pemeriksaan pada kontrol keamanan lainnya baik pada tahapan implementasi dan tahapan efektivitas yang relevan terhadap tugas dan tanggung jawab penanggung jawab Keamanan SPBE.</p>
--------------------	---	--

		Indikator dalam pemeriksaan substansial ini adalah memastikan tidak ada bukti kejadian / insiden keamanan dalam kurun waktu pemeriksaan audit.
Bukti	:	Bukti K3 merujuk pada pemeriksaan kontrol keamanan lain yang relevan. Contoh : Bukti pada kontrol 12 terkait dukungan pengoperasian keamanan dan kontrol 13 terkait evaluasi kinerja
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

#### KEF.4

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan bahwa Pelaksana teknis Keamanan SPBE pada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah menjalankan tugas dan tanggung jawabnya.</p> <p>Pemeriksaan yang dilakukan meliputi :</p> <ol style="list-style-type: none"><li>1) Memastikan substansi dokumen standar teknis dan prosedur keamanan yang ada sesuai dengan standar teknis dan prosedur Keamanan SPBE;</li><li>2) Memastikan penerapan standar teknis dan prosedur keamanan telah dilaksanakan;</li><li>3) Memastikan program kerja Keamanan SPBE dilaksanakan;</li><li>4) Memastikan pelaporan kepada koordinator telah dilaksanakan dan terdokumentasi; dan</li><li>5) Memastikan perbaikan berkelanjutan meningkatkan performa keamanan.</li></ol>
--------------------	---	--

Bukti	:	<ul style="list-style-type: none"><li>- Bukti poin 1) berupa dokumen Standar teknis dan prosedur Keamanan yang sesuai dengan Standar Teknis dan prosedur Keamanan SPBE;</li><li>- Bukti poin 2) berupa penerapan standar teknis dan prosedur keamanan yang telah berjalan di aplikasi dan atau infrastruktur pada instansi;</li><li>- Bukti poin 3) berupa pelaksanaan program kerja keamanan yang telah selesai dan memenuhi persentase yang ditetapkan auditor Keamanan SPBE;</li><li>- Bukti poin 4) berupa Laporan pelaksanaan kegiatan Keamanan SPBE dan nota dinas penyampaian kepada Koordinator SPBE;</li><li>- Bukti poin 5) berupa Laporan perbaikan berkelanjutan ( merujuk pada pengujian KEF.9) 2 tahun berturut-turut pada periode sebelumnya untuk melihat perbandingan dan peningkatan performa keamanan.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

#### KEF.5

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan bahwa Pelaksana teknis Keamanan SPBE yang membawahi, membangun, memelihara dan atau mengembangkan Aplikasi menjalankan tugas dan tanggung jawabnya.</p> <p>Pemeriksaan tersebut meliputi :</p> <ol style="list-style-type: none"><li>1) Pengujian terhadap penerapan Standar Teknis dan Prosedur Keamanan sesuai kriteria Keamanan SPBE pada unit</li></ol>
--------------------	---	---

		<p>kerja dengan metode Survei (uji sampling);</p> <p>2) Pengujian terhadap kesesuaian pembangunan/pengembangan aplikasi dengan metode Survei (uji sampling);</p> <p>3) Memastikan keberlangsungan Proses Bisnis.</p> <p>Memastikan koordinasi kepada pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan TIK Instansi Pusat dan Pemerintah Daerah telah dilaksanakan dan terdokumentasi.</p>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti untuk poin 1) dapat berupa laporan atau hasil pengujian penerapan Standar Teknis dan Prosedur Keamanan dengan <i>passing grade</i> yang ditetapkan auditor Keamanan SPBE.</li><li>- Bukti untuk poin 2) dapat berupa laporan pembangunan/pengembangan aplikasi atau hasil pengujian pembangunan/pengembangan dengan <i>passing grade</i> yang ditetapkan auditor Keamanan SPBE.</li><li>- Bukti untuk poin 3) dapat berupa laporan keberlangsungan Proses Bisnis atau hasil pengujian keberlangsungan Proses Bisnis dengan <i>passing grade</i> yang ditentukan tetapkan auditor Keamanan SPBE.</li><li>- Bukti untuk poin 4) berupa laporan pelaksanaan simulasi keberlangsungan bisnis terhadap bencana.</li><li>- Bukti untuk poin 5) berupa Laporan dan nota dinas penyampaian pelaksanaan</li></ul>

		kegiatan keamanan kepada fungsi bidang keamanan Teknologi Informasi dan Komunikasi Instansi Pusat dan Pemerintah Daerah dan atau Koordinator SPBE.
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

KEF.6

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan Pelaksana teknis Keamanan SPBE melaksanakan perencanaan program kerja dan membuat target realisasi program kerja keamanan sesuai pedoman manajemen Keamanan SPBE</p> <p>Pemeriksaan tersebut meliputi :</p> <ul style="list-style-type: none"><li>- Memastikan mitigasi risiko relevan dan dijalankan sesuai target</li><li>- Memastikan progres pelaksanaan program kerja Keamanan SPBE</li><li>- Memastikan target realisasi program kerja Keamanan SPBE tercapai</li></ul>
Bukti	:	<ul style="list-style-type: none"><li>- Dokumen yang menjelaskan 90% mitigasi risiko telah dilaksanakan;</li><li>- <i>Risk Register</i> yang telah diperbaharui;</li><li>- 100% program kerja keamanan selesai sesuai target realisasinya.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

KEF.7

Teknik pemeriksaan	:	Pemeriksaan substansial untuk memastikan tujuan peningkatan pengetahuan kesadaran Keamanan SPBE telah terpenuhi melalui sosialisasi dan
--------------------	---	---

		<p>pelatihan untuk internal Organisasi dan pihak eksternal terkait.</p> <p>Pemeriksaan dilakukan dengan metode Survei (uji sampling) terhadap personel Internal Organisasi dan pihak eksternal dilakukan.</p> <p>Personel yang menjadi subjek sampling adalah yang hadir dalam kegiatan sosialisasi dan atau pelatihan Keamanan SPBE.</p> <p>Penggunaan metode uji sampling disampaikan kepada audit, dan melihat kondisi dan waktu yang tersedia.</p>
Bukti	:	<ul style="list-style-type: none"><li>- Hasil sampling terhadap kehadiran perwakilan internal organisasi dan pihak eksternal terkait dengan hasil yang melebihi nilai <i>passing grade</i> yang ditentukan tetapkan auditor;</li><li>- Bukti lain yang mendukung adalah hasil <i>post test</i> kegiatan edukasi keamanan;</li><li>- Hasil uji kompetensi atau ujian akhir untuk pelatihan.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

#### KEF.8

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan tujuan penilaian kerentanan Keamanan SPBE dilaksanakan.</p> <p>Pemeriksaan tersebut meliputi :</p> <ol style="list-style-type: none"><li>1) Memastikan daftar aset diperbarui secara berkala;</li></ol>
--------------------	---	---

		<p>2) Memastikan daftar risiko terhadap aset diperbaharui secara berkala;</p> <p>3) Memastikan tingkat risiko terhadap aset diperbaharui secara berkala.</p>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti poin 1) berupa daftar aset SPBE yang sudah diperbaharui;</li><li>- Bukti poin 2) berupa daftar Risiko Aset yang telah diperbaharui;</li><li>- Bukti poin 3) berupa daftar tingkat risiko yang telah diperbaharui.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

KEF.9

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan :</p> <p>1) Peningkatan Keamanan SPBE dilaksanakan terus menerus dengan menerapkan Standar Teknis dan Prosedur keamanan pada pengelolaan aplikasi dan Infrastruktur SPBE;</p> <p>2) Rencana perbaikan terhadap penerapan dan laporan perbaikan penerapan;</p> <p>3) Memastikan adanya rencana peningkatan keamanan dari aplikasi SPBE dan infrastruktur yang telah diuji dan Laporan perbaikan serta pengujian ulang keamanan.</p>
Bukti	:	Hasil pemeriksaan terhadap penerapan Standar dan Prosedur Keamanan SPBE pada pengelolaan dan Infrastruktur di atas persentase yang ditentukan tetapkan auditor Keamanan SPBE sesuai dengan dokumennya.

		<ul style="list-style-type: none"><li>- Dokumen rencana perbaikan terhadap penerapan standar pada aplikasi dan infrastruktur;</li><li>- Laporan perbaikan terhadap penerapan standar pada aplikasi dan infrastruktur;</li><li>- Dokumen atau daftar yang menjelaskan rencana perbaikan keamanan aplikasi;</li><li>- Laporan perbaikan keamanan aplikasi dan infrastruktur serta pengujian ulang keamanan.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

KEF.10

Teknik pemeriksaan	:	Pemeriksaan substansial untuk memastikan penanganan insiden Keamanan SPBE ditangani sesuai tujuan.
Bukti	:	<ul style="list-style-type: none"><li>- Hasil analisis penanganan insiden yang telah dilaksanakan dengan prosedur penanganan insiden sesuai pedoman Manajemen Keamanan Informasi SPBE dengan pemenuhan persentase yang ditetapkan auditor Keamanan SPBE;</li><li>- Untuk menghasilkan analisis di atas, dibutuhkan sampling atau keseluruhan laporan-laporan penanganan insiden yang terjadi dalam kurun waktu rentang audit;</li><li>- Penggunaan metode uji sampling disampaikan kepada auditan, dan melihat kondisi dan waktu yang tersedia;</li><li>- Hasil Verifikasi insiden-insiden yang terjadi telah selesai (persentase ditetapkan auditor) dan ditutup secara formal;</li></ul>

		<ul style="list-style-type: none"><li>- Tidak ditemukannya insiden yang sama berulang pada 1 tahun terakhir.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

**KEF.11**

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan bahwa :</p> <ol style="list-style-type: none"><li>1) Ruang lingkup audit keamanan telah dilaksanakan mencakup keseluruhan ruang lingkup pengaturan SMKI;</li><li>2) Memastikan bahwa hasil audit sebelumnya telah ditindaklanjuti.</li></ol>
Bukti	:	<ul style="list-style-type: none"><li>- Bukti poin 1) berupa Laporan Pelaksanaan Audit meliputi ruang lingkup Aplikasi dan Infrastruktur, tata kelola / SMKI dan fungsionalitas;</li><li>- Bukti poin 2) berupa Laporan Tindak lanjut atas perbaikan temuan pada ruang lingkup di atas.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

**KEF.12**

Teknik pemeriksaan	:	<p>Pemeriksaan substansial untuk memastikan bahwa dukungan pengoperasian mendapat dukungan pimpinan dan berjalan sesuai tujuannya.</p>
Bukti	:	<ul style="list-style-type: none"><li>- Hasil analisis pengajuan dukungan penganggaran keamanan didukung atau disetujui baik dari sisi nominal penganggaran dan kuantitatif jenis kegiatan atau anggaran Keamanan SPBE (membandingkan dokumen pengajuan anggaran tahun lalu &amp; KAK RAB tahun berjalan dan persentase persetujuan rencana tersebut ditetapkan auditor Keamanan SPBE);</li></ul>

		<ul style="list-style-type: none"><li>- Hasil analisis konsistensi perencanaan program peningkatan kapasitas SDM Keamanan sesuai dengan dokumen kompetensi unit kerja terkait keamanan (membandingkan dokumen pengajuan anggaran tahun lalu &amp; tahun berjalan).</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

KEF.13

Teknik pemeriksaan	:	Pemeriksaan substansial untuk memastikan tindak lanjut dari evaluasi kinerja dilaksanakan.
Bukti	:	<ul style="list-style-type: none"><li>- Dokumen tindak lanjut evaluasi kinerja (rencana perbaikan berkelanjutan);</li><li>- Dokumen yang menunjukkan adanya arahan/rekomendasi/persetujuan dari koordinator SPBE dalam rapat evaluasi kinerja.</li></ul>
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

KEF.14

Teknik pemeriksaan	:	Pemeriksaan substansial untuk memastikan Instansi Pusat dan Pemerintah Daerah telah melaksanakan perbaikan berkelanjutan dari rencana Perbaikan Berkelanjutan.
Bukti	:	Hasil analisa dari setiap Laporan pelaksanaan perbaikan berkelanjutan antara lain tindak lanjut audit, dan insiden dan lain-lain.
Status Pemeriksaan	:	Efektif / Perlu Peningkatan / Belum Efektif

### BAB III

#### STANDAR TEKNIS DAN PROSEDUR KEAMANAN APLIKASI BERBASIS WEB

Petunjuk Teknis, Penjelasan dan Pengujian setiap fungsi kontrol keamanan Standar Teknis Dan Prosedur Keamanan Aplikasi berbasis Web merupakan prosedur yang dapat dilakukan oleh Auditor Keamanan SPBE Keamanan untuk mendapatkan bukti data dukung pengujian kontrol keamanan.

A. Kontrol Keamanan pada area Standar Teknis dan Prosedur Keamanan  
Kontrol Keamanan pada area Standar Teknis dan Prosedur Keamanan Aplikasi Berbasis Web berjumlah 72 kontrol keamanan yang terdiri dari 13 fungsi diuraikan sebagai berikut :

1. Fungsi : Pasal 27 ayat (1) tentang Autentikasi (Kontrol 1-7);
2. Fungsi : Pasal 27 ayat (2) tentang Manajemen Sesi (Kontrol 8-14);
3. Fungsi : Pasal 27 ayat (3) tentang Kontrol Akses (Kontrol 15-18);
4. Fungsi : Pasal 27 ayat (4) tentang Validasi Input (Kontrol 19-25);
5. Fungsi : Pasal 27 ayat (5) tentang Kriptografi pada Verifikasi Statis (Kontrol 26-29);
6. Fungsi : Pasal 27 ayat (6) tentang Penanganan Error dan Pencatatan Log (Kontrol 30-36);
7. Fungsi : Pasal 27 ayat (7) tentang Proteksi Data (Kontrol 37-42);
8. Fungsi : Pasal 27 ayat (8) tentang Keamanan Komunikasi (Kontrol 43-46);
9. Fungsi : Pasal 27 ayat (9) tentang Pengendalian Kode Berbahaya (Kontrol 47-51);
10. Fungsi : Pasal 27 ayat (10) tentang Logika Bisnis (Kontrol 52-56);
11. Fungsi : Pasal 27 ayat (11) tentang File (Kontrol 57-61);
12. Fungsi : Pasal 27 ayat (12) tentang Keamanan *Application programming interface* dan Web Service (Kontrol 62-67); dan
13. Fungsi : Pasal 27 ayat (13) tentang Keamanan Konfigurasi (Kontrol 68-72).

K1. Menggunakan manajemen kata sandi untuk proses autentikasi

Deskripsi/ Tujuan	Memastikan penerapan manajemen kata sandi yang memadai dalam rangka proses autentikasi yang efektif.
----------------------	--

Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin a</li> <li>• OWASP ASVS v.4.0.3 – 2</li> <li>• WSTG-ATHN-02</li> <li>• CWE-521</li> </ul>
----------------------------------	---

K2. Menerapkan verifikasi kata sandi pada sisi server

Deskripsi/ Tujuan	Memastikan bahwa tidak ada penggunaan kata sandi yang masuk dalam kategori lemah (baik itu lemah karena sering digunakan ataupun lemah dikarenakan bersifat default dari suatu produk).
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin b</li> <li>• OWASP ASVS v.4.0.3 – 2.2.1</li> <li>• WSTG-ATHN-02</li> <li>• CAPEC-16</li> <li>• CWE-307</li> <li>• CWE-1392</li> <li>• CWE-1393</li> <li>• CAPEC-70</li> </ul>

K3. Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi

Deskripsi/ Tujuan	Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin c</li> <li>• OWASP ASVS v.4.0.3 – 2.1.1; 2.1.2; 2.1.4</li> <li>• WSTG-ATHN-02</li> <li>• CAPEC-16</li> <li>• CWE-521</li> <li>• CWE-1392</li> <li>• CWE-1393</li> <li>• CAPEC-70</li> </ul>

K4. Mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi

Deskripsi/ Tujuan	Melindungi sistem dari percobaan menebak kata sandi dan akses ilegal ke dalam sistem.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin d</li> <li>• OWASP ASVS v.4.0.3 – 2.2.1</li> <li>• WSTG-ATHN-03</li> <li>• CWE-307</li> <li>• CWE-654</li> </ul>

K5. Mengatur mekanisme pemulihan kata sandi

Deskripsi/ Tujuan	Memastikan bahwa terdapat mekanisme pemulihan kata sandi yang memadai pada aplikasi.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin e</li> <li>● OWASP ASVS v.4.0.3 – 2.1.5; 2.1.6; 2.5.3</li> <li>● WSTG-ATHN-09</li> <li>● CAPEC-50</li> <li>● CWE-620</li> <li>● CWE-640</li> </ul>

K6. Menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi.

Deskripsi/ Tujuan	Memastikan kerahasiaan kata sandi yang disimpan dalam keadaan terenkripsi dan memitigasi risiko pengungkapan kata sandi dalam keadaan terbaca dengan jelas ( <i>Clear text</i> ).
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin f</li> <li>● OWASP ASVS v.4.0.3 – 2.4.1</li> <li>● WSTG-ATHN-02</li> <li>● CWE-916</li> </ul>

K7. Menggunakan jalur komunikasi yang diamankan untuk proses autentikasi

Deskripsi/ Tujuan	Memastikan bahwa jalur komunikasi yang digunakan oleh aplikasi telah sesuai dengan <i>common practice</i> dan standar keamanan yang menjadi rujukan secara internasional.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 1 poin g</li> <li>● OWASP ASVS v.4.0.3 – 2.7.4</li> <li>● WSTG-CRYP-01</li> <li>● WSTG-CRYP-03</li> <li>● CWE-295</li> <li>● CWE-311</li> <li>● CWE-523</li> <li>● CAPEC-217</li> </ul>

K8. Menggunakan pengendali sesi untuk proses manajemen sesi

Deskripsi/ Tujuan	Memastikan aplikasi memiliki pengendali sesi yang memiliki fungsi untuk membatasi suatu peran dari pengguna.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin a</li> <li>● OWASP ASVS v.4.0.3 – 3</li> </ul>

	<ul style="list-style-type: none"><li>● WSTG-SESS-01</li><li>● WSTG-SESS-02</li><li>● WSTG-SESS-03</li><li>● CWE-598</li></ul>
K9.	Menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi
Deskripsi/ Tujuan	Memastikan penerapan sesi pada aplikasi untuk autentikasi berkelanjutan.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin b</li><li>● WSTG-SESS-01</li></ul>
K10.	Mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi
Deskripsi/ Tujuan	Memastikan pembuatan dan keacakan token sesi yang dibuat.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin c</li><li>● OWASP ASVS v.4.0.3 – 3.2.1; 3.2.4</li><li>● WSTG-SESS-01</li><li>● CWE-384</li><li>● CWE-331</li></ul>
K11.	Mengatur kondisi dan jangka waktu habis sesi
Deskripsi/ Tujuan	Memastikan terdapatnya mekanisme log out otomatis, manajemen batas waktu, kadaluarsa, serta penghancuran sesi dalam rangka memitigasi penggunaan berulang nilai sesi yang sama pada kondisi idle di rentang waktu tertentu.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin d</li><li>● OWASP ASVS v.4.0.3 – 3.3.1; 3.3.2</li><li>● WSTG-SESS-07</li><li>● CWE-613</li></ul>
K12.	Validasi dan pencantuman session id
Deskripsi/ Tujuan	Memastikan bahwa setiap sesi yang terbentuk memiliki keunikan session ID tersendiri
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>● Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin e</li><li>● OWASP ASVS v.4.0.3 – 3.4.1; 3.4.2; 3.4.3; 3.4.4</li><li>● WSTG-SESS-01</li><li>● WSTG-SESS-02</li></ul>

	<ul style="list-style-type: none"><li>• WSTG-SESS-03</li><li>• CWE-614</li><li>• CWE-1004</li><li>• CWE-16</li></ul>
--	--

K13. Pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi

Deskripsi/ Tujuan	Memastikan bahwa pengiriman token hanya dilakukan pada jalur yang aman dan dengan atribut yang sesuai <i>best practice</i> .
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin f</li><li>• OWASP ASVS v.4.0.3 – 3.2.3</li><li>• WSTG-SESS-02</li><li>• WSTG-SESS-03</li><li>• CWE-539</li></ul>

K14. Pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna

Deskripsi/ Tujuan	Memastikan aplikasi melakukan pembangkitan session baru saat pengguna login kembali.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 2 poin g</li><li>• OWASP ASVS v.4.0.3 – 3.2.1</li><li>• CWE-384</li></ul>

K15. Menetapkan otorisasi pengguna untuk membatasi kontrol akses

Deskripsi/ Tujuan	Memastikan supaya setiap peran (role) dari pengguna berjalan sesuai dengan yang telah ditentukan (baik dari eksekusi Create, Read, Update, maupun Delete).
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 3 poin a</li><li>• OWASP ASVS v.4.0.3 – 4.1.3</li><li>• CAPEC-180</li><li>• CWE-284</li><li>• CWE-285</li><li>• WSTG-ATHZ-03</li><li>• WSTG-ATHZ-04</li></ul>

K16. Mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi

Deskripsi/ Tujuan	Mencegah terjadinya serangan secara otomatis yang dapat membuat seorang penyerang untuk dapat meraih akses ke dalam suatu aplikasi, melakukan pengambilan data secara masif dan
----------------------	---

	otomatis, atau bahkan membuat suatu sistem menjadi down.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 3 poin b</li><li>• OWASP ASVS v.4.0.3 – 4.2.2</li><li>• WSTG-ERRH-01</li><li>• CAPEC-112</li><li>• CAPEC-125</li><li>• CWE-352</li><li>• CWE-400</li><li>• CWE-770</li><li>• CWE-799</li></ul>

K17. Mengatur antarmuka pada sisi administrator

Deskripsi/ Tujuan	Memastikan bahwa suatu aplikasi memiliki pengaturan pada sisi administrator yang dapat digunakan untuk memperkuat keamanan akses terhadap sisi administrator itu sendiri.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 3 poin c</li><li>• WSTG-CONF-05</li><li>• CWE-419</li></ul>

K18. Mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan

Deskripsi/ Tujuan	Memastikan bahwa suatu data dan informasi hanya dapat diakses oleh pengguna yang legitimate.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 3 poin d</li><li>• OWASP ASVS v.4.0.3 – 4.3.3</li><li>• CWE-732</li></ul>

K19. Menerapkan fungsi validasi input pada sisi server

Deskripsi/ Tujuan	Melakukan sanitasi terhadap input yang dilakukan pengguna dalam rangka mitigasi serangan seperti XSS, SQLi, dan lain-lain
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin a</li><li>• OWASP ASVS v.4.0.3 – 5.1.3</li><li>• WSTG-INPV-01</li><li>• WSTG-INPV-02</li><li>• CWE-20</li></ul>

K20. Menerapkan mekanisme penolakan input jika terjadi kesalahan validasi

Deskripsi/ Tujuan	Untuk melakukan pemeriksaan terhadap input yang dilakukan pengguna , dalam rangka
----------------------	---

	mitigasi format data yang tidak sesuai, dan telah ditetapkan oleh aplikasi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin b</li><li>• OWASP ASVS v.4.0.3 – 5.1.5</li><li>• CWE-601</li></ul>

K21. Melakukan validasi positif pada seluruh input

Deskripsi/ Tujuan	Untuk melakukan penyaringan terhadap input yang dilakukan pengguna melalui mekanisme mendefinisikan daftar putih (white listing), terhadap tag atau atribut html yang diperbolehkan pada aplikasi.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin c</li><li>• OWASP ASVS v.4.0.3 – 5.1.3</li><li>• CWE-20</li></ul>

K22. Melakukan filter terhadap data yang tidak dipercaya

Deskripsi/ Tujuan	Melakukan penyaringan terhadap input yang diberikan pengguna, melalui entry point seperti form yang di-submit, atau parameter pada url.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin e</li><li>• OWASP ASVS v.4.0.3 – 5.1; 5.2</li><li>• WSTG-INPV-04</li><li>• CWE-94</li><li>• CWE-95</li><li>• CWE-116</li><li>• CWE-138</li><li>• CWE-147</li><li>• CWE-159</li><li>• CWE-918</li></ul>

K23. Menggunakan fitur kode dinamis

Deskripsi/ Tujuan	Menemukan penggunaan dari fitur kode dinamis pada aplikasi dalam rangka melakukan proses encoding atau mengganti dengan karakter unicode terhadap inputan penggunaan yang tidak sesuai dengan aturan yang ditetapkan.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin f</li><li>• OWASP ASVS v.4.0.3 – 5.2.4; 5.3</li><li>• CWE-95</li></ul>

K24. Melakukan pelindungan terhadap akses yang mengandung konten skrip

Deskripsi/ Tujuan	Melindungi aplikasi dari inputan pengguna yang mengandung skrip, ataupun percobaan serangan melalui entry point (seperti form yang di-submit, atau parameter pada url, textfield pada fitur pencarian, dan lain - lain).
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin g</li><li>• OWASP ASVS v.4.0.3 – 5.1; 5.2.7; 5.2.8</li><li>• WSTG-INPV-01</li><li>• WSTG-INPV-02</li><li>• WSTG-INPV-03</li><li>• CWE-94</li><li>• CWE-159</li></ul>

K25. Melakukan pelindungan dari serangan injeksi basis data

Deskripsi/ Tujuan	Mengidentifikasi potensi injeksi pada aplikasi, guna memitigasi potensi serangan seperti SQLi, terganggunya kerahasiaan data seperti kebocoran data, akses yang tidak sah ke data yang bersifat sensitif atau terganggunya aspek integritas data ataupun ketersediaannya.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 4 poin h</li><li>• OWASP ASVS v.4.0.3 – 5.1; 5.3.4; 5.3.5</li><li>• WSTG-INPV-05</li><li>• CWE-89</li></ul>

K26. Menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan

Deskripsi/ Tujuan	Memastikan bahwa aplikasi telah didesain dengan identifikasi dan implementasi penerapan kriptografi dalam arsitektur aplikasinya guna melindungi aset data sesuai dengan kebutuhan dan klasifikasi informasinya untuk memberikan jaminan keamanan aspek kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan/atau ketersediaan. Desain kontrol yang dapat menjadi rujukan umumnya berupa kebijakan password, arsitektur aplikasi, arsitektur database, ataupun saluran komunikasi yang digunakan, baik itu data at rest dan data in transit.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 5 poin a</li><li>• OWASP ASVS v.4.0.3 – 6.1; 6.2.3</li><li>• CWE-311</li><li>• CWE-326</li></ul>

K27. Melakukan autentikasi data yang dienkripsi

Deskripsi/ Tujuan	Memastikan bahwa aplikasi memenuhi persyaratan seluruh modul kriptografi yang digunakan telah diimplementasikan dengan benar untuk menjamin data yang dienkripsi adalah asli dan utuh sehingga dapat dilakukan verifikasi atau validasi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 5 poin b</li><li>• OWASP ASVS v.4.0.3 – 6.2.7</li><li>• CWE-326</li></ul>

K28. Menerapkan manajemen kunci kriptografi

Deskripsi/ Tujuan	Memastikan bahwa aplikasi mengimplementasikan manajemen kunci kriptografi yang aman dari seluruh tahapan siklus hidup kunci kriptografi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 5 poin c</li><li>• OWASP ASVS v.4.0.3 – 6.4.1</li><li>• CWE-798</li></ul>

K29. Membuat angka acak yang menggunakan generator angka acak kriptografi

Deskripsi/ Tujuan	Memastikan bahwa aplikasi mengimplementasikan pembangkitan angka acak kriptografi yang aman dalam setiap modul aplikasi yang membutuhkan angka acak seperti token, initialization vector, seed, ataupun master key
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 5 poin d</li><li>• OWASP ASVS v.4.0.3 – 6.3.1</li><li>• CWE-338</li></ul>

K30. Mengatur konten pesan yang ditampilkan ketika terjadi kesalahan

Deskripsi/ Tujuan	Memastikan bahwa Aplikasi hanya akan menampilkan pesan bersifat umum yang muncul ketika terjadi eror
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin a</li><li>• OWASP ASVS v.4.0.3 – 7.4.1</li><li>• CWE-210</li></ul>

K31. Menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani

Deskripsi/ Tujuan	Memastikan bahwa Aplikasi memiliki metode untuk menangani error untuk mencegah kesalahan terprediksi dan tidak terduga
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin b</li><li>• OWASP ASVS v.4.0.3 – 7.4.1</li><li>• CWE-210</li></ul>

K32. Tidak mencantumkan informasi yang dikecualikan dalam pencatatan log

Deskripsi/ Tujuan	Memastikan bahwa Aplikasi tidak mencantumkan informasi yang dikecualikan dalam pencatatan log, dan hanya mencatat log keamanan yang relevan dengan insiden seperti autentikasi berhasil dan gagal, kegagalan akses kontrol, kegagalan validasi input.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin c</li><li>• OWASP ASVS v.4.0.3 – 7.1.1; 7.1.2; 7.1.3</li><li>• CWE-532</li><li>• CWE-778</li></ul>

K33. Mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden

Deskripsi/ Tujuan	Memastikan bahwa Aplikasi telah mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin d</li></ul>

K34. Mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah

Deskripsi/ Tujuan	Memastikan bahwa aplikasi telah mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin e</li><li>• OWASP ASVS v.4.0.3 – 7.3.3</li><li>• CWE-200</li></ul>

K35. Melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log

Deskripsi/ Tujuan	Memastikan bahwa semua komponen log harus mendapatkan pengamanan, dengan cara enkripsi pada data sebelum dicatat pada log, yang berguna sebagai pencegahan injeksi log
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin f</li><li>• OWASP ASVS v.4.0.3 – 7.3.1</li><li>• CWE-117</li></ul>

K36. Melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar

Deskripsi/ Tujuan	Memastikan bahwa sumber waktu pada Aplikasi telah disinkronisasi dengan waktu dan zona waktu yang tepat, dan disarankan menggunakan UTC untuk memudahkan analisis forensik pasca insiden
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 6 poin g</li><li>• OWASP ASVS v.4.0.3 – 7.3.4</li></ul>

K37. Melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan

Deskripsi/ Tujuan	Memastikan bahwa seluruh data yang teridentifikasi dibuat dan diproses oleh aplikasi harus dipastikan terletak sesuai direktori yang ditetapkan.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 7 poin a</li><li>• OWASP ASVS v.4.0.3 – 8.3.4</li><li>• CWE-200</li></ul>

K38. Melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi

Deskripsi/ Tujuan	Memastikan bahwa informasi sensitif yang disimpan sementara dalam aplikasi diterapkan perlindungan dari akses yang tidak sah
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 7 poin b</li><li>• OWASP ASVS v.4.0.3 – 8.3.6</li><li>• CWE-226</li></ul>

K39. Melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan

Deskripsi/ Tujuan	Memastikan bahwa pada Aplikasi terdapat mekanisme pertukaran, penghapusan, dan audit informasi yang dikecualikan
----------------------	--

Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 7 poin c</li><li>• OWASP ASVS v.4.0.3 – 8.3.5</li><li>• CWE-532</li></ul>
----------------------------	---

K40. Memastikan data disimpan dengan aman

Deskripsi/ Tujuan	Memastikan data disimpan dengan aman dan backup data dilakukan secara aman
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 7 poin e</li><li>• OWASP ASVS v.4.0.3 – 8.3.7</li><li>• CWE-327</li></ul>

K41. Menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna

Deskripsi/ Tujuan	Memastikan terdapat metode untuk menghapus dan mengekspor data sesuai permintaan pengguna
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 7 poin f</li><li>• OWASP ASVS v.4.0.3 – 8.3.2</li><li>• CWE-212</li></ul>

K42. Membersihkan memori setelah tidak diperlukan

Deskripsi/ Tujuan	Memastikan bahwa dilakukan pembersihan memori setelah tidak diperlukan
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 7 poin g</li><li>• OWASP ASVS v.4.0.3 – 8.3.6</li><li>• CWE-226</li></ul>

K43. Menggunakan komunikasi terenkripsi

Deskripsi/ Tujuan	Memastikan bahwa aplikasi memenuhi persyaratan menggunakan TLS dengan enkripsi yang kuat dan terbaru, serta dikonfigurasi untuk menonaktifkan penggunaan algoritma yang lemah, telah usang, atau telah diketahui tidak aman.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 8 poin a</li><li>• OWASP ASVS v.4.0.3 – 9.1.1</li><li>• CWE-319</li></ul>

K44. Mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna

Deskripsi/ Tujuan	Memastikan bahwa aplikasi mengimplementasikan setiap koneksi transaksi elektronik yang dikirimkan pengguna selalu melalui jaringan yang terenkripsi, serta mereview konfigurasi dari sisi klien untuk memastikan implementasi TLS 1.2 atau yang terbaru telah terverifikasi.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 8 poin b</li><li>• OWASP ASVS v.4.0.3 – 9.2.2</li><li>• CWE-319</li></ul>

K45. Mengatur jenis algoritma yang digunakan dan alat pengujinya

Deskripsi/ Tujuan	Memastikan bahwa hanya versi protokol TLS terbaru yang diaktifkan, serta memastikan terdapat pengaturan alat pengujian TLS yang akan digunakan oleh pemilik Aplikasi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 8 poin c</li><li>• OWASP ASVS v.4.0.3 – 9.1.2; 9.1.3</li><li>• CWE-326</li></ul>

K46. Mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik

Deskripsi/ Tujuan	Memastikan terdapat pengaturan mekanisme dan waktu aktivasi dan konfigurasi sertifikat TLS yang dipakai pada aplikasi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 8 poin d</li><li>• OWASP ASVS v.4.0.3 – 9.1.2; 9.1.3</li><li>• CWE-295</li></ul>

K47. Menggunakan analisis kode dalam kontrol kode berbahaya

Deskripsi/ Tujuan	Memastikan bahwa terdapat tools analisis kode yang dapat mendeteksi kode yang berpotensi malicious
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 9 poin a</li><li>• OWASP ASVS v.4.0.3 – 10.1.1</li><li>• CWE-749</li></ul>

K48. Memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan

Deskripsi/ Tujuan	Memastikan bahwa kode sumber dan library pihak ketiga pada aplikasi, tidak mengandung kode berbahaya serta tidak memiliki kemampuan
----------------------	---

	untuk mengumpulkan data. Jika memang harus menggunakan data maka harus meminta persetujuan dari user.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 9 poin b</li> <li>• OWASP ASVS v.4.0.3 – 10.2.1</li> <li>• CWE-359</li> </ul>

K49. Mengatur izin terkait fitur atau sensor terkait privasi

Deskripsi/ Tujuan	Memastikan aplikasi tidak akan meminta izin kepada fitur atau akses yang tidak diperlukan/berlebihan kepada sensor seperti kamera, microphone dan lokasi.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 9 poin c</li> <li>• OWASP ASVS v.4.0.3 – 10.2.2</li> <li>• CWE-272</li> </ul>

K50. Mengatur pelindungan integritas

Deskripsi/ Tujuan	Memastikan bahwa aplikasi menggunakan perlindungan integritas, seperti kode integritas signature atau subresource.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 9 poin d</li> <li>• OWASP ASVS v.4.0.3 – 10.3.2</li> <li>• CWE-353</li> </ul>

K51. Mengatur mekanisme fitur pembaruan

Deskripsi/ Tujuan	Memastikan bahwa aplikasi yang memiliki mekanisme pembaruan otomatis klien atau server, pembaruan harus diperoleh melalui saluran aman dan ditandatangani secara digital
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 9 poin e</li> <li>• OWASP ASVS v.4.0.3 – 10.3.1</li> <li>• CWE-16</li> </ul>

K52. Memproses alur logika bisnis dalam urutan langkah dan waktu yang realistik

Deskripsi/ Tujuan	Memastikan aplikasi hanya akan memproses aksi yang sesuai dengan logika bisnis dalam urutan langkah dan waktu yang realistik
Referensi Kontrol Keamanan	<ul style="list-style-type: none"> <li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 10 poin a</li> <li>• OWASP ASVS v.4.0.3 – 11.1.1; 11.1.2</li> <li>• CWE-841</li> <li>• CWE-799</li> </ul>

K53. Memastikan logika bisnis memiliki batasan dan validasi

Deskripsi/ Tujuan	Memastikan aplikasi mampu memvalidasi bahwa aksi sesuai dengan logika bisnis
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 10 poin b</li><li>• OWASP ASVS v.4.0.3 – 11.1.5</li><li>• CWE-841</li></ul>

K54. Memonitor aktivitas yang tidak biasa

Deskripsi/ Tujuan	Aplikasi mampu melakukan pemantauan terhadap aktivitas anomali atau yang tidak sesuai dengan logika bisnis
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 10 poin c</li><li>• OWASP ASVS v.4.0.3 – 11.1.7</li><li>• CWE-754</li></ul>

K55. Membantu dalam kontrol anti otomatisasi

Deskripsi/ Tujuan	Aplikasi memiliki kontrol anti-otomatisasi untuk melindungi dari permintaan akses berlebihan, seperti serangan eksfiltrasi data secara masif dan DDOS
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 10 poin d</li><li>• OWASP ASVS v.4.0.3 – 11.1.4</li><li>• CWE-770</li></ul>

K56. Memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa

Deskripsi/ Tujuan	Aplikasi mampu memberikan peringatan yang dapat dikonfigurasi ketika terdeteksinya serangan otomatis atau aktivitas yang tidak biasa
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 10 poin f</li><li>• OWASP ASVS v.4.0.3 – 11.1.8</li><li>• CWE-390</li></ul>

K57. Mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah

Deskripsi/ Tujuan	Aplikasi mengatur file dan kuota ukuran file yang diunggah untuk memastikan bahwa satu pengguna tidak dapat mengisi penyimpanan dengan banyak file, atau file yang terlalu besar.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 11 poin a</li><li>• OWASP ASVS v.4.0.3 – 12.1.3</li></ul>

• CWE-770

K58. Melakukan validasi file sesuai dengan tipe konten yang diharapkan

Deskripsi/ Tujuan	Memastikan file yang diunggah pada aplikasi dilakukan validasi sesuai dengan metadata untuk mencegah adanya fungsi yang tidak diinginkan.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 11 poin b</li><li>• OWASP ASVS v.4.0.3 – 12.3</li><li>• CWE-22</li><li>• CWE-73</li><li>• CWE-78</li><li>• CWE-98</li><li>• CWE-641</li><li>• CWE-829</li></ul>

K59. Melakukan pelindungan terhadap metadata input dan metadata file

Deskripsi/ Tujuan	Memastikan aplikasi memiliki mekanisme pelindungan terhadap metadata input dan metadata file
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 11 poin c</li><li>• OWASP ASVS v.4.0.3 – 12.3.1; 12.3.2; 12.3.3</li><li>• CWE-22</li><li>• CWE-73</li><li>• CWE-98</li></ul>

K60. Melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya

Deskripsi/ Tujuan	Memastikan setiap file yang didapatkan dari sumber yang tidak dipercaya dilakukan pemindaian untuk mencegah adanya konten berbahaya ( <i>malicious content</i> ) pada aplikasi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 11 poin d</li><li>• OWASP ASVS v.4.0.3 – 12.4.2</li><li>• CWE-509</li></ul>

K61. Melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan

Deskripsi/ Tujuan	Memastikan terdapat konfigurasi pada server yang mengatur proses unduh file untuk memastikan aplikasi hanya menyajikan file
----------------------	---

	tertentu guna mencegah kebocoran informasi dan kode sumber yang tidak disengaja.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 11 poin e</li><li>• OWASP ASVS v.4.0.3 – 12.5.1</li><li>• CWE-552</li></ul>

K62. Melakukan konfigurasi layanan web

Deskripsi/ Tujuan	Memastikan bahwa layanan web (Web Service) pada aplikasi telah dikonfigurasikan dengan baik.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 12 poin a</li><li>• OWASP ASVS v.4.0.3 – 13</li></ul>

K63. Memverifikasi uniform resource identifier *Application programming interface* tidak menampilkan informasi yang berpotensi sebagai celah keamanan

Deskripsi/ Tujuan	Memastikan bahwa tahap verifikasi pada Uniform Resource Identifier (URI) <i>Application programming interface</i> tidak menampilkan informasi yang berpotensi sebagai celah keamanan.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 12 poin b</li><li>• OWASP ASVS v.4.0.3 – 13.1.1</li><li>• CWE-116</li></ul>

K64. Membuat keputusan otorisasi

Deskripsi/ Tujuan	Memastikan otorisasi pada <i>Application programming interface</i> berjalan dan terkontrol dengan baik
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 12 poin c</li><li>• OWASP ASVS v.4.0.3 – 13.1.4</li><li>• CWE-285</li></ul>

K65. Menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid

Deskripsi/ Tujuan	Memastikan restful http valid berjalan dan dapat mencegah pengguna normal untuk menggunakan fitur DELETE atau PUT pada
----------------------	--

	<i>Application programming interface</i> dan resource yang terlindungi
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 12 poin d</li><li>• OWASP ASVS v.4.0.3 – 13.2.1</li><li>• CWE-650</li></ul>

K66. Menggunakan validasi skema dan verifikasi sebelum menerima input

Deskripsi/ Tujuan	Memastikan validasi skema XSD berjalan pada dokumen XML yang ada pada <i>Application programming interface</i> , dan memverifikasi input pada kode sumber
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 12 poin e</li><li>• OWASP ASVS v.4.0.3 – 13.3.1</li><li>• CWE-20</li></ul>

K67. Menerapkan kontrol anti otomatisasi

Deskripsi/ Tujuan	Memastikan Aplikasi memiliki kontrol anti-otomasi sebagai langkah pengamanan dari serangan exfiltrasi data yang masif, DDOS, dan file uploads
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 12 poin g</li><li>• OWASP ASVS v.4.0.3 – 11.1.4</li><li>• CWE-770</li></ul>

K68. Mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan

Deskripsi/ Tujuan	Memastikan konfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 13 poin a</li><li>• OWASP ASVS v.4.0.3 – 14.1.3</li><li>• CWE-16</li></ul>

K69. Mendokumentasi, menyalin konfigurasi, dan semua dependensi

Deskripsi/ Tujuan	Memastikan aplikasi memiliki konfigurasi/terdapat mekanisme dari pemilik/pengelola aplikasi untuk mendokumentasikan, menyalin konfigurasi, dan
----------------------	--

	semua dependensi, dan memanfaatkan hasil dokumentasi untuk keperluan kritikal.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 13 poin b</li><li>• OWASP ASVS v.4.0.3 – 14.1.4</li></ul>

K70. Menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan

Deskripsi/ Tujuan	Memastikan aplikasi memiliki konfigurasi/terdapat mekanisme dari pemilik/pengelola aplikasi agar semua fitur, dokumentasi, contoh aplikasi, dan konfigurasi yang tidak diperlukan telah dihapus.
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 13 poin c</li><li>• OWASP ASVS v.4.0.3 – 14.2.2</li><li>• CWE-1002</li></ul>

K71. Memvalidasi integritas asset jika asset aplikasi diakses secara eksternal

Deskripsi/ Tujuan	Memastikan terdapat konfigurasi atau mekanisme pada aplikasi terkait validasi integritas asset jika asset aplikasi diakses secara eksternal
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 13 poin d</li><li>• OWASP ASVS v.4.0.3 – 14.2.3</li><li>• CWE-829</li></ul>

K72. Menggunakan respons aplikasi dan konten yang aman

Deskripsi/ Tujuan	Memastikan HTTP Header atau komponen lain pada aplikasi yang muncul saat respons tidak boleh memperlihatkan adanya informasi mendetail mengenai versi komponen sistem yang digunakan
Referensi Kontrol Keamanan	<ul style="list-style-type: none"><li>• Perban Peraturan Badan Siber dan Sandi Negara No. 4 Tahun 2021 pasal 27 ayat 13 poin e</li><li>• OWASP ASVS v.4.0.3 – 14.3.3</li><li>• CWE-200</li></ul>

## B. Teknik Pengujian dan Pengumpulan Data

1. Teknik pengujian dan pengumpulan data pada tahap evaluasi desain kontrol keamanan:
  - a) Auditor Keamanan SPBE melakukan identifikasi kontrol keamanan yang akan diuji pada tahap evaluasi desain;
  - b) Auditor Keamanan SPBE melakukan wawancara dengan auditan terkait desain kontrol keamanan yang dimiliki, dalam pengembangan dan pengelolaan Aplikasi;
  - c) Auditan memberikan bukti atau data dukung desain kontrol keamanan yang dimiliki;
  - d) Auditor Keamanan SPBE melakukan evaluasi kesesuaian terhadap bukti atau data dukung.
2. Teknik pengujian dan pengumpulan data pada tahap evaluasi implementasi kontrol keamanan
  - a) Auditor Keamanan SPBE melakukan identifikasi kontrol keamanan yang akan diuji pada tahap evaluasi implementasi
  - b) Auditor Keamanan SPBE melakukan wawancara dengan auditan terkait implementasi dari kontrol keamanan pada aplikasi
  - c) Auditan memberikan bukti atau data dukung Implementasi Kontrol Keamanan
  - d) Auditor Keamanan SPBE melakukan reviu/observasi bukti atau data dukung
  - e) Auditor Keamanan SPBE melakukan pengujian langsung terhadap aplikasi pada tahap Implementasi Kontrol Keamanan jika diperlukan.
3. Teknik pengujian dan pengumpulan data pada tahap evaluasi efektivitas kontrol keamanan
  - a) Pengujian secara statis dan pengumpulan data Pengujian secara statis sama halnya seperti yang dilakukan pada tahap evaluasi implementasi. Pengujian ini dilakukan dengan cara melakukan wawancara kepada Auditan untuk memperoleh keyakinan bahwa kontrol keamanan dapat diyakini implementasinya telah dapat mencapai tujuannya dengan efektif.
  - b) Pengujian secara dinamis dan pengumpulan data

Pengujian ini dilakukan melalui metode *Penetration Test* (Pentest), pengujian yang dilakukan untuk menguji keamanan sistem dalam hal ini adalah aplikasi sesuai metodologi *Penetration Test*.

### C. Petunjuk Teknis Pemeriksaan Kontrol Keamanan pada Evaluasi Desain Kontrol

Petunjuk Teknis pemeriksaan kontrol keamanan merupakan prosedur audit yang dilakukan oleh Auditor TIK Cakupan Keamanan untuk menguji kontrol keamanan dan mendapatkan bukti kontrol keamanan telah dilaksanakan.

72 (tujuh puluh dua) Kontrol keamanan yang diperiksa pada tahap evaluasi desain kontrol dikodefikasi ulang menyesuaikan tahap evaluasi desain kontrol sehingga kodefikasinya ditambahkan ED (Evaluasi Desain). Contoh Kontrol keamanan pertama yang dikodefikasikan K1 menjadi KED.1 dalam tahapan evaluasi desain.

Hasil pemeriksaan tiap kontrol keamanan pada tahapan evaluasi desain akan menghasilkan status pemeriksaan yaitu Sesuai atau Tidak Sesuai dengan Desain Kontrol Keamanan.

#### KED.1

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penggunaan manajemen kata sandi untuk proses autentikasi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan manajemen kata sandi untuk proses autentikasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

#### KED.2

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penerapan verifikasi kata sandi pada sisi server kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penerapan verifikasi kata sandi pada sisi server yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

#### KED.3

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur jumlah karakter, kombinasi jenis
--------------------	---	---

	:	karakter, dan masa berlaku dari kata sandi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.4

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.5

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur mekanisme pemulihan kata sandi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan mekanisme pemulihan kata sandi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.6

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur mekanisme menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.7

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penggunaan jalur komunikasi yang diamankan untuk proses autentikasi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan jalur komunikasi yang diamankan untuk proses autentikasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.8

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penggunaan pengendali sesi untuk proses manajemen sesi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan pengendali sesi untuk proses manajemen sesi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.9

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penggunaan pengendali sesi yang disediakan oleh kerangka kerja aplikasi kepada Auditor
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan pengendali sesi yang disediakan oleh kerangka kerja aplikasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.10

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi yang diakui oleh organisasi

Status Pemeriksaan	:	Sesuai / Tidak Sesuai
--------------------	---	-----------------------

KED.11

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur kondisi dan jangka waktu habis sesi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat kondisi dan jangka waktu habis sesi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.12

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur validasi dan pencantuman session id kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat validasi dan pencantuman session id yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.13

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi kepada Auditor
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.14

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna yang diakui oleh organisasi

Status Pemeriksaan	:	Sesuai / Tidak Sesuai
--------------------	---	-----------------------

KED.15

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penetapan otorisasi pengguna untuk membatasi kontrol akses kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penetapan otorisasi pengguna untuk membatasi kontrol akses yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.16

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.17

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur antarmuka pada sisi administrator kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat antarmuka pada sisi administrator yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.18

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang
--------------------	---	--

	: dikecualikan kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.19

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur penerapan validasi input pada sisi server kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penerapan validasi input pada sisi server yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.20

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur penerapan mekanisme penolakan input jika terjadi kesalahan validasi kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penerapan mekanisme penolakan input jika terjadi kesalahan validasi yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.21

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur validasi positif pada seluruh input kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat validasi positif pada seluruh input yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.22

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur filter terhadap data yang tidak dipercaya kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat filter terhadap data yang tidak dipercaya yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.23

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penggunaan fitur kode dinamis kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan penggunaan fitur kode dinamis kepada yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.24

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur pelindungan terhadap akses yang mengandung konten skrip kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan terhadap akses yang mengandung konten skrip kepada Auditor yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.25

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur pelindungan dari serangan injeksi basis data kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan dari serangan injeksi basis data yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.26

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur penggunaan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan kepada Auditor
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.27

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur autentikasi data yang dienkripsi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat autentikasi data yang dienkripsi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.28

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur penerapan manajemen kunci kriptografi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penerapan manajemen kunci kriptografi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.29

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pembuatan angka acak yang menggunakan generator angka acak kriptografi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pembuatan angka acak yang menggunakan generator

	angka acak kriptografi yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.30

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur konten pesan yang ditampilkan ketika terjadi kesalahan kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan konten pesan yang ditampilkan ketika terjadi kesalahan yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.31

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur penggunaan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.32

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur pencantuman informasi yang dikecualikan dalam pencatatan log kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan pencantuman informasi yang dikecualikan dalam pencatatan log yang diakui oleh organisasi

Status Pemeriksaan	:	Sesuai / Tidak Sesuai
--------------------	---	-----------------------

KED.33

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.34

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan log aplikasi dari akses dan modifikasi yang tidak sah yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.35

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur enkripsi pada data yang disimpan untuk mencegah injeksi log kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat enkripsi pada data yang disimpan untuk mencegah injeksi log yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.36

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar kepada Auditor Keamanan SPBE
--------------------	---	--

Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.37

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur identifikasi dan penyimpanan salinan informasi yang dikecualikan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat identifikasi dan penyimpanan salinan informasi yang dikecualikan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.38

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.39

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur pertukaran, penghapusan, dan audit informasi yang dikecualikan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pertukaran, penghapusan, dan audit informasi yang dikecualikan yang diakui oleh organisasi

Status Pemeriksaan	:	Sesuai / Tidak Sesuai
--------------------	---	-----------------------

KED.40

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur mekanisme memastikan data disimpan dengan aman kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme memastikan data disimpan dengan aman yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.41

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penentuan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penentuan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.42

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur pembersihan memori setelah tidak diperlukan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pembersihan memori setelah tidak diperlukan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.43

Teknik Pemeriksaan	:	Audit membuktikan desain kontrol yang mengatur penggunaan komunikasi terenkripsi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan

	komunikasi terenkripsi yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.44

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.45

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur jenis algoritma yang digunakan dan alat pengujinya kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat jenis algoritma yang digunakan dan alat pengujinya yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.46

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.47

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur penggunaan analisis kode dalam kontrol kode berbahaya kepada Auditor Keamanan SPBE
--------------------	---	--

Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan analisis kode dalam kontrol kode berbahaya yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.48

Teknik Pemeriksaan	:	Audit menunjukkan desain kontrol yang mengatur mekanisme memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.49

Teknik Pemeriksaan	:	Audit menunjukkan desain kontrol yang mengatur izin terkait fitur atau sensor terkait privasi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan izin terkait fitur atau sensor terkait privasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.50

Teknik Pemeriksaan	:	Audit menunjukkan desain kontrol yang mengatur pelindungan integritas kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan integritas yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.51

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur mekanisme fitur pembaruan kepada Auditor
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme fitur pembaruan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.52

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pemrosesan alur logika bisnis dalam urutan langkah dan waktu yang realistik kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pemrosesan alur logika bisnis dalam urutan langkah dan waktu yang realistik yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.53

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur batasan dan validasi pada logika bisnis kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat batasan dan validasi pada logika bisnis yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.54

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pemantauan/monitor aktivitas yang tidak biasa kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pemantauan/monitor aktivitas yang tidak biasa yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.55

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur mekanisme kontrol anti
--------------------	---	--

	: otomatisasi kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme kontrol anti otomatisasi yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.56

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur mekanisme pemberian peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme pemberian peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.57

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.58

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur validasi file sesuai dengan tipe konten yang diharapkan kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan validasi file sesuai dengan tipe konten yang diharapkan yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.59

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur pelindungan terhadap metadata input dan metadata file kepada Auditor
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pelindungan terhadap metadata input dan metadata file yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.60

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur mekanisme pemindaian file yang diperoleh dari sumber yang tidak dipercaya kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme pemindaian file yang diperoleh dari sumber yang tidak dipercaya yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.61

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur mekanisme konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.62

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur mekanisme konfigurasi layanan web kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme konfigurasi layanan web yang diakui oleh organisasi

Status Pemeriksaan	:	Sesuai / Tidak Sesuai
--------------------	---	-----------------------

KED.63

Teknik Pemeriksaan	:	Audit menunjukkan desain kontrol yang mengatur mekanisme verifikasi uniform resource identifier <i>Application programming interface</i> tidak menampilkan informasi yang berpotensi sebagai celah keamanan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme verifikasi uniform resource identifier <i>Application programming interface</i> tidak menampilkan informasi yang berpotensi sebagai celah keamanan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.64

Teknik Pemeriksaan	:	Audit menunjukkan desain kontrol yang mengatur mekanisme pembuatan keputusan otorisasi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme pembuatan keputusan otorisasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.65

Teknik Pemeriksaan	:	Audit menunjukkan desain kontrol yang mengatur mekanisme menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.66

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur penggunaan validasi skema dan verifikasi sebelum menerima input kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan validasi skema dan verifikasi sebelum menerima input yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.67

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur penerapan kontrol antiotomatisasi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat pengaturan penerapan kontrol anti otomatisasi yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.68

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur konfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat konfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan yang diakui oleh organisasi
Status Pemeriksaan	:	Sesuai / Tidak Sesuai

KED.69

Teknik Pemeriksaan	:	Audit membatikan desain kontrol yang mengatur mekanisme mendokumentasi, menyalin konfigurasi, dan semua dependensi kepada Auditor Keamanan SPBE
Bukti	:	Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme mendokumentasi, menyalin konfigurasi,

	: dan semua dependensi yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.70

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur mekanisme menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat mekanisme menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.71

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur validasi integritas aset jika aset aplikasi diakses secara eksternal kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat validasi integritas aset jika aset aplikasi diakses secara eksternal yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

KED.72

Teknik Pemeriksaan	: Auditan membuktikan desain kontrol yang mengatur penggunaan respons aplikasi dan konten yang aman kepada Auditor Keamanan SPBE
Bukti	: Dokumen Standar Teknis dan Prosedur Keamanan yang memuat penggunaan respons aplikasi dan konten yang aman yang diakui oleh organisasi
Status Pemeriksaan	: Sesuai / Tidak Sesuai

D. Petunjuk Teknis Pemeriksaan Kontrol Keamanan pada Evaluasi Implementasi Kontrol

Petunjuk Teknis pemeriksaan kontrol keamanan merupakan prosedur audit yang dilakukan oleh Auditor Keamanan SPBE untuk menguji kontrol keamanan dan mendapatkan bukti kontrol keamanan telah dilaksanakan.

72 (tujuh puluh dua) Kontrol keamanan yang diperiksa pada tahap evaluasi implementasi kontrol dikodefikasi ulang menyesuaikan tahap evaluasi implementasi kontrol sehingga kodefikasinya ditambahkan EI (Evaluasi Implementasi). Contoh Kontrol keamanan pertama yang dikodefikasikan K1 menjadi KEI.1 dalam tahapan evaluasi Implementasi.

Hasil pemeriksaan tiap kontrol keamanan pada tahapan evaluasi implementasi akan menghasilkan status pemeriksaan yaitu Sesuai dengan Implementasi Desain Kontrol atau Tidak Sesuai dengan Implementasi Desain Kontrol Keamanan.

#### KEI.1

Teknik Pemeriksaan	: <ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan manajemen kata sandi untuk proses autentikasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan manajemen kata sandi untuk proses autentikasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan memperhatikan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme manajemen kata sandi yang digunakan pada proses autentikasi pada aplikasi.</li><li>2.2. Teknologi yang digunakan dalam proses autentikasi pada aplikasi.</li><li>2.3. Proses autentikasi pada aplikasi.</li><li>2.4. Kode sumber yang mengatur proses autentikasi pada aplikasi.</li></ol></li></ol>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan : <ol style="list-style-type: none"><li>1. Mekanisme manajemen kata sandi yang digunakan pada proses autentikasi pada aplikasi.</li></ol>

		<ol style="list-style-type: none"><li>2. Teknologi yang digunakan dalam proses autentikasi pada aplikasi.</li><li>3. Proses autentikasi pada aplikasi.</li><li>4. Kode sumber yang mengatur proses autentikasi pada aplikasi.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

**KEI.2**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan verifikasi kata sandi pada sisi server telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan verifikasi kata sandi pada sisi server telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme verifikasi kata sandi yang dilakukan oleh aplikasi.</li><li>2.2. Kemampuan aplikasi untuk dapat mendeteksi penggunaan kata sandi bawaan atau umum atau yang lemah (penggunaan nama software, kata umum seperti “admin”, “P@ssw0rd1”, dan lain lain).</li><li>2.3. Kode sumber yang mengatur verifikasi kata sandi pada aplikasi.</li><li>2.4. Username dan kata sandi yang tersimpan pada aplikasi.</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan :</p> <ol style="list-style-type: none"><li>1. Mekanisme verifikasi kata sandi yang dilakukan oleh aplikasi.</li><li>2. Kemampuan aplikasi untuk dapat mendeteksi penggunaan kata sandi bawaan atau umum atau yang lemah (penggunaan</li></ol>

		<p>nama software, kata umum seperti “admin”, “P@ssw0rd1”, dan lain lain).</p> <ol style="list-style-type: none"><li>3. Kode sumber yang mengatur verifikasi kata sandi pada aplikasi.</li><li>4. Username dan kata sandi yang tersimpan pada aplikasi.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.3

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Fitur pembuatan kata sandi baru ataupun reset kata sandi yang disediakan pada aplikasi.</li><li>2.2. Fitur petunjuk jumlah dan kombinasi jenis karakter kata sandi pada aplikasi saat pembuatan kata sandi baru ataupun reset kata sandi.</li><li>2.3. Mekanisme yang dilakukan aplikasi ketika terdapat kata sandi pengguna yang melebihi masa berlaku.</li><li>2.4. Kode sumber yang menyatakan pengaturan berikut:<ol style="list-style-type: none"><li>a. jumlah karakter kata sandi;</li><li>b. kombinasi jenis karakter;</li><li>c. masa berlaku kata sandi.</li></ol></li></ol></li></ol>
--------------------	---	---

Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan :</p> <ol style="list-style-type: none"><li>1. Fitur pembuatan kata sandi baru ataupun reset kata sandi yang disediakan pada aplikasi.</li><li>2. Fitur petunjuk jumlah dan kombinasi jenis karakter kata sandi pada aplikasi saat pembuatan kata sandi baru ataupun reset kata sandi.</li><li>3. Mekanisme yang dilakukan aplikasi ketika terdapat kata sandi pengguna yang melebihi masa berlaku.</li><li>4. Kode sumber yang menyatakan pengaturan berikut:<ol style="list-style-type: none"><li>a. jumlah karakter kata sandi;</li><li>b. kombinasi jenis karakter;</li><li>c. masa berlaku kata sandi.</li></ol></li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

**KEI.4**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi.</li><li>2.2. Mekanisme yang dilakukan aplikasi apabila terdapat percobaan</li></ol></li></ol>
--------------------	---	---

		<p>pemasukan kata sandi yang sudah mencapai maksimum kesalahan.</p> <p>2.3. Kode sumber yang menyatakan pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi.</p> <p>2.4. Kode sumber yang menyatakan mekanisme yang dilakukan aplikasi apabila terdapat percobaan pemasukan kata sandi yang sudah mencapai maksimum kesalahan.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan :</p> <ol style="list-style-type: none"><li>1. Pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi.</li><li>2. Mekanisme yang dilakukan aplikasi apabila terdapat percobaan pemasukan kata sandi yang sudah mencapai maksimum kesalahan.</li><li>3. Kode sumber yang menyatakan pengaturan jumlah maksimum kesalahan dalam pemasukan kata sandi.</li><li>4. Kode sumber yang menyatakan mekanisme yang dilakukan aplikasi apabila terdapat percobaan pemasukan kata sandi yang sudah mencapai maksimum kesalahan.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.5

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan mekanisme pemulihan kata sandi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan mekanisme pemulihan kata sandi telah diterapkan pada aplikasi, Auditor</li></ol>
--------------------	---	---

	<p>Keamanan SPBE memperhatikan hal-hal sebagai berikut:</p> <ol style="list-style-type: none"><li>2.1. Mekanisme pemulihan kata sandi yang disediakan pada aplikasi.</li><li>2.2. Media yang digunakan aplikasi untuk memberikan notifikasi kepada pengguna ketika melakukan pemulihan kata sandi</li><li>2.3. Isi notifikasi yang dikirimkan kepada pengguna ketika melakukan pemulihan kata sandi.</li><li>2.4. Kode sumber yang menyatakan mekanisme pemulihan kata sandi pada aplikasi.</li></ol>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan : <ol style="list-style-type: none"><li>1. Mekanisme pemulihan kata sandi yang disediakan pada aplikasi.</li><li>2. Media yang digunakan aplikasi untuk memberikan notifikasi kepada pengguna ketika melakukan pemulihan kata sandi.</li><li>3. Isi notifikasi yang dikirimkan kepada pengguna ketika melakukan pemulihan kata sandi.</li><li>4. Kode sumber yang menyatakan mekanisme pemulihan kata sandi pada aplikasi.</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.6

Teknik Pemeriksaan	: <ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan mekanisme kriptografi untuk menjaga kerahasiaan kata sandi yang disimpan telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan mekanisme kriptografi untuk menjaga kerahasiaan</li></ol>
--------------------	--

		<p>kata sandi yang disimpan telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:</p> <ol style="list-style-type: none"> <li>2.1. Pengamanan password pada penyimpanan di <i>database</i> dengan cara melakukan <i>hashing</i>.</li> <li>2.2. Algoritma yang digunakan.</li> <li>2.3. Kode sumber pengamanan password saat penyimpanan di <i>database</i>.</li> </ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan :</p> <ol style="list-style-type: none"> <li>1. Atribut password pada tabel pengguna di database untuk memastikan penyimpanan password secara plaintext atau tidak.</li> <li>2. Kode sumber yang menunjukkan algoritma dalam proses hashing.</li> <li>3. Kode sumber pengamanan password saat penyimpanan di <i>database</i>.</li> </ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.7

Teknik Pemeriksaan	:	<ol style="list-style-type: none"> <li>1. Auditor Keamanan SPBE memastikan penggunaan jalur komunikasi yang diamankan untuk proses autentikasi telah diterapkan pada aplikasi.</li> <li>2. Dalam hal memastikan penggunaan jalur komunikasi yang diamankan untuk proses autentikasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut: <ol style="list-style-type: none"> <li>2.1. Protokol keamanan komunikasi yang digunakan</li> <li>2.2. Sertifikat SSL/TLS yang digunakan</li> <li>2.3. Cakupan penerapan SSL/TLS</li> <li>2.4. Konfigurasi penerapan SSL/TLS</li> </ol> </li> </ol>
--------------------	---	---

Bukti	:	Gambar/Video/Dokumen yang memperlihatkan : 1. Protokol keamanan komunikasi yang digunakan 2. Sertifikat SSL/TLS yang digunakan 3. Cakupan penerapan SSL/TLS 4. Konfigurasi penerapan SSL/TLS
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.8

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE memastikan penggunaan pengendali sesi untuk proses manajemen sesi telah diterapkan pada aplikasi. 2. Dalam hal memastikan penggunaan pengendali sesi untuk proses manajemen sesi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut: 2.1. Sesi-cookie yang terbentuk ketika mengakses aplikasi 2.2. Pihak/aplikasi/framework yang membuat dan mengelola sesi
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan : 1. Sesi-cookie pada aplikasi 2. Kode sumber yang menunjukkan pembuatan sesi
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.9

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE memastikan penggunaan pengendali sesi yang
--------------------	---	---

	<p>disediakan oleh kerangka kerja aplikasi telah diterapkan pada aplikasi.</p> <p>2. Dalam hal memastikan penggunaan pengendali sesi yang disediakan oleh kerangka kerja aplikasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:</p> <p>2.1. Header response HTTP untuk melihat penggunaan header Set-Cookie. Cookie sering digunakan untuk menyimpan informasi sesi.</p> <p>2.2. Kode sumber HTML dan JavaScript halaman web untuk melihat penggunaan skrip JavaScript yang menangani sesi, atau elemen HTML yang menyimpan informasi sesi.</p> <p>2.3. Indikator Session ID atau Token, dengan meninjau kode sumber halaman web untuk mencari pencantuman session ID atau token. Ini bisa terlihat dalam URL, form data, atau di dalam JavaScript.</p> <p>2.4. Kode sumber yang menunjukkan mekanisme pengaturan sesi pada aplikasi</p>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan :

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.10

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme dari generate token session.</li><li>2.2. Algoritma yang digunakan dalam generate token sesi</li><li>2.3. Mekanisme token yang dihasil sudah acak</li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan kode sumber berisi mekanisme generate token session yang acak
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.11

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan kondisi dan jangka waktu habis sesi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan kondisi dan jangka waktu habis sesi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:</li></ol>
--------------------	---	--

		<ol style="list-style-type: none"><li>2.1. Kondisi aplikasi yang dapat otomatis logout atau tidak, ketika di rentang waktu tertentu tidak terdapat aktivitas (idle).</li><li>2.2. Kondisi manajemen batas waktu dan kadaluarsa dari sesi diatur ataupun diberlakukan pada sisi server bukan client atau pengguna.</li><li>2.3. Kondisi sesi yang telah habis batas waktu dan kadaluarsa nya telah dihancurkan di sisi server.</li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan :</p> <ol style="list-style-type: none"><li>1. Aktivitas login kedalam aplikasi yang memaksa auditan Logout secara otomatis.</li><li>2. Informasi batas waktu sebuah sesi.</li><li>3. Informasi terkait penghancuran sesi yang telah habis batas waktunya.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.12

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan validasi dan pencantuman session ID telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan validasi dan pencantuman session ID telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 9, Kontrol 10, Kontrol 11, dan Kontrol 13.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan atribut pada session ID
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.13

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentifikasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentifikasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Penggunaan Attribute secure ketika dikirimkan melalui jalur pengiriman yang aman (seperti HTTPS).</li><li>2.2. Penggunaan Atribut "HttpOnly" untuk mencegah penggunaan cookie yang terpapar.</li><li>2.3. Penggunaan Atribut "Domain", "path", &amp; "SameSite" yang dikonfigurasi dengan memadai.</li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan atribut: <ol style="list-style-type: none"><li>1. "Secure"</li><li>2. "HttpOnly"</li><li>3. "Strict-Transport-Security"</li><li>4. "Domain"</li><li>5. "Path"</li><li>6. "SameSite"</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.14

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pelindungan terhadap duplikasi dan mekanisme</li></ol>
--------------------	---	--

		<p>persetujuan pengguna telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan bahwa aplikasi telah melakukan pembangkitan session baru saat pengguna login ke aplikasi, sehingga dapat menjamin tidak adanya duplikasi pengguna yang login ke aplikasi.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan :</p> <ol style="list-style-type: none"><li>1. Sesi-cookie pada interface aplikasi</li><li>2. Kode sumber yang mengatur sesi</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.15

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan otorisasi pengguna untuk membatasi kontrol akses telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan otorisasi pengguna untuk membatasi kontrol akses telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Dokumentasi yang mendefinisikan aturan untuk pengguna pada aplikasi.</li><li>2.2. Mekanisme pemberian akses telah mempertimbangkan prinsip "least privilege", dimana pengguna hanya diberikan otorisasi sesuai dengan peran, fungsi, dan kewenangannya terhadap fungsi, url, pengaturan, dan sumber daya lainnya pada aplikasi.</li><li>2.3. Pengguna akhir yang tidak memiliki otorisasi, apakah dapat melakukan manipulasi terhadap semua data atau</li></ol></li></ol>
--------------------	---	--

		<p>informasi (seperti parameter user atau user id, account, groupid menu item, img atau image, file, dan lain-lain) yang digunakan pada proses kontrol akses.</p> <p>2.4. Jika menggunakan authentication-server (middleware), terdapat penjelasan mekanisme otorisasinya.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"> <li>1. Dokumentasi terkait aturan kontrol akses pada aplikasi</li> <li>2. Fitur atau menu dalam rangka pemberian otorisasi pada pengguna tertentu</li> <li>3. Dokumen pengajuan akses</li> </ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.16

Teknik Pemeriksaan	:	<p>Auditor Keamanan SPBE memastikan pengaturan peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi telah diterapkan pada aplikasi. Dalam hal memastikan hal tersebut, auditor Keamanan SPBE melakukan pemeriksaan terhadap potongan kode dan fitur yang mengindikasikan mekanisme Anti-CSRF atau Anti-Otomatisasi pada aplikasi.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan interface aplikasi dan juga potongan kode sumber yang mengindikasikan atau menunjukkan penerapan dari anti-CSRF dan anti-automation.</p>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.17

Teknik Pemeriksaan	: <ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan antarmuka pada sisi administrator telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan antarmuka pada sisi administrator telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Halaman antarmuka yang hanya dapat diakses oleh administrator.</li><li>2.2. Konfigurasi file robots.txt</li><li>2.3. Penggunaan kata sandi untuk halaman administrator.</li><li>2.4. Penggunaan parameter yang mengindikasikan Role atau peran dari pengguna misalkan user atau user id, account, group id pada URL.</li><li>2.5. Pembatasan akses terhadap halaman administrator.</li></ol></li></ol>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Halaman antarmuka yang hanya dapat diakses oleh administrator.</li><li>2. Konfigurasi file robots.txt</li><li>3. Penggunaan kata sandi untuk halaman administrator.</li><li>4. Penggunaan parameter yang mengindikasikan Role atau peran dari pengguna misalkan user atau user id, account, groupid pada URL.</li><li>5. Pembatasan akses terhadap halaman administrator.</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.18

Teknik Pemeriksaan	: <ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan mekanisme verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan mekanisme verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Penerapan token CSRF pada header dari http request ketika melakukan permintaan pada aplikasi.</li><li>2.2. Penerapan token CSRF yang selalu baru berbeda saat pengiriman dan submit Request.</li></ol></li></ol>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Cara melakukan akses ke halaman yang dikecualikan seperti antarmuka antar administrator, atau bukti yang mengindikasikan terdapatnya CSRF-Token pada header dari permintaan tersebut.</li><li>2. Perbedaan antar token csrf pada setiap kali dilakukan http request</li><li>3. Hasil wawancara dengan auditan untuk mengetahui ketertautan CSRF-Token dengan waktu</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.19

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan fungsi validasi input pada sisi server telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan fungsi validasi input pada sisi server telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Validasi inputan yang telah diterapkan.</li><li>2.2. Kode sumber Aplikasi terkait penerapan proses encode atau mengganti dengan karakter unicode terhadap inputan penggunaan karakter khusus HTML. Adapun inputan tersebut antara lain:<ol style="list-style-type: none"><li>a. &gt; (greater than).</li><li>b. &lt; (less than).</li><li>c. &amp; (ampersand).</li><li>d. ' (apostrophe or single quote).</li><li>e. " (double quote).</li></ol></li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan pengaturan validasi input pada kode sumber aplikasi
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.20

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan mekanisme penolakan input jika terjadi kesalahan validasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan mekanisme penolakan input jika terjadi kesalahan validasi telah diterapkan pada aplikasi,</li></ol>
--------------------	---	---

		<p>Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:</p> <ol style="list-style-type: none"><li>2.1. Validasi inputan yang telah diterapkan.</li><li>2.2. Mekanisme proses yang diimplementasikan jika input yang dimasukan user tidak berhasil melewati proses validasi.</li><li>2.3. Mekanisme penerapan keamanan untuk mencegah injeksi di sisi URL.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan mekanisme penolakan input jika terjadi kesalahan validasi
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.21

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan mekanisme validasi positif pada seluruh input telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan mekanisme validasi positif pada seluruh input telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme yang disematkan pada kode sumber aplikasi, yang bertugas melakukan penyaringan terhadap tag atau atribut html yang diperbolehkan.</li><li>2.2. Tools/Software seperti Web Application Firewall yang digunakan.</li><li>2.3. Dokumen ataupun konfigurasi yang mengindikasikan pendefinisian daftar putih (white listing), terhadap tag atau</li></ol></li></ol>
--------------------	---	--

		<p>atribut html yang diperbolehkan (HTML yang aman).</p> <p>2.4. Catatan atau daftar terkait inputan yang tidak sesuai (terblokir) dengan daftar putih (white listing) yang telah didefinisikan.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Kode sumber yang mengindikasikan proses penyaringan tag atau atribut html yang diperbolehkan.</li><li>2. Penggunaan tools/Software seperti Web Application Firewall.</li><li>3. Konfigurasi terkait daftar putih (white listing), terhadap tag atau atribut html yang diperbolehkan (HTML yang aman).</li><li>4. Catatan atau daftar terkait inputan yang tidak sesuai (terblokir) dengan daftar putih (white listing) yang telah didefinisikan.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.22

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan filter terhadap data yang tidak dipercaya telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan filter terhadap data yang tidak dipercaya telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 19, Kontrol 20, dan Kontrol 21.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan penerapan filter terhadap data yang tidak dipercaya.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.23

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mengidentifikasi fitur kode dinamis telah diterapkan pada aplikasi.</li><li>2. Dalam hal mengidentifikasi penggunaan fitur kode dinamis yang diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap entry point (seperti text field di form), apakah ada fungsi khusus yang disematkan pada source code aplikasi (seperti htmlentities, js escape, dan lain – lain).</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan sumber kode yang bertugas melakukan proses <i>encoding</i> atau mengganti dengan karakter <i>unicode</i> terhadap input pengguna yang tidak sesuai dengan aturan yang ditetapkan.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.24

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Dalam hal memastikan pelindungan terhadap akses yang mengandung konten skrip telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 19.</li><li>2. Auditor Keamanan SPBE memastikan terdapat kontrol tambahan yang digunakan untuk melakukan pelindungan terhadap akses yang mengandung konten skrip.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan pelindungan terhadap akses yang mengandung konten skrip telah diterapkan.

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.25

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Dalam hal memastikan pelindungan dari serangan injeksi basis data telah diterapkan pada aplikasi, Auditor memperhatikan teknik pengujian pada Kontrol 19.</li><li>2. Auditor Keamanan SPBE memastikan terdapat kontrol tambahan yang digunakan untuk melakukan pelindungan dari serangan injeksi basis data.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan pelindungan dari serangan injeksi basis data telah diterapkan.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.26

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan telah diterapkan pada aplikasi.</li><li>2. Dalam memastikan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan memperhatikan terhadap hal-hal sebagai berikut:</li></ol>
--------------------	---	---

	<p>2.1. Pengujian dilakukan dengan melakukan pemeriksaan tidak terbatas pada:</p> <ul style="list-style-type: none"><li>a. Data pribadi yang bersifat spesifik dan umum</li><li>b. Kredensial yang digunakan aplikasi dan sistem pendukung</li><li>c. Informasi yang dipersyaratkan oleh peraturan perundang-undangan tertentu, baik selama data dimasukkan (entry point), disimpan di dalam database, diolah, ataupun hingga data tersebut dihancurkan.</li></ul> <p>2.2. Auditor Keamanan SPBE memastikan klasifikasi data dan informasi yang sensitif di dalam aplikasi, sehingga perlu diamankan dengan kriptografi. Klasifikasi data dan informasi yang sensitif harus merujuk pada pengaturan seperti pelindungan data pribadi, keterbukaan informasi publik, ataupun kebijakan organisasi dalam memproses, menyimpan, dan mentransmisikan data dan informasi.</p> <p>2.3. Auditor Keamanan SPBE memastikan jenis algoritma kriptografi dan mode enkripsi yang digunakan di dalam aplikasi untuk mengamankan data dan informasi berdasarkan klasifikasinya.</p> <p>2.4. Auditor Keamanan SPBE memastikan protokol kriptografi berjalan dalam setiap modul kriptografi yang digunakan di dalam aplikasi.</p>
--	---

		<p>2.5. Auditor Keamanan SPBE memastikan aplikasi mengimplementasikan kriptografi yang terbarukan dan berdasarkan rekomendasi pengaturan dan praktik terbaik.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan sumber kode atau konfigurasi yang menunjukkan:</p> <ol style="list-style-type: none"><li>1. Klasifikasi data dan informasi sensitif</li><li>2. Penggunaan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.27

Teknik Pemeriksaan	:	<p>1. Auditor Keamanan SPBE memastikan autentikasi data yang dienkripsi telah diterapkan pada aplikasi.</p> <p>2. Dalam memastikan autentikasi data yang dienkripsi telah diterapkan pada aplikasi, Auditor melakukan memperhatikan hal-hal sebagai berikut:</p> <p>2.1. Auditor Keamanan SPBE memastikan klasifikasi data dan informasi yang sensitif di dalam aplikasi sehingga perlu diamankan dengan kriptografi. Klasifikasi data dan informasi yang sensitif harus merujuk pada pengaturan seperti pelindungan data pribadi, keterbukaan informasi publik, ataupun kebijakan organisasi dalam memproses, menyimpan, dan mentransmisikan data dan informasi.</p>
--------------------	---	---

	<p>2.2. Auditor Keamanan SPBE memastikan jenis algoritma kriptografi dan mode enkripsi yang digunakan di dalam aplikasi untuk mengamankan data dan informasi berdasarkan klasifikasinya.</p> <p>2.3. Auditor Keamanan SPBE memastikan protokol kriptografi berjalan dalam setiap modul kriptografi yang digunakan di dalam aplikasi.</p> <p>2.4. Auditor Keamanan SPBE memastikan aplikasi mengimplementasikan kriptografi yang terbarukan dan berdasarkan rekomendasi pengaturan dan praktik terbaik.</p>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan sumber kode atau konfigurasi yang menunjukkan: <ol style="list-style-type: none"><li>1. Klasifikasi data dan informasi sensitif</li><li>2. Penggunaan algoritma kriptografi, mode enkripsi</li><li>3. Protokol kriptografi yang berjalan dalam modul kriptografi</li><li>4. Implementasi kriptografi yang terbarukan</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.28

Teknik Pemeriksaan	: Auditor Keamanan SPBE memastikan manajemen kunci kriptografi telah diterapkan pada aplikasi
Bukti	: Gambar/Video/Dokumen yang memperlihatkan sumber kode atau konfigurasi yang menunjukkan penerapan manajemen kunci kriptografi

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.29

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan mendapat penjelasan tentang tools/algoritma/library yang digunakan aplikasi target audit dalam generate angka acak kriptografi</li><li>2. Auditor Keamanan SPBE memastikan mendapat penjelasan tentang keterjaminan keamanan dan tidak mudah ditebaknya output yang dihasilkan dari tools/algoritma/library yang digunakan untuk generate angka acak kriptografi</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan sumber kode atau konfigurasi yang menunjukan pembuatan angka acak yang menggunakan generator angka acak kriptografi
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.30

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan konten pesan yang ditampilkan ketika terjadi kesalahan telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan mekanisme pengaturan konten pesan yang ditampilkan ketika terjadi kesalahan telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap kode sumber aplikasi, untuk memastikan bahwa konten pesan yang akan ditampilkan tidak memberikan atau mengindikasikan</li></ol>
--------------------	---	--

		informasi yang bersifat sensitif atau memberikan petunjuk untuk penyerang.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan halaman aplikasi berisi pesan yang ditampilkan jika terjadi error.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.31

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan mekanisme pengaturan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Library/package/pihak yang digunakan sebagai exception handler</li><li>2.2. Mekanisme cara menangani error yang sudah berhasil diidentifikasi/terprediksi oleh tim pengembang aplikasi.</li><li>2.3. Mekanisme cara menangani error yang tidak terdefinisi/terprediksi oleh tim pengembang aplikasi.</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Kode sumber Library/package sebagai exception handler</li></ol>

	<ol style="list-style-type: none"><li>2. Kode sumber penanganan error yang diidentifikasi/terprediksi</li><li>3. Kode sumber mekanisme cara menangani error yang tidak terdefinisi/terprediksi</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.32

Teknik Pemeriksaan	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan untuk tidak mencantumkan informasi yang dikecualikan dalam pencatatan log telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan untuk tidak mencantumkan informasi yang dikecualikan dalam pencatatan log, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Ada atau tidaknya informasi yang dikecualikan dalam pencatatan log pada sisi user maupun sisi server.</li><li>2.2. Pencatatan log aplikasi berupa log otentikasi, log kegagalan validasi input, log aktivitas user di aplikasi dan kegagalan akses kontrol.</li><li>2.3. Pencatatan log saat terjadi error.</li></ol></li></ol>
Bukti	<p>: Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Ada atau tidaknya informasi yang dikecualikan dalam pencatatan log</li><li>2. Pencatatan log aplikasi berupa log otentikasi, log kegagalan validasi input, log aktivitas user di aplikasi dan kegagalan akses kontrol</li><li>3. Pencatatan log saat terjadi error</li></ol>

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.33

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Cakupan log yang dicatat</li><li>2.2. Masa retensi log</li><li>2.3. Daftar insiden yang pernah terjadi pada aplikasi</li><li>2.4. Kebermanfaatan log aplikasi dalam penyelesaian insiden yang terjadi melalui investigasi</li><li>2.5. Auditor Keamanan SPBE melakukan pemeriksaan apakah cakupan log yang dicatat, sudah cukup untuk mendukung upaya penyelidikan ketika terjadi insiden</li><li>2.6. Dalam hal penilaian dalam pemeriksaan, auditor Keamanan SPBE dapat menggunakan standar log dari organisasi audit atau dari berbagai standar dan atau best practice terkait log</li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan:

	<ol style="list-style-type: none"><li>1. Cakupan log yang dicatat</li><li>2. Masa retensi log</li><li>3. Daftar Insiden yang pernah terjadi pada aplikasi</li><li>4. Kebermanfaatan log</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.34

Teknik Pemeriksaan	<p>:</p> <ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan pelindungan log aplikasi dari akses dan modifikasi yang tidak sah telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan pelindungan log aplikasi dari akses dan modifikasi yang tidak sah telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:</li><ol style="list-style-type: none"><li>2.1. Mekanisme keamanan dengan tujuan untuk menjamin keutuhan dari log aplikasi.</li><li>2.2. Pihak-pihak yang bisa akses ke log, dan role aksesnya.</li><li>2.3. Mekanisme monitoring seluruh log pada sistem yang dilakukan secara terpusat atau tidak.</li><li>2.4. Auditor Keamanan SPBE melakukan pemeriksaan apakah kondisi perlindungan log aplikasi dapat melindungi log dari modifikasi tidak sah. Auditor Keamanan SPBE dapat menggunakan standar log dari Organisasi Audit atau dari berbagai standar dan atau best practice terkait log.</li></ol></ol>
--------------------	--

Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: 1. Mekanisme perlindungan terhadap keutuhan log. 2. Pengaturan role akses ke log. 3. Mekanisme monitoring log.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.35

Teknik Pemeriksaan	:	Auditor Keamanan SPBE memastikan penerapan mekanisme enkripsi pada data sebelum dicatat di log telah diterapkan pada aplikasi.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan penerapan mekanisme encode pada data sebelum dicatat di log.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.36

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE memastikan pengaturan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar telah diterapkan pada aplikasi. 2. Dalam hal memastikan pengaturan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap sinkronisasi sumber waktu pada beberapa server dari sistem aplikasi target audit.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan sinkronisasi sumber waktu pada beberapa server

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.37

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan identifikasi dan penyimpanan salinan informasi yang dikecualikan telah dilakukan terhadap aplikasi, dan sudah sesuai dengan mekanisme yang ditetapkan dalam peraturan instansi Audit dan mengikuti best practice.</li><li>2. Dalam hal memastikan identifikasi dan penyimpanan salinan informasi yang dikecualikan telah dilakukan terhadap aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Identifikasi daftar informasi yang dikecualikan/daftar informasi rahasia/sensitif pada aplikasi</li><li>2.2. Mekanisme penyimpanan dan pengamanan informasi yang dikecualikan</li><li>2.3. Mekanisme penyimpanan dan pengamanan salinan informasi yang dikecualikan</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Daftar informasi yang dikecualikan</li><li>2. Penyimpanan dan pengamanan informasi yang dikecualikan</li><li>3. Penyimpanan dan pengamanan salinan informasi yang dikecualikan</li><li>4. Hasil pemeriksaan penyimpanan informasi dibandingkan dengan peraturan yang ditetapkan</li></ol>

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.38

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme penyimpanan dan pengamanan informasi dikecualikan yang disimpan secara temporary</li><li>2.2. Direktori yang diperkirakan merupakan direktori temporary</li><li>2.3. Mekanisme akses kontrol/perlindungan akses dari data temporary</li><li>2.4. Mekanisme penyimpanan informasi/file yang dilakukan di sisi client</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Penyimpanan dan pengamanan informasi dikecualikan yang disimpan secara temporary</li><li>2. Direktori temporary</li><li>3. Perlindungan akses dari data temporary</li><li>4. Penyimpanan informasi/file yang dilakukan di sisi client</li></ol>

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.39

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pertukaran, penghapusan, dan audit informasi yang dikecualikan telah dilakukan pada Aplikasi.</li><li>2. Dalam hal memastikan pertukaran, penghapusan, dan audit informasi yang dikecualikan telah dilakukan pada Aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme pertukaran informasi yang dikecualikan/sensitif pada aplikasi.</li><li>2.2. Mekanisme penghapusan informasi yang dikecualikan/sensitif pada aplikasi.</li><li>2.3. Audit terhadap informasi yang dikecualikan/sensitif</li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Pertukaran informasi yang dikecualikan</li><li>2. Penghapusan informasi yang dikecualikan</li><li>3. Audit terhadap informasi yang dikecualikan</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.40

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan data disimpan dengan aman telah diterapkan pada aplikasi.</li></ol>
--------------------	---	---

	<p>2. Dalam hal memastikan data disimpan dengan aman telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:</p> <ol style="list-style-type: none"><li>2.1. Mekanisme penyimpanan dan pengamanan data/informasi pada Aplikasi</li><li>2.2. Mekanisme back-up seluruh data (seperti file, Database, konfigurasi) terkait sistem dilakukan secara aman untuk menjamin ketersediaan data/app/sistem</li><li>2.3. Pengaturan yang mensyaratkan uji coba pemulihan data secara berkala</li></ol>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Penyimpanan dan pengamanan data/informasi pada Aplikasi</li><li>2. Mekanisme backup seluruh data</li><li>3. Lokasi backup data</li><li>4. Laporan uji coba pemulihan data secara berkala</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.41

Teknik Pemeriksaan	: Auditor Keamanan SPBE memastikan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna telah ditentukan pada aplikasi. Dalam hal memastikan, Auditor Keamanan SPBE meminta penjelasan terkait hal tersebut.
Bukti	: Gambar/Video/Dokumen yang memperlihatkan fitur untuk menghapus dan melakukan eksport data

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.42

Teknik Pemeriksaan	:	Auditor Keamanan SPBE memastikan pembersihan memori setelah tidak diperlukan telah diterapkan pada Aplikasi. Dalam hal memastikan, Auditor Keamanan SPBE meminta penjelasan terkait hal tersebut.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan mekanisme pembersihan data pada memori setelah tidak diperlukan
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.43

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan komunikasi terenkripsi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan komunikasi terenkripsi telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap penggunaan protokol TLS pada seluruh koneksi masuk dan keluar, termasuk port manajemen, autentikasi, <i>Application programming interface</i>, database, dan komponen lainnya.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan penggunaan protokol TLS pada seluruh koneksi masuk dan keluar, termasuk port manajemen, autentikasi, <i>Application programming interface</i> , database, dan komponen lainnya.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.44

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan komunikasi terenkripsi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan komunikasi terenkripsi telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap penggunaan protokol TLS pada seluruh koneksi masuk dan keluar, termasuk port manajemen, autentikasi, <i>Application programming interface</i>, database, dan komponen lainnya.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan penggunaan protokol TLS pada seluruh koneksi masuk dan keluar, termasuk port manajemen, autentikasi, <i>Application programming interface</i> , database, dan komponen lainnya.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.45

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan jenis algoritma yang digunakan dan alat pengujinya telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan jenis algoritma yang digunakan dan alat pengujinya telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap versi TLS yang digunakan dan jenis algoritma yang digunakan.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan versi TLS yang digunakan dan jenis algoritma yang digunakan.

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.46

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan sertifikat TLS, yaitu:<ol style="list-style-type: none"><li>2.1. Domain yang tercakup dalam penggunaan TLS</li><li>2.2. Periode validitas sertifikat</li><li>2.3. Organisasi yang mengeluarkan sertifikat</li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Domain yang tercakup dalam penggunaan TLS</li><li>2. Periode validitas sertifikat</li><li>3. Organisasi yang mengeluarkan sertifikat</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.47

Teknik Pemeriksaan	:	Auditor Keamanan SPBE memastikan dalam pengembangan dan pengelolaan Aplikasi telah menggunakan analisis kode untuk menghindari kode berbahaya. Dalam hal memastikan, Auditor Keamanan SPBE memperhatikan bahwa terdapat Tools untuk
--------------------	---	---

		analisis kode, yang dapat mendeteksi kode yang berpotensi malicious.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan mekanisme dan hasil analisis kode sumber
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

**KEI.48**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Pengujian dapat dilakukan dengan cara Auditor Keamanan SPBE memastikan mendapatkan penjelasan terkait mekanisme pengecekan secara otomatis terhadap kode sumber seperti library atau dependency atau container atau dll tidak mengandung kode berbahaya.</li><li>2. Pengujian secara manual dapat dilakukan dengan cara auditor Keamanan SPBE memeriksa kode sumber seperti library atau dependency atau container atau dll tidak mengandung kode berbahaya berdasarkan keterbaruan versi serta mencocokan dengan CVE.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan mekanisme pengecekan kode sumber aplikasi dan pustaka supaya tidak mengandung kode berbahaya.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

**KEI.49**

Teknik Pemeriksaan	:	Auditor Keamanan SPBE memastikan Mengatur izin terkait fitur atau sensor terkait privasi telah diterapkan pada aplikasi. Dalam hal memastikan Auditor Keamanan SPBE memperhatikan bahwa aplikasi tidak akan
--------------------	---	---

	meminta izin kepada fitur atau akses yang tidak diperlukan/berlebihan kepada sensor seperti kamera, microphone atau lokasi, dan seterusnya.
Bukti	: Gambar/Video/Dokumen yang memperlihatkan pengaturan izin terkait fitur atau sensor terkait privasi
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.50

Teknik Pemeriksaan	: Auditor Keamanan SPBE memastikan pengaturan pelindungan integritas telah diterapkan pada aplikasi. Dalam hal memastikan, Auditor Keamanan SPBE memperhatikan untuk mendapatkan penjelasan terkait mekanisme keamanan dengan tujuan menjamin keutuhan dari file aplikasi, antara lain File Integrity Monitoring.
Bukti	: Gambar/Video/Dokumen yang memperlihatkan pengaturan izin terkait File Integrity Monitoring
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.51

Teknik Pemeriksaan	: Auditor Keamanan SPBE memastikan pengaturan mekanisme fitur pembaruan telah diterapkan pada aplikasi. Dalam hal memastikan hal tersebut, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut: 1. Terdapat mekanisme pembaruan (update dan upgrade aplikasi) untuk memastikan pembaruan dilakukan dengan aman. 2. Terdapat mekanisme pembaruan yang diperoleh melalui saluran aman dan
--------------------	---

		ditandatangani secara digital, apabila dilakukan secara otomatis.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Mekanisme pembaruan fitur aplikasi</li><li>2. Mekanisme pembaruan yang diperoleh melalui saluran aman dan ditandatangani secara digital, apabila dilakukan secara otomatis.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

**KEI.52**

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE memastikan pemrosesan alur logika bisnis dalam urutan langkah dan waktu yang realistik telah diterapkan pada aplikasi. 2. Dalam hal memastikan alur logika bisnis dalam urutan langkah dan waktu yang realistik, Auditor Keamanan SPBE meminta auditan untuk ditunjukkan secara sampling alur Proses Bisnis utama dari awal sampai akhir sesuai dengan urutan langkah dan waktu yang realistik pada desain kontrol.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan alur Proses Bisnis utama dari awal sampai akhir sesuai dengan urutan langkah dan waktu yang realistik pada desain kontrol.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.53

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan logika bisnis dengan batasan dan validasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan logika bisnis dengan batasan dan validasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE meminta auditan untuk ditunjukkan secara sampling alur Proses Bisnis utama dari awal sampai akhir sesuai dengan hak akses yang diberikan untuk role tertentu pada desain kontrol.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan bahwa alur Proses Bisnis utama dari awal sampai akhir sesuai dengan hak akses yang diberikan untuk role tertentu pada desain kontrol.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.54

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan proses monitor aktivitas yang tidak biasa telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan pelindungan log aplikasi dari akses dan modifikasi yang tidak sah telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme monitoring terhadap insiden atau aktivitas yang tidak biasa dari perspektif logika bisnis, seperti contoh percobaan aksi yang tidak biasa dilakukan user biasanya. Hal yang dapat diperiksa antara lain:</li></ol></li></ol>
--------------------	---	---

		<ul style="list-style-type: none"><li>a. Sistem monitoring log aktivitas aplikasi.</li><li>b. Sistem monitoring pada perimeter keamanan, seperti Firewall, dll.</li><li>2.2. Konfigurasi yang diterapkan pada dashboard monitoring, diklasifikasikan berdasarkan kategori dampak aktivitasnya terhadap aplikasi.</li><li>2.3. Kode sumber aplikasi sistem monitoring aktivitas yang digunakan.</li></ul>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ul style="list-style-type: none"><li>1. Mekanisme monitoring terhadap insiden atau aktivitas yang tidak biasa dari perspektif logika bisnis, seperti:<ul style="list-style-type: none"><li>a. Sistem monitoring log aktivitas aplikasi.</li><li>b. Sistem monitoring pada perimeter keamanan, seperti Firewall, dll.</li></ul></li><li>2. Konfigurasi yang diterapkan pada dashboard monitoring, diklasifikasikan berdasarkan kategori dampak aktivitasnya terhadap aplikasi.</li><li>3. Kode sumber aplikasi sistem monitoring aktivitas yang digunakan.</li></ul>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.55

Teknik Pemeriksaan	:	<ul style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan kontrol anti otomatisasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan kontrol anti otomatisasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE dapat melakukan pemeriksaan terhadap pengaturan kontrol</li></ul>
--------------------	---	---

		anti-automasi sebagai langkah pengamanan dari serangan request query terhadap data, exfiltrasi data yang masif, DDOS, dan file uploads, beserta kode sumber yang menunjukkan pengaturan tersebut.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan pengaturan kontrol anti-automasi beserta kode sumber yang menunjukkan pengaturan tersebut.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.56

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pemberian peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pemberian peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme notifikasi hasil monitoring terhadap insiden atau aktivitas yang tidak biasa dari perspektif logika bisnis, seperti percobaan aksi yang tidak biasa dilakukan user biasanya. Hal yang dapat diperiksa antara lain:<ol style="list-style-type: none"><li>a. Bentuk notifikasi dari sistem monitoring log aktivitas aplikasi.</li><li>b. Bentuk notifikasi dari sistem monitoring pada perimeter keamanan, seperti Firewall, dll.</li></ol></li></ol></li></ol>
--------------------	---	---

		<p>2.2. Konfigurasi yang diterapkan pada pemberian notifikasi hasil monitoring.</p> <p>2.3. Kode sumber aplikasi sistem monitoring aktivitas yang menunjukkan mekanisme pemberian peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <p>1. Mekanisme notifikasi hasil monitoring terhadap insiden atau aktivitas yang tidak biasa dari perspektif logika bisnis, seperti percobaan aksi yang tidak biasa dilakukan user biasanya. Hal yang dapat diperiksa antara lain:</p> <ol style="list-style-type: none"><li>a. Bentuk notifikasi dari sistem monitoring log aktivitas aplikasi.</li><li>b. Bentuk notifikasi dari sistem monitoring pada perimeter keamanan, seperti Firewall, dll.</li></ol> <p>2. Konfigurasi yang diterapkan pada pemberian notifikasi hasil monitoring.</p> <p>3. Kode sumber aplikasi sistem monitoring aktivitas yang menunjukkan mekanisme pemberian peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.</p>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.57

Teknik Pemeriksaan	:	<p>1. Auditor Keamanan SPBE memastikan pengaturan jumlah file untuk pengguna dan kuota ukuran file yang diunggah telah diterapkan pada aplikasi.</p>
--------------------	---	--

	<p>2. Dalam hal memastikan pengaturan jumlah file untuk pengguna dan kuota ukuran file yang diunggah telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:</p> <ol style="list-style-type: none"><li>2.1. Fitur unggah file pada aplikasi</li><li>2.2. Pembatasan jumlah file pada fitur unggah</li><li>2.3. Pembatasan ukuran file pada fitur unggah</li><li>2.4. Kode sumber yang menunjukkan pembatasan jumlah dan ukuran file yang diunggah</li></ol>
Bukti	: Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Fitur unggah file pada aplikasi</li><li>2. Pembatasan jumlah file pada fitur unggah</li><li>3. Pembatasan ukuran file pada fitur unggah</li><li>4. Kode sumber yang menunjukkan pembatasan jumlah dan ukuran file yang diunggah</li></ol>
Status Pemeriksaan	: Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.58

Teknik Pemeriksaan	: <ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pengaturan jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pengaturan jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:</li></ol>
--------------------	---

		<ol style="list-style-type: none"><li>2.1. Fitur unggah file pada aplikasi</li><li>2.2. Pembatasan jenis file pada fitur unggah file</li><li>2.3. Mekanisme validasi jenis file berdasarkan tipe kontennya</li><li>2.4. Kode sumber yang menunjukkan mekanisme validasi jenis file berdasarkan tipe konten pada fitur unggah file</li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Fitur unggah file pada aplikasi</li><li>2. Pembatasan jenis file pada fitur unggah file</li><li>3. Mekanisme validasi jenis file berdasarkan tipe kontennya</li><li>4. Kode sumber yang menunjukkan mekanisme validasi jenis file berdasarkan tipe konten pada fitur unggah file</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.59

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan pelindungan terhadap metadata input dan metadata file telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan pelindungan terhadap metadata input dan metadata file telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Fitur unggah file pada aplikasi</li><li>2.2. Fitur unduh file pada aplikasi</li><li>2.3. Mekanisme penyimpanan metadata input dan metadata file pada aplikasi</li></ol></li></ol>
--------------------	---	---

		<p>2.4. Kode sumber yang menunjukkan mekanisme penyimpanan file pada fitur unggah file</p> <p>2.5. Kode sumber yang menunjukkan mekanisme unduh file</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Fitur unggah file pada aplikasi</li><li>2. Fitur unduh file pada aplikasi</li><li>3. Mekanisme penyimpanan metadata input dan metadata file pada aplikasi</li><li>4. Kode sumber yang menunjukkan mekanisme penyimpanan file pada fitur unggah file</li><li>5. Kode sumber yang menunjukkan mekanisme unduh file</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.60

Teknik Pemeriksaan	:	<p>1. Auditor Keamanan SPBE memastikan pemindaian file yang diperoleh dari sumber yang tidak dipercaya telah diterapkan pada aplikasi.</p> <p>2. Dalam hal memastikan pemindaian file yang diperoleh dari sumber yang tidak dipercaya telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:</p> <ol style="list-style-type: none"><li>2.1. Fitur pemindaian file yang diperoleh dari sumber yang tidak dipercaya, seperti proses pemindaian antivirus</li><li>2.2. Kode sumber yang menunjukkan fitur pemindaian file yang diperoleh dari sumber yang tidak dipercaya</li></ol>
--------------------	---	---

Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Fitur pemindaian file yang diperoleh dari sumber yang tidak dipercaya, seperti proses pemindaian antivirus</li><li>2. Kode sumber yang menunjukkan fitur pemindaian file yang diperoleh dari sumber yang tidak dipercaya</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.61

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan telah diterapkan pada aplikasi, Auditor Keamanan SPBE melakukan pemeriksaan terhadap hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Fitur unduh file pada aplikasi</li><li>2.2. Konfigurasi yang diterapkan pada proses unduh file, seperti pembatasan jumlah dan ekstensi file yang dapat diunduh</li><li>2.3. Kode sumber yang menunjukkan konfigurasi pada proses unduh file</li></ol></li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Fitur unduh file pada aplikasi</li><li>2. Konfigurasi yang diterapkan pada proses unduh file, seperti pembatasan jumlah dan ekstensi file yang dapat diunduh</li></ol>

		3. Kode sumber yang menunjukkan konfigurasi pada proses unduh file
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.62

Teknik Pemeriksaan	:	Dalam hal memastikan melakukan konfigurasi layanan web telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 63, Kontrol 64, Kontrol 65, dan Kontrol 66.
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan konfigurasi layanan web telah dilakukan.
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.63

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE memverifikasi uniform resource identifier <i>Application programming interface</i> tidak menampilkan informasi yang berpotensi sebagai celah keamanan telah diterapkan pada aplikasi. 2. Dalam hal verifikasi uniform resource identifier <i>Application programming interface</i> agar tidak menampilkan informasi yang berpotensi sebagai celah keamanan telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut: 2.1. Layanan <i>Application programming interface</i> dan dokumentasi <i>Application programming interface</i> yang tersedia pada aplikasi 2.2. Perimeter keamanan (fungsi otentikasi, manajemen sesi dan
--------------------	---	---

		<p>otorisasi) yang diimplementasikan pada <i>Application programming interface</i> secara memadai</p> <p>2.3. Auditor Keamanan SPBE meminta agar Auditan melakukan demonstrasi request <i>Application programming interface</i> dari Aplikasi.</p>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Daftar Layanan <i>Application programming interface</i> dan dokumentasi <i>Application programming interface</i> yang tersedia pada aplikasi</li><li>2. Perimeter keamanan (fungsi otentikasi, manajemen sesi dan otorisasi) yang diimplementasikan pada <i>Application programming interface</i> secara memadai</li><li>3. Demonstrasi request <i>Application programming interface</i> dari Aplikasi.</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.64

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan konfigurasi layanan web telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan konfigurasi layanan web telah diterapkan pada aplikasi, Auditor Keamanan SPBE menanyakan terkait proses otorisasi pada <i>Application programming interface</i> yang disediakan oleh aplikasi.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan mekanisme otorisasi <i>Application programming interface</i>

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.65

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa web menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan bahwa web menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Pada sisi source code, method request <i>Application programming interface</i> seperti apa yang telah didefinisikan.</li><li>2.2. Pada sisi source code, mekanisme pengaturan seperti apa yang telah didefinisikan jika user mengirimkan request menggunakan method yang tidak diatur.</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Kode sumber method request <i>Application programming interface</i></li><li>2. Kode sumber yang mengatur penanganan jika ada method request tidak sesuai dengan yang telah didefinisikan</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.66

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa penggunaan validasi skema dan</li></ol>
--------------------	---	---

		<p>verifikasi sebelum menerima input telah diterapkan pada aplikasi.</p> <p>2. Dalam hal memastikan bahwa penggunaan validasi skema dan verifikasi sebelum menerima input telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:</p> <ol style="list-style-type: none"><li>2.1. Apakah <i>Application programming interface</i> aplikasi menggunakan format dokumen XML.</li><li>2.2. Jika format XML, apakah <i>Application programming interface</i> aplikasi sudah menerapkan validasi skema XSD.</li><li>2.3. Apakah sudah menerapkan verifikasi input yang merujuk pada Kontrol 19.</li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Format dokumen XML</li><li>2. Penerapan validasi skema XSD</li><li>3. Verifikasi input yang merujuk pada Kontrol 19</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.67

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa penggunaan kontrol anti otomatisasi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan bahwa penggunaan kontrol anti otomatisasi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Mekanisme penerapan keamanan atas request query terhadap data, exfiltrasi data yang masif, DDOS, dan file uploads.</li></ol></li></ol>
--------------------	---	---

		2.2. Mekanisme monitoring akses terhadap <i>Application programming interface</i>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan penerapan keamanan atas request masif (DDOS) pada Aplikasi
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.68

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan bahwa mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Sistem Operasi dan perangkat lunak yang digunakan sudah sesuai dengan patches terbaru, dan tidak ada bentrokan versi antar softwarenya.</li><li>2.2. Server sesuai dengan rekomendasi server, dan kerangka kerja aplikasi yang digunakan.</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Versi patch sistem operasi, dan perangkat lunak.</li><li>2. Kesesuaian konfigurasi server dengan rekomendasi server dan kerangka kerja aplikasi yang digunakan.</li></ol>

Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol
--------------------	---	---

KEI.69

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa mendokumentasi, menyalin konfigurasi, dan semua dependensi telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan bahwa mendokumentasi, menyalin konfigurasi, dan semua dependensi telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan hal-hal sebagai berikut:<ol style="list-style-type: none"><li>2.1. Media/pihak yang melakukan dokumentasi kode sumber, menyalin konfigurasi dan semua dependensi dari Aplikasi.</li><li>2.2. Daftar dependensi dan konfigurasi yang disalin dan di dokumentasi.</li></ol></li></ol>
Bukti	:	<p>Gambar/Video/Dokumen yang memperlihatkan:</p> <ol style="list-style-type: none"><li>1. Media penyimpanan salinan konfigurasi, dan dependensi yang ada.</li><li>2. Daftar dependensi dan konfigurasi yang disalin dan di dokumentasi</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

KEI.70

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa Menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan bahwa menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan telah diterapkan</li></ol>
--------------------	---	--

		<p>pada aplikasi. Auditor Keamanan SPBE memperhatikan bahwa aplikasi sudah:</p> <ol style="list-style-type: none"><li>Menonaktifkan daftar direktori yang berisi informasi sensitif yang mungkin dapat dimanfaatkan penyerang.</li><li>Menghapus semua fitur, dokumentasi, sampel, konfigurasi, dan file yang tidak perlu.</li><li>Menghapus kode uji atau fungsi apa pun yang tidak ditujukan untuk produksi sebelum di deploy.</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan proses menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

#### KEI.71

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>Auditor Keamanan SPBE memastikan bahwa penggunaan validasi integritas asset jika asset aplikasi diakses secara eksternal telah diterapkan pada aplikasi.</li><li>Dalam hal memastikan bahwa penggunaan validasi integritas asset jika asset aplikasi diakses secara eksternal telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan bahwa aplikasi sudah:<ol style="list-style-type: none"><li>Memvalidasi integritas asset jika asset aplikasi diakses secara eksternal.</li><li>Memastikan sistem kontrol perubahan software tersedia untuk mengelola dan mencatat perubahan pada source code baik dalam tahapan pengembangan maupun produksi.</li></ol></li></ol>
--------------------	---	--

Bukti	:	Gambar/Video/Dokumen yang memperlihatkan indikator integritas aset pada <i>source code</i> aplikasi
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

**KEI.72**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan bahwa penggunaan respons aplikasi dan konten yang aman telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan bahwa penggunaan respons aplikasi dan konten yang aman telah diterapkan pada aplikasi, auditor Keamanan SPBE memeriksa pengaturan/konfigurasi HTTP header, dan merujuk pada kontrol 31</li></ol>
Bukti	:	Gambar/Video/Dokumen yang memperlihatkan: <ol style="list-style-type: none"><li>1. Respon aplikasi atas input yang dilakukan</li><li>2. Konfigurasi HTTP Header</li></ol>
Status Pemeriksaan	:	Sesuai Desain Kontrol / Tidak Sesuai Desain Kontrol

## E. Petunjuk Teknis Pemeriksaan Kontrol Keamanan pada Evaluasi Efektivitas Kontrol

Petunjuk Teknis pemeriksaan kontrol keamanan merupakan prosedur audit yang dilakukan oleh Auditor Keamanan SPBE untuk menguji kontrol keamanan dan mendapatkan bukti kontrol keamanan telah dilaksanakan.

72 (tujuh puluh dua) Kontrol keamanan yang diperiksa pada tahap evaluasi efektivitas kontrol dikodefikasi ulang menyesuaikan tahap evaluasi efektivitas kontrol sehingga kodefikasinya ditambahkan EF (Evaluasi Efektivitas). Contoh Kontrol keamanan pertama yang dikodefikasikan K1 menjadi KEF.1 dalam tahapan evaluasi Efektivitas.

Hasil pemeriksaan tiap kontrol keamanan pada tahapan evaluasi efektivitas akan menghasilkan status pemeriksaan yaitu Efektif, atau Perlu Peningkatan atau Belum efektif.

### KEF.1

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan pengujian terhadap manajemen kata sandi yang diterapkan dan spesifik pemeriksaan yang ditetapkan oleh auditor Keamanan SPBE.</li><li>2. Mengamati proses yang diberikan oleh aplikasi.</li></ol>
Bukti	:	Hasil pengujian keamanan terhadap manajemen kata sandi (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

### KEF.2

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan intercept pada saat melakukan proses autentikasi.</li><li>2. Melakukan modifikasi kata sandi pada HTTP request yang tertangkap di interceptor dan mengirimkan request ke host/server.</li><li>3. Mengamati respon yang diberikan oleh aplikasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan HTTP request yang telah

	dimodifikasi beserta HTTP response pada interceptor (gambar/video).
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

**KEF.3**

Teknik Pemeriksaan	<p>: 1. Pengujian langsung pada aplikasi</p> <p>1.1. Melakukan input kata sandi secara beragam dengan mempertimbangkan variasi jumlah dan kombinasi jenis karakter kata sandi pada beberapa kondisi yang tidak terbatas pada:</p> <p>a. Saat pembuatan akun;</p> <p>b. Saat menggunakan fitur ganti kata sandi;</p> <p>c. Saat menggunakan fitur reset kata sandi.</p> <p>1.2. Mengamati respon yang diberikan oleh aplikasi.</p> <p>2. Pengujian pada aplikasi menggunakan interceptor</p> <p>2.1. Melakukan intercept pada saat melakukan input kata sandi pada beberapa kondisi yang tercantum pada Langkah 1.1.</p> <p>2.2. Melakukan modifikasi kata sandi secara beragam dengan mempertimbangkan variasi jumlah dan kombinasi jenis karakter kata sandi pada HTTP request yang tertangkap di interceptor dan mengirimkan request ke host/server. Lakukan percobaan dengan menginput karakter spasi pada kata sandi yang dibuat, untuk memastikan spasi tidak memotong</p>
--------------------	---

		<p>kata sandi namun dihitung sebagai satu karakter dalam kata sandi.</p> <p>2.3. Lakukan percobaan dengan menginput karakter double spasi pada kata sandi yang dibuat, untuk memastikan spasi tidak memotong kata sandi namun dihitung sebagai satu karakter dalam kata sandi dan double spasi diperlakukan sebagai satu karakter.</p> <p>2.4. Mengamati respon yang diberikan oleh aplikasi.</p> <p>3. Pengujian terkait masa berlaku kata sandi</p> <p>3.1. Meminta auditan untuk memodifikasi nilai pada parameter waktu di dalam database menjadi melebihi batas masa berlaku kata sandi.</p> <p>3.2. Mencoba login dengan akun yang telah dimodifikasi.</p> <p>3.3. Mengamati respon yang diberikan oleh aplikasi.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Respon aplikasi saat pengujian input kata sandi sebagaimana Langkah 1.</li><li>2. HTTP request yang telah dimodifikasi beserta HTTP response pada interceptor sebagaimana Langkah 2.</li><li>3. Respon aplikasi saat login menggunakan akun yang masa berlaku kata sandinya telah dimodifikasi sebagaimana Langkah 3.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.4

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan input kata sandi dengan kata sandi yang salah pada beberapa kondisi yang tidak terbatas pada:<ol style="list-style-type: none"><li>1.1. Saat login;</li><li>1.2. Saat menggunakan fitur ganti kata sandi.</li></ol></li><li>2. Mengamati respon yang diberikan oleh aplikasi.</li><li>3. Apabila aplikasi memberikan respon berupa penundaan login ketika jumlah maksimum kesalahan dalam pemasukan kata sandi telah tercapai, maka tunggu dalam rentang waktu tertentu kemudian ulangi Langkah 1 dan 2 untuk mengetahui respon yang diberikan oleh aplikasi.</li></ol>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Respon aplikasi saat jumlah maksimum kesalahan dalam pemasukan kata sandi telah tercapai.</li><li>2. Respon aplikasi saat pengujian ulang pemasukan kata sandi setelah mendapatkan respon dari aplikasi sebagaimana Langkah 3.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.5

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Pemulihan kata sandi oleh pengelola aplikasi<ol style="list-style-type: none"><li>1.1. Melakukan permintaan pemulihan kata sandi sesuai dengan prosedur yang telah ditetapkan.</li><li>1.2. Mengamati proses yang dilakukan, khususnya terkait mekanisme verifikasi data pengguna yang</li></ol></li></ol>
--------------------	---	---

	<p>dibutuhkan ketika pemulihan kata sandi.</p> <p>2. Pemulihan kata sandi oleh pengguna</p> <p>2.1. Melakukan pemulihan kata sandi menggunakan fitur yang disediakan pada aplikasi.</p> <p>2.2. Apabila menggunakan OTP, maka lakukan langkah berikut:</p> <p>a. Gunakan kode OTP, lalu lakukan pemulihan kata sandi yang kedua kali dengan menggunakan kode OTP yang sama. Hal ini untuk memastikan bahwa kode OTP yang dikirimkan ke pemilik akun melalui media tertentu (email/nomor seluler) hanya dapat digunakan 1 kali dan tidak dapat digunakan lagi (baik dengan percobaan secara manual, maupun dengan teknik race condition).</p> <p>b. Lakukan percobaan input kode OTP yang salah berulang kali dan amati respon yang diberikan oleh aplikasi. Hal ini untuk memastikan bahwa field untuk input kode OTP tidak dapat dilakukan serangan bruteforce.</p> <p>2.3. Menggunakan interceptor ketika melakukan pemulihan kata sandi untuk memodifikasi parameter yang berkaitan dengan identitas (misalnya email atau nomor seluler) di dalam request pengiriman kata sandi baru.</p> <p>2.4. Mengamati respon yang diberikan oleh aplikasi.</p>
--	---

Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Proses pemulihan kata sandi yang dilakukan oleh pengelola aplikasi.</li><li>2. Fitur pemulihan kata sandi pada aplikasi.</li><li>3. Respon yang diberikan aplikasi setelah menggunakan fitur pemulihan kata sandi pada aplikasi.</li><li>4. Kode OTP yang dikirimkan kepada pengguna.</li><li>5. Respon aplikasi setelah percobaan input kode OTP yang sudah pernah digunakan.</li><li>6. Respon aplikasi setelah percobaan kesalahan input kode OTP berulang kali.</li><li>7. HTTP request yang telah dimodifikasi beserta HTTP response pada interceptor sebagaimana Langkah 2.4.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.6

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Lakukan pemeriksaan bahwa kata sandi disimpan dengan menggunakan enkripsi.</li><li>2. Mencoba membuat beberapa akun dengan beberapa sampel kata sandi yang lemah untuk kemudian melihat algoritma yang digunakan di dalam penyimpanan kata sandi di dalam <i>database</i>.</li><li>3. Dalam konteks dokumentasi manajemen kata sandi ataupun prosedur manajemen akses, periksa:<ol style="list-style-type: none"><li>3.1. Langkah yang dilakukan pengelola/administrator dalam mengingat setiap kata sandi yang dikelolanya</li><li>3.2. Penggunaan teknologi seperti vault ataupun password manager.</li></ol></li></ol>
--------------------	---	--

Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Penyimpanan kata sandi pada database yang menunjukkan Langkah 1 dan 2. 2. Langkah yang dilakukan pengelola/administrator dalam mengingat setiap kata sandi yang dikelolanya. 3. Penggunaan teknologi seperti vault ataupun password manager.
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.7

Teknik Pemeriksaan	:	1. Verifikasi penggunaan sertifikat SSL pada domain aplikasi, khususnya selama proses autentikasi. 2. Memeriksa kadaluarsa sertifikat digital untuk memastikan sertifikat digital yang digunakan masih dalam periode yang valid.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Penggunaan sertifikat SSL pada domain aplikasi selama proses autentikasi. 2. Masa kadaluwarsa sertifikat SSL.
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.8

Teknik Pemeriksaan	:	1. Melakukan intercept terhadap transaksi CRUD yang secara kontrol akses dapat dilakukan oleh user terautentikasi, kemudian melakukan transaksi tanpa token sesi dan memastikan transaksi tidak dapat dilakukan. 2. Melakukan intercept terhadap transaksi CRUD yang secara kontrol akses hanya dapat dilakukan oleh role akun tertentu, kemudian melakukan aktivitas CRUD
--------------------	---	---

		kembali menggunakan sesi role akun yang berbeda dan memastikan transaksi tidak dapat dilakukan.
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Aktivitas CRUD saat mendapatkan otorisasi (dengan sesi).</li><li>2. Aktivitas CRUD (tanpa sesi).</li><li>3. Aktivitas CRUD role akun tertentu menggunakan sesi role akun yang berbeda.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.9

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Setiap kerangka kerja pada umumnya memiliki pengendali sesi tersendiri yang sudah dapat langsung digunakan oleh pengguna. Oleh karena itu, Auditor Keamanan SPBE meminta kepada Auditam untuk ditunjukan kode sumber yang memuat proses mendapatkan nilai sesi.</li><li>2. Auditor Keamanan SPBE dapat mempertimbangkan untuk menggunakan alat bantu <i>source code review</i> untuk dapat mempermudah pemeriksaan secara menyeluruh.</li></ol>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Proses mendapatkan nilai sesi</li><li>2. Hasil menggunakan alat bantu <i>source code review</i></li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.10

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Memastikan algoritma <i>generate token</i> sesi tidak rentan.</li></ol>
--------------------	---	--

	<p>2. Melakukan intercept menggunakan interceptor, terhadap beberapa transaksi token sesi dan memastikan setiap transaksi menghasilkan token sesi yang berbeda.</p> <p>3. Melakukan intercept terhadap transaksi token sesi yang diberikan server, dan melakukan pengujian keacakan token sesi secara otomatis.</p>
Bukti	: Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Nilai sesi yang dihasilkan dengan menggunakan input yang sama. 2. Nilai sesi yang dihasilkan dengan menggunakan input yang beda.
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.11

Teknik Pemeriksaan	: <p>1. Melakukan pengujian terkait session idle termination, berupa:</p> <p>1.1. Menyepakati jangka waktu habis sesi yang dirujuk (ada yang bernilai 15 menit, ada pula yang bernilai 30 menit).</p> <p>1.2. Login ke dalam aplikasi.</p> <p>1.3. Diamkan sampai melewati batas waktu yang dirujuk (misal 16 menit atau 31 menit).</p> <p>1.4. Refresh peramban untuk melihat apakah pengguna dipaksa logout atau masih dalam keadaan memiliki otorisasi.</p> <p>2. Melakukan pengujian terkait aktifnya suatu sesi "tanpa idle", berupa:</p> <p>2.1. Menyepakati jangka waktu habis sesi yang dirujuk (ada yang bernilai 15 menit, ada pula yang bernilai 30 menit)</p>
--------------------	--

		<ul style="list-style-type: none"><li>- default bawaan aplikasi pada umumnya 120 menit).</li><li>2.2. Login ke dalam aplikasi.</li><li>2.3. Terus beraktivitas dari saat awal memperoleh sesi aktif, sampai melewati batas waktu yang dirujuk</li><li>2.4. Perhatikan nilai sesi setelah batas waktu dilewati.</li></ul>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Hasil pengujian 1, yaitu dalam konteks session idle termination</li><li>2. Hasil pengujian 2, yaitu dalam konteks aktifnya suatu sesi "tanpa idle"</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.12

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan validasi dan pencantuman session ID telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan validasi dan pencantuman session ID telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada kontrol 9, kontrol 10, kontrol 11, dan kontrol 13.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan atribut pada session IDE (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.13

Teknik Pemeriksaan	:	Melakukan intercept terhadap transaksi user login yang terautentikasi dan melakukan pemeriksaan terhadap penerapan atribut: <ol style="list-style-type: none"><li>a. "Secure"</li><li>b. "HttpOnly"</li></ol>
--------------------	---	---

	<ul style="list-style-type: none"> <li>c. "Strict-Transport-Security"</li> <li>d. "Domain"</li> <li>e. "Path"</li> <li>f. "SameSite"</li> </ul>
Bukti	<p>: Hasil pengujian keamanan yang memperlihatkan adanya atribut (gambar/video):</p> <ul style="list-style-type: none"> <li>a. "Secure"</li> <li>b. "HttpOnly"</li> <li>c. "Strict-Transport-Security"</li> <li>d. "Domain"</li> <li>e. "Path"</li> <li>f. "SameSite"</li> </ul>
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.14

Teknik Pemeriksaan	: <ul style="list-style-type: none"> <li>1. Auditor Keamanan SPBE mendapatkan informasi penerapan pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna dari hasil evaluasi implementasi.</li> <li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li> </ul>
Bukti	<p>: Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ul style="list-style-type: none"> <li>1. Sesi-cookie pada interface aplikasi</li> <li>2. Kode sumber yang mengatur sesi</li> </ul>
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.15

Teknik Pemeriksaan	: <ul style="list-style-type: none"> <li>1. Melakukan pengujian eksekusi CRUD (Create, Read, Update, Delete) melalui perubahan URL, seperti manipulasi nilai angka (numerik), peran (role), pengguna (user), isi konten/judul data, dan semacamnya.</li> </ul>
--------------------	--

	<ol style="list-style-type: none"><li>1.1. Login dengan dua akun berbeda. Konteks di sini dapat dirinci dengan keadaan sebagai berikut:<ol style="list-style-type: none"><li>a. Dua akun di dalam entitas sama (namun berbeda role), atau</li><li>b. Dua akun di dalam entitas berbeda.</li></ol></li><li>1.2. Lihat perubahan yang terjadi pada URL ketika mengunjungi suatu bagian yang melakukan eksekusi CRUD (contoh: profil, data transaksi/laporan, informasi pengguna / user management, dan semacamnya). Misalnya:<ol style="list-style-type: none"><li>a. Melihat profile diri: target.tld/?user=nama_user</li><li>b. Melihat data transaksi: target.tld/?transactionid=nilai_id_transaksi</li><li>c. Melihat informasi pengguna: target.tld/?user-management</li></ol></li><li>1.3. Ganti nilai URL pada akun yang diperankan sebagai attacker. Contohnya:<ol style="list-style-type: none"><li>a. Akun dengan low privilege mencoba mengakses URL target.tld/?user-management langsung</li><li>b. Akun dengan privilege setara mencoba mengakses nilai transaksi tertentu (yang pada dasarnya bukan untuk dirinya)</li><li>c. Akun dengan entitas berbeda mencoba mengakses nilai transaksi tertentu</li></ol></li><li>1.4. Perhatikan perubahan yang terjadi pada akun attacker.</li></ol>
	<ol style="list-style-type: none"><li>2. Melakukan pengujian eksekusi CRUD melalui POST request (atau selainnya seperti PUT) dengan format form data (application/x-www-form-urlencoded), JSON data, maupun selainnya - seperti manipulasi nilai angka (numerik), peran (role), pengguna (user), isi konten/judul data, dan semacamnya.</li></ol>

		<ol style="list-style-type: none"><li>2.1. Login dengan dua akun berbeda. Konteks dapat dirinci dengan keadaan sebagai berikut:<ol style="list-style-type: none"><li>a. Dua akun di dalam entitas sama (namun berbeda role), atau</li><li>b. Dua akun di dalam entitas berbeda.</li></ol></li><li>2.2. Lihat data yang dikirimkan (pada interceptor) ketika melakukan eksekusi CRUD</li><li>2.3. Ganti value pada parameter yang tampak pada request di interceptor (dengan menggunakan akun yang diperankan sebagai attacker). Model penggantian value-nya tidak jauh berbeda dengan yang ada diterangkan sebelumnya.</li><li>2.4. Perhatikan perubahan yang terjadi.</li><li>3. Melakukan pengujian berupa penggantian value pada header (seperti nilai bearer, nilai token, dan semacamnya). Perhatikan mengenai kemungkinan nilai-nilai ini dapat ditebak atau diganti tanpa adanya validasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): <ol style="list-style-type: none"><li>1. Eksekusi CRUD melalui perubahan URL</li><li>2. Eksekusi CRUD melalui POST request</li><li>3. Penggantian Value pada header</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.16

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan pengujian di dalam login form<ol style="list-style-type: none"><li>1.1. Pastikan telah memiliki 1 akun login yang valid</li><li>1.2. Masukan username dengan benar.</li><li>1.3. Masukan kata sandi secara asal.</li><li>1.4. Kirimkan request ke host (biasanya dengan menekan tombol enter, klik</li></ol></li></ol>
--------------------	---	---

	<p>tombol login, atau klik tombol submit).</p> <p>1.5. Ulangi request dengan cepat (dapat menggunakan alat bantu interceptor)</p> <p>1.6. Lihat response dari setiap request yang dikirim. Bila host terus menerima tanpa melakukan limitasi, maka aplikasi belum menerapkan kontrol yang diinginkan</p> <p>2. Melakukan pengujian eksekusi CRUD di luar login form</p> <p>2.1 Tidak jauh berbeda dengan langkah sebelumnya, yaitu penguji mencoba untuk melakukan perulangan terhadap suatu request yang dikirim, baik itu request untuk membuat sesuatu, membaca sesuatu, memperbarui sesuatu, atau bahkan menghapus sesuatu.</p> <p>Beberapa contoh di antaranya:</p> <ul style="list-style-type: none"><li>a. Membuat user baru,</li><li>b. Membaca data berdasarkan nilai ID atau nilai user tertentu,</li><li>c. Memperbarui biodata ataupun data lainnya,</li><li>d. Menghapus user, menghapus dokumen, dan semacamnya.</li></ul> <p>2.2 Dengan memberikan pembatasan pada eksekusi otomatis, maka setidaknya aplikasi telah melakukan pencegahan secara dini ketika terjadi pembuatan, penarikan, pembuatan, ataupun penghapusan data secara masif.</p>
Bukti	: Hasil pengujian keamanan yang memperlihatkan (gambar/video): <ul style="list-style-type: none"><li>1. Request banyak di dalam login form</li><li>2. Request banyak di luar login form</li></ul>

Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif
--------------------	---	--

**KEF.17**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan informasi penerapan pengaturan antarmuka pada sisi administrator dari hasil evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Proses pemulihan kata sandi yang dilakukan oleh pengelola aplikasi.</li><li>2. Halaman antarmuka yang hanya dapat diakses oleh administrator.</li><li>3. Konfigurasi file robots.txt</li><li>4. Penggunaan kata sandi untuk halaman administrator.</li><li>5. Penggunaan parameter yang mengindikasikan Role atau peran dari pengguna misalkan user atau user id, account, groupid pada URL.</li><li>6. Pembatasan akses terhadap halaman administrator</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

**KEF.18**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Lakukan permintaan token (biasanya didapat setelah berhasil login dengan username dan password, ataupun saat melakukan penghapusan data tertentu) dengan cara: Lakukan sembarang input terhadap form yang meminta token, lalu lihat responsenya.</li></ol>
--------------------	---	---

	<p>2. Pada skenario <i>re-use token</i>, lakukan input token sesuai dengan nilai yang benar, Kemudian ulangi input token, dan masukan kembali token yang telah digunakan sebelumnya (1 nilai yang sama).</p> <p>3. Pada skenario <i>race condition</i>: Lakukan input token sesuai dengan nilai yang benar. Kemudian ulangi input token, dan masukan kembali token yang telah digunakan sebelumnya (1 nilai yang sama). Perbedaan di langkah ini adalah, lakukan secara paralel dan dalam waktu yang cepat (ini akan dapat men-trigger <i>issue race condition</i> bila aplikasi gagal melakukan verifikasi).</p>
Bukti	: Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Nilai Token yang valid. 2. Nilai token yang dimasukan (baik random, maupun re-use).
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.19

Teknik Pemeriksaan	: <p>1. Melakukan pengujian pada setiap fungsi inputan melalui interface aplikasi, berupa:</p> <p>1.1. Lakukan percobaan input karakter khusus HTML atau tag HTML, kemudian perhatikan respon dari aplikasi. Jika Aplikasi belum menerapkan validasi input, maka inputan tersebut dapat terefleksi pada interface aplikasi.</p> <p>1.2. Amati response aplikasi, dan lakukan pengambilan gambar dari hasil uji pada poin 1.1</p>
--------------------	---

	<ol style="list-style-type: none"><li>2. Melakukan pengujian pada setiap fungsi inputan melalui interface Aplikasi, berupa:<ol style="list-style-type: none"><li>2.1. Penguji dapat mencoba memasukan berbagai jenis special character di dalam setiap parameter yang tersedia.</li><li>2.2. Pastikan bahwa input berupa special character dilakukan encoding, dimana tidak hanya terbatas pada eksekusi XSS, melainkan juga eksekusi lain seperti Path Traversal, SSRF, dan eksekusi injeksi lainnya.</li></ol></li><li>3. Melakukan pengujian pada setiap fungsi inputan melalui interceptor, berupa:<ol style="list-style-type: none"><li>3.1. Pastikan bahwa mekanisme sanitasi tidak hanya terbatas pada client side saja.</li><li>3.2. Input karakter normal, menangkap permintaan (request), mengirimkan permintaan dengan karakter normal, lalu mengubah inputannya menjadi karakter khusus pembentuk injeksi di interceptor sebelum mengirimkannya ke host.</li><li>3.3. Amati response pada interceptor, dan lakukan pengambilan gambar dari hasil uji pada poin 2.2</li></ol></li><li>4. Melakukan pengujian pada setiap fungsi inputan melalui interface Aplikasi, berupa bila terdapat eksekusi input yang hanya dapat dilihat di backend, maka penguji harus meminta akses kepada stakeholder untuk dapat melihat setiap respon yang muncul di backend terkait. Hal ini akan sangat bermanfaat untuk menguji kerentanan seperti blind XSS.</li></ol>
--	--

Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Eksekusi injeksi 2. Hasil injeksi 3. Hasil reviu kode sumber yang telah dilakukan 4. Perlindungan yang telah diterapkan pada kode sumber yang ada di fungsi-fungsi yang tersedia.
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.20

Teknik Pemeriksaan	:	1. Melakukan pengujian validasi input sebagai berikut: 1.1. memberikan sembarang input sesuai dengan format 1.2. intercept request sebelum dikirim ke host 1.3. kirimkan input ke host 1.4. pada layar interceptor, ubah setiap input yang dimasukan menjadi berbeda dengan format yang telah ditentukan 1.5. bila ternyata host menerima, maka aplikasi berarti hanya memberikan penyaringan di sisi client saja, adapun bila terjadi penolakan, maka sesuai dengan ekspektasi. 1.6. Hal terpenting di dalam poin ini adalah mempelajari terlebih dahulu format data yang diizinkan secara kasat mata oleh aplikasi di suatu fungsi. 2. Melakukan pengujian validasi input sebagai berikut:
--------------------	---	---

		<p>2.1. Penolakan di sini juga dapat berarti berupa penolakan terhadap suatu data yang disimpan di dalam database.</p> <p>2.2. Ketika didapati adanya ketidaksesuaian antara data yang diinput dengan data yang disimpan, maka mekanisme penolakan di sini akan “berfungsi” untuk mengembalikan inputan kepada user (untuk kemudian diulang).</p> <p>2.3. Perlu menjadi informasi bahwa mekanisme penolakan terkait sudut pandang ini harus bersifat umum, yaitu tidak memberikan informasi mengenai letak kesalahannya.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Kondisi saat input data</li> <li>2. Kondisi saat intercept request</li> <li>3. Respon yang dihasilkan</li> </ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.21

Teknik Pemeriksaan	:	<ol style="list-style-type: none"> <li>1. Mempelajari terlebih dahulu format data yang diizinkan untuk diinput di suatu fungsi.</li> <li>2. Lakukan percobaan input sesuai format yang diizinkan, kemudian perhatikan respon dari aplikasi.</li> <li>3. Lakukan percobaan input karakter khusus yang tidak sesuai format yang diizinkan, kemudian perhatikan respon dari aplikasi.</li> <li>4. Lakukan intercept dan ubah input dengan karakter khusus yang tidak sesuai format</li> </ol>
--------------------	---	--

		yang diizinkan, kemudian perhatikan respon dari aplikasi.
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Hasil percobaan input sesuai format yang diizinkan.</li><li>2. Hasil percobaan input karakter khusus yang tidak sesuai format yang diizinkan.</li><li>3. Hasil intercept dengan input karakter khusus yang tidak sesuai format yang diizinkan.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.22

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memastikan filter terhadap data yang tidak dipercaya telah diterapkan pada aplikasi.</li><li>2. Dalam hal memastikan filter terhadap data yang tidak dipercaya telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada kontrol 19, kontrol 20, dan kontrol 21.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan penerapan filter terhadap data yang tidak dipercaya (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.23

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan pemeriksaan terhadap kode sumber, salah satunya dengan memeriksa jika terdapat fungsi khusus seperti fungsi eval() maka hal ini akan membuka celah untuk melakukan injeksi kode malicious ke dalam aplikasi.</li><li>2. Auditor Keamanan SPBE memastikan filter terhadap data yang tidak dipercaya telah diterapkan pada aplikasi.</li></ol>
--------------------	---	---

		<p>3. Dalam hal memastikan validasi dan pencantuman session ID telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 19.</p>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil reviu kode sumber yang telah dilakukan (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.24

Teknik Pemeriksaan	:	<p>1. Melakukan pengujian validasi input terkait Cross Site Scripting Reflected berupa pengujian sampel pada suatu entry point (Text Field pada form, Parameter pada url, dan lain sebagainya) dengan masukan berupa nilai script seperti "&lt;H1&gt;\$(string)&lt;/H1&gt;", "&lt;script&gt;alert(1)&lt;/script&gt;", atau script lainnya. Kemudian memperhatikan apakah response aplikasi merefleksikan inputan atau nilai yang diberikan.</p> <p>2. Melakukan pengujian validasi input terkait Cross Site Scripting Stored berupa pengujian sampel pada suatu entry point dengan masukan berupa nilai script seperti "&lt;H1&gt;\$(string)&lt;/H1&gt;", "&lt;script&gt;alert(1)&lt;/script&gt;", atau script lainnya. Kemudian memperhatikan apakah aplikasi menyimpan nilai script tersebut. Selanjutnya periksa halaman lain aplikasi yang akan memanggil data berupa nilai script tersebut untuk diperiksa apakah respon aplikasi menjalankan nilai script yang telah disimpan sebelumnya.</p>
--------------------	---	---

		<p>3. Dalam hal memastikan pelindungan terhadap akses yang mengandung konten skrip telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 19.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Hasil pengujian Cross Site Scripting Reflected</li><li>2. Hasil pengujian Cross Site Scripting Stored</li><li>3. Penerapan pelindungan terhadap akses yang mengandung konten skrip.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.25

Teknik Pemeriksaan	:	<p>1. Melakukan pengujian validasi input terkait pelindungan dari serangan injeksi basis data berupa :</p> <ol style="list-style-type: none"><li>1.1. Pemeriksaan entry point yang mengindikasikan pengguna dapat mengirimkan data yang kemudian disimpan ke dalam database.</li><li>1.2. Review kode sumber aplikasi yang bersesuaian dengan poin 1 dan identifikasi bagian kode yang mengindikasikan terdapatnya perintah SQL query, dan analisis potensi atau kemungkinan injeksi dari perintah SQL query tersebut.</li><li>1.3. Dalam rangka pencegahan percobaan injeksi code kedalam aplikasi, melalui statement SQL query, auditor Keamanan SPBE memastikan pada sumber kode aplikasi telah melakukan mitigasi, seperti:</li></ol>
--------------------	---	---

		<ul style="list-style-type: none"> <li>a. Penerapan parameter pada statement SQL query atau yang lebih dikenal dengan “prepared statement”.</li> <li>b. Melakukan whitelist terhadap input pengguna seperti yang telah didefinisikan (lihat Kontrol 21).</li> </ul> <p>2. Dalam hal memastikan pelindungan dari serangan injeksi basis data telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada kontrol 19.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Hasil pemeriksaan entry point</li> <li>2. Hasil reviu kode sumber</li> <li>3. Penerapan parameter pada SQL query</li> <li>4. Mekanisme whitelist terhadap input pengguna</li> <li>5. Penerapan pelindungan dari serangan injeksi basis data</li> </ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.26

Teknik Pemeriksaan	:	<ol style="list-style-type: none"> <li>1. Auditor Keamanan SPBE meminta kepada Auditam untuk menjalankan test vector seluruh penggunaan algoritma, modul, protokol, dan manajemen kunci kriptografi sehingga dipastikan aplikasi dapat memproses kriptografi yang dibutuhkan dalam library.</li> <li>2. Auditor Keamanan SPBE meminta kepada Auditam untuk ditunjukan hasil Pengujian lab terhadap algoritma, modul, protokol, dan manajemen kunci kriptografi telah dilakukan dan lulus sertifikasi. Pengujian</li> </ol>
--------------------	---	--

	<p>juga dapat dilakukan dengan memastikan aplikasi dapat melakukan upgrade algoritma, modul, protokol, dan manajemen kunci kriptografi yang memiliki spesifikasi lebih tinggi sesuai klasifikasi data/informasi.</p> <p>3. Auditor Keamanan SPBE melakukan pengujian secara brute force jika memungkinkan untuk mengetahui terdapat implementasi yang lemah dari mode operasi, kunci lemah, atau algoritma yang sudah usang.</p> <p>4. Auditor Keamanan SPBE dapat juga melakukan Randomness Test terhadap penggunaan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi pada Aplikasi.</p>
Bukti	<p>:</p> <p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Pengujian Test Vector</li> <li>2. Pengujian lab kriptografi</li> <li>3. Implementasi dari mode operasi kriptografi</li> <li>4. Pengujian Randomness Test</li> </ol>
Status Pemeriksaan	<p>:</p> <p>Efektif, Perlu Peningkatan / Belum Efektif</p>

#### KEF.27

Teknik Pemeriksaan	: <ol style="list-style-type: none"> <li>1. Auditor Keamanan SPBE mendapatkan informasi penerapan autentikasi data yang dienkripsi dari hasil evaluasi implementasi.</li> <li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li> </ol>
Bukti	: <p>Hasil pengujian keamanan yang memperlihatkan sumber kode atau konfigurasi yang menunjukkan (gambar/video):</p>

	<ol style="list-style-type: none"><li>1. Klasifikasi data dan informasi sensitif</li><li>2. Penggunaan algoritma kriptografi, mode enkripsi</li><li>3. Protokol kriptografi yang berjalan dalam modul kriptografi</li><li>4. Implementasi kriptografi yang terbarukan</li></ol>
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.28

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan informasi penerapan manajemen kunci kriptografi dari hasil evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang menunjukkan penerapan manajemen kunci kriptografi (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.29

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan Randomness Test terhadap pembuatan angka acak yang menggunakan generator angka acak kriptografi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan Randomness Test (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.30

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan percobaan kesalahan input pada beberapa entry point</li><li>2. Mengamati respon yang ditampilkan pada interface aplikasi.</li><li>3. Jika respon yang ditampilkan bersifat sensitif atau memberikan petunjuk untuk penyerang, maka terindikasi aplikasi belum mencegah kesalahan terprediksi dan tidak terduga</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan konten pesan yang ditampilkan (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.31

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan percobaan kesalahan input pada beberapa entry point</li><li>2. Mengamati respon yang ditampilkan pada interface aplikasi.</li><li>3. Jika respon yang ditampilkan bersifat sensitif atau memberikan petunjuk untuk penyerang, maka terindikasi aplikasi belum mencegah kesalahan terprediksi dan tidak terduga</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan konten pesan yang ditampilkan (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.32

Teknik Pemeriksaan	:	Melakukan pengujian secara dinamis pada aplikasi yang berdampak pada Error dan Pencatatan Log, salah satunya dengan cara berikut: <ol style="list-style-type: none"><li>1. Mencari menu log pada aplikasi</li><li>2. Mengamati log yang dicatat</li></ol>
--------------------	---	---

		3. Identifikasi ada atau tidaknya informasi yang dikecualikan pada pencatatan log
Bukti	:	Hasil pengujian keamanan yang memperlihatkan informasi yang dicatat pada log (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.33

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE mendapatkan informasi yang dicatat pada log dari hasil evaluasi implementasi 2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Cakupan log yang dicatat 2. Masa retensi log 3. Daftar Insiden yang pernah terjadi pada aplikasi 4. Kebermanfaatan log
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.34

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE memastikan pengaturan perlindungan log aplikasi dari akses dan modifikasi yang tidak sah dari hasil evaluasi implementasi 2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Mekanisme perlindungan terhadap keutuhan log.

		2. Pengaturan role akses ke log. 3. Mekanisme monitoring log.
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.35

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE mendapatkan penjelasan terkait enkripsi pada data yang disimpan untuk mencegah injeksi log pada tahap evaluasi implementasi. 2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan penerapan mekanisme encode pada data sebelum dicatat di log (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.36

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE mendapatkan penjelasan terkait sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar pada tahap evaluasi implementasi. 2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan sinkronisasi sumber waktu pada beberapa server (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.37

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE mendapatkan penjelasan terkait mekanisme
--------------------	---	---

		<p>penyimpanan dan pengamanan informasi yang dikecualikan pada tahap evaluasi implementasi.</p> <p>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Daftar informasi yang dikecualikan</li> <li>2. Penyimpanan dan pengamanan informasi yang dikecualikan</li> <li>3. Penyimpanan dan pengamanan salinan informasi yang dikecualikan</li> <li>4. Hasil pemeriksaan penyimpanan informasi dibandingkan dengan peraturan yang ditetapkan</li> </ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.38

Teknik Pemeriksaan	:	<p>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi pada tahap evaluasi implementasi.</p> <p>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Penyimpanan dan pengamanan informasi dikecualikan yang disimpan secara temporary.</li> <li>2. Direktori temporary.</li> </ol>

		<ol style="list-style-type: none"><li>3. Perlindungan akses dari data temporary</li><li>4. Penyimpanan informasi/file yang dilakukan di sisi client</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.39

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pertukaran, penghapusan, dan audit informasi yang dikecualikan pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Pertukaran informasi yang dikecualikan</li><li>2. Penghapusan informasi yang dikecualikan</li><li>3. Audit terhadap informasi yang dikecualikan</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.40

Teknik Pemeriksaan	:	<p>Melakukan pengujian secara dinamis terhadap aplikasi yang berdampak pada:</p> <ol style="list-style-type: none"><li>1. Data/informasi (file, database, dan konfigurasi) dapat diambil oleh pihak yang tidak berhak</li><li>2. Kegagalan fungsi backup atau restore data</li></ol>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Data atau informasi yang dapat diambil oleh penyerang</li><li>2. Kegagalan fungsi backup atau restore data</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.41

Teknik Pemeriksaan	:	Memastikan fitur dan mekanisme untuk menghapus dan melakukan ekspor data sesuai permintaan pengguna di aplikasi berjalan sebagaimana mestinya.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan pengujian fitur hapus dan ekspor data sesuai permintaan pengguna (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.42

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pembersihan memori setelah tidak digunakan pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan mekanisme pembersihan data pada memori setelah tidak diperlukan (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.43

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE memeriksa sertifikat SSL/TLS yang digunakan pada domain aplikasi</li><li>2. Auditor Keamanan SPBE memeriksa penggunaan protokol HTTP pada aplikasi dengan beberapa hal berikut:<ol style="list-style-type: none"><li>2.1. Mengakses aplikasi menggunakan IP address</li><li>2.2. Mengakses aplikasi menggunakan HTTP:// pada URL</li></ol></li></ol>
--------------------	---	---

		Apabila aplikasi masih menerapkan penggunaan protokol HTTP, maka aplikasi tidak menggunakan komunikasi terenkripsi.
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Sertifikat SSL/TLS yang digunakan pada domain aplikasi</li> <li>2. Hasil pengujian ketika mengakses aplikasi menggunakan IP address</li> <li>3. Hasil pengujian ketika mengakses aplikasi menggunakan HTTP:// pada URL</li> </ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.44

Teknik Pemeriksaan	:	<p>1. Auditor Keamanan SPBE memeriksa sertifikat SSL/TLS yang digunakan pada domain aplikasi</p> <p>2. Auditor Keamanan SPBE memeriksa penggunaan protokol HTTP pada aplikasi dengan beberapa hal berikut:</p> <ol style="list-style-type: none"> <li>2.1. Mengakses aplikasi menggunakan IP address</li> <li>2.2. Mengakses aplikasi menggunakan HTTP:// pada URL</li> </ol> <p>Apabila aplikasi masih menerapkan penggunaan protokol HTTP, maka aplikasi tidak menggunakan komunikasi terenkripsi.</p>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"> <li>1. Sertifikat SSL/TLS yang digunakan pada domain aplikasi</li> <li>2. Hasil pengujian ketika mengakses aplikasi menggunakan IP address</li> <li>3. Hasil pengujian ketika mengakses aplikasi menggunakan HTTP:// pada URL</li> </ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.45

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan pengujian kualitas SSL/TLS yang digunakan aplikasi menggunakan scanning tools meliputi: 1. Tingkat kesesuaian konfigurasi SSL berdasarkan <i>scanning tools</i> 2. Versi SSL/TLS yang diizinkan pada aplikasi
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Tingkat kesesuaian konfigurasi SSL berdasarkan <i>scanning tools</i> 2. Versi SSL/TLS yang diizinkan pada aplikasi berdasarkan <i>scanning tools</i>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.46

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan pemeriksaan terkait konfigurasi SSL/TLS yang diterapkan menggunakan scanning tools meliputi: 1. Domain yang tercakup dalam penggunaan SSL/TLS 2. Periode validitas sertifikat 3. Organisasi yang mengeluarkan sertifikat
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): 1. Domain yang tercakup dalam penggunaan SSL/TLS berdasarkan <i>scanning tools</i> 2. Periode validitas sertifikat berdasarkan <i>scanning tools</i> 3. Organisasi yang mengeluarkan sertifikat berdasarkan <i>scanning tools</i>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.47

Teknik Pemeriksaan	:	1. Auditor Keamanan SPBE mendapatkan penjelasan terkait analisis kode dalam
--------------------	---	---

		<p>kontrol kode berbahaya pada tahap evaluasi implementasi.</p> <p>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</p>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan mekanisme dan hasil analisis kode sumber (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.48

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan <i>Vulnerability Assessment</i> secara otomatis untuk memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan
Bukti	:	Hasil pengujian keamanan yang memperlihatkan mekanisme dan hasil analisis kode sumber (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.49

Teknik Pemeriksaan	:	<p>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pengaturan izin terkait fitur atau sensor terkait privasi pada tahap evaluasi implementasi.</p> <p>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</p>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan pengaturan izin terkait fitur atau sensor terkait privasi (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.50

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pengaturan pelindungan integritas pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan pengaturan izin terkait File Integrity Monitoring (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.51

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pengaturan mekanisme fitur pembaruan pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan (gambar/video): <ol style="list-style-type: none"><li>1. Mekanisme pembaruan fitur aplikasi</li><li>2. Mekanisme pembaruan yang diperoleh melalui saluran aman dan ditandatangani secara digital, apabila dilakukan secara otomatis.</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.52

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan pengujian terhadap alur logika bisnis secara sampling yang dapat berkaitan dengan fungsi kontrol
--------------------	---	--

	: keamanan lainnya, seperti Autentikasi dan Manajemen Sesi.
Bukti	: Hasil pengujian keamanan yang memperlihatkan alur logika bisnis dalam urutan langkah dan waktu yang realistik (gambar/video).
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.53

Teknik Pemeriksaan	: Auditor Keamanan SPBE melakukan pengujian terhadap alur logika bisnis secara sampling yang dapat berkaitan dengan fungsi kontrol keamanan lainnya, seperti Validasi Input dan Kontrol Akses.
Bukti	: Hasil pengujian keamanan yang memperlihatkan batasan dan validasi logika bisnis (gambar/video).
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.54

Teknik Pemeriksaan	: Auditor Keamanan SPBE melakukan pengujian dari fungsi kontrol keamanan lainnya dan meminta kepada Auditam untuk ditunjukkan apakah aktivitas pengujian tersebut tercatat di dalam sistem monitoring.
Bukti	: Hasil pengujian keamanan yang memperlihatkan aktivitas pengujian yang telah tercatat di dalam sistem monitoring (gambar/video).
Status Pemeriksaan	: Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.55

Teknik Pemeriksaan	: Auditor Keamanan SPBE melakukan pengujian dari fungsi kontrol keamanan lainnya dan meminta kepada Auditam untuk ditunjukkan apakah aktivitas pengujian tersebut berhasil
--------------------	--

		dicegah oleh kontrol anti otomatisasi pada aplikasi atau sistem monitoring.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan pengaturan kontrol anti-automasi beserta kode sumber yang menunjukkan pengaturan tersebut (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.56

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan pengujian dari fungsi kontrol keamanan lainnya dan meminta kepada Auditam untuk ditunjukkan apakah aplikasi atau sistem monitoring memberikan peringatan terkait aktivitas pengujian tersebut.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan peringatan yang diberikan oleh aplikasi atau sistem monitoring terkait efektivitas pengujian (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.57

Teknik Pemeriksaan	:	Melakukan pengujian unggah file yang tidak sesuai dengan ketentuan jumlah dan ukuran file, lalu melihat respon yang diberikan oleh aplikasi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan respon yang diberikan oleh aplikasi (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.58

Teknik Pemeriksaan	:	1. Melakukan pengujian unggah file yang tidak sesuai dengan ketentuan jenis file yang diizinkan, lalu melihat respon yang diberikan oleh aplikasi.
--------------------	---	--

		<ol style="list-style-type: none"><li>2. Melakukan perubahan ekstensi pada file dengan tipe konten yang tidak diizinkan menjadi ekstensi file yang diizinkan, kemudian melakukan percobaan unggah file tersebut, lalu melihat respon yang diberikan oleh aplikasi.</li><li>3. Melakukan intercept pada transaksi unggah file, kemudian mengganti isi file dengan isi file jenis selain yang diizinkan, lalu mengirim request dan melihat respon yang diberikan oleh aplikasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan respon yang diberikan oleh aplikasi (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.59

Teknik Pemeriksaan	:	Melakukan pengujian unggah file kemudian melakukan unduh pada file yang sama, lalu membandingkan metadata pada file yang diunggah dan diunduh untuk memastikan tidak ada perubahan pada metadata file.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil perbandingan metadata pada file yang diunggah dan diunduh untuk memastikan tidak ada perubahan pada metadata file (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.60

Teknik Pemeriksaan	:	Melakukan pengujian unggah file dengan tipe <i>executable file / malicious file</i> , kemudian melihat respon yang diberikan oleh aplikasi.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan respon yang diberikan oleh aplikasi (gambar/video).

Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif
--------------------	---	--

**KEF.61**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Melakukan pengujian unduh file untuk memeriksa mekanisme unduh file telah sesuai dengan yang dikonfigurasikan berdasarkan keterangan pada tahap implementasi.</li><li>2. Melakukan pengujian unduh file yang tidak sesuai dengan kontrol akses yang telah dikonfigurasi sebelumnya.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil pengujian unduh file yang tidak sesuai dengan kontrol akses yang telah dikonfigurasi sebelumnya (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

**KEF.62**

Teknik Pemeriksaan	:	Dalam hal memastikan konfigurasi layanan web telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 63, Kontrol 64, Kontrol 65, dan Kontrol 66.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan konfigurasi layanan web telah diterapkan secara efektif (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

**KEF.63**

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Meminta dokumentasi <i>Application programming interface</i> aplikasi untuk dicoba pada <i>Application programming interface Tester</i></li><li>2. Mencoba melakukan running seluruh Request <i>Application programming interface</i></li></ol>
--------------------	---	--

		<p>aplikasi menggunakan <i>Application programming interface Tester</i></p> <p>3. Memeriksa uniform resource identifier <i>Application programming interface</i> tidak menampilkan informasi yang berpotensi sebagai celah keamanan berdasarkan hasil request <i>Application programming interface</i> yang dikirim</p>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil running dari request <i>Application programming interface</i> aplikasi menggunakan <i>Application programming interface tester</i> (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.64

Teknik Pemeriksaan	:	<p>1. Meminta dokumentasi <i>Application programming interface</i> aplikasi untuk dicoba pada <i>Application programming interface Tester</i></p> <p>2. Mencoba melakukan running seluruh Request <i>Application programming interface</i> aplikasi menggunakan <i>Application programming interface Tester</i></p> <p>3. Memeriksa apakah ada penggunaan parameter berupa token saat hendak melakukan Request <i>Application programming interface</i></p>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil running dari request <i>Application programming interface</i> aplikasi menggunakan <i>Application programming interface tester</i> (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.65

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Meminta dokumentasi <i>Application programming interface</i> aplikasi untuk dicoba pada <i>Application programming interface Tester</i></li><li>2. Melakukan running seluruh Request <i>Application programming interface</i> aplikasi menggunakan <i>Application programming interface Tester</i>, menggunakan berbagai method (GET, POST, PUT, DELETE, HEAD, OPTIONS, dan lain-lain) selain yang dicantumkan pada dokumentasi <i>Application programming interface</i></li><li>3. Memeriksa respon yang ditampilkan <i>Application programming interface</i> aplikasi</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil running dari request <i>Application programming interface</i> aplikasi menggunakan <i>Application programming interface tester</i> (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.66

Teknik Pemeriksaan	:	Dalam hal memastikan penggunaan validasi skema dan verifikasi sebelum menerima input telah diterapkan pada aplikasi, Auditor Keamanan SPBE memperhatikan teknik pengujian pada Kontrol 19.
Bukti	:	Hasil pengujian keamanan yang memperlihatkan validasi skema dan verifikasi sebelum menerima input telah diterapkan secara efektif (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.67

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Meminta dokumentasi <i>Application programming interface</i> aplikasi untuk dicoba pada Interceptor</li><li>2. Mencoba melakukan serangan yang menggunakan otomatisasi, seperti request query terhadap data, exfiltrasi data yang masif, DDOS, dan file uploads pada <i>Application programming interface</i> aplikasi</li><li>3. Memeriksa respon yang ditampilkan <i>Application programming interface</i> aplikasi</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil <i>running</i> dari <i>brute force request</i> terhadap <i>Application programming interface</i> menggunakan <i>Interceptor</i> (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.68

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait pengaturan konfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan proses mendokumentasi, menyalin konfigurasi, dan semua dependensi (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.69

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait mendokumentasi, menyalin konfigurasi, dan semua dependensi yang digunakan pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	<p>Hasil pengujian keamanan yang memperlihatkan (gambar/video):</p> <ol style="list-style-type: none"><li>1. Media penyimpanan salinan konfigurasi, dan dependensi yang ada.</li><li>2. Daftar dependensi dan konfigurasi yang disalin dan di dokumentasi</li></ol>
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.70

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Auditor Keamanan SPBE mendapatkan penjelasan terkait proses menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan pada tahap evaluasi implementasi.</li><li>2. Auditor Keamanan SPBE melakukan penilaian dalam pemeriksaan tahap ini, sama dengan hasil penilaian dalam pemeriksaan tahap implementasi.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan proses menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

KEF.71

Teknik Pemeriksaan	:	Auditor Keamanan SPBE melakukan reviu pada kode sumber aplikasi dengan cara:
--------------------	---	--

		<ol style="list-style-type: none"><li>1. Akses aplikasi, kemudian lihat dari sisi kode sumber dan periksa penerapan integritas pada asset yang diakses dari eksternal.</li><li>2. Jika pada kode sumber sudah ada keterangan integrity="nilai hash", maka sudah menerapkan validasi integritas asset yang diakses dari eksternal.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan penerapan integritas asset berdasarkan hasil reviu kode sumber (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

#### KEF.72

Teknik Pemeriksaan	:	<ol style="list-style-type: none"><li>1. Intercept halaman aplikasi, kemudian melihat konten pada HTTP Header</li><li>2. Jika pada HTTP header terdapat konten atau informasi sensitif, maka aplikasi tidak menggunakan respon dan konten yang aman.</li></ol>
Bukti	:	Hasil pengujian keamanan yang memperlihatkan hasil intercept yang dilakukan pada tahap pengujian (gambar/video).
Status Pemeriksaan	:	Efektif, Perlu Peningkatan / Belum Efektif

## BAB IV

### METODE PENILAIAN DALAM PEMERIKSAAN DAN APLIKASI INSTRUMEN AUDIT KEAMANAN SPBE

#### A. METODE PENILAIAN DALAM PEMERIKSAAN

Metode penilaian dalam pemeriksaan yang dilakukan oleh auditor Keamanan SPBE dilakukan untuk setiap kontrol keamanan yang dipersyaratkan, penilaian terhadap setiap hasil evaluasi (3 tahapan evaluasi) dan konklusi akhir Audit.

Pemeriksaan dilakukan terhadap 2 (dua) area keamanan yaitu Manajemen Keamanan Informasi (14 kontrol keamanan) dan Standar Teknis dan Prosedur Keamanan (72 kontrol keamanan).

Pada saat tahapan Pemahaman desain kontrol atau saat Pra Audit (sebelum kegiatan audit), khususnya dalam area Standar Teknis dan Prosedur Keamanan, kontrol keamanan yang diperiksa dapat berkurang. Hal ini dikarenakan dalam objek audit (Aplikasi berbasis Web) yang akan diperiksa baik secara tujuan, persyaratan desain, dan kompleksitas tidak mengakomodir beberapa kontrol keamanan yang dipersyaratkan sehingga akan mengurangi pemeriksaan kontrol keamanan dalam area Standar Teknis dan Prosedur Keamanan. Hal tersebut wajib dikomunikasikan antara Auditor Keamanan SPBE dan Audit sebelum dilakukan kegiatan audit dan dituangkan dalam dokumen rencana audit.

- Penilaian dalam pemeriksaan setiap kontrol keamanan Audit Keamanan SPBE

Pada tahap evaluasi desain kontrol keamanan, status pemeriksaan kontrol adalah Sesuai dengan Desain Kontrol keamanan (bernilai 1 Poin) atau Tidak Sesuai dengan Desain Kontrol keamanan (bernilai 0 Poin). Dengan demikian jika seluruh kontrol keamanan dilaksanakan akan menghasilkan 14 poin untuk area Manajemen Keamanan Informasi dan 72 poin untuk area Standar Teknis dan Prosedur Keamanan.

Pada tahap evaluasi Implementasi kontrol keamanan, status pemeriksaan kontrol adalah Sesuai dengan Implementasi Desain Kontrol keamanan (bernilai 1 Poin) atau Tidak Sesuai dengan Implementasi Desain Kontrol keamanan (bernilai 0 Poin). Dengan demikian jika seluruh kontrol keamanan dilaksanakan akan

menghasilkan 14 poin untuk area Manajemen Keamanan Informasi dan 72 poin untuk area Standar Teknis dan Prosedur Keamanan.

Sedangkan untuk tahap evaluasi efektivitas kontrol keamanan, status pemeriksaan kontrol adalah Efektif ( bernilai 1 Poin) atau Perlu Peningkatan (bernilai 1) atau Belum Efektif (bernilai 0 Poin). Dengan demikian jika seluruh kontrol keamanan dilaksanakan sesuai tujuan akan menghasilkan 14 poin untuk area Manajemen Keamanan Informasi dan 72 poin untuk area Standar Teknis dan Prosedur Keamanan.

- Penilaian konklusi tahapan evaluasi Audit Keamanan SPBE

Pada setiap tahapannya, terdapat 2 (dua) area keamanan yang diperiksa yaitu Manajemen Keamanan Informasi (14 kontrol ) dan Standar Teknis dan Prosedur Keamanan( 72 kontrol ). Mekanisme penilaian dalam pemeriksaan audit keamanan, tidak ada ketentuan proporsional bahwa bobot pemeriksaan area yang satu lebih besar dari pada area yang lain. Pembobotan penilaian dalam pemeriksaan adalah sama ( 1:1) untuk area Manajemen Keamanan informasi dan Standar Teknis dan Prosedur Keamanan. Penilaian akhir untuk dua area keamanan yang diperiksa akan menghasilkan persentase nilai contohnya adalah 70%.

Untuk mendapatkan konklusi tahapan, evaluasi tiap tahapan diperlukan *passing grade* persentase yang menjadi acuan penarikan konklusi pemeriksaan yaitu sebagai berikut :

a. Evaluasi Desain Kontrol

- Lebih dari 90 % artinya Memadai;
- Antara 40% - 90% artinya Perlu Peningkatan; dan
- Kurang dari 40% artinya Tidak Memadai.

b. Evaluasi Implementasi Kontrol

- Lebih dari 65 % artinya Sesuai dengan Desain Kontrol; dan
- Kurang dari sama dengan 65% artinya Tidak Sesuai dengan Desain Kontrol;

c. Evaluasi Efektivitas Kontrol

- Lebih dari 95 % artinya Efektif;
- Antara 40% - 95% artinya Perlu Peningkatan; dan
- Kurang dari 40% artinya Tidak Efektif.

- Penilaian konklusi Audit Keamanan SPBE

Konklusi Audit Keamanan SPBE didapatkan berdasarkan dari jalur skema hasil 3 (tiga) evaluasi yang dilalui. Variasi untuk mendapatkan konklusi hasil audit adalah sebagai berikut :

- a. Untuk memperoleh konklusi Audit Keamanan **MEMADAI**, maka status pemeriksaan yang harus dicapai dalam evaluasi Desain Kontrol paling minimal adalah **Perlu Peningkatan**, dan kemudian dalam evaluasi implementasi kontrol memberikan konklusi **Sesuai Desain Kontrol** dan status pemeriksaan dalam evaluasi efektivitas adalah **Efektif**. Jika evaluasi desain kontrol memberikan konklusi **Memadai**, dan evaluasi implementasi kontrol memberikan konklusi **Sesuai Desain Kontrol**, maka untuk hasil konklusi dalam evaluasi efektivitas cukup mendapatkan konklusi **Perlu Peningkatan**, tidak harus Efektif.
- b. Untuk memperoleh konklusi Audit Keamanan **PERLU PENINGKATAN**, maka status pemeriksaan yang harus dicapai dalam evaluasi desain kontrol paling minimal adalah **Perlu Peningkatan**, kemudian dalam evaluasi implementasi kontrol memberikan konklusi **Sesuai Desain Kontrol** dan status pemeriksaan dalam evaluasi efektivitas adalah **Perlu Peningkatan**. Jika kondisi status pemeriksaan dalam evaluasi desain kontrol adalah **Memadai**, kemudian dalam evaluasi implementasi kontrol memberikan konklusi Tidak **Sesuai Desain Kontrol**, maka dalam pemeriksaan dalam evaluasi efektivitas adalah status yang harus diperoleh adalah **Efektif**.
- c. Sedangkan untuk konklusi Audit Keamanan **TIDAK MEMADAI**, diperoleh dari variasi lain yang tidak disebutkan di atas. Adapun keseluruhan variasi penilaian dalam pemeriksaan dapat dilihat di tabel bawah ini.

KONKLUSI AUDIT	EVALUASI DESAIN KONTROL	EVALUASI IMPLEMENTASI KONTROL	EVALUASI EFEKTIVITAS KONTROL
MEMADAI	MEMADAI	SESUAI DESAIN KONTROL	EFEKTIF / PERLU PENINGKATAN
	PERLU PENINGKATAN	SESUAI DESAIN KONTROL	EFEKTIF

PERLU PENINGKATAN	MEMADAI	SESUAI DESAIN KONTROL	BELUM EFEKTIF
	MEMADAI	TIDAK SESUAI DESAIN KONTROL	EFEKTIF
	PERLU PENINGKATAN	SESUAI DESAIN KONTROL	PERLU PENINGKATAN
TIDAK MEMADAI	MEMADAI	TIDAK SESUAI DESAIN KONTROL	PERLU PENINGKATAN / BELUM EFEKTIF
	PERLU PENINGKATAN	SESUAI DESAIN KONTROL	BELUM EFEKTIF
		TIDAK SESUAI DESAIN KONTROL	EFEKTIF/PERLU PENINGKATAN / BELUM EFEKTIF
	TIDAK MEMADAI	-	EFEKTIF/PERLU PENINGKATAN / BELUM EFEKTIF

Penjelasan lebih lanjut terkait proses penilaian dalam pemeriksaan Audit Keamanan SPBE diberikan contoh kasus sebagai berikut :

Instansi A akan melakukan audit terhadap aplikasi X miliknya. Dari tahapan pemahaman desain kontrol dan koordinasi yang dilakukan oleh Auditor Keamanan SPBE dan Pemilik Aplikasi dinyatakan bahwa Aplikasi X sesuai persyaratan desain dan kebutuhan tidak dapat menerapkan 2 (dua) kontrol keamanan pada Standar Teknis dan Prosedur Keamanan. Dengan pemeriksaan yang akan dilakukan pada audit keamanan adalah 14 kontrol keamanan pada area Manajemen Keamanan Informasi dan 70 kontrol Keamanan pada Standar Teknis dan Prosedur Keamanan.

Hasil pemeriksaan dalam tahapan evaluasi desain kontrol memberikan status penilaian kontrol keamanan sebagai berikut :

- 1) Pada Area Manajemen Keamanan Informasi, 12 kontrol keamanan dinyatakan Sesuai, dan
- 2) Pada area Standar Teknis dan Prosedur Keamanan, 65 kontrol keamanan dinyatakan Sesuai.

Maka perhitungan persentase per Area Keamanan sebagai berikut :

- Area                  Manajemen                  Keamanan                  Informasi

$$\frac{12 \text{ kontrol keamanan terpenuhi}}{14 \text{ kontrol keamanan dipersyaratkan}} \times 100\% = 85,71\%$$

- Area Standar Teknis dan Prosedur Keamanan

$$\frac{65 \text{ kontrol keamanan terpenuhi}}{70 \text{ kontrol keamanan dipersyaratkan}} \times 100\% = 92,86\%$$

Hasil Evaluasi Desain Kontrol adalah  $\frac{85,71\% + 92,86\%}{2} = 89,29\%$

Merujuk penjelasan *passing grade* yang digunakan diatas, maka konklusi Evaluasi Desain Kontrol pada Aplikasi X adalah **Perlu Peningkatan**. Karena perlu peningkatan, maka dapat dilanjutkan untuk dilakukan penilaian dalam pemeriksaan Evaluasi Implementasi Kontrol.

Selanjutnya, pada tahapan Evaluasi Implementasi Kontrol (EIK) terdapat penyesuaian terhadap kontrol keamanan yang diperiksa sesuai dengan hasil pemeriksaan kontrol keamanannya. Pada tahapan EDK, Desain kontrol yang dinyatakan sesuai berjumlah 12 kontrol pada area Manajemen Keamanan Informasi dan 65 kontrol pada area Standar Teknis dan Prosedur Keamanan. Oleh karena itu, penilaian dalam pemeriksaan EIK hanya dilakukan terhadap kontrol yang sesuai pada tahapan EDK.

Hasil pemeriksaan dalam tahapan evaluasi implementasi kontrol memberikan status penilaian dalam pemeriksaan kontrol keamanan sebagai berikut:

- 1) Pada Area Manajemen Keamanan Informasi, 9 kontrol keamanan dinyatakan Sesuai, dan
- 2) Pada area Standar Teknis dan Prosedur Keamanan, 55 kontrol keamanan dinyatakan Sesuai.

Maka perhitungan persentase per Area Keamanan sebagai berikut :

- Area Manajemen Keamanan Informasi

$$\frac{9 \text{ kontrol keamanan terpenuhi}}{12 \text{ kontrol keamanan dipersyaratkan}} \times 100\% = 75\%$$

- Area Standar Teknis dan Prosedur Keamanan

$$\frac{55 \text{ kontrol keamanan terpenuhi}}{65 \text{ kontrol keamanan dipersyaratkan}} \times 100\% = 84,61\%$$

Hasil Evaluasi Implementasi Kontrol adalah  $\frac{75\% + 84,61\%}{2} = 79,80\%$

Merujuk penjelasan *passing grade* yang digunakan diatas, maka konklusi Evaluasi Desain Kontrol pada Aplikasi X adalah **Sesuai dengan Desain Kontrol**.

Tahapan evaluasi selanjutnya adalah Evaluasi Efektivitas Kontrol (EFK). Pada tahapan EFK, seluruh kontrol keamanan yang dilakukan

pemeriksaan pada evaluasi desain kontrol diperiksa kembali. harus diuji. Jadi, untuk area Manajemen Keamanan Informasi ada 14 kontrol, sedangkan area Standar Teknis dan Prosedur Keamanan ada 70 kontrol.

Hasil pemeriksaan dalam tahapan evaluasi efektivitas kontrol memberikan status penilaian dalam pemeriksaan kontrol keamanan sebagai berikut:

- 1) Pada Area Manajemen Keamanan Informasi, 7 kontrol keamanan dinyatakan Efektif, 3 kontrol keamanan dinyatakan Perlu Peningkatan, dan 4 kontrol keamanan dinyatakan belum efektif;
- 2) Pada area Standar Teknis dan Prosedur Keamanan, 50 kontrol keamanan dinyatakan Efektif, 10 kontrol dinyatakan Perlu Peningkatan, dan 10 kontrol keamanan dinyatakan belum efektif.

Maka, perhitungan persentase per Area Keamanan sebagai berikut:

- Area Manajemen Keamanan Informasi
$$\frac{10 \text{ kontrol keamanan terpenuhi}}{14 \text{ kontrol keamanan dipersyaratkan}} \times 100\% = 71,42\%$$
- Area Standar Teknis dan Prosedur Keamanan
$$\frac{60 \text{ kontrol keamanan terpenuhi}}{70 \text{ kontrol keamanan dipersyaratkan}} \times 100\% = 85,71\%$$

Hasil Evaluasi Efektivitas Kontrol adalah  $\frac{71,42\% + 85,71\%}{2} = 78,56\%$

Merujuk penjelasan sebelumnya, maka konklusi Evaluasi Efektivitas Kontrol pada Aplikasi X adalah **Perlu Peningkatan**.

Konklusi Audit Keamanan SPBE pada Aplikasi X Instansi A adalah **PERLU PENINGKATAN** yang divisualisasikan alur (path) nya sebagai berikut.

Hasil Evaluasi Desain Kontrol	Hasil Evaluasi Implementasi Kontrol	Hasil Evaluasi Efektivitas Kontrol	Konklusi Hasil Audit
Perlu Peningkatan	Sesuai Desain Kontrol	Perlu Peningkatan	

## B. PENGGUNAAN APLIKASI INSTRUMEN AUDIT KEAMANAN SPBE

Instrumen Audit Keamanan SPBE dirancang dalam bentuk elektronik. Aplikasi instrumen Audit Keamanan SPBE terdiri atas:

1. Cover Instrumen;
2. Rencana Audit (Audit Plan);
3. Pembagian Tugas Tim Auditor Keamanan SPBE;
4. Kontrol Keamanan Area Manajemen Keamanan Informasi (MKI);
5. Kontrol Keamanan Area Standar Teknis dan Prosedur Keamanan (STP);  
dan
6. *Dashboard* Konklusi Audit Keamanan SPBE

Tahapan penggunaan aplikasi instrumen Audit Keamanan SPBE sebagai berikut :

- a. Tahap Persiapan
  - 1) Auditor Keamanan SPBE menyiapkan perangkat kerja seperti komputer / *notebook* yang terinstal aplikasi pengolah kata dan *spreadsheet*;
  - 2) Auditor Keamanan SPBE memastikan perangkat kerja yang digunakan bebas dari virus dan *malware*. Auditor Keamanan SPBE dapat menjalankan proses *scanning* pada aplikasi antivirus yang tertanam pada perangkat kerja terhadap *Operating System* yang digunakan dan *storage* pada perangkat kerja. Jika tidak ada aplikasi antivirus, auditor Keamanan SPBE dapat melakukan instalasi terlebih dahulu atau mengganti perangkat kerja tersebut;
  - 3) Proses persiapan ini dapat dimulai pada saat sebelum kegiatan audit atau pada saat pemahaman desain kontrol untuk melakukan pengisian pada *sheet* Rencana Audit ( Audit Plan )
- b. Tahap Pelaksanaan
  - 1) Auditor Keamanan SPBE membuka dokumen instrumen audit keamanan SPBE .xlsx , dan memulai pekerjaan dengan mempersiapkan informasi - informasi yang dibutuhkan dalam *sheet* Rencana Audit (Audit Plan);
  - 2) Auditor Keamanan SPBE memastikan perangkat kerja yang digunakan bebas dari virus dan *malware*. Auditor Keamanan SPBE dapat menjalankan proses *scanning* pada aplikasi antivirus yang tertanam pada perangkat kerja terhadap *Operating System* yang digunakan dan *storage* pada perangkat kerja. Jika tidak ada aplikasi antivirus, auditor Keamanan SPBE dapat melakukan instalasi terlebih dahulu atau mengganti perangkat kerja tersebut.

- 3) Auditor Keamanan SPBE memulai pengisian pada *sheet* Rencana Audit, Auditor Keamanan SPBE diminta untuk mengisi informasi - informasi sebagai berikut :

a)	Judul Rencana Audit	:	Diisikan informasi nama objek Audit milik Instansi.
b)	Jenis Audit Plan	:	Diisikan objek audit keamanan.
c)	Tanggal Dokumen	:	Diisikan tanggal persetujuan rencana audit dengan auditan.
d)	Nomor Dokumen	:	Diisikan nomor internal pelaksanaan audit oleh lembaga pelaksana audit TIK Pemerintah.
e)	Instansi (auditan)	:	Diisikan Instansi dan Unit kerja yang akan dilakukan audit.
f)	Alamat	:	Diisikan lokasi atau Alamat Auditan yang mengelola atau bertanggung jawab terhadap objek audit.
g)	Kriteria Audit	:	Diisikan peraturan-peraturan yang menjadi kriteria audit.
h)	Ruang lingkup Audit	:	Diisikan objek audit, ruang lingkup pemeriksaan, dan periode pemeriksaan audit.
i)	Tujuan Audit	:	Diisikan tujuan pelaksanaan audit keamanan
j)	<i>Entry Meeting</i>	:	Diisikan hari, dan tanggal mulainya pelaksanaan audit
k)	<i>Exit Meeting</i>	:	Diisikan hari dan tanggal berakhirnya pelaksanaan audit
l)	Serah terima LHAK	:	Diisikan hari dan tanggal penyerahan LHAK
m)	Tim Auditor Keamanan SPBE	:	Diisikan nama ketua Tim Audit, Anggota, Supervisi dan Observer (jika ada kebutuhan)

n)	Tim Audit	:	Diisikan nama personel dari Instansi Audit untuk menjadi Narahubung atau PIC
o)	Catatan Tambahan	:	Diisikan hal-hal lain yang perlu dikomunikasikan oleh auditor Keamanan SPBE dan audit untuk mendukung kelancaran proses pelaksanaan audit yang akan dilaksanakan



### BADAN SIBER DAN SANDI NEGARA

#### AUDIT PLAN (a)

Jenis Audit Plan	(b)	Nomor Dokumen	(d)
Instansi (Audit)	(e)		
Alamat	(f)		
Kriteria Audit	(g)		
Ruang Lingkup Objek Audit	(h)		
Tujuan Audit	(i)		
Entry Meeting	(j)	Tim Auditor Keamanan SPBE :	
Exit Meeting	(k)	Supervisi	(m)
Tim Audit	(n)	Ketua Tim	(m)
Serah Terima Laporan Hasil Audit	(l)	Anggota & Observer	(m)
Catatan tambahan : (o)			
Menyetujui Representative Audit		Tanggal :	
ttd (nama)			Ketua Tim Auditor ttd (nama)
Revisi Audit Plan Representative Audit		Tanggal :	
ttd (nama)			Ketua Tim Auditor ttd (nama)

Gambar Tampilan Sheet Rencana Audit (Audit Plan)

- 4) Pada Sheet kedua yaitu tim Auditor Keamanan SPBE, penggunaan sheet ini dikhkususkan untuk Ketua Tim Audit untuk memberikan penugasan pemeriksaan kontrol keamanan kepada Auditor Keamanan SPBE (anggota tim). Dalam rangka pembagian tugas, Ketua Tim dapat mempertimbangkan kompetensi, spesialisasi dan pemahaman kontrol yang dimiliki oleh anggotanya.

	AREA MANAJEMEN KEAMANAN INFORMASI													
	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14
KETUA TIM														
AUDITOR 1														
AUDITOR 2														
AUDITOR 3														
AUDITOR 4														
AUDITOR 5														

Tabel Tampilan *Sheet* Rencana Audit (Audit Plan)

- 5) *Sheet* ketiga yaitu kontrol keamanan area Manajemen Keamanan Informasi berisi format pengisian yang harus diisi Auditor Keamanan SPBE pada saat dan atau sesudah melaksanakan pemeriksaan terhadap Audit.

Informasi-informasi yang harus diisi dalam *form* ini antara lain:

a)	Penanggung Jawab	:	Diisi nama auditor Keamanan SPBE yang memeriksa kontrol keamanan
b)	Bukti	:	Diisi bukti-bukti yang didapatkan dari audit saat dilaksanakannya prosedur audit. Perolehan bukti yang diisi untuk seluruh tahapan evaluasi keamanan.
c)	Catatan	:	Informasi-informasi yang didapatkan dari jawaban audit saat wawancara dan verifikasi dokumen. Catatan yang dibuat auditor Keamanan SPBE diisi untuk seluruh tahapan evaluasi keamanan.
d)	Status Pemeriksaan	:	Diisi dengan opsi pilihan yang tersedia, yaitu <ul style="list-style-type: none"> <li>- Evaluasi Desain Kontrol, dengan pilihan Sesuai atau Tidak Sesuai</li> <li>- Evaluasi Implementasi Kontrol dengan pilihan</li> </ul>

		Sesuai Implementasi Kontrol atau Tidak Sesuai Implementasi Kontrol - Evaluasi Efektivitas Kontrol dengan pilihan Efektif, Perlu Peningkatan atau Belum Efektif
--	--	---

No.	Peraturan BSSN Nomor 4 Tahun 2021 (Area Manajemen Keamanan Informasi)	PENANGGUNG JAWAB	EVALUASI DESAIN KONTROL			EVALUASI IMPLEMENTASI KONTROL			EVALUASI EFektivitas KONTROL		
			Bukti	Catatan	Status Pemeriksaan	Bukti	Catatan	Status Pemeriksaan	Bukti	Catatan	Status Pemeriksaan
1	Manajemen keamanan informasi SPBE ditetapkan oleh pimpinan Instansi Pusat dan Pemerintah Daerah dikomunikasikan, dilaksanakan, dan dikumentasikan berdasarkan pedoman manajemen keamanan informasi SPBE	[a]	[b]	[c]	Sesuai	[d]	[e]	Sesuai Implementasi Kontrol	[f]	[g]	Efektif
2	Ruang lingkup Manajemen Keamanan Informasi mendefinisikan: a. Isu internal keamanan informasi SPBE dalam Organisasi "area prioritas organisasi yang meliputi : 1) data dan informasi 2) aplikasi SPBE 3) Aset Infrastruktur SPBE 4) Kebijakan keamanan yang telah dimiliki" b. Isu eksternal keamanan informasi SPBE yang sesuai dengan ketentuan perundang-undangan				Tidak Sesuai			Tidak Sesuai Implementasi Kontrol			Perlu Peningkatan
3	"Penanggung jawab keamanan dalam SPBE sesuai dengan pedoman manajemen keamanan informasi SPBE dalam organisasi adalah Sekretaris pada IPFD dan disebut Koordinator SPBE"										

Tabel Tampilan *Sheet* Penilaian dalam pemeriksaan untuk kontrol keamanan area Manajemen Keamanan Informasi

- 6) *Sheet* keempat yaitu kontrol keamanan pada area Standar Teknis dan Prosedur Keamanan berisi format pengisian yang harus diisi Auditor Keamanan SPBE pada saat dan atau sesudah melaksanakan pemeriksaan dan pengujian keamanan terhadap objek audit. Informasi-informasi yang harus diisi dalam *form* ini antara lain:

a)	Penanggung Jawab	:	Diisikan nama auditor Keamanan SPBE yang memeriksa kontrol keamanan
b)	Bukti	:	Diisikan bukti-bukti yang didapatkan dari auditan saat dilaksanakannya prosedur audit. Perolehan bukti yang diisi untuk seluruh tahapan evaluasi keamanan.

c)	Catatan	:	Informasi-informasi yang didapatkan dari jawaban audit saat wawancara dan verifikasi dokumen. Catatan yang dibuat auditor Keamanan SPBE diisi untuk seluruh tahapan evaluasi keamanan.
d)	Status Pemeriksaan	:	<p>Diisikan dengan opsi pilihan yang tersedia, yaitu</p> <ul style="list-style-type: none"> <li>- Evaluasi Desain Kontrol, dengan pilihan Sesuai atau Tidak Sesuai</li> <li>- Evaluasi Implementasi Kontrol dengan pilihan Sesuai Implementasi Kontrol atau Tidak Sesuai Implementasi Kontrol</li> <li>- Evaluasi Efektivitas Kontrol dengan pilihan Efektif, Perlu Peningkatan atau Belum Efektif</li> </ul>

No.	Peraturan BSSN Nomor 4 Tahun 2021 (Area Standar Teknis dan Prosedur Keamanan SPBE)	PENANGGUNG JAWAB	EVALUASI DESAIN KONTROL			EVALUASI IMPLEMENTASI KONTROL			EVALUASI EFektivitas KONTROL		
			Bukti	Catatan	Status Pemeriksaan	Bukti	Catatan	Status Pemeriksaan	Bukti	Catatan	Status Pemeriksaan
1	Kontrol 1 Menggunakan manajemen kata sandi untuk proses autentikasi	(a)	(b)	(c)	Sesuai	(d)	(e)	Sesuai Implementasi Kontrol	(f)	(g)	Belum Efektif
2	Kontrol 2 Menerapkan verifikasi kata sandi pada sisi server.										
3	Kontrol 3 Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;										

Tabel Tampilan *Sheet* Penilaian dalam pemeriksaan untuk kontrol keamanan area Standar Teknis dan Prosedur Keamanan

- 7) *Sheet* kelima menunjukkan *dashboard* status pemeriksaan dari evaluasi desain kontrol, evaluasi implementasi kontrol, dan evaluasi efektivitas kontrol keamanan yang telah diotomatisasi.

MATRIKS KESIMPULAN AUDIT KEAMANAN SPBE				HASIL KESIMPULAN AUDIT KEAMANAN SPBE APLIKASI [X]			
HASIL EVALUASI DESAIN KONTROL	HASIL EVALUASI IMPLEMENTASI KONTROL	HASIL EVALUASI EFektivitas KONTROL	KESIMPULAN AUDIT	HASIL EVALUASI DESAIN KONTROL	HASIL EVALUASI IMPLEMENTASI KONTROL	HASIL EVALUASI EFektivitas KONTROL	KESIMPULAN AUDIT
Memadai	Sesuai dengan Desain Kontrol	Efektif	Memadai	Memadai	Sesuai dengan Desain Kontrol	Perlu Peningkatan	MEMADAI
		Perlu Peningkatan	Memadai				
	Tidak Sesuai dengan Desain Kontrol	Belum Efektif	Perlu Peningkatan				
		Efektif	Perlu Peningkatan				
Perlu Peningkatan	Sesuai dengan Desain Kontrol	Perlu Peningkatan	Tidak Memadai	-	Perlu Peningkatan	Belum Efektif	-
		Belum Efektif	Tidak Memadai				
	Tidak Sesuai dengan Desain Kontrol	Efektif	Tidak Memadai				
		Perlu Peningkatan	Tidak Memadai				
Tidak Memadai	-	Belum Efektif	Tidak Memadai	-	Perlu Peningkatan	Efektif	-
		Efektif	Tidak Memadai				
		Perlu Peningkatan	Tidak Memadai				
Penetapan Kesimpulan Audit dilakukan berdasarkan pada jumlah hasil evaluasi dengan bobot sebagai berikut:							
Memadai > 90%	Perlu Peningkatan 41% - 90%	Tidak Memadai < 40%					

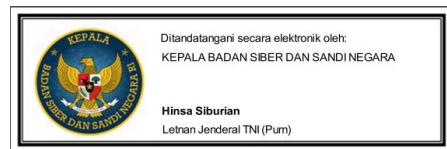
Tabel Tampilan *Sheet Dashboard* Konklusi Audit Keamanan

### c. Tahap Pengakhiran

Setelah auditor Keamanan SPBE memastikan bahwa semua langkah-langkah penggunaan instrumen ini dilaksanakan, penyimpanan hasil pemeriksaan dalam rangka Audit Keamanan SPBE disimpan dengan memberikan nama file “<tahun.bulan>spasi Instrumen Audit spasi <nama instansi>\_<unit kerja instansi>\_<jenis audit>\_<objek audit>.

Contoh : **2024.03 Instrumen Audit Kemenpari\_Pusdatin\_Aplikasi khusus\_Mail Internal**

KEPALA BADAN SIBER DAN SANDI NEGARA,



HINSA SIBURIAN