MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 24 TAHUN 2022
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA NASIONAL INDONESIA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG AUDIT KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KETENAGAKERJAAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 31 Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia, perlu menetapkan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Audit Keamanan Informasi;

b. bahwa Rancangan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Audit Keamanan Informasi telah disepakati melalui Konvensi Nasional pada 24-25 November 2021 di Jakarta;

KODE UNIT : **J.62AKI00.005.1**

JUDUL UNIT : **Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Organisasi**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam memerinci dan menguji kendali organisasi sesuai dengan kriteria.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memerinci kendali organisasi keamanan informasi	1.1 **Kendali organisasi keamanan informasi** diidentifikasi sesuai dengan prosedur Audit Keamanan Informasi (AKI). 1.2 Kendali organisasi keamanan informasi dijabarkan sesuai kondisi.
2. Menguji kendali organisasi keamanan informasi	2.1 **Bukti kendali** organisasi keamanan informasi dikumpulkan sesuai dengan prosedur AKI. 2.2 Bukti kendali organisasi keamanan informasi dievaluasi sesuai dengan kriteria.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kendali organisasi keamanan informasi, sebagaimana merujuk pada ISO/IEC 27002 terdiri dari:
      1.1.1 Kendali tata kelola keamanan informasi
      1.1.2 Kendali manajemen aset
      1.1.3 Kendali manajemen data/informasi
      1.1.4 Kendali manajemen akses
      1.1.5 Kendali manajemen kerjasama dengan pihak ketiga
      1.1.6 Kendali manajemen insiden
      1.1.7 Kendali kelangsungan bisnis
      1.1.8 Kendali atas aspek regulasi.

1.2 Bukti kendali adalah bukti adanya proses, kebijakan, perangkat, praktik, aksi atau kondisi yang digunakan untuk mempertahankan atau memodifikasi risiko.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak alat bantu audit
   2.2 Perlengkapan
      2.2.1 Kertas kerja pelaksanaan prosedur AKI terhadap kendali organisasi keamanan informasi

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      4.1.1 Prinsip-prinsip AKI
      4.1.2 Kode etik auditor keamanan informasi
   4.2 Standar
      4.2.1 SNI ISO/IEC 27001 Sistem Manajemen Keamanan Informasi.
      4.2.2 SNI ISO/IEC 27002 Teknologi informasi - Teknik keamanan - Panduan praktik kendali keamanan informasi
      4.2.3 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen
      4.2.4 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)
      4.2.5 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)
      4.2.6 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.2 Penilaian kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.
   1.4 Metode penilaian yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Keamanan informasi
      3.1.2 Manajemen keamanan informasi
      3.1.3 Audit keamanan informasi
      3.1.4 Pengujian kendali organisasi keamanan informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan identifikasi dan penjabaran kendali organisasi keamanan informasi
   4.2 Objektif dalam evaluasi bukti kendali organisasi keamanan informasi

4.3 Komunikatif dalam pengumpulan dan evaluasi bukti kendali organisasi keamanan informasi

5. Aspek kritis
   5.1 Ketepatan dalam mengevaluasi bukti kendali organisasi keamanan informasi sesuai dengan kriteria

KODE UNIT : **J.62AKI00.006.1**

JUDUL UNIT : **Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Teknologi**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam memerinci dan menguji kendali teknologi sesuai dengan kriteria.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memerinci kendali teknologi keamanan informasi	1.1 **Kendali teknologi keamanan informasi** diidentifikasi sesuai dengan prosedur Audit Keamanan Informasi (AKI). 1.2 Kendali teknologi keamanan informasi dijabarkan sesuai kondisi.
2. Menguji kendali teknologi keamanan informasi	2.1 **Bukti kendali** teknologi keamanan informasi dikumpulkan sesuai dengan prosedur AKI. 2.2 Bukti kendali teknologi keamanan informasi dievaluasi sesuai dengan kriteria.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kendali teknologi informasi yang dimaksud sebagaimana merujuk kepada ISO/IEC 27002 terdiri dari:
      1.1.1 Kendali manajemen siklus pengembangan sistem
      1.1.2 Kendali manajemen kerentanan keamanan informasi
      1.1.3 Kendali manajemen pengelolaan log
      1.1.4 Kendali manajemen pengelolaan jaringan.
   1.2 Bukti kendali adalah bukti adanya proses, kebijakan, perangkat, praktik, aksi, atau kondisi yang digunakan untuk mempertahankan atau memodifikasi risiko.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak alat bantu audit

2.2 Perlengkapan

2.2.1 Kertas kerja pelaksanaan prosedur AKI terhadap kendali teknologi keamanan informasi

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

4.1.1 Prinsip-prinsip AKI

4.1.2 Kode etik auditor keamanan informasi

4.2 Standar

4.2.1 SNI ISO/IEC 27001 Sistem Manajemen Keamanan Informasi

4.2.2 SNI ISO/IEC 27002 Teknologi informasi - Teknik keamanan - Panduan praktik kendali keamanan informasi

4.2.3 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen

4.2.4 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)

4.2.5 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)

4.2.6 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Penilaian kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

1.4 Metode penilaian yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Keamanan informasi
      3.1.2 Manajemen keamanan informasi
      3.1.3 Audit keamanan informasi
      3.1.4 Pengujian pengendalian teknologi keamanan informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan identifikasi dan penjabatan kendali teknologi keamanan informasi
   4.2 Objektif dalam evaluasi bukti kendali teknologi keamanan informasi
   4.3 Komunikatif pengumpulan dan evaluasi bukti kendali teknologi keamanan informasi

5. Aspek kritis
   5.1 Ketepatan dalam mengevaluasi bukti kendali teknologi keamanan informasi sesuai dengan kriteria

KODE UNIT : **J.62AKI00.007.1**

JUDUL UNIT : **Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Fisik**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan prosedur Audit Keamanan Informasi (AKI) terhadap kendali fisik.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memerinci kendali fisik terkait keamanan informasi	1.1 **Kendali fisik keamanan informasi** diidentifikasi sesuai dengan prosedur AKI. 1.2 Kendali fisik keamanan informasi dijabarkan sesuai kondisi.
2. Menguji kendali fisik terkait keamanan informasi	2.1 **Bukti kendali** fisik keamanan informasi dikumpulkan sesuai dengan prosedur AKI. 2.2 Bukti kendali fisik keamanan informasi dievaluasi sesuai dengan kriteria.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kendali fisik keamanan informasi yang dimaksud sebagaimana merujuk pada ISO/IEC 27002 terdiri dari:
      1.1.1 Perimeter keamanan fisik
      1.1.2 Kendali entri fisik
      1.1.3 Mengamankan kantor, ruangan dan fasilitas
      1.1.4 Pemantauan keamanan fisik
      1.1.5 Melindungi dari ancaman fisik dan lingkungan
      1.1.6 Bekerja di area aman
      1.1.7 Meja bersih dan layar bersih
      1.1.8 Penempatan dan perlindungan peralatan
      1.1.9 Keamanan aset di luar lokasi
      1.1.10 Media penyimpanan
      1.1.11 Utilitas pendukung
      1.1.12 Keamanan pengkabelan

1.1.13 Pemeliharaan peralatan

1.1.14 Disposal atau penggunaan kembali peralatan secara aman.

1.2 Bukti kendali adalah bukti adanya proses, kebijakan, perangkat, praktik, aksi atau kondisi yang digunakan untuk mempertahankan atau memodifikasi risiko.

2. Peralatan dan perlengkapan

2.1 Peralatan

2.1.1 Perangkat komputasi

2.1.2 Perangkat lunak alat bantu audit

2.2 Perlengkapan

2.2.1 Kertas kerja pelaksanaan prosedur AKI terhadap kendali fisik keamanan informasi

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

4.1.1 Prinsip-prinsip AKI

4.1.2 Kode etik auditor keamanan informasi

4.2 Standar

4.2.1 SNI ISO/IEC 27001 Sistem Manajemen Keamanan Informasi

4.2.2 SNI ISO/IEC 27002 Teknologi informasi - Teknik keamanan - Panduan praktik kendali keamanan informasi

4.2.3 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen

4.2.4 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)

4.2.5 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)

4.2.6 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.
   1.2 Penilaian kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.
   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.
   1.4 Metode penilaian yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Keamanan informasi
      3.1.2 Manajemen keamanan informasi
      3.1.3 Audit keamanan informasi
      3.1.4 Pengujian pengendalian fisik keamanan informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan identifikasi kendali fisik keamanan informasi
   4.2 Objektif dalam evaluasi kendali fisik keamanan informasi
   4.3 Komunikatif dalam pengumpulan dan evaluasi kendali fisik keamanan informasi

5. Aspek kritis
    5.1 Ketepatan dalam mengidentifikasi kendali keamanan fisik keamanan informasi sesuai dengan prosedur AKI

KODE UNIT : **J.62AKI00.008.1**

JUDUL UNIT : **Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Personel**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melaksanakan prosedur Audit Keamanan Informasi (AKI) terhadap kendali personel.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memerinci kendali personel terkait keamanan informasi	1.1 **Kendali personel keamanan informasi** diidentifikasi sesuai dengan prosedur AKI. 1.2 Kendali personel keamanan informasi dijabarkan sesuai kondisi.
2. Menguji kendali personel terkait keamanan informasi	2.1 **Bukti kendali** personel keamanan informasi dikumpulkan sesuai dengan prosedur AKI. 2.2 Bukti kendali personel keamanan informasi dievaluasi sesuai dengan kriteria.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kendali personel keamanan informasi yang dimaksud sebagaimana merujuk pada ISO/IEC 27002 terdiri dari:
      1.1.1 Kendali pada proses rekruitmen personel
      1.1.2 Kendali pada masa kerja personel
      1.1.3 Kendali pada penghentian masa kerja dan perubahan tanggung jawab kerja personel.
   1.2 Bukti kendali adalah bukti adanya proses, kebijakan, perangkat, praktik, aksi atau kondisi yang digunakan untuk mempertahankan atau memodifikasi risiko.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak alat bantu audit

2.2 Perlengkapan

2.2.1 Kertas kerja pelaksanaan prosedur AKI terhadap kendali personel keamanan informasi

3. Peraturan yang diperlukan

(Tidak ada.)

4. Norma dan standar

4.1 Norma

4.1.1 Prinsip-prinsip AKI

4.1.2 Kode etik auditor keamanan informasi

4.2 Standar

4.2.1 SNI ISO/IEC 27001 Sistem Manajemen Keamanan Informasi

4.2.2 SNI ISO/IEC 27002 Teknologi informasi - Teknik keamanan - Panduan praktik kendali keamanan informasi

4.2.3 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen

4.2.4 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)

4.2.5 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)

4.2.6 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian

1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Penilaian kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

1.4 Metode penilaian yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Keamanan informasi
      3.1.2 Manajemen keamanan informasi
      3.1.3 Audit keamanan informasi
      3.1.4 Pengujian pengendalian personel keamanan informasi
      3.1.5 Pengetahuan aspek hukum tentang ketenagakerjaan
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan identifikasi kendali personal keamanan informasi
   4.2 Objektif dalam evaluasi kendali personel keamanan informasi
   4.3 Komunikatif dalam pengumpulan dan evaluasi kendali personel keamanan informasi

5. Aspek kritis
   5.1 Ketepatan dalam mengidentifikasi kendali personel keamanan informasi sesuai prosedur AKI

KODE UNIT : **J.62AKI00.009.1**

JUDUL UNIT : **Membuat Kertas Kerja Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam membuat kertas kerja Audit Keamanan Informasi (AKI).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyiapkan kertas kerja AKI	1.1 Rancangan **kertas kerja AKI** ditentukan sesuai prosedur AKI. 1.2 Kertas kerja AKI disusun sesuai dengan rancangan.
2. Mengisi kertas kerja AKI	2.1 **Aktivitas AKI** diidentifikasi sesuai dengan Prosedur AKI. 2.2 Kertas kerja AKI diisi berdasarkan aktivitas prosedur AKI.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kertas Kerja AKI adalah dokumentasi yang berisi kumpulan data dan informasi terkait prosedur AKI, aktivitas prosedur AKI yang telah dijalankan, serta bukti AKI yang didapatkan dari pelaksanaan prosedur AKI yang kemudian dianalisis untuk menjadi dasar dalam penyusunan temuan, rekomendasi, dan kesimpulan AKI.
   1.2 Aktivitas AKI adalah kegiatan yang diperlukan untuk melaksanakan prosedur AKI terhadap suatu kendali.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak alat bantu audit
   2.2 Perlengkapan
      2.2.1 Kertas kerja AKI

3. Peraturan yang diperlukan

   (Tidak ada.)

4. Norma dan standar

   4.1 Norma

      4.1.1 Prinsip-prinsip AKI

      4.1.2 Kode etik auditor keamanan informasi

   4.2 Standar

      4.2.1 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen

      4.2.2 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)

      4.2.3 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)

      4.2.4 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Audit keamanan informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam menyiapkan dan mengisi kertas kerja AKI
   4.2 Objektif dalam menyiapkan dan mengisi kertas kerja AKI
   4.3 Asertif dalam menyiapkan dan mengisi kertas kerja AKI

5. Aspek kritis

   Ketepatan dalam menyusun kertas kerja AKI sesuai dengan rancangan

KODE UNIT : **J.62AKI00.010.1**

JUDUL UNIT : **Membuat Dokumentasi Bukti Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam membuat dokumentasi bukti Audit Keamanan Informasi (AKI).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memperoleh bukti AKI	1.1 **Bukti AKI** diidentifikasi sesuai aktivitas AKI. 1.2 **Sumber bukti AKI** diidentifikasi sesuai aktivitas AKI. 1.3 Bukti AKI dikumpulkan sesuai aktivitas AKI.
2. Mendokumentasikan bukti AKI	2.1 **Sistematika bukti AKI** disusun sesuai dengan standar yang berlaku. 2.2 **Dokumentasi bukti AKI** dibuat sesuai dengan sistematika. 2.3 Dokumentasi bukti AKI diarsipkan sesuai dengan standar yang berlaku.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Bukti AKI adalah seluruh data dan informasi yang digunakan oleh auditor keamanan informasi untuk mendukung argumentasi, pendapat, atau simpulan dan rekomendasinya dalam meyakinkan tingkat kesesuaian antara kondisi dengan kriterianya. Jenis bukti AKI dapat berupa bukti fisik, dokumentasi, analisis, performansi ulang.
   1.2 Sumber bukti AKI adalah sistem, proses, aktivitas, prosedur, atau objek lainnya yang menjadi asal dalam perolehan bukti AKI.
   1.3 Sistematika bukti AKI adalah susunan, urutan, klasifikasi, dan pengelompokkan tertentu yang digunakan dalam mendokumentasikan bukti AKI.

1.4 Dokumentasi bukti AKI adalah catatan atau rekaman terhadap bukti AKI pada suatu media tertentu yang digunakan untuk menggambarkan dan menjelaskan bukti AKI yang diperoleh.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak alat bantu audit
   2.2 Perlengkapan
      2.2.1 Kertas kerja perolehan dan pendokumentasian bukti AKI

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      4.1.1 Prinsip-prinsip AKI
      4.1.2 Kode etik auditor keamanan informasi
   4.2 Standar
      4.2.1 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen
      4.2.2 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)
      4.2.3 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)
      4.2.4 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen, serta jadwal asesmen.

1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja dan/atau Tempat Uji Kompetensi (TUK) dan/atau pada tempat yang disimulasikan.

1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan.

1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan wawancara, serta metode lain yang relevan.

2. Persyaratan kompetensi

(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan

3.1 Pengetahuan

3.1.1 Manajemen keamanan informasi

3.1.2 Pengendalian keamanan informasi

3.1.3 Audit keamanan informasi

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan

4.1 Teliti dalam memperoleh dan mendokumentasikan bukti AKI

4.2 Objektif dalam memperoleh dan mendokumentasikan bukti AKI

4.3 Asertif dalam memperoleh dan mendokumentasikan bukti AKI

5. Aspek kritis

5.1 Ketepatan dalam membuat dokumentasi bukti AKI sesuai dengan sistematika

KODE UNIT : **J.62AKI00.020.1**

JUDUL UNIT : **Mengumpulkan Bukti Pelaksanaan Tindak Lanjut Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengkaji dan memperoleh bukti pelaksanaan tindak lanjut rekomendasi Audit Keamanan Informasi (AKI) yang telah disepakati.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengkaji bentuk tindak lanjut atas rekomendasi AKI	1.1 **Tindak lanjut** rekomendasi AKI diidentifikasi berdasarkan laporan AKI. 1.2 Tindak lanjut rekomendasi AKI dipertimbangkan sesuai dengan rekomendasi.
2. Memperoleh bukti tindak lanjut rekomendasi AKI	2.1 **Bukti tindak lanjut** rekomendasi AKI diidentifikasi berdasarkan rekomendasi AKI. 2.2 Bukti tindak lanjut atas rekomendasi AKI didokumentasikan sesuai dengan prosedur AKI.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Tindak lanjut rekomendasi AKI adalah tindakan yang dilakukan auditan atau pihak terkait atas dasar rekomendasi AKI yang disepakati yang dapat berupa tindakan korektif maupun preventif.
   1.2 Bukti tindak lanjut rekomendasi AKI merupakan dokumentasi tindakan yang telah dilakukan auditan atau pihak terkait.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak alat bantu audit
   2.2 Perlengkapan
      2.2.1 Kertas kerja pemantauan tindak lanjut rekomendasi AKI

3. Peraturan yang diperlukan

   (Tidak ada.)

4. Norma dan standar

   4.1 Norma

      4.1.1 Prinsip-prinsip audit

      4.1.2 Kode etik auditor keamanan informasi

   4.2 Standar

      4.2.1 SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen

      4.2.2 *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA)

      4.2.3 *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA)

      4.2.4 Standar Audit Sistem Informasi (SASI) dari Ikatan Audit Sistem Informasi Indonesia (IASII)

PANDUAN PENILAIAN

1. Konteks penilaian

   1.1 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, tempat asesmen serta jadwal asesmen.

   1.2 Pelaksanaan asesmen kompetensi pada unit ini dapat dilakukan di tempat kerja/Tempat Uji Kompetensi (TUK)/pada tempat yang disimulasikan.

   1.3 Asesi/peserta harus dilengkapi dengan peralatan/perlengkapan, dokumen, bahan serta fasilitasi asesmen yang dibutuhkan.

   1.4 Metode asesmen yang diterapkan dapat meliputi kombinasi dari metode tes lisan, tes tertulis, observasi tempat kerja/demonstrasi/simulasi, verifikasi bukti/portofolio dan/atau wawancara serta metode lain yang relevan.

2. Persyaratan kompetensi

   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
    3.1 Pengetahuan
        3.1.1 Keamanan informasi
        3.1.2 Manajemen keamanan informasi
        3.1.3 Pengendalian keamanan informasi
        3.1.4 Audit keamanan informasi
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
    4.1 Ketelitian dalam menganalisis rekomendasi AKI
    4.2 Asertif dalam mendapatkan bukti tindak lanjut rekomendasi AKI
    4.3 Independensi dalam menganalisis rekomendasi AKI
    4.4 Obyektifitas mendapatkan bukti tindak lanjut rekomendasi AKI

5. Aspek kritis
    5.1 Ketepatan dalam mengidentifikasi bukti tindak lanjut rekomendasi AKI berdasarkan rekomendasi AKI