MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA

KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 236 TAHUN 2024
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 KESADARAN 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 Kesadaran 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 Kesadaran Keamanan Informasi telah disepakati melalui konvensi nasional pada tanggal 3 November 2023 di Jakarta;

c. bahwa sesuai surat Deputi Bidang Strategi dan Kebijakan Kemanan Siber dan Sandi Nomor 7018/BSSN/D1/PS.02.01/12/2023 tanggal 1 Desember 2023 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 Kesadaran Keamanan Informasi, perlu ditindaklanjuti dengan penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan Yang Berhubungan Dengan Itu (YBDI) Bidang Kesadaran 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 Kesadaran 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. 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);
3. Peraturan Presiden Nomor 8 Tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 24);
4. Peraturan Presiden Nomor 95 Tahun 2020 tentang Kementerian Ketenagakerjaan (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 213);
5. Peraturan Menteri Ketenagakerjaan Nomor 21 Tahun 2014 tentang Pedoman Penerapan Kerangka Kualifikasi Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2014 Nomor 1792);
6. Peraturan Menteri Ketenagakerjaan Nomor 3 Tahun 2016 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia (Berita Negara Republik Indonesia Tahun 2016 Nomor 258);
7. 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 KESADARAN 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 Kesadaran 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, pelatihan, dan 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 Kepala 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 12 September 2024

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH

LAMPIRAN
KEPUTUSAN MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA
NOMOR 236 TAHUN 2024
TENTANG
PENETAPAN STANDAR KOMPETENSI KERJA KATEGORI INFORMASI DAN KOMUNIKASI GOLONGAN POKOK AKTIVITAS PEMROGRAMAN, KONSULTASI KOMPUTER DAN KEGIATAN YANG BERHUBUNGAN DENGAN ITU (YBDI) BIDANG KESADARAN KEAMANAN INFORMASI

BAB I
PENDAHULUAN

A. Latar Belakang

Digitalisasi, perkembangan teknologi informasi, dan akses internet memberikan kemudahan dalam berbagai kehidupan masyarakat. Teknologi informasi dan komunikasi yang berkembang saat ini membuat segala sesuatu dapat diselesaikan dengan cara-cara yang praktis. Dalam hal penggunaan internet, penggunaan internet Indonesia terus meningkat, bahkan Indonesia memiliki potensi untuk menjadi pemain ekonomi digital terbesar di Asia Tenggara. Sektor *e-commerce* menjadi penopang utama pertumbuhan ekonomi digital Indonesia.

Menurut survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada periode 2022-2023, pengguna internet di Indonesia mencapai 215,63 juta orang. Jumlah tersebut meningkat 2,67% dibandingkan pada periode sebelumnya yang sebanyak 210,03 juta pengguna. Jumlah pengguna internet tersebut setara dengan 78,19% dari total populasi Indonesia yang sebanyak 275,77 juta jiwa. Penggunaan internet di Indonesia terus meningkat dari tahun ke tahun. Hal ini didorong oleh penggunaan internet yang kian jadi kebutuhan masyarakat, khususnya semenjak pandemi Covid-19 pada 2020. Tingkat penetrasi internet di Indonesia mencapai 77% pada awal 2023.

Tren positif perkembangan ekonomi digital juga sejalan dengan perkembangan investasi. Hasil studi Google, Temasek, Bain & Company (2021) menunjukkan bahwa nilai investasi ekonomi digital Indonesia sepanjang *Quarter* Pertama (Q1)-2021 sebesar 4,7 miliar USD dan telah melampaui nilai tertinggi selama empat tahun terakhir. Capaian tersebut menjadikan Indonesia sebagai tujuan investasi terpopuler di Asia Tenggara, melampaui Singapura. Lebih lanjut Bank Indonesia (BI) melaporkan nilai transaksi perdagangan elektronik atau *e-commerce* di Indonesia terus meningkat dari tahun ke tahun. Pada tahun 2022 nilai transaksi perdagangan elektronik atau *e-commerce* sebesar Rp 476,3 triliun, sedangkan volume transaksi *e-commerce* tercatat sebanyak 3,49 miliar kali. Nilai transaksi *e-commerce* pada 2022 lebih tinggi 18,8% dari tahun sebelumnya yang sebesar Rp 401 triliun. Pada 2023 BI menargetkan transaksi *e-commerce* tetap bertumbuh 12%. Bahkan menurut Asosiasi *E-Commerce* Indonesia (idEA) menilai hal ini diprediksi bisa tumbuh lagi sebesar 20 persen hingga mencapai Rp 572 triliun pada 2023. Prediksi itu salah satunya didasarkan pada penetrasi internet nasional yang terus meningkat yang akan menjadi pendukung tumbuhnya bisnis *e-commerce* di masa depan.

Berdasarkan laporan Lanskap Keamanan Siber Indonesia Tahun 2022 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), terdapat 714.170.967 lalu lintas anomali atau serangan siber yang terjadi di Indonesia sepanjang tahun 2022. Laporan tersebut juga memuat informasi mengenai isu menonjol terkait pengelolaan keamanan siber tahun 2022, seperti kampanye *phishing*, penilaian keamanan TI, dukungan keamanan siber dan sandi BSSN pada kegiatan nasional dan internasional, kolaborasi BSSN dengan institusi keamanan siber negara lain, insiden siber, serta prediksi ancaman siber tahun 2023.

Selain itu, pada Mei 2021 terdapat 448.491.256 serangan siber di Indonesia dengan tren serangan *Ransomware* dan Insiden *Data Leaks*. Kepala BSSN, Letnan Jenderal TNI (Purn) Hinsa Siburian, menuturkan bahwa tingginya tingkat pemanfaatan Teknologi Informasi dan Komunikasi (TIK) berbanding lurus dengan risiko dan ancaman keamanannya.

Perkembangan teknologi informasi saat ini sangat pesat dan memiliki dampak positif bagi masyarakat diantaranya:

1. Kemudahan dalam berkomunikasi dan berinteraksi dengan orang lain dari berbagai belahan dunia.
2. Memudahkan akses informasi dan penyebaran berita secara cepat dan mudah.
3. Meningkatkan efisiensi dan produktivitas dalam berbagai bidang, seperti bisnis, pendidikan, dan pelayanan publik.
4. Membuka peluang baru dalam menciptakan lapangan kerja dan pengembangan industri.

Akan tetapi selayaknya dua sisi mata pisau, perkembangan teknologi informasi juga memiliki dampak negatif berupa munculnya ancaman yang mungkin timbul atas penggunaannya yaitu:

1. Ancaman terhadap keamanan informasi dan privasi, seperti pencurian data dan identitas, serta penyebaran informasi palsu/hoaks.
2. Ancaman terhadap stabilitas sistem dan infrastruktur teknologi seperti serangan siber dan gangguan jaringan.
3. Ancaman terhadap kesehatan akibat paparan radiasi elektromagnetik dari perangkat teknologi.
4. Ancaman terhadap keamanan nasional dan keamanan publik, seperti terorisme dan kejahatan siber.

Agar dapat terhindar dari berbagai ancaman yang muncul dari penggunaan teknologi informasi maka kita perlu memperhatikan dan menerapkan pengamanan informasi. Pengamanan informasi meliputi tiga aspek, yaitu manusia *(people),* tata kelola *(proses),* dan teknologi *(technology).* Dari ketiga aspek tersebut aspek manusia memegang peranan penting karena manusia mempunyai kendali atas dua aspek lainnya. Akan tetapi manusia juga merupakan rantai terlemah dalam keamanan informasi karena manusia cenderung rentan terhadap serangan siber dan kesalahan manusia sendiri.

Berdasarkan data Verizon *Data Breach Investigations Report* pada tahun 2023, faktor manusia masih tetap menjadi ancaman terbesar. Meskipun jumlah kumulatif pelanggaran dalam basis data Verizon terus meningkat tajam, elemen manusia yang menjadi pusat perhatian dalam laporan terbaru. Pencurian kredensial, *phishing*, dan eksploitasi kerentanan merupakan tiga cara utama penjahat dunia maya mendapatkan akses ke suatu perusahaan. Kesalahan manusia terus menjadi elemen integral setiap kali keamanan organisasi gagal dalam menghadapi pelanggaran data. Laporan tersebut menunjukkan bahwa elemen manusia terdapat dalam 74% dari seluruh pelanggaran, di mana faktor manusia terlibat baik melalui kesalahan, penyalahgunaan hak istimewa,

penggunaan kredensial yang dicuri, atau rekayasa sosial. Laporan tersebut juga menemukan bahwa serangan *social engineering* seringkali sangat berhasil dan sangat menguntungkan bagi penjahat dunia maya. Laporan tersebut menyajikan data dari analisis terhadap 16.312 insiden keamanan siber, di mana 5.199 di antaranya terkonfirmasi sebagai *data breaches*.

Dari beberapa sumber di atas, dapat disimpulkan bahwa *human error, human behavior,* dan *social engineering* merupakan penyebab utama *cybersecurity breach*. Kepedulian masyarakat terhadap risiko ancaman keamanan siber sangat diperlukan, masyarakat diharapkan untuk meningkatkan kepedulian terhadap risiko ancaman serangan siber serta kesadaran akan keamanan informasi. Oleh karena itu, perlu dilakukan program peningkatan kesadaran keamanan informasi *(Information Security Awareness)* untuk meningkatkan kesadaran dan kewaspadaan terhadap ancaman keamanan informasi yang berasal dari faktor manusia.

Upaya kesadaran keamanan informasi dirancang untuk mengubah perilaku atau memperkuat praktik keamanan yang baik. Dalam Publikasi Khusus NIST 800-16, kesadaran didefinisikan sebagai berikut: “Kesadaran bukanlah pelatihan. Tujuan presentasi penyadaran hanya untuk memusatkan perhatian pada keamanan. Presentasi kesadaran dimaksudkan untuk memungkinkan individu untuk mengenali masalah keamanan Teknologi Informasi dan menanggapinya. Dalam kegiatan penyadaran, pembelajar adalah penerima informasi, sedangkan pembelajar dalam sebuah lingkungan pelatihan memiliki peran yang lebih aktif. Kesadaran bergantung pada menjangkau khalayak luas teknik pengemasan yang menarik. Pelatihan lebih formal, memiliki tujuan untuk membangun pengetahuan dan keterampilan untuk memfasilitasi kinerja pekerjaan.” Menurut NIST *Special Publication* 800-50, terdapat empat tahapan utama dalam penyelenggaraan Program kesadaran keamanan informasi diantaranya merancang program kesadaran, mengembangkan materi kesadaran, melaksanakan program penyadaran, dan pasca implementasi.

Saat ini, di Indonesia sudah ada beberapa program terkait kesadaran keamanan informasi diantaranya program Duta Internet Cakap, Relawan TIK dan Gerakan Nasional Literasi Digital (GNLD) Siber Kreasi. Ketiga program tersebut dibentuk oleh Direktorat Pemberdayaan Informatika Dirjen Aplikasi Informatika, Kementerian Komunikasi dan Informatika. Duta Internet Cakap merupakan sosok generasi muda yang cerdas, kreatif dan produktif dan mampu menularkan pemanfaatan internet ke lingkungan sekitarnya dan masyarakat luar. Relawan TIK bertugas untuk membantu pemerintah menyosialisasikan program penggunaan akses informasi (internet), sekaligus pemberdayaan masyarakat melalui informasi, edukasi sosial, teknologi dan komunikasi. GNLD Siber Kreasi merupakan Gerakan nasional untuk menanggulangi ancaman potensi bahaya terbesar yang sedang dihadapi oleh Indonesia. BSSN juga gencar melaksanakan Program kesadaran keamanan informasi dalam rangka membentuk budaya sadar akan keamanan siber masyarakat Indonesia melalui program Kampanye Literasi Keamanan Siber (KLiKS) BSSN. Pada tahun 2021 BSSN juga telah menetapkan Peraturan Kepala BSSN Nomor 3 Tahun 2021 tentang Penyelenggaraan Literasi Media dan Literasi Keamanan Siber.

Selain standar dan program tersebut di atas, dalam Peta Okupasi Nasional Keamanan Siber yang ditetapkan oleh BSSN pada Tahun 2019, dari 30 (tiga puluh) okupasi bidang keamanan siber terdapat 2 (dua) okupasi yang berhubungan erat dengan bidang kesadaran keamanan informasi *(Information Security Awareness).* Okupasi yang dimaksud merupakan *Cybersecurity Awareness Lead Officer* dan *Cybersecurity*

Awareness Officer. Kedua okupasi tersebut telah dilengkapi deskripsinya, namun belum ada unit kompetensi yang dapat menjadi rujukan. Karenanya, penyusunan SKKNI Kesadaran Keamanan Informasi merupakan suatu kebutuhan yang penting dilakukan untuk menumbuhkan profesi-profesi bidang kesadaran keamanan informasi yang berkompeten.

B. Pengertian

1. Prinsip Dasar Keamanan Informasi adalah melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
2. Kesadaran Keamanan Informasi adalah kemampuan individu atau organisasi untuk mengenali dan memahami risiko keamanan informasi, serta melakukan tindakan untuk mengurangi risiko tersebut.
3. Program Kesadaran Keamanan Informasi adalah upaya untuk meningkatkan Kesadaran Keamanan Informasi secara sistematis, terstruktur, dan terukur.

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 atau industri dan penggunaan 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 atau 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 Kesadaran Keamanan Informasi dibentuk melalui Keputusan Kepala Badan Siber dan Sandi Negara Nomor 186.2 tanggal 3 April 2023 dapat dilihat pada Tabel 1.

Tabel 1. Susunan Komite Standar Kompetensi SKKNI Bidang Kesadaran Keamanan Informasi

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi	Badan Siber dan Sandi Negara	Pengarah

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
2.	Direktur Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi, Deputi I	Badan Siber dan Sandi Negara	Ketua
3.	Direktur Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media, dan Transportasi, Deputi IV	Badan Siber dan Sandi Negara	Sekretaris
4.	Ketua Bidang Pengembangan Kultur dan SDM Digital Nasional	Masyarakat Telematika Indonesia	Anggota
5.	Guru Besar Tetap Universitas Indonesia	Universitas Indonesia	Anggota
6.	Direktur Operasi Keamanan dan Pengendalian Informasi, Deputi II	Badan Siber dan Sandi Negara	Anggota
7.	Kepala Biro Hukum dan Komunikasi Publik, Sekretariat Utama	Badan Siber dan Sandi Negara	Anggota
8	Managing Director PT Pijar Edukasi Teknologi	PT Pijar Edukasi Teknologi (Xynexis International)	Anggota

Tabel 2. Susunan Tim Perumus SKKNI Bidang Kesadaran Keamanan Informasi dibentuk melalui keputusan Kepala Badan Siber dan Sandi Negara Nomor 187.2 tanggal 3 April 2023

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Nur Achmadi Salmawan, S.Kom., M.M.	Badan Siber dan Sandi Negara	Ketua
2.	Mohamad Syahral, S.T., M.T.	Politeknik Siber dan Sandi Negara	Sekretaris
3.	Yogiswara, S.Si.	PT Pijar Edukasi Teknologi	Anggota
4.	Ika Dyah Agustia Rachmawati, S.Kom., M.Kom., EHE., DFE	Binus University	Anggota
5.	Syarbeni, S.T.	Huawei Indonesia	Anggota
6.	Melwin Syafrizal, S.Kom., M.Eng.	Universitas Amikom Yogyakarta	Anggota
7.	Agrian Pangestu	Mastercard	Anggota
8.	Satriyo Wibowo, S.T., M.B.A., M.H.	Indonesia Cyber Security Forum (ICSF)	Anggota

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
9.	Alex Budiyanto	Ketua Umum Asosiasi Cloud Computing Indonesia	Anggota
10.	Muhammad Ismu Hadi, S.ST.	Badan Siber dan Sandi Negara	Anggota
11.	Azis Kurniawan, S.ST.	Badan Siber dan Sandi Negara	Anggota
12.	Iqbal Firmansyah, M.T.	Huawei Indonesia	Anggota

Tabel 3. Susunan Tim Verifikasi SKKNI Bidang Kesadaran Keamanan Informasi dibentuk melalui Keputusan Kepala Badan Siber dan Sandi Negara Nomor 187.2 tanggal 3 April 2023

NO.	NAMA	INSTANSI/LEMBAGA	JABATAN DALAM TIM
1	*2*	*3*	*4*
1.	Anas Hilal, S.Pd.	Badan Siber dan Sandi Negara	Ketua
2.	Galylia Aryanita Darmawan, S.ST.	Badan Siber dan Sandi Negara	Anggota
3.	Dessy Diah Pratiwi, S.ST., M.P., M.AP.	Badan Siber dan Sandi Negara	Anggota
4.	Ratih Kumala Dewi, S.SI.	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
Mengurangi risiko keamanan informasi sesuai Prinsip Dasar Keamanan Informasi dengan meningkatkan Kesadaran Keamanan Informasi kepada organisasi dan masyarakat terkait	Mempersiapkan Program Kesadaran Keamanan Informasi	Membuat persiapan rencana aksi Program Kesadaran Keamanan Informasi	Merumuskan dasar Program Kesadaran Keamanan Informasi
			Melakukan penilaian risiko pelaksanaan Program Kesadaran Keamanan Informasi
			Melakukan analisis kebutuhan Program Kesadaran Keamanan Informasi
		Membuat rencana aksi Program Kesadaran Keamanan Informasi	Merumuskan indikator keberhasilan Program Kesadaran Keamanan Informasi
			Menyusun dokumen perencanaan Program Kesadaran Keamanan Informasi
	Menyelenggarakan Program Kesadaran Keamanan Informasi	Melaksanakan Program Kesadaran Keamanan Informasi	Menyusun kebutuhan materi Program Kesadaran Keamanan Informasi yang relevan
			Mengembangkan materi kesadaran keamanan informasi
			Melakukan penyampaian materi Kesadaran Keamanan Informasi
		Mengevaluasi Program Kesadaran Keamanan Informasi	Mengawasi Program Kesadaran Keamanan Informasi
			Mengukur tingkat keberhasilan

TUJUAN UTAMA	FUNGSI KUNCI	FUNGSI UTAMA	FUNGSI DASAR
			Program Kesadaran Keamanan Informasi
		Membuat tindak lanjut Program Kesadaran Keamanan Informasi	Menyusun rekomendasi perbaikan Program Kesadaran Keamanan Informasi
			Menyusun laporan kegiatan Program Kesadaran Keamanan Informasi

B. Daftar Unit Kompetensi

NO.	KODE UNIT	JUDUL UNIT KOMPETENSI
1	*2*	*3*
1.	J.62KKI00.001.1	Merumuskan Dasar Program Kesadaran Keamanan Informasi
2.	J.62KKI00.002.1	Melakukan Penilaian Risiko Pelaksanaan Program Kesadaran Keamanan Informasi
3.	J.62KKI00.003.1	Melakukan Analisis Kebutuhan Program Kesadaran Keamanan Informasi
4.	J.62KKI00.004.1	Merumuskan Indikator Keberhasilan Program Kesadaran Keamanan Informasi
5.	J.62KKI00.005.1	Menyusun Dokumen Perencanaan Program Kesadaran Keamanan Informasi
6.	J.62KKI00.006.1	Menyusun Kebutuhan Materi Program Kesadaran Keamanan Informasi yang Relevan
7.	J.62KKI00.007.1	Mengembangkan Materi Kesadaran Keamanan Informasi
8.	J.62KKI00.008.1	Melakukan Penyampaian Materi Kesadaran Keamanan Informasi
9.	J.62KKI00.009.1	Mengawasi Program Kesadaran Keamanan Informasi
10.	J.62KKI00.010.1	Mengukur Tingkat Keberhasilan Program Kesadaran Keamanan Informasi
11.	J.62KKI00.011.1	Menyusun Rekomendasi Perbaikan Program Kesadaran Keamanan Informasi
12.	J.62KKI00.012.1	Menyusun Laporan Kegiatan Program Kesadaran Keamanan Informasi

C. Uraian Unit Kompetensi

KODE UNIT : J.62KKI00.001.1

JUDUL UNIT : Merumuskan Dasar Program Kesadaran Keamanan Informasi

DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam merumuskan dasar program yang terdiri atas mengembangkan tujuan dan mendefinisikan ruang lingkup Program Kesadaran Keamanan Informasi sesuai Prinsip Dasar Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengembangkan tujuan Program Kesadaran Keamanan Informasi	1.1 **Latar belakang** Program Kesadaran Keamanan Informasi diidentifikasi berdasarkan Prinsip Dasar Keamanan Informasi. 1.2 **Tujuan Program Kesadaran Keamanan Informasi** ditentukan berdasarkan latar belakang. 1.3 Tujuan Program Kesadaran Keamanan Informasi dijabarkan sesuai Prinsip Dasar Keamanan Informasi.
2. Mendefinisikan ruang lingkup Program Kesadaran Keamanan Informasi	2.1 **Ruang lingkup Program Kesadaran Keamanan Informasi** ditentukan berdasarkan tujuan program. 2.2 Ruang lingkup Program Kesadaran Keamanan Informasi dijabarkan berdasarkan **kebutuhan**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mendefinisikan tujuan dan ruang lingkup Program Kesadaran Keamanan Informasi.
   1.2 Latar belakang meliputi peraturan, hasil audit, masukan *stakeholder*, hasil survei, dan profil keamanan.
   1.3 Tujuan program merupakan tujuan yang ingin dicapai melalui pelaksanaan Program Kesadaran Keamanan Informasi.
   1.4 Prinsip Dasar Keamanan Informasi yaitu melindungi kerahasiaan *(confidentiality),* keutuhan *(integrity),* dan ketersediaan *(availability)* informasi.
   1.5 Ruang lingkup program dapat meliputi:
      1.5.1 Batasan kelompok unit organisasi, kelompok individu, jumlah individu, dan wilayah/area peserta Program Kesadaran Keamanan Informasi.
      1.5.2 Batasan waktu pelaksanaan Program Kesadaran Keamanan Informasi.
   1.6 Kebutuhan merupakan kebutuhan yang melandasi perlunya dilakukan Program Kesadaran Keamanan Informasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Jaringan internet

2.2 Perlengkapan
2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
(Tidak ada.)

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
1.1. Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam merumuskan dasar program yang terdiri atas mengembangkan tujuan dan mendefinisikan ruang lingkup Program Kesadaran Keamanan Informasi sesuai Prinsip Dasar Keamanan Informasi.
1.2. Dalam pelaksanaannya peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
1.3. 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.
1.4. Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio, dan metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
3.1 Pengetahuan
3.1.1 Aspek-aspek keamanan informasi
3.1.2 Metode analisis perencanaan strategis
3.2 Keterampilan
3.2.1 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
4.1 Teliti dalam mendefinisikan tujuan Program Kesadaran Keamanan Informasi
4.2 Objektif dalam mendefinisikan ruang lingkup Program Kesadaran Keamanan Informasi
4.3 Asertif dalam merumuskan tujuan dan ruang lingkup Program Kesadaran Keamanan Informasi yang terukur

5. Aspek kritis
5.1 Kesesuaian dalam menentukan ruang lingkup Program Kesadaran Keamanan Informasi berdasarkan tujuan program

KODE UNIT : **J.62KKI00.002.1**
JUDUL UNIT : **Melakukan Penilaian Risiko Pelaksanaan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan penilaian risiko pada saat pelaksanaan Program Kesadaran Keamanan Informasi melalui analisis risiko, dan evaluasi risiko sasaran Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menganalisis risiko pelaksanaan Program Kesadaran Keamanan Informasi	1.1 **Risiko pelaksanaan Program Kesadaran Keamanan Informasi** diobservasi berdasarkan ruang lingkup Program Kesadaran Keamanan Informasi. 1.2 Risiko pelaksanaan Program Kesadaran Keamanan Informasi dirumuskan berdasarkan hasil observasi.
2. Melakukan evaluasi risiko pelaksanaan Program Kesadaran Keamanan Informasi	2.1 Risiko pelaksanaan Program Kesadaran Keamanan Informasi dinilai berdasarkan hasil analisis risiko pelaksanaan program. 2.2 **Perlakuan risiko** pelaksanaan Program Kesadaran Keamanan Informasi ditentukan sesuai hasil analisis risiko pelaksanaan program.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi profil keamanan, menganalisis risiko, dan mengevaluasi risiko sasaran Program Kesadaran Keamanan Informasi.
   1.2 Risiko pelaksanaan program merupakan kemungkinan terjadinya hambatan, kendala, atau peristiwa yang dapat mengganggu atau menghambat pencapaian tujuan Program Kesadaran Keamanan Informasi seperti ketersediaan sumber daya dan waktu pelaksana program, media komunikasi, sarana dan prasarana, anggaran, perubahan dalam lingkungan bisnis, masalah kualitas, atau konflik dalam tim.
   1.3 Perlakuan risiko antara lain:
      1.3.1 Penerimaan risiko
      1.3.2 Penolakan risiko
      1.3.3 Mitigasi risiko atau pengalihan risiko.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
      4.2.1 Standar Nasional Indonesia - *International Organization of Standardization/International Electrotechnical Commission* (SNI ISO/IEC) 27001 Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan penilaian risiko pada saat pelaksanaan Program Kesadaran Keamanan Informasi melalui analisis risiko, dan evaluasi risiko sasaran Program Kesadaran Keamanan Informasi.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 Perencanaan dan proses asesmen ditetapkan dan disepakati bersama dengan mempertimbangkan aspek-aspek tujuan dan konteks asesmen, ruang lingkup, kompetensi, persyaratan peserta, sumber daya asesmen, dan tempat asesmen, serta jadwal asesmen.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio, dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen risiko
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan analisis risiko sasaran Program Kesadaran Keamanan Informasi
   4.2 Objektif dalam melakukan penilaian risiko sasaran Program Kesadaran Keamanan Informasi

5. Aspek kritis
   5.1 Ketepatan dalam menentukan perlakuan risiko pelaksanaan Program Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.003.1**
JUDUL UNIT : **Melakukan Analisis Kebutuhan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan analisis kebutuhan pada saat pelaksanaan Program Kesadaran Keamanan Informasi melalui penyusunan konteks sasaran, penginventarisasian kebutuhan pemangku kepentingan, penentuan kebutuhan media, serta kebutuhan sumber daya Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyusun konteks sasaran Program Kesadaran Keamanan Informasi	1.1 **Konteks sasaran** Program Kesadaran Keamanan Informasi ditentukan berdasarkan kebutuhan. 1.2 Konteks sasaran Program Kesadaran Keamanan Informasi dirumuskan berdasarkan kebijakan keamanan informasi terkait.
2. Menginventarisasi kebutuhan pemangku kepentingan Program Kesadaran Keamanan Informasi	2.1 Kebutuhan pemangku kepentingan Program Kesadaran Keamanan Informasi diidentifikasi berdasarkan metode yang sesuai. 2.2 Kebutuhan pemangku kepentingan Program Kesadaran Keamanan Informasi dirumuskan sesuai konteks sasaran.
3. Menentukan kebutuhan media sesuai materi Program Kesadaran Keamanan Informasi	3.1 **Materi Program Kesadaran Keamanan Informasi** ditelaah sesuai konteks sasaran. 3.2 Media Program Kesadaran Keamanan Informasi dipilih sesuai dengan materi program.
4. Merumuskan sumber daya Program Kesadaran Keamanan Informasi	4.1 **Sumber daya** Program Kesadaran Keamanan Informasi ditentukan sesuai kebutuhan program. 4.2 Sumber daya Program Kesadaran Keamanan Informasi disusun sesuai konteks sasaran.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengidentifikasi konteks sasaran Program Kesadaran Keamanan Informasi, menginventarisasi kebutuhan pemangku kepentingan Program Kesadaran Keamanan Informasi, mengidentifikasi kebutuhan materi dan media Program Kesadaran Keamanan Informasi, dan mengidentifikasi sumber daya yang dibutuhkan Program Kesadaran Keamanan Informasi.
   1.2 Konteks sasaran merupakan status sasaran sebagai bagian internal atau eksternal dari organisasi penyelenggara dan kebijakan terkait yang mengatur penyelenggaraan Program Kesadaran Keamanan Informasi.
   1.3 Materi program berhubungan dengan latar belakang dilaksanakannya Program Kesadaran Keamanan Informasi ini antara lain peraturan,

hasil audit, masukan *stakeholder*, hasil survei, dan profil keamanan (substansinya).

1.4 Sumber daya merupakan anggaran, sarana-prasarana, manusia, aplikasi, dan aset lainnya yang dibutuhkan dalam menyelenggarakan Program Kesadaran Keamanan Informasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      4.1.1 Etika Komunikasi
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan analisis kebutuhan pada saat pelaksanaan Program Kesadaran Keamanan Informasi melalui penyusunan konteks sasaran, penginventarisasian kebutuhan pemangku kepentingan, penentuan kebutuhan media, serta kebutuhan sumber daya Program Kesadaran Keamanan Informasi.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Manajemen proyek
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Kreatif dalam menentukan bentuk kegiatan Program Kesadaran Keamanan Informasi
   4.2 Cermat dalam merumuskan substansi Program Kesadaran Keamanan Informasi

5. Aspek kritis
   5.1 Kesesuaian dalam mengidentifikasi kebutuhan pemangku kepentingan Program Kesadaran Keamanan Informasi berdasarkan metode yang sesuai

KODE UNIT : **J.62KKI00.004.1**
JUDUL UNIT : **Merumuskan Indikator Keberhasilan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam merumuskan indikator keberhasilan Program Kesadaran Keamanan Informasi melalui penentuan indikator keberhasilan, penyusunan instrumen evaluasi keberhasilan dan target Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan indikator keberhasilan Program Kesadaran Keamanan Informasi	1.1 **Indikator keberhasilan** Program Kesadaran Keamanan Informasi diuraikan sesuai tujuan program. 1.2 Indikator keberhasilan Program Kesadaran Keamanan Informasi ditentukan berdasarkan konteks sasaran.
2. Merancang instrumen evaluasi keberhasilan Program Kesadaran Keamanan Informasi	2.1 **Instrumen evaluasi** didefinisikan berdasarkan indikator keberhasilan. 2.2 Butir-butir pertanyaan disusun berdasarkan relevansi materi sosialisasi.
3. Menyusun target Program Kesadaran Keamanan Informasi	3.1 Target Program Kesadaran Keamanan Informasi dihitung sesuai indikator keberhasilan. 3.2 Target Program Kesadaran Keamanan Informasi ditentukan berdasarkan **skala prioritas**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk memerinci indikator keberhasilan Program Kesadaran Keamanan Informasi, menentukan target indikator keberhasilan Program Kesadaran Keamanan Informasi dan merancang instrumen evaluasi keberhasilan Program Kesadaran Keamanan Informasi.
   1.2 Indikator keberhasilan merupakan acuan capaian atas keberhasilan tujuan Program Kesadaran Keamanan Informasi.
   1.3 Instrumen evaluasi merupakan alat ukur untuk menilai pencapaian indikator keberhasilan pelaksanaan Program Kesadaran Keamanan Informasi meliputi metrik pengukuran antara lain objektif-subjektif, kuantitatif-kualitatif, statik-dinamik, absolut-relatif, dan metrik langsung maupun tidak langsung.
   1.4 Skala prioritas merupakan ukuran kebutuhan dari profil keamanan sasaran Program Kesadaran Keamanan Informasi berdasarkan tingkat urgensinya dengan tujuan yang sudah ditentukan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Perangkat lunak pengolah data
      2.1.3 Jaringan internet

2.2 Perlengkapan
2.2.1 Alat Tulis Kantor (ATK)
2.2.2 Kertas kerja

3. Peraturan yang diperlukan
(Tidak ada.)

4. Norma dan standar
4.1 Norma
(Tidak ada.)
4.2 Standar
(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam merumuskan indikator keberhasilan Program Kesadaran Keamanan Informasi melalui penentuan indikator keberhasilan, penyusunan instrumen evaluasi keberhasilan dan target Program Kesadaran Keamanan Informasi.
1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan, serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
1.3 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.
1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio, dan metode lain yang relevan.

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
3.1 Pengetahuan
3.1.1 Metode evaluasi
3.2 Keterampilan
3.2.1 Mengoperasikan perangkat lunak pengolah kata
3.2.2 Mengoperasikan perangkat lunak pengolah data

4. Sikap kerja yang diperlukan
4.1 Cermat dalam menyusun indikator keberhasilan Program Kesadaran Keamanan Informasi
4.2 Objektif dalam menentukan target indikator keberhasilan Program Kesadaran Keamanan Informasi

5. Aspek kritis
5.1 Kesesuaian dalam menentukan indikator keberhasilan Program Kesadaran Keamanan Informasi sesuai dengan tujuan program

KODE UNIT : **J.62KKI00.005.1**
JUDUL UNIT : **Menyusun Dokumen Perencanaan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun dokumen perencanaan Program Kesadaran Keamanan Informasi melalui penguraian komponen-komponen program serta pembuatan dokumen perencanaan Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Merangkaikan komponen Program Kesadaran Keamanan Informasi	1.1 Komponen Program Kesadaran Keamanan Informasi disusun berdasarkan ruang lingkup Program Kesadaran Keamanan Informasi. 1.2 **Komponen Program Kesadaran Keamanan Informasi** diidentifikasi berdasarkan analisis kebutuhan.
2. Membuat narasi perencanaan Program Kesadaran Keamanan Informasi	2.1 **Narasi perencanaan Program Kesadaran Keamanan Informasi** disusun berdasarkan komponen program. 2.2 Dokumen perencanaan Program Kesadaran Keamanan Informasi disusun secara lengkap sesuai format yang ditentukan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk merangkaikan komponen Program Kesadaran Keamanan Informasi dan membuat narasi perencanaan Program Kesadaran Keamanan Informasi.
   1.2 Komponen program yang dimaksud meliputi dokumen latar belakang, tujuan, ruang lingkup serta sumber daya yang dibutuhkan untuk menyelenggarakan program yaitu sarana dan prasarana, sumber daya manusia, anggaran, materi, waktu, penjadwalan, dan komponen lainnya.
   1.3 Narasi perencanaan Program Kesadaran Keamanan Informasi merupakan uraian rencana dalam upaya pencapaian tujuan Program Kesadaran Keamanan Informasi.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)

4.2 Standar
(Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun dokumen perencanaan Program Kesadaran Keamanan Informasi melalui penguraian komponen-komponen program serta pembuatan dokumen perencanaan Program Kesadaran Keamanan Informasi.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Dokumen perencanaan
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Komunikatif dalam menyusun narasi perencanaan Program Kesadaran Keamanan Informasi
   4.2 Cermat dalam menentukan komponen Program Kesadaran Keamanan Informasi
   4.3 Sistematis dan informatif dalam menyusun dokumen perencanaan Program Kesadaran Keamanan Informasi

5. Aspek kritis
   5.1 Ketepatan dalam menyusun dokumen perencanaan Program Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.006.1**
JUDUL UNIT : **Menyusun Kebutuhan Materi Program Kesadaran Keamanan Informasi yang Relevan**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun kebutuhan materi Program Kesadaran Keamanan Informasi melalui penentuan topik kesadaran keamanan serta sumber referensi yang relevan.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menentukan topik Program Kesadaran Keamanan Informasi	1.1 **Topik Program Kesadaran Keamanan Informasi** dirumuskan berdasarkan tujuan program. 1.2 **Kerangka materi Kesadaran Keamanan Informasi** dirancang sesuai dengan topik Program Kesadaran Keamanan Informasi.
2. Menentukan sumber referensi yang relevan	2.1 Sumber referensi dikumpulkan sesuai kerangka materi Kesadaran Keamanan Informasi. 2.2 Sumber referensi diverifikasi kelayakannya berdasarkan **prinsip ilmiah**.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk menentukan sumber referensi yang relevan dan memverifikasi kelayakan sumber referensi.
   1.2 Topik Program Kesadaran Keamanan Informasi merupakan tema besar terkait keamanan informasi yang menjadi isu utama pelaksanaan Program Kesadaran Keamanan Informasi.
   1.3 Kerangka materi Kesadaran Keamanan Informasi merupakan poin-poin utama dari topik yang dibahas yang akan menghasilkan materi Kesadaran Keamanan Informasi.
   1.4 Prinsip ilmiah yang dimaksud merupakan metode berpikir yang meliputi aspek logis, sistematis, objektif, berdasarkan fakta, berasal dari sumber yang dapat dipercaya, dan dapat dipertanggungjawabkan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyusun kebutuhan materi Program Kesadaran Keamanan Informasi melalui penentuan topik kesadaran keamanan serta sumber referensi yang relevan.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Prinsip ilmiah
   3.2 Keterampilan
      3.2.1 Mencari referensi
      3.2.2 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Cermat dalam menentukan sumber referensi
   4.2 Bertanggung jawab dalam memvalidasi sumber referensi

5. Aspek kritis
   5.1 Kesesuaian dalam merancang kerangka materi Kesadaran Keamanan Informasi sesuai dengan topik Program Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.007.1**
JUDUL UNIT : **Mengembangkan Materi Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja dalam mengembangkan materi Kesadaran Keamanan Informasi melalui perumusan metode sosialisasi dan penyusunan materi Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Merumuskan metode penyampaian materi Kesadaran Keamanan Informasi	1.1 Sasaran Program Kesadaran Keamanan Informasi diperiksa berdasarkan perencanaan Program Kesadaran Keamanan Informasi. 1.2 **Metode penyampaian materi** Kesadaran Keamanan Informasi ditetapkan sesuai dengan target dan sasaran Program Kesadaran Keamanan Informasi.
2. Menyusun materi Kesadaran Keamanan Informasi	2.1 Materi Kesadaran Keamanan Informasi dibuat berdasarkan **kerangka materi kesadaran keamanan informasi**. 2.2 **Media penyampaian materi** Kesadaran Keamanan Informasi ditentukan sesuai metode penyampaian materi Kesadaran Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit Kompetensi ini berlaku untuk mengidentifikasi metode penyampaian materi dan menyusun materi kesadaran keamanan dan informasi.
   1.2 Metode penyampaian materi yang dimaksud merupakan metode penyampaian materi Kesadaran Keamanan Informasi baik dengan satu arah atau dua arah.
   1.3 Kerangka materi Kesadaran Keamanan Informasi merupakan poin-poin utama dari topik yang dibahas yang akan menghasilkan materi Kesadaran Keamanan Informasi.
   1.4 Media penyampaian materi merupakan sarana yang digunakan untuk menyampaikan materi Kesadaran Keamanan Informasi dalam berbagai bentuk seperti poster, spanduk, buletin, maskot, situs web, aplikasi berbasis komputer, telekonferensi, tatap muka, pelatihan dengan instruktur, seminar, teka teki silang, program penghargaan, iklan layanan masyarakat, *podcast*, dan seminar daring.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak multimedia
      2.1.2 Perangkat lunak pengolah kata
      2.1.3 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Kertas kerja

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
   (Tidak ada.)
   4.2 Standar
   4.2.1 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-16 *Information Technology Security Training Requirements.*
   4.2.2 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-50 *Building an Information Technology Security Awareness and Training Program.*

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengembangkan materi Kesadaran Keamanan Informasi melalui perumusan metode sosialisasi dan penyusunan materi Kesadaran Keamanan Informasi.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
   3.1.1 Komunikasi publik
   3.1.2 Media komunikasi
   3.2 Keterampilan
   3.2.1 Mengoperasikan perangkat lunak multimedia
   3.2.2 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Kreatif dalam merancang konsep materi Kesadaran Keamanan Informasi
   4.2 Tepat dalam memaksimalkan penggunaan media sosialisasi

5. Aspek kritis
   5.1 Kesesuaian dalam membuat materi Kesadaran Keamanan Informasi berdasarkan kerangka materi Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.008.1**
JUDUL UNIT : **Melakukan Penyampaian Materi Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja dalam melakukan penyampaian materi Kesadaran Keamanan Informasi untuk mencapai target dan sasaran Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Menyiapkan pelaksanaan penyampaian materi Program Kesadaran Keamanan Informasi	1.1 Sarana dan prasarana penyampaian materi Program Kesadaran Keamanan Informasi disediakan sesuai kebutuhan. 1.2 **Bahan paparan** Program Kesadaran Keamanan Informasi disediakan sesuai kebutuhan.
2. Memberikan materi Program Kesadaran Keamanan Informasi	2.1 Materi Program Kesadaran Keamanan Informasi disampaikan berdasarkan perencanaan Program Kesadaran Keamanan Informasi. 2.2 Penyampaian materi Kesadaran Keamanan Informasi didokumentasikan sesuai kebutuhan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melakukan persiapan teknis sosialisasi Program Kesadaran Keamanan Informasi.
   1.2 Bahan paparan merupakan materi Program Kesadaran Keamanan Informasi yang meliputi dan tidak terbatas pada *file*, dokumen, video, audio, aplikasi dan sebagainya.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Perangkat lunak multimedia
      2.1.3 Perangkat keras multimedia
      2.1.4 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dapat dilakukan dalam melakukan penyampaian materi

Kesadaran Keamanan Informasi untuk mencapai target dan sasaran Program Kesadaran Keamanan Informasi.

1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.

1.3 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.

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

2. Persyaratan kompetensi
(Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Komunikasi publik
      3.1.2 Media komunikasi
   3.2 Keterampilan
      3.2.1 Melakukan transfer *knowledge*
      3.2.2 Mengoperasikan perangkat lunak pengolah kata
      3.2.3 Mengoperasikan perangkat lunak multimedia
      3.2.4 Mengoperasikan perangkat keras multimedia

4. Sikap kerja yang diperlukan
   4.1 Komunikatif dalam menyampaikan materi kesadaran keamanan informasi
   4.2 Adaptif di berbagai situasi dan membangun interaksi dengan lingkungan dalam menyampaikan Program Kesadaran Keamanan Informasi
   4.3 Bertanggung jawab dalam menjamin kesiapan teknis pelaksanaan sosialisasi Program Kesadaran Keamanan Informasi

5. Aspek kritis
   5.1 Kesesuaian penyampaian materi Kesadaran Keamanan Informasi berdasarkan perencanaan Program Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.009.1**
JUDUL UNIT : **Mengawasi Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam memastikan dan memantau kesesuaian antara perencanaan dan pelaksanaan Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan pemantauan kesesuaian pelaksanaan Program Kesadaran Keamanan Informasi	1.1 **Metode pemantauan** ditentukan sesuai narasi perencanaan Program Kesadaran Keamanan Informasi. 1.2 Pelaksanaan Program Kesadaran Keamanan Informasi dipantau kesesuaiannya dengan rencana aksi Program Kesadaran Keamanan Informasi.
2. Melakukan dokumentasi hasil pengawasan kesesuaian pelaksanaan Program Kesadaran Keamanan Informasi	2.1 Pemantauan kesesuaian pelaksanaan program didokumentasikan berdasarkan rencana aksi Program Kesadaran Keamanan Informasi. 2.2 Dokumentasi hasil pengawasan dilengkapi dengan bukti dukung hasil pemantauan.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk memastikan dan memantau kesesuaian pelaksanaan Program Kesadaran Keamanan Informasi dan mendokumentasikan hasil pemantauan kesesuaian pelaksanaan Program Kesadaran Keamanan Informasi.
   1.2 Metode pemantauan merupakan metode pengumpulan data untuk mengamati dan meninjau secara cermat dan langsung untuk mengetahui kesesuaian antara narasi perencanaan program dengan pelaksanaan di lapangan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Kertas kerja

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dapat dilakukan dalam memastikan dan memantau kesesuaian antara perencanaan dan pelaksanaan Program Kesadaran Keamanan Informasi.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Metode pengawasan
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Teliti dalam melakukan pemeriksaan terhadap pelaksanaan Program Kesadaran Keamanan Informasi
   4.2 Objektif dalam mengawasi pelaksanaan Program Kesadaran Keamanan Informasi

5. Aspek kritis
   5.1 Ketepatan dalam memantau kesesuaian pelaksanaan Program Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.010.1**
JUDUL UNIT : **Mengukur Tingkat Keberhasilan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengukur tingkat keberhasilan Program Kesadaran Keamanan Informasi melalui pengumpulan data dukung pengukuran dan analisis data hasil pengukuran sesuai indikator keberhasilan Program Kesadaran Keamanan Informasi.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Mengumpulkan data dukung pengukuran tingkat keberhasilan Program Kesadaran Keamanan Informasi	1.1 **Data hasil pengukuran** dikompilasi sesuai dengan **instrumen evaluasi**. 1.2 Data kompilasi hasil pengukuran diklasifikasikan berdasarkan tujuan dan konteks sasaran.
2. Melakukan analisis data pengukuran tingkat keberhasilan Program Kesadaran Keamanan Informasi	2.1 Data kompilasi hasil pengukuran ditelaah sesuai instrumen evaluasi Program Kesadaran Keamanan Informasi. 2.2 Data telaah hasil pengukuran tingkat keberhasilan Program Kesadaran Keamanan Informasi disimpulkan sesuai indikator keberhasilan Program Kesadaran Keamanan Informasi.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk mengumpulkan data dukung pengukuran tingkat keberhasilan Program Kesadaran Keamanan Informasi dan melakukan analisis data pengukuran tingkat keberhasilan Program Kesadaran Keamanan Informasi.
   1.2 Data hasil pengukuran meliputi data hasil pengukuran tingkat pemahaman, sikap, dan perilaku peserta Program Kesadaran Keamanan Informasi terhadap aspek keamanan informasi (kerahasiaan, integritas, dan ketersediaan), hasil pengukuran tingkat efektivitas metode sosialisasi, dan data lain yang dibutuhkan dalam penyusunan laporan.
   1.3 Instrumen evaluasi merupakan alat ukur untuk menilai pencapaian indikator keberhasilan pelaksanaan Program Kesadaran Keamanan Informasi meliputi metrik pengukuran antara lain objektif-subjektif, kuantitatif-kualitatif, statik-dinamik, absolut-relatif, dan metrik langsung maupun tidak langsung.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah data
      2.1.2 Perangkat lunak pengolah kata
      2.1.3 Internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Kertas kerja

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
       (Tidak ada.)
   4.2 Standar
       4.2.1 *National Institute of Standards and Technology Special Publication* (NIST SP) 800-50 *Building an Information Technology Security Awareness and Training Program*

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dapat dilakukan dalam mengukur tingkat keberhasilan Program Kesadaran Keamanan Informasi melalui pengumpulan data dukung pengukuran dan analisis data hasil pengukuran sesuai indikator keberhasilan Program Kesadaran Keamanan Informasi.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
       3.1.2 Metode evaluasi
   3.2 Keterampilan
       3.2.1 Mengoperasikan perangkat lunak pengolah data
       3.2.2 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Teliti dan cermat dalam melakukan pengukuran tingkat keberhasilan program keamanan informasi
   4.2 Objektif dalam melakukan analisis pengukuran tingkat keberhasilan program keamanan informasi
   4.3 Bertanggung jawab dalam melakukan pengukuran tingkat keberhasilan program keamanan informasi

5. Aspek kritis
   5.1 Kesesuaian dalam menyimpulkan data hasil pengukuran terhadap indikator keberhasilan Program Kesadaran Keamanan Informasi

KODE UNIT : **J.62KKI00.011.1**
JUDUL UNIT : **Menyusun Rekomendasi Perbaikan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam melakukan analisis kesenjangan capaian Program Kesadaran Keamanan Informasi dan merumuskan daftar tindak lanjut berdasarkan skala prioritas.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Melakukan analisis kesenjangan capaian Program Kesadaran Keamanan Informasi yang berjalan	1.1 **Data dukung** dikompilasi ke dalam capaian Program Kesadaran Keamanan Informasi. 1.2 **Capaian Program Kesadaran Keamanan Informasi** ditelaah sesuai indikator keberhasilan.
2. Merumuskan daftar tindak lanjut sebagai rekomendasi perbaikan Program Kesadaran Keamanan Informasi	2.1 **Daftar tindak lanjut** diidentifikasi sesuai hasil telaah capaian program. 2.2 Daftar tindak lanjut disusun berdasarkan skala prioritas.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk melakukan analisis kesenjangan capaian Program Kesadaran Keamanan Informasi yang berjalan dan menginventarisasi daftar tindak lanjut.
   1.2 Data dukung meliputi data perencanaan, data hasil pelaksanaan, dan data telaah pengukuran.
   1.3 Capaian program merupakan tingkat pencapaian aktual untuk Program Kesadaran Keamanan Informasi.
   1.4 Daftar tindak lanjut berisi rencana tindakan yang harus dilakukan setelah Program Kesadaran Keamanan Informasi dilaksanakan baik berupa evaluasi, perbaikan, atau pengembangan.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah data
      2.1.2 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Kertas kerja

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dapat dilakukan dalam melakukan analisis kesenjangan capaian Program Kesadaran Keamanan Informasi dan merumuskan daftar tindak lanjut berdasarkan skala prioritas.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Analisis rekomendasi kebijakan
      3.1.2 Prinsip Dasar Keamanan Informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak pengolah data

4. Sikap kerja yang diperlukan
   4.1 Teliti dan cermat dalam menyusun rekomendasi perbaikan Program Kesadaran Keamanan Informasi
   4.2 Objektif dalam menilai capaian program sesuai indikator keberhasilan

5. Aspek kritis
   5.1 Kesesuaian dalam menyusun daftar tindak lanjut berdasarkan skala prioritas

KODE UNIT : **J.62KKI00.012.1**
JUDUL UNIT : **Menyusun Laporan Kegiatan Program Kesadaran Keamanan Informasi**
DESKRIPSI UNIT : Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam membuat laporan Program Kesadaran Keamanan Informasi dan mengomunikasikan laporan tersebut kepada pihak terkait.

ELEMEN KOMPETENSI	KRITERIA UNJUK KERJA
1. Membuat narasi laporan Program Kesadaran Keamanan Informasi	1.1 **Dokumentasi kegiatan** dikelompokkan sesuai kebutuhan. 1.2 **Narasi Laporan Program Kesadaran Keamanan Informasi** disusun secara komprehensif berdasarkan format yang telah ditentukan.
2. Mengomunikasikan laporan Program Kesadaran Keamanan Informasi	2.1 **Ringkasan eksekutif** disusun sesuai ketentuan. 2.2 Ringkasan eksekutif disampaikan kepada pihak terkait.

BATASAN VARIABEL

1. Konteks variabel
   1.1 Unit kompetensi ini berlaku untuk membuat narasi laporan Program Kesadaran Keamanan Informasi dan mengkomunikasikan laporan Program Kesadaran Keamanan Informasi.
   1.2 Dokumentasi kegiatan merupakan catatan atau rekaman terhadap kegiatan pada suatu media tertentu yang digunakan untuk menggambarkan dan menjelaskan bukti pelaksanaan Program Kesadaran Keamanan Informasi.
   1.3 Narasi laporan program berisi dokumentasi kegiatan, analisis tingkat keberhasilan, hasil evaluasi, rekomendasi perbaikan, dan daftar tindak lanjut.
   1.4 Ringkasan eksekutif merupakan ringkasan yang berisi informasi-informasi penting mengenai segala hal yang ada di dalam laporan program.

2. Peralatan dan perlengkapan
   2.1 Peralatan
      2.1.1 Perangkat lunak pengolah kata
      2.1.2 Jaringan internet
   2.2 Perlengkapan
      2.2.1 Alat Tulis Kantor (ATK)
      2.2.2 Kertas kerja

3. Peraturan yang diperlukan
   (Tidak ada.)

4. Norma dan standar
   4.1 Norma
      (Tidak ada.)
   4.2 Standar
      (Tidak ada.)

PANDUAN PENILAIAN

1. Konteks penilaian
   1.1 Penilaian dilakukan terhadap pengetahuan, keterampilan, dan sikap kerja yang dapat dilakukan dalam membuat laporan Program Kesadaran Keamanan Informasi dan mengomunikasikan laporan tersebut kepada pihak terkait.
   1.2 Dalam pelaksanaannya, peserta/asesi harus dilengkapi dengan peralatan dan/atau perlengkapan, dokumen, bahan serta fasilitas asesmen yang dibutuhkan serta dilakukan pada tempat kerja atau Tempat Uji Kompetensi (TUK) yang aman.
   1.3 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.
   1.4 Metode asesmen yang dapat diterapkan meliputi kombinasi metode tes lisan, tes tertulis, wawancara, observasi tempat kerja atau demonstrasi atau simulasi, verifikasi bukti/portofolio dan metode lain yang relevan.

2. Persyaratan kompetensi
   (Tidak ada.)

3. Pengetahuan dan keterampilan yang diperlukan
   3.1 Pengetahuan
      3.1.1 Metode pelaporan
      3.1.2 Prinsip Dasar Keamanan Informasi
   3.2 Keterampilan
      3.2.1 Mengoperasikan perangkat lunak pengolah kata

4. Sikap kerja yang diperlukan
   4.1 Teliti dan cermat dalam mengompilasi dokumentasi kegiatan Program Kesadaran Keamanan Informasi
   4.2 Objektif dalam menyusun laporan program sesuai indikator keberhasilan
   4.3 Bertanggung jawab dalam menyampaikan simpulan eksekutif Program Kesadaran Keamanan Informasi

5. Aspek kritis
   5.1 Kesesuaian dalam menyusun narasi laporan Program Kesadaran Keamanan Informasi secara komprehensif

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 Kesadaran Keamanan Informasi maka SKKNI ini menjadi acuan dalam penyusunan jenjang kualifikasi nasional, penyelenggaraan pendidikan, pelatihan, dan sertifikasi kompetensi.

MENTERI KETENAGAKERJAAN
REPUBLIK INDONESIA,

IDA FAUZIYAH