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;

c. bahwa sesuai surat a.n. Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi, Badan Siber dan Sandi Negara Nomor 4708/BSSN/D1/PP.01.06/12/2021 tanggal 7 Desember 2021 perihal permohonan Penetapan 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;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Keputusan Menteri Ketenagakerjaan 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;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 39, Tambahan Lembaran Negara Republik Indonesia Nomor 4279);

2. Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

3. Peraturan Pemerintah Nomor 31 Tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4637);

4. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);

5. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);

6. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);
7. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);
8. Peraturan Menteri Ketenagakerjaan Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Ketenagakerjaan (Berita Negara Republik Indonesia Tahun 2021 Nomor 108);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN MENTERI KETENAGAKERJAAN 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.

KESATU : 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, sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Menteri ini.

KEDUA : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

KETIGA : Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dan penyusunan jenjang kualifikasi nasional sebagaimana dimaksud dalam Diktum KEDUA ditetapkan oleh Badan Siber dan Sandi Negara dan/atau kementerian/lembaga teknis terkait sesuai dengan tugas dan fungsinya.

KEEMPAT : Standar Kompetensi Kerja Nasional Indonesia sebagaimana dimaksud dalam Diktum KESATU dikaji ulang setiap 5 (lima) tahun atau sesuai dengan kebutuhan.

KELIMA : Keputusan Menteri ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 14 Maret 2022
MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
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 (AKI)

BAB I
PENDAHULUAN

A. Latar Belakang

Pesatnya perkembangan teknologi dan informasi membuat keamanan informasi menjadi prioritas utama dalam organisasi modern. Keamanan informasi bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan nirsangkal dari pengelolaan informasi. Tidak dapat dipungkiri lagi bahwa informasi merupakan salah satu aset berharga dari sebuah organisasi yang harus dilindungi dari berbagai ancaman, baik eksternal maupun internal.

Mengingat risiko ancaman serangan keamanan informasi yang terus meningkat setiap tahunnya, organisasi perlu mengembangkan pemahaman di lingkungannya terkait manajemen keamanan informasi untuk setiap proses di dalam organisasi. Keamanan informasi adalah prioritas utama bagi organisasi yang telah menerapkan teknologi informasi ke dalam proses bisnis dan merupakan tanggung jawab semua pihak yang terkait dengan organisasi. Setiap pihak memiliki perannya masing-masing dalam mengendalikan keamanan informasi untuk pemenuhan tujuan keamanan informasi. Kesuksesan organisasi dalam implementasi manajemen keamanan informasi bergantung kepada efektifitas dari kendali keamanan informasi pada organisasi tersebut, yang berujung kepada pencapaian tujuan organisasi.

Sebuah proses yang dinamakan Audit Keamanan Informasi (AKI) diperlukan untuk mendapatkan keyakinan yang memadai atas

kesesuaian kondisi dengan kriteria kendali keamanan informasi. Audit Keamanan Informasi, yang selanjutnya disingkat AKI, adalah suatu proses sistematis untuk memperoleh keyakinan yang memadai bahwa penerapan kendali keamanan informasi pada suatu organisasi telah dilakukan sesuai dengan kriteria yang ditentukan.

Menurut SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen, sebuah audit harus dilakukan dengan mematuhi prinsip integritas, adil, profesional, kerahasiaan, independen, dan berbasis bukti. Prinsip integritas diwujudkan melalui kejujuran, kepatuhan terhadap hukum yang berlaku, kecukupan kompetensi, ketekunan, dan kepekaan terhadap lingkungan sekitar. Prinsip adil diwujudkan dengan keakuratan, tepat waktu, jelas, lengkap, objektif, dan tidak memihak. Prinsip profesional dapat dilakukan melalui penjagaan mutu dan kualitas hasil berdasarkan analisis dan hasil kesimpulan dari audit dengan kompetensi yang memadai. Prinsip kerahasiaan dilakukan melalui perlindungan terhadap informasi agar hanya dapat diakses oleh pihak yang berwenang dan terhindar dari kebocoran dan penyalahgunaan untuk kepentingan tertentu. Prinsip independen dilakukan melalui sikap yang netral (tidak memihak siapapun dan apapun), bebas konflik kepentingan dan objektif dari hasil kesimpulan audit berdasarkan bukti audit yang terlampir. Berbasis bukti dilakukan dengan penggunaan metode rasional, sistematis, kecukupan sampel, dan terverifikasi dengan baik.

Auditor keamanan informasi harus memiliki kompetensi yang memadai untuk dapat melakukan AKI mulai dari tahap perencanaan, pelaksanaan, pengawasan, dan pelaporan AKI sesuai standar audit dan kode etik auditor serta untuk dapat menerapkan prinsip-prinsip audit tersebut. Kompetensi auditor keamanan informasi dapat dimiliki secara individu oleh seorang auditor, maupun secara kombinasi dari beberapa peran dalam sebuah tim AKI. Beberapa peran dalam tim AKI dapat disesuaikan dengan kebutuhan, seperti Asisten Auditor, Auditor, dan Supervisor.

Atas dasar pertimbangan di atas, Badan Siber dan Sandi Negara (BSSN) mendorong berbagai upaya yang diperlukan untuk membangun

skema kompetensi dalam pelaksanaan AKI yang dapat diterima secara luas oleh semua organisasi maupun industri. Standar kompetensi AKI diharapkan dapat menjadi panduan bagi organisasi maupun industri dalam mendapatkan pengakuan kompetensi terkait Auditor Keamanan Informasi, baik di sektor pemerintahan maupun swasta di berbagai sektor industri.

Proses pengembangan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang AKI merujuk kepada berbagai metodologi AKI yang berlaku saat ini. Berbagai rujukan tersebut dijadikan sebagai acuan dalam pembuatan SKKNI AKI. Beberapa rujukan yang digunakan, antara lain SNI ISO 19011:2018 Pedoman Audit Sistem Manajemen, *Information Technology Audit Framework* (ITAF) dari *Information System Audit and Control Association* (ISACA), dan *International Professional Practice Framework* (IPPF) dari *The Institute of Internal Audit* (IIA).

Regulasi yang mendasari kebutuhan Audit Keamanan Informasi antara lain sebagai berikut :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir pada Undang-Undang Nomor 19 Tahun 2016.
2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagaimana diubah terakhir pada Peraturan Pemerintah Nomor 71 Tahun 2019.
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
4. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik.
5. 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.
6. Peraturan Bank Indonesia Nomor 23/7/PBI/2021 tentang Penyelenggara Infrastruktur Sistem Pembayaran.

7. Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran.
8. Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 2 Tahun 2020 tentang Perubahan Kedua atas Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (*Crypto Asset*) di Bursa Berjangka.

B. Pengertian

1. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari organisasi.
2. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
3. Audit Keamanan Informasi yang selanjutnya disebut AKI adalah proses yang sistematis, independen, dan terdokumentasi dalam memperoleh dan mengevaluasi bukti penerapan Keamanan Informasi secara objektif untuk menentukan sejauh mana kesesuaiannya dengan kriteria dan/atau standar yang telah ditetapkan.
4. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan audit Keamanan Informasi.
5. Auditan adalah keseluruhan atau sebagian dari organisasi yang diaudit.
6. Prosedur AKI adalah instruksi AKI terdiri dari langkah-langkah yang harus dilakukan untuk dapat menyelesaikan AKI, seperti: peroleh dokumen, evaluasi desain kendali, uji kendali, uji terinci dan lainnya.

C. Penggunaan SKKNI

Standar Kompetensi dibutuhkan oleh beberapa lembaga/institusi yang berkaitan dengan pengembangan sumber daya manusia, sesuai dengan kebutuhan masing- masing:

1. Untuk institusi pendidikan dan pelatihan
    a. Memberikan informasi untuk pengembangan program dan kurikulum.
    b. Sebagai acuan dalam penyelenggaraan pelatihan, penilaian, dan sertifikasi.
2. Untuk dunia usaha/industri dan pengguna tenaga kerja
    a. Membantu dalam rekrutmen.
    b. Membantu penilaian unjuk kerja.
    c. Membantu dalam menyusun uraian jabatan.
    d. Membantu dalam mengembangkan program pelatihan yang spesifik berdasar kebutuhan dunia usaha/industri.
3. Untuk institusi penyelenggara pengujian dan sertifikasi
    a. Sebagai acuan dalam merumuskan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya.
    b. Sebagai acuan dalam penyelenggaraan pelatihan penilaian dan sertifikasi.

D. Komite Standar Kompetensi

Susunan komite standar kompetensi pada Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Bidang Audit Keamanan Informasi melalui keputusan Kepala Badan Siber dan Sandi Negara Nomor 394.1 Tahun 2021 tentang Pembentukan Komite, Tim Perumus, Tim Verifikasi, dan Sekretariat Penyusunan Standar Kompetensi Kerja Nasional Indonesia Area Fungsi Keamanan Siber Tahun Anggaran 2021 tanggal 1 Oktober 2021 dapat dilihat pada Tabel 1.

Tabel 1. Susunan komite standar kompetensi SKKNI Bidang Audit Keamanan Informasi

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Dono Indarto, S.IK., M.H.	Badan Siber dan Sandi Negara	Pengarah

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
2.	Mohamad Ikro, S.Si., M.Si.	Badan Siber dan Sandi Negara	Ketua
3.	Asri Setyowati, S.Si., M.M.	Badan Siber dan Sandi Negara	Sekretaris
4.	Wida Sandrayanti, S.E.	Badan Siber dan Sandi Negara	Anggota
5.	Soetedjo Joewono, S.E, M.M.	Badan Siber dan Sandi Negara	Anggota
6.	M.Novel Ariyadi, S.T., MPM, CDPSE	Indonesia Cyber Security Forum (ICSF)	Anggota
7.	Dr. Ayi Purbasari, M.T.	Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM)	Anggota

Tabel 2. Susunan Tim Perumus SKKNI Bidang Audit Keamanan Informasi

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Prof. DR. Ir. Eko Kuswardono Budiardjo, M.Sc.	Universitas Indonesia	Pengarah
2.	Chandra Yulistia, CISA CISM.	Ikatan Auditor Sistem Informasi Indonesia (IASII)	Ketua
3.	Harun Al Rasyid, , CISA, CDPSE, COBIT5-F, COBIT2019-F, CSX-F, ISO27001-LA (ISACA ID CH)	ISACA Indonesia Chapter	Sekretaris
4.	Dr. rer. nat. I Made Wiryana, S.Si., S.Kom., M.Sc.	Universitas Gunadarma	Anggota

NO	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
5.	Tri Achmadi, Ak., CA, CIA, CISA, CGEIT	Inspektorat Jenderal Kementerian Keuangan	Anggota
6.	Drajad Wiryawan, S.E., M.M., CEH., CHFI	BINUS University	Anggota
7.	Anwar Siregar	PT CBQA Global Indonesia	Anggota
8.	Yullyan, CIA	Indonesia Financial Group (IFG)	Anggota
9.	Ade Firman Triangga, CISA, CSX-F, CEH, ECSA, eMAPT, CCNA Cyber Ops, OFCE	Cyber Defense Community (CDEF)	Anggota
10.	I Made Mustika Kerta Astawa, S.ST.	Asosiasi Fungsional Sandiman Indonesia	Anggota
11.	Furqoni, S.Kom., M.M., LA-27001	PT Collega Inti Pratama	Anggota
12.	Muhammad Yusuf Bambang Setiadji, S.ST, M.Kom.	Politeknik Siber dan Sandi Negara (PSSN)	Anggota

Tabel 3. Susunan Tim verifikasi SKKNI Bidang Audit Keamanan Informasi

NO	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Lucia Sri Istiyowati, M.Kom.	Perbanas Institute	Ketua
2.	Ir. Siswanto, M.M., M.Kom.	Universitas Budi Luhur/Ikatan Ahli Informatika Indonesia (IAII)	Anggota
3.	Irmawanti, S.E.	Badan Siber dan Sandi Negara	Anggota

NO	NAMA	INSTANSI/ LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
4.	Wuri Handayani, S.Tr.TP.	Badan Siber dan Sandi Negara	Anggota

BAB II
STANDAR KOMPETENSI KERJA NASIONAL INDONESIA

A. Pemetaan Standar Kompetensi

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
Memperoleh keyakinan yang memadai bahwa penerapan kendali keamanan informasi pada suatu organisasi telah dilakukan sesuai dengan kriteria yang ditentukan	Merencanakan Audit Keamanan Informasi (AKI)	Menyusun rencana Audit Keamanan Informasi (AKI)	Menentukan tujuan dan lingkup Audit Keamanan Informasi (AKI)
			Melakukan analisis risiko Audit Keamanan Informasi (AKI)
		Menyusun kebutuhan sumber daya Audit Keamanan Informasi (AKI)	Membuat prosedur Audit Keamanan Informasi (AKI)
			Menentukan kebutuhan sumber daya Audit Keamanan Informasi (AKI)
	Melaksanakan Audit Keamanan Informasi (AKI)	Menjalankan prosedur Audit Keamanan Informasi (AKI)	Melaksanakan prosedur Audit Keamanan Informasi (AKI) terhadap kendali organisasi
			Melaksanakan prosedur Audit Keamanan Informasi (AKI) terhadap kendali teknologi
			Melaksanakan prosedur Audit Keamanan Informasi (AKI) terhadap kendali fisik
			Melaksanakan prosedur Audit Keamanan Informasi (AKI) terhadap kendali personel

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
		Mendokumentasikan hasil pelaksanaan prosedur Audit Keamanan Informasi (AKI)	Membuat kertas kerja Audit Keamanan Informasi (AKI)
			Membuat dokumentasi bukti Audit Keamanan Informasi (AKI)
	Melakukan supervisi pelaksanaan Audit Keamanan Informasi (AKI)	Melakukan supervisi kelayakan pelaksanaan prosedur Audit Keamanan Informasi (AKI)	Mengawasi kecukupan pelaksanaan audit sesuai dengan prosedur Audit Keamanan Informasi (AKI)
			Mengawasi kelayakan teknis pelaksanaan prosedur Audit Keamanan Informasi (AKI)
		Melakukan supervisi kelayakan dokumentasi pelaksanaan prosedur Audit Keamanan Informasi (AKI)	Mengawasi kelayakan dokumentasi kertas kerja Audit Keamanan Informasi (AKI)
			Mengawasi kelayakan dokumentasi bukti Audit Keamanan Informasi (AKI)
	Melaporkan Audit Keamanan Informasi (AKI)	Mengemukakan hasil pelaksanaan prosedur Audit Keamanan Informasi (AKI)	Menyampaikan prosedur Audit Keamanan Informasi (AKI) yang dilaksanakan di dalam laporan AKI
			Menyampaikan sumber daya Audit Keamanan Informasi (AKI) yang digunakan dalam laporan AKI

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
		Mengemukakan temuan, rekomendasi, dan kesimpulan Audit Keamanan Informasi (AKI)	Menyampaikan temuan Audit Keamanan Informasi (AKI) dalam laporan AKI
			Menyampaikan rekomendasi Audit Keamanan Informasi (AKI) dalam laporan AKI
			Menyampaikan kesimpulan Audit Keamanan Informasi (AKI)
		Mengemukakan hasil pemantauan tindak lanjut Audit Keamanan Informasi (AKI)	Mengumpulkan bukti pelaksanaan tindak lanjut Audit Keamanan Informasi (AKI)
			Mengevaluasi bukti pelaksanaan tindak lanjut rekomendasi Audit Keamanan Informasi (AKI)

B. Daftar Unit Kompetensi

NO	Kode Unit	Judul Unit Kompetensi
1	*2*	*3*
1.	J.62AKI00.001.1	Menentukan Tujuan dan Lingkup Audit Keamanan Keamanan Informasi (AKI)
2.	J.62AKI00.002.1	Melakukan Analisis Risiko Audit Keamanan Informasi (AKI)
3.	J.62AKI00.003.1	Membuat Prosedur Audit Keamanan Informasi (AKI)
4.	J.62AKI00.004.1	Menentukan Kebutuhan Sumber Daya Audit Keamanan Informasi (AKI)
5.	J.62AKI00.005.1	Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Organisasi
6.	J.62AKI00.006.1	Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Teknologi
7.	J.62AKI00.007.1	Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Fisik
8.	J.62AKI00.008.1	Melaksanakan Prosedur Audit Keamanan Informasi (AKI) terhadap Kendali Personel
9.	J.62AKI00.009.1	Membuat Kertas Kerja Audit Keamanan Informasi (AKI)
10.	J.62AKI00.010.1	Membuat Dokumentasi Bukti Audit Keamanan Informasi (AKI)
11.	J.62AKI00.011.1	Mengawasi Kecukupan Pelaksanaan Audit Sesuai dengan Prosedur Audit Keamanan Informasi (AKI)
12	J.62AKI00.012.1	Mengawasi Kelayakan Teknis Pelaksanaan Prosedur Audit Keamanan Informasi (AKI)
13	J.62AKI00.013.1	Mengawasi Kelayakan Dokumentasi Kertas Kerja Audit Keamanan Informasi (AKI)
14.	J.62AKI00.014.1	Mengawasi Kelayakan Dokumentasi Bukti Audit Keamanan Informasi (AKI)
15.	J.62AKI00.015.1	Menyampaikan Prosedur Audit Keamanan Informasi (AKI) yang Dilaksanakan di dalam Laporan AKI
16.	J.62AKI00.016.1	Menyampaikan Sumber Daya Audit Keamanan Informasi (AKI) yang Digunakan dalam Laporan AKI

NO	Kode Unit	Judul Unit Kompetensi
1	*2*	*3*
17.	J.62AKI00.017.1	Menyampaikan Temuan Audit Keamanan Informasi (AKI) dalam Laporan AKI
18.	J.62AKI00.018.1	Menyampaikan Rekomendasi Audit Keamanan Informasi (AKI) dalam Laporan AKI
19.	J.62AKI00.019.1	Menyampaikan Kesimpulan Audit Keamanan Informasi (AKI)
20.	J.62AKI00.020.1	Mengumpulkan Bukti Pelaksanaan Tindak Lanjut Audit Keamanan Informasi (AKI)
21.	J.62AKI00.021.1	Mengevaluasi Bukti Pelaksanaan Tindak Lanjut Rekomendasi Audit Keamanan Informasi (AKI)

C. Uraian Unit Kompetensi

KODE UNIT : **J.62AKI00.001.1**

JUDUL UNIT : **Menentukan Tujuan dan Lingkup Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mendefinisikan dan menjabarkan tujuan dan lingkup AKI berdasarkan kebutuhan AKI.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mendefinisikan tujuan AKI	1.1 **Tujuan AKI** ditentukan berdasarkan **kebutuhan**. 1.2 Tujuan AKI dijabarkan berdasarkan kebutuhan.
2. Mendefinisikan lingkup AKI	2.1 **Lingkup AKI** ditentukan berdasarkan kebutuhan. 2.2 Lingkup AKI dijabarkan berdasarkan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Tujuan AKI adalah hasil akhir yang diharapkan dari sebuah AKI, seperti kesimpulan atas kepatuhan manajemen keamanan informasi, kesimpulan atas efektivitas manajemen keamanan informasi, kesimpulan atas efisiensi manajemen keamanan informasi, dan kesimpulan atas investigasi insiden keamanan informasi.
   1.2 Kebutuhan adalah latar belakang atau pengguna utama dari hasil AKI, seperti manajemen internal, pihak eksternal termasuk mitra usaha, konsumen, dan pihak regulator, serta untuk tujuan legal.
   1.3 Lingkup AKI adalah batasan cakupan dari sebuah AKI, seperti sumber daya informasi tertentu, pengendalian keamanan informasi tertentu, dan jangka waktu tertentu, serta kriteria AKI tertentu.

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 pendefinisian tujuan dan lingkup AKI berdasarkan kebutuhan 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 Keamanan informasi

3.1.2 Manajemen keamanan informasi

3.1.3 Audit keamanan informasi

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat lunak alat bantu perencanaan audit

4. Sikap kerja yang diperlukan

4.1 Teliti dalam mendefinisikan kebutuhan dan lingkup AKI

4.2 Objektif dalam mendefinisikan tujuan AKI

5. Aspek kritis

5.1 Ketepatan dalam menentukan tujuan AKI berdasarkan kebutuhan

KODE UNIT : **J.62AKI00.002.1**

JUDUL UNIT : **Melakukan Analisis Risiko Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan analisis risiko AKI berupa risiko kesalahan pengambilan keputusan AKI berdasarkan temuan AKI.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi risiko AKI	1.1 **Model risiko AKI** dirumuskan berdasarkan kebutuhan. 1.2 Risiko AKI dirumuskan berdasarkan komponen risiko AKI.
2. Menilai risiko AKI	2.1 **Komponen risiko AKI** dinilai berdasarkan kondisi auditan. 2.2 Risiko AKI disimpulkan berdasarkan **tingkat risiko AKI**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Model risiko AKI dapat menggunakan model sebagai berikut: risiko AKI = risiko inheren x risiko kontrol x risiko deteksi.
   1.2 Komponen risiko AKI terdiri dari:
      1.2.1 Risiko inheren adalah risiko dimana terdapat kesalahan yang material dalam sebuah area audit, secara tunggal atau gabungan dengan kesalahan lain, dengan asumsi bahwa tidak ada pengendalian internal terkait.
      1.2.2 Risiko kontrol adalah risiko adanya kesalahan yang dapat terjadi di area audit yang dapat bersifat material, secara tunggal atau gabungan dengan kesalahan lain, tidak dapat dicegah atau dideteksi dan dikoreksi secara tepat waktu oleh sistem pengendalian internal.
      1.2.3 Risiko deteksi adalah risiko bahwa prosedur substantif auditor tidak dapat mendeteksi kesalahan yang material, secara tunggal atau gabungan dengan kesalahan lainnya.

1.3 Tingkat risiko AKI pada umumnya dapat dianalisis menggunakan pendekatan kualitatif seperti tinggi, sedang, rendah, dan menggunakan pendekatan kuantitatif seperti angka persentase.

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 perumusan dan analisis risiko 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 Keamanan informasi

3.1.2 Manajemen keamanan informasi

3.1.3 Audit keamanan informasi

3.2 Keterampilan

3.2.1 Melakukan perhitungan matematika sederhana

3.2.2 Mengoperasikan perangkat lunak alat bantu perhitungan risiko audit

4. Sikap kerja yang diperlukan

4.1 Teliti dalam menganalisis risiko

4.2 Objektif dalam menganalisis risiko

4.3 Asertif dalam menganalisis risiko

5. Aspek kritis

5.1 Ketepatan dalam merumuskan risiko AKI berdasarkan komponen risiko AKI

KODE UNIT : **J.62AKI00.003.1**

JUDUL UNIT : **Membuat Prosedur Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengidentifikasi dan menguraikan prosedur Audit Keamanan Informasi (AKI) yang akan dilakukan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengidentifikasi prosedur AKI yang akan dilakukan	1.1 **Tahapan AKI** ditentukan sebagai **prosedur AKI** sesuai dengan kebutuhan. 1.2 **Metode AKI** dalam setiap tahapan ditentukan sebagai prosedur AKI sesuai kebutuhan.
2. Menguraikan prosedur AKI yang akan dilakukan	2.1 Tahapan AKI dijabarkan dalam prosedur AKI sesuai dengan kebutuhan. 2.2 Metode AKI pada setiap tahapan dijabarkan dalam prosedur AKI sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Tahapan AKI adalah urutan kegiatan pelaksanaan AKI yang terdiri dari perencanaan AKI, pelaksanaan AKI, supervisi AKI, pelaporan AKI, dan pemantauan AKI.
   1.2 Prosedur AKI adalah instruksi AKI terdiri dari langkah-langkah yang harus dilakukan untuk dapat menyelesaikan AKI, seperti: peroleh dokumen, evaluasi desain kendali, uji kendali, uji terinci.
   1.3 Metode AKI adalah cara atau teknik pelaksanaan AKI yang ditetapkan pada saat perencanaan, seperti audit *desktop*, audit jarak jauh, observasi aktivitas, reperformansi, dan lainnya.

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 pendefinisian prosedur AKI berdasarkan tujuan dan lingkup audit

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 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 keamanan informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam menentukan dan menjabarkan prosedur AKI
   4.2 Objektif dalam menentukan dan menjabarkan prosedur AKI
   4.3 Asertif dalam menentukan prosedur AKI
   4.4 Bertanggung jawab dalam menentukan prosedur AKI

5. Aspek kritis
   5.1 Ketepatan dalam menjabarkan metode AKI pada setiap tahapan dalam prosedur AKI sesuai dengan kebutuhan

KODE UNIT : **J.62AKI00.004.1**

JUDUL UNIT : **Menentukan Kebutuhan Sumber Daya Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menelaah dan menetapkan kebutuhan sumber daya Audit Keamanan Informasi (AKI).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menelaah kebutuhan sumber daya AKI	1.1 **Waktu pelaksanaan AKI** diidentifikasi sesuai dengan kebutuhan. 1.2 **Personel pelaksana AKI** diidentifikasi sesuai dengan kebutuhan. 1.3 **Alat bantu AKI** diidentifikasi sesuai dengan kebutuhan.
2. Menetapkan sumber daya AKI yang dibutuhkan	2.1 Waktu pelaksanaan AKI ditentukan sesuai kebutuhan. 2.2 Personel pelaksana AKI ditentukan sesuai kebutuhan. 2.3 Alat bantu AKI ditentukan sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Waktu pelaksanaan AKI adalah jumlah hari yang dibutuhkan bagi pelaksanaan AKI sejak saat dimulai hingga selesai.
   1.2 Personel pelaksana AKI adalah seluruh sumber daya manusia yang terlibat dalam tim pelaksana AKI.
   1.3 Alat bantu AKI adalah berbagai peralatan yang dibutuhkan bagi pelaksanaan AKI, baik berupa perangkat lunak maupun perangkat keras.

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 pendefinisian sumber daya 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 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 keamanan informasi

   3.2 Keterampilan

      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan

   4.1 Teliti dalam menentukan sumber daya AKI

   4.2 Objektif dalam menganalisis kebutuhan sumber daya AKI

   4.3 Komunikatif dalam menentukan sumber daya AKI

   4.4 Asertif dalam menentukan sumber daya AKI

   4.5 Berpikir kritis dalam menentukan sumber daya AKI

5. Aspek kritis

   5.1 Ketepatan dalam menentukan personel pelaksana AKI sesuai kebutuhan

   5.2 Ketepatan dalam menentukan waktu pelaksanaan AKI sesuai kebutuhan

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.62AKI00.011.1**

JUDUL UNIT : **Mengawasi Kecukupan Pelaksanaan Audit Sesuai dengan Prosedur Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengawasi kesesuaian perencanaan dan pelaksanaan audit dengan prosedur Audit Keamanan Informasi (AKI).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menelaah prosedur AKI yang direncanakan	1.1 Prosedur AKI diidentifikasi sesuai dengan standar. 1.2 Prosedur AKI dijabarkan sesuai dengan standar. 1.3 Prosedur AKI diidentifikasi dalam tahapan identifikasi risiko dengan mempertimbangkan **risiko-risiko signifikan**.
2. Mengevaluasi pelaksanaan prosedur AKI dengan rencana AKI	2.1 Realisasi pelaksanaan prosedur AKI dibandingkan dengan prosedur yang dibuat. 2.2 **Catatan supervisi** informasi dibuat sesuai dengan realisasi pelaksanaan prosedur AKI. 2.3 Catatan supervisi terkait realisasi pelaksanaan prosedur AKI disampaikan kepada pihak terkait. 2.4 Perubahan-perubahan prosedur AKI didokumentasikan dengan tepat.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Risiko-risiko signifikan adalah kemungkinan kemungkinan terjadinya kesalahan yang bersifat material dan telah diidentifikasi dalam tahap identifikasi dan penilaian risiko yang memiliki dampak dan kemungkinan.

1.2 Catatan supervisi adalah hal hal yang menjadi perhatian dan koreksi dari pengendali mutu audit terhadap realisasi pelaksanaan prosedur audit yang dijalankan.

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 Prosedur audit yang telah dibuat
      2.2.2 Kertas kerja yang dibuat oleh auditor

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 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 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 Teliti dalam mengevaluasi prosedur yang dibuat dan langkah langkah yang telah dilakukan sesuai dengan prosedur yang telah dibuat

4.2 Objektif dalam mengevaluasi prosedur yang dibuat dan menilai langkah langkah yang telah dilakukan

4.3 Komunikatif dalam menyampaikan catatan catatan supervisi

4.4 Konstruktif dalam menyampaikan perbaikan-perbaikan yang diperlukan

5. Aspek kritis
    5.1 Ketepatan dalam membuat catatan supervisi informasi sesuai dengan realisasi pelaksanaan prosedur AKI

KODE UNIT : **J.62AKI00.012.1**

JUDUL UNIT : **Mengawasi Kelayakan Teknis Pelaksanaan Prosedur Audit Keamanan Informasi (AKI)**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengawasi kelayakan/kecukupan teknis pelaksanaan prosedur Audit Keamanan Informasi (AKI).

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan aspek aspek teknis dari prosedur AKI	1.1 **Aspek-aspek teknis** dalam prosedur AKI diidentifikasi sesuai dengan standar. 1.2 **Kriteria-kriteria kecukupan teknis** dalam prosedur AKI diidentifikasi sesuai dengan norma, standar, atau rujukan lain yang relevan.
2. Menganalisis kecukupan teknis prosedur AKI	2.1 Pelaksanaan prosedur AKI dibandingkan dengan prosedur AKI yang dibuat. 2.2 Prosedur yang telah dijalankan dinilai **kecukupan teknisnya** berdasarkan kriteria yang diidentifikasikan. 2.3 **Catatan supervisi** kecukupan teknis dibuat sesuai dengan realisasi pelaksanaan prosedur audit keamanan dan penilaian kelayakan teknis prosedur yang telah dijalankan. 2.4 Catatan supervisi terkait kecukupan teknis prosedur AKI disampaikan kepada pihak terkait.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Aspek-aspek teknis, meliputi teknik perancangan dan implementasi pengendalian keamanan informasi, dan teknik peroleh dan pendokumentasian bukti AKI.
   1.2 Kriteria-kriteria kecukupan teknis, meliputi kebijakan, prosedur atau persyaratan yang dipakai sebagai rujukan AKI.
   1.3 Kecukupan teknisnya adalah kesesuaian prosedur audit yang dijalankan dengan standar, metodologi, teknik, praktik terbaik yang

dibutuhkan dalam menjalankan prosedur tersebut. Misal: pelaksanaan prosedur pengujian keamanan informasi sudah dilakukan sesuai dengan standar, metodologi, teknik, menggunakan alat bantu yang layak.

1.4 Catatan supervisi adalah hal hal yang menjadi perhatian dan koreksi dari pengendali mutu audit terhadap realisasi pelaksanaan prosedur audit yang dijalankan.

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 Prosedur audit yang telah dibuat

2.2.2 Kertas kerja yang dibuat oleh auditor

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 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 Pengendalian keamanan informasi
      3.1.4 Audit keamanan informasi
      3.1.5 Aspek teknis dari hasil pengujian keamanan informasi.
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam mengevaluasi kecukupan teknis prosedur yang dijalankan
   4.2 Objektif dalam mengevaluasi kecukupan teknis prosedur yang telah dijalankan

4.3 Komunikatif dalam menyampaikan catatan-catatan supervisi

4.4 Konstruktif dalam menyampaikan perbaikan-perbaikan yang diperlukan

5. Aspek kritis

5.1 Ketepatan dalam membuat catatan supervisi kecukupan teknis sesuai dengan realisasi pelaksanaan prosedur audit keamanan dan penilaian kelayakan teknis prosedur yang telah dijalankan

KODE UNIT : **J.62AKI00.013.1**

JUDUL UNIT : **Mengawasi Kelayakan Dokumentasi Kertas Kerja Audit Keamanan Informasi (AKI)**

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

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan kertas kerja AKI yang akan disupervisi	1.1 Kertas kerja AKI yang telah dibuat diidentifikasi sesuai dengan dokumentasi kertas kerja AKI. 1.2 **Kelengkapan dokumentasi** kertas kerja AKI diperiksa sesuai kertas kerja yang disusun.
2. Menganalisis kelayakan kertas kerja AKI yang telah dibuat	2.1 **Kelayakan dokumentasi** kertas kerja AKI dievaluasi sesuai dengan prosedur dokumentasi kertas kerja AKI. 2.2 **Catatan supervisi** terkait kelayakan kertas kerja AKI dibuat sesuai dengan kebutuhan. 2.3 Catatan supervisi terkait kelayakan kertas kerja AKI disampaikan kepada pihak terkait. 2.4 Tindak lanjut atas catatan dievaluasi sesuai catatan supervisi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Kelengkapan dokumentasi adalah kecukupan dari kertas kerja AKI yang sudah diidentifikasi dan dibandingkan dengan kebutuhan audit AKI.
   1.2 Kelayakan dokumentasi adalah kualitas cara pengisian dari kertas kerja AKI sesuai dengan kertas kerja AKI.
   1.3 Catatan supervisi kelayakan kertas kerja adalah tanggapan, respons atau umpan balik terkait kecukupan dari kertas kerja.

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 evaluasi kelayakan dokumentasi 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 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 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

3.1.2 Pengujian pengendalian keamanan informasi

3.1.3 Aspek kelayakan pendokumentasian kertas kerja AKI

3.2 Keterampilan

3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan

4.1 Teliti dalam menentukan kelengkapan dokumen AKI

4.2 Objektif dalam menentukan kelengkapan dokumen AKI

4.3 Komunikatif dalam menginformasikan kelengkapan dokumen AKI

5. Aspek kritis

5.1 Ketepatan dalam mengevaluasi kelayakan dokumentasi kertas kerja AKI dievaluasi sesuai dengan prosedur dokumentasi kertas kerja AKI

KODE UNIT : **J.62AKI00.014.1**

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

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

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan bukti AKI yang akan disupervisi	1.1 **Bukti objektif AKI** yang telah dibuat diidentifikasi sesuai dengan dokumentasi bukti AKI. 1.2 **Kelengkapan dokumentasi** bukti AKI diperiksa sesuai bukti yang didokumentasikan.
2. Menganalisis kelayakan bukti AKI yang telah didokumentasikan	2.1 **Kelayakan dokumentasi** bukti AKI dievaluasi sesuai dengan prosedur dokumentasi bukti AKI. 2.2 **Catatan supervisi** terkait kelayakan bukti AKI dibuat sesuai dengan kebutuhan. 2.3 Catatan supervisi terkait kelayakan bukti AKI disampaikan kepada pihak terkait. 2.4 Tindak lanjut atas catatan dievaluasi dengan sesuai catatan supervisi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Bukti objektif AKI adalah data yang mendukung keberadaan atau kebenaran, yang mana data dukung dapat diperoleh melalui pengamatan, pengujian, pengukuran dan metode lainnya.
   1.2 Kelengkapan dokumentasi adalah kecukupan dan kelengkapan dari bukti audit AKI yang sudah diperiksa.
   1.3 Kelayakan dokumentasi adalah kesesuaian dan kelayakan dari bukti audit AKI yang disajikan oleh auditor AKI.
   1.4 Catatan supervisi adalah tanggapan, respons atau umpan balik terkait kecukupan dari bukti audit dan kelayakan bukti audit.

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 evaluasi kelayakan dokumentasi 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 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 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
      3.2.1 Keamanan informasi
      3.2.2 Manajemen keamanan informasi
      3.2.3 Audit keamanan informasi
      3.2.4 Pengendalian keamanan informasi
      3.2.5 Aspek kelayakan pendokumentasian bukti AKI
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam menentukan kelayakan dokumentasi bukti AKI
   4.2 Objektif dalam menentukan kelayakan dokumentasi bukti AKI
   4.3 Komunikatif dalam menginformasikan kelayakan dokumentasi bukti AKI
   4.4 Berpikir kritis dalam melakukan analisa kelayakan dokumentasi bukti AKI

5. Aspek kritis
   5.1 Ketepatan dalam mengevaluasi kelayakan dokumentasi bukti AKI sesuai dengan prosedur dokumentasi bukti AKI

KODE UNIT : **J.62AKI00.015.1**

JUDUL UNIT : **Menyampaikan Prosedur Audit Keamanan Informasi (AKI) yang Dilaksanakan di dalam Laporan AKI**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyampaikan langkah-langkah prosedur Audit Keamanan Informasi (AKI) yang telah dilaksanakan selama proses AKI berlangsung.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan langkah-langkah AKI yang telah dilaksanakan dalam laporan AKI	1.1 **Langkah-langkah AKI** diidentifikasi sesuai dengan dokumentasi kertas kerja AKI. 1.2 Langkah-langkah AKI dikompilasi sesuai dengan prosedur pelaporan.
2. Mengkomunikasikan langkah-langkah AKI yang telah dilaksanakan dalam laporan AKI	2.1 Langkah-langkah AKI didokumentasikan sesuai dengan prosedur pelaporan. 2.2 Langkah-langkah AKI disampaikan kepada pihak terkait sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Langkah-langkah AKI adalah kegiatan yang telah dilakukan dalam proses AKI disampaikan kepada auditan sesuai dengan batasan cakupan dari AKI, seperti sumber daya informasi tertentu, pengendalian keamanan informasi tertentu, peraturan dan standar tertentu, serta jangka waktu tertentu sesuai dengan prosedur pelaporan.

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 hasil pelaksanaan AKI

2.2.2 Dokumen bukti hasil pelaksanaan AKI

2.2.3 Dokumen hasil analisa 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 menyampaikan prosedur AKI yang telah dilaksanakan

   4.2 Komunikatif dalam menyampaikan laporan hasil AKI

   4.3 Independensi dalam menyampaikan laporan AKI

5. Aspek kritis

   5.1 Ketepatan dalam menyampaikan langkah-langkah AKI kepada pihak terkait sesuai dengan kebutuhan

KODE UNIT : **J.62AKI00.016.1**

JUDUL UNIT : **Menyampaikan Sumber Daya Audit Keamanan Informasi (AKI) yang Digunakan dalam Laporan AKI**

DESKRIPSI UNIT : Unit ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyampaikan penggunaan sumber daya Audit Keamanan Informasi (AKI) yang digunakan dalam proses pelaksanaan AKI.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan sumber daya AKI yang digunakan dalam Laporan AKI	1.1 **Sumber daya AKI** diidentifikasi sesuai dengan dokumentasi kertas kerja AKI. 1.2 Sumber daya AKI dikompilasi sesuai dengan prosedur pelaporan.
2. Mengkomunikasikan sumber daya AKI yang digunakan	2.1 Sumber daya AKI didokumentasikan sesuai dengan prosedur pelaporan. 2.2 Sumber daya AKI disampaikan kepada pihak terkait sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Sumber daya AKI untuk mengkompilasi hasil pelaksanaan AKI dan menyusun laporan hasil pelaksanaan AKI berdasarkan sumber daya yang diperoleh dalam pelaksanaan AKI.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat komputasi
      2.1.2 Perangkat lunak pengolah kata
   2.2 Perlengkapan
      2.2.1 Kertas kerja AKI hasil pelaksanaan AKI
      2.2.2 Dokumen bukti hasil pelaksanaan AKI
      2.2.3 Dokumen hasil analisa 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
        3.1.2 Pengujian pengendalian keamanan informasi
    3.2 Keterampilan
        3.2.1 Mengoperasikan perangkat lunak alat bantu audit

4. Sikap kerja yang diperlukan
    4.1 Teliti dalam menyampaikan sumber daya AKI
    4.2 Objektif dalam menyampaikan sumber daya AKI
    4.3 Komunikatif dalam menyampaikan sumber daya AKI

5. Aspek kritis
    5.1 Ketepatan dalam mengkompilasi sumber daya AKI sesuai dengan prosedur pelaporan

KODE UNIT : **J.62AKI00.017.1**

JUDUL UNIT : **Menyampaikan Temuan Audit Keamanan Informasi (AKI) dalam Laporan AKI**

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

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Memformulasikan temuan AKI	1.1 **Temuan AKI** dirumuskan berdasarkan kertas kerja AKI. 1.2 Temuan AKI dijabarkan sesuai dengan prosedur AKI.
2. Mengkomunikasikan temuan AKI dalam laporan AKI	2.1 **Metode komunikasi** penyampaian temuan AKI ditentukan sesuai dengan kebutuhan. 2.2 Temuan AKI disampaikan kepada **pihak terkait** sesuai dengan kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Temuan AKI merupakan hasil yang didapat pada pelaksanaan audit meliputi ketidaksesuaian (tidak dipenuhinya sebuah persyaratan) baik minor maupun mayor.
   1.2 Metode komunikasi merupakan tata cara yang meliputi desiminasi langsung dan tidak langsung dalam pelaksanaan komunikasi.
   1.3 Pihak terkait merupakan Individu atau organisasi yang terlibat dalam kegiatan audit atau merupakan pengguna hasil temuan audit meliputi pimpinan, sejawat, pengguna hasil audit.

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

2.2.2 Bukti temuan 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/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 Objektif dalam menyampaikan temuan AKI

   4.2 Teliti dalam menyampaikan temuan AKI

   4.3 Tanggung jawab dalam melaksanakan prosedur AKI

   4.4 Komunikatif dalam menyampaikan temuan AKI

5. Aspek kritis

   5.1 Ketepatan dalam menjabarkan temuan AKI sesuai dengan prosedur AKI

KODE UNIT : **J.62AKI00.018.1**

JUDUL UNIT : **Menyampaikan Rekomendasi Audit Keamanan Informasi (AKI) dalam Laporan AKI**

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

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Merumuskan rekomendasi untuk temuan AKI	1.1 Rekomendasi untuk temuan AKI diidentifikasi sesuai dengan kebutuhan. 1.2 Rekomendasi untuk **temuan AKI** dijabarkan sesuai dengan kebutuhan.
2. Mengkomunikasikan rekomendasi AKI dalam laporan AKI	2.1 **Metode komunikasi** penyampaian rekomendasi AKI ditentukan sesuai dengan kebutuhan. 2.2 **Rekomendasi AKI** disampaikan dalam laporan kepada **pihak terkait** sesuai kebutuhan.
3. Memperoleh tanggapan atas rekomendasi yang disampaikan	3.1 Tanggapan atas rekomendasi ditelaah sesuai dengan temuan AKI. 3.2 Tanggapan atas rekomendasi didokumentasikan sesuai dengan prosedur AKI.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Temuan AKI merupakan hasil yang didapat pada pelaksanaan audit meliputi kesesuaian dan ketidaksesuaian (Minor dan Mayor).
   1.2 Metode komunikasi merupakan tata cara yang meliputi diseminasi langsung dan tidak langsung dalam pelaksanaan komunikasi.
   1.3 Rekomendasi AKI merupakan pemberian saran dan masukan dari temuan audit.
   1.4 Pihak terkait merupakan Individu atau organisasi yang terlibat dalam kegiatan audit atau merupakan pengguna hasil temuan audit meliputi pimpinan, sejawat, pengguna hasil audit.

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
      2.2.2 Bukti temuan 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/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 Objektif dalam menyampaikan rekomendasi AKI

4.2 Teliti dalam menyampaikan rekomendasi AKI

4.3 Tanggung jawab dalam melaksanakan prosedur

4.4 Komunikatif dalam menyampaikan rekomendasi AKI

5. Aspek kritis

5.1 Ketepatan dalam menjabarkan rekomendasi untuk temuan AKI sesuai dengan kebutuhan

KODE UNIT : **J.62AKI00.019.1**

JUDUL UNIT : **Menyampaikan Kesimpulan Audit Keamanan Informasi (AKI)**

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

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menarik kesimpulan dari hasil pelaksanaan AKI	1.1 Hasil pelaksanaan prosedur AKI diidentifikasi sesuai dengan dokumentasi kertas kerja dan bukti AKI. 1.2 Kesimpulan dari hasil pelaksanaan AKI dirumuskan berdasarkan hasil pelaksanaan prosedur AKI.
2. Mengkomunikasikan kesimpulan AKI dalam laporan AKI	2.1 **Metode komunikasi** penyampaian kesimpulan AKI ditentukan sesuai dengan kebutuhan. 2.2 **Kesimpulan AKI** disampaikan dalam laporan kepada **pihak terkait** sesuai dengan prosedur AKI.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Metode komunikasi merupakan tata cara yang meliputi diseminasi langsung dan tidak langsung dalam pelaksanaan komunikasi.
   1.2 Kesimpulan AKI merupakan ikhtisar dari hasil pelaksanaan AKI.
   1.3 Pihak terkait merupakan individu atau organisasi yang terlibat dalam kegiatan audit atau merupakan pengguna hasil temuan audit meliputi pimpinan, sejawat, pengguna hasil audit.

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

2.2 Perlengkapan

2.2.1 Kertas kerja pengambilan kesimpulan 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/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 Keterampilan mengoperasikan perangkat lunak alat bantu audit

      3.2.2 Keterampilan melaksanakan metode komunikasi yang tepat

4. Sikap kerja yang diperlukan

   4.1 Teliti dalam mengidentifikasi temuan dan rekomendasi AKI

   4.2 Objektif dalam menyusun kesimpulan rekomendasi AKI

   4.3 Independen saat menyusun kesimpulan rekomendasi AKI

   4.4 Jujur dalam menyampaikan kesimpulan rekomendasi AKI

   4.5 Tepercaya dalam menyimpan/mengetahui kesimpulan hasil AKI

5. Aspek kritis

   5.1 Ketepatan dalam menyampaikan kesimpulan AKI dalam laporan kepada pihak terkait sesuai dengan prosedur AKI

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

KODE UNIT : **J.62AKI00.021.1**

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

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

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menguji bentuk tindak lanjut rekomendasi AKI	1.1 **Bentuk tindak lanjut rekomendasi AKI** diidentifikasi berdasarkan bukti tindak lanjut rekomendasi AKI. 1.2 Bentuk tindak lanjut rekomendasi AKI dinilai berdasarkan kriteria audit.
2. Menguji agenda tindak lanjut rekomendasi AKI	2.1 **Agenda tindak lanjut rekomendasi** AKI diidentifikasi berdasarkan bukti tindak lanjut rekomendasi AKI. 2.2 Agenda tindak lanjut rekomendasi AKI dinilai berdasarkan kriteria audit.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Bentuk tindak lanjut rekomendasi AKI adalah bentuk dari tindakan yang dilakukan auditan yang dapat berupa kebijakan, prosedur, penugasan personel, penggunaan alat bantu, dalam rangka perbaikan dan/atau penambahan pengendalian keamanan informasi.
   1.2 Agenda tindak lanjut rekomendasi AKI terdiri dari:
      1.2.1 Waktu tindak lanjut rekomendasi AKI adalah saat pelaksanaan tindak lanjut yang telah dilakukan.
      1.2.2 Pelaksana tindak lanjut rekomendasi AKI adalah pelaksana dari tindak lanjut yang telah dilakukan.

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 evaluasi tindak lanjut rekomendasi 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 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 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 mengidentifikasi bukti tindak lanjut rekomendasi AKI

   4.2 Asertif dalam mengidentifikasi bukti tindak lanjut rekomendasi AKI

   4.3 Independensi dalam menganalisis tindak lanjut rekomendasi AKI

   4.4 Obyektifitas dalam menganalisis tindak lanjut rekomendasi AKI

5. Aspek kritis

   5.1 Ketepatan dalam mengidentifikasi bentuk tindak lanjut rekomendasi AKI berdasarkan bukti tindak lanjut rekomendasi AKI

BAB III
PENUTUP

Dengan ditetapkannya 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, maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan dan pelatihan serta sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH