PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2020
TENTANG
KAMUS KOMPETENSI TEKNIS
BIDANG KEAMANAN SIBER DAN PERSANDIAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang :

a. bahwa dalam menyelenggarakan manajemen Aparatur Sipil Negara berbasis sistem merit, setiap instansi pemerintah menyusun standar kompetensi jabatan;
b. bahwa sebagai pedoman penyusunan standar kompetensi jabatan perlu disusun kamus kompetensi teknis;
c. bahwa sesuai dengan ketentuan Pasal 7 ayat (1) Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 38 Tahun 2017 tentang Standar Kompetensi Jabatan Aparatur Sipil Negara, Kepala Badan Siber dan Sandi Negara selaku pejabat pembina kepegawaian berwenang menyusun dan menetapkan kamus kompetensi teknis bidang keamanan siber dan persandian;
d. bahwa kamus kompetensi teknis bidang keamanan siber dan persandian telah memperoleh persetujuan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi;
e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a sampai dengan huruf d, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Kamus Kompetensi Teknis Bidang Keamanan Siber dan Persandian;

Mengingat : 1. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100), sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 277);

2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 38 Tahun 2017 tentang Standar Kompetensi Jabatan Aparatur Sipil Negara (Berita Negara Republik Indonesia Tahun 2017 Nomor 1907);

3. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 1464);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG KAMUS KOMPETENSI TEKNIS BIDANG KEAMANAN SIBER DAN PERSANDIAN.

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Kompetensi Teknis adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur, dan dikembangkan yang spesifik berkaitan dengan bidang teknis jabatan.
2. Kamus Kompetensi Teknis Bidang Keamanan Siber dan Persandian yang selanjutnya disebut Kamus Kompetensi Teknis adalah kumpulan Kompetensi Teknis yang meliputi daftar jenis Kompetensi Teknis, definisi Kompetensi Teknis, deskripsi Kompetensi Teknis, dan indikator perilaku untuk setiap level Kompetensi Teknis yang diperlukan dalam jabatan pimpinan tinggi, jabatan administrasi, dan jabatan fungsional dalam bidang keamanan siber dan persandian.

Pasal 2

Kamus Kompetensi Teknis terdiri atas:

a. nama Kompetensi Teknis;
b. kode Kompetensi Teknis;
c. definisi Kompetensi Teknis;
d. level Kompetensi Teknis;
e. deskripsi level Kompetensi Teknis; dan
f. indikator perilaku.

Pasal 3

(1) Nama Kompetensi Teknis sebagaimana dimaksud dalam Pasal 2 huruf a merupakan pernyataan singkat yang menggambarkan ruang lingkup unit kompetensi.
(2) Kode Kompetensi Teknis sebagaimana dimaksud dalam Pasal 2 huruf b merupakan keterangan yang berisi kombinasi huruf dan angka untuk menerangkan bidang dan urutan Kompetensi Teknis.
(3) Definisi Kompetensi Teknis sebagaimana dimaksud dalam Pasal 2 huruf c merupakan bentuk kalimat yang menjelaskan secara singkat isi dari judul unit kompetensi yang mendeskripsikan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam menyelesaikan suatu tugas pekerjaan yang dipersyaratkan dalam judul unit kompetensi.
(4) Level Kompetensi Teknis sebagaimana dimaksud dalam Pasal 2 huruf d merupakan tingkatan suatu kompetensi dari tingkat mengerti dan memahami atau dalam pengembangan, tingkat dasar atau mampu menerapkan sesuai pedoman, tingkat menengah atau menerapkan dengan analisis, tingkat mumpuni atau mengevaluasi dan mampu memperoleh dukungan serta tingkat ahli atau mengembangkan.
(5) Deskripsi level Kompetensi Teknis sebagaimana dimaksud dalam Pasal 2 huruf e merupakan kalimat singkat yang menunjukkan suatu tingkatan kompetensi atau tingkat penguasaan kompetensi tertentu.

(6) Indikator perilaku sebagaimana dimaksud dalam Pasal 2 huruf f merupakan kalimat yang menunjukkan rincian lebih lanjut dari deskripsi level berupa perilaku yang dapat diukur yang menunjukan ciri-ciri dari suatu tingkat penguasaan suatu kompetensi.

Pasal 4

(1) Kamus Kompetensi Teknis digunakan sebagai acuan dalam menyusun standar kompetensi jabatan pimpinan tinggi, jabatan administrasi, dan jabatan fungsional di bidang keamanan siber dan persandian sesuai dengan karakteristik tugas jabatan.

(2) Kamus Kompetensi Teknis sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 5

Kamus Kompetensi Teknis sebagaimana dimaksud dalam Pasal 4 dievaluasi dan disesuaikan secara berkelanjutan sesuai dinamika perubahan dan kebutuhan di bidang keamanan siber dan persandian.

Pasal 6

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Badan ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 17 Desember 2020

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 21 Desember 2020

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd.

WIDODO EKATJAHJANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2020 NOMOR 1562

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 11 TAHUN 2020
TENTANG
KAMUS KOMPETENSI TEKNIS BIDANG KEAMANAN SIBER DAN PERSANDIAN

KOMPETENSI TEKNIS BIDANG KEAMANAN SIBER DAN PERSANDIAN

No.	Kompetensi
1.	Manajemen Keamanan Siber dan Persandian
2.	Advokasi Kebijakan Keamanan Siber
3.	Manajemen Risiko Keamanan Siber
4.	Penilaian Keamanan Teknologi Informasi
5.	Intelijen Siber
6.	*Monitoring* Keamanan Jaringan
7.	Audit Keamanan Informasi
8.	Penyediaan Layanan Keamanan Informasi
9.	Pengelolaan CSIRT
10.	Manajemen Insiden Siber
11.	Manajemen Krisis Siber
12.	Forensik Digital
13.	Investigasi Siber
14.	*Data Science* Keamanan Siber dan Sandi Negara
15.	Analisis Kripto
16.	Rekayasa Kriptografi
17.	Rancang Bangun Perangkat Keamanan Teknologi Informasi
18.	Pengkajian Teknologi Keamanan Siber dan Sandi
19.	Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara
20.	Pengelolaan *Security Operation Center* (SOC)
21.	Pengelolaan Pusat Kontak Siber Nasional
22.	Analisis Kelaikan Sertifikasi Elektronik
23.	Pemenuhan Teknis Sistem Sertifikasi Elektronik
24.	Pengelolaan Jaringan dan Infrastruktur Sertifikasi Elektronik
25.	Verifikasi Algoritma Kriptografi
26.	*Functional Testing*
27.	Analisis Kerawanan Produk Keamanan Siber dan Sandi Negara
28.	Pengelolaan Pengujian Produk Keamanan Siber dan Sandi Negara
29.	Pengelolaan Sertifikasi Produk Keamanan Siber dan Sandi Negara

30.	Validasi Dokumen Sertifikasi
31.	Diplomasi Siber
32.	Penapisan Konten
33.	Penyusunan Kebijakan Keamanan Siber

KAMUS KOMPETENSI TEKNIS BIDANG KEAMANAN SIBER DAN PERSANDIAN

1. MANAJEMEN KEAMANAN SIBER DAN PERSANDIAN

Nama Kompetensi	:	Manajemen Keamanan Siber dan Persandian
Kode Kompetensi	:	T.KSS-01
Definisi	:	Kemampuan dalam memahami, menerapkan, menganalisis, mengevaluasi, dan mengembangkan suatu kebijakan untuk mengelola keamanan informasi.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar dan menguasai teori manajemen keamanan siber dan persandian.	1.1. Mampu menjelaskan konsep dasar manajemen keamanan siber dan persandian. 1.2. Mampu menguraikan tahapan implementasi teori manajemen keamanan siber dan persandian. 1.3. Mampu mengasosiasikan teori manajemen keamanan informasi dengan norma, standar, prosedur, dan kriteria manajemen keamanan siber dan persandian.
2	Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan siber dan persandian.	2.1. Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian. 2.2. Mampu mengklasifikasikan aset-aset penting yang rentan terhadap ancaman. 2.3. Mampu mengkalkulasikan risiko keamanan siber dan persandian.

3	Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian.	3.1. Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku. 3.2. Mampu menganalisis prosedur teknis penerapan kontrol keamanan siber dan persandian ke dalam format norma, standar, prosedur, dan kriteria yang berlaku. 3.3. Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian.
4	Mengevaluasi penyelenggaraan manajemen keamanan informasi	4.1. Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan siber dan persandian. 4.2. Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian. 4.3. Mampu memproyeksikan kebutuhan pengembangan kebijakan manajemen keamanan siber dan persandian berdasarkan peraturan maupun standar yang berlaku. 4.4. Mampu mensosialisasikan kebijakan manajemen keamanan siber dan persandian.
5	Merumuskan manajemen keamanan informasi	5.1. Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian. 5.2. Mampu merumuskan kebijakan manajemen keamanan siber dan persandian yang lugas dan jelas

		untuk menghindari perbedaan dalam penafsiran. 5.3. Mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian.

2. ADVOKASI KEBIJAKAN KEAMANAN SIBER

Nama Kompetensi	:	Advokasi Kebijakan Keamanan Siber
Kode Kompetensi	:	T.KSS-02
Definisi	:	Kemampuan yang berkaitan dengan pengetahuan dan keterampilan untuk melakukan usaha untuk memengaruhi serta mengupayakan terjadinya perubahan dalam diri pemangku kepentingan melalui sosialisasi, pendekatan, fasilitasi bimbingan, dan pendampingan untuk mengadopsi dan menerapkan kebijakan.

Level	Deskripsi	Indikator Perilaku
1	Memahami substansi kebijakan, teknik, dan metode advokasi.	1.1. Mampu menjelaskan konsep dasar dan tujuan kebijakan, landasan filosofis, landasan hukum, landasan sosiologis, proses, pokok materi substansi kebijakan, tahap perumusan dan implementasi, serta ukuran keberhasilan penerapan kebijakan. 1.2. Mampu memahami tahapan kegiatan advokasi, pembinaan, fasilitasi, dan pendampingan penerapan kebijakan. 1.3. Mampu mengidentifikasi kebutuhan advokasi dari pemangku kepentingan.
2	Mampu melakukan advokasi kebijakan keamanan siber.	2.1. Mampu menyusun rencana pelaksanaan kegiatan advokasi kebijakan.

		2.2. Mampu membuat alat bantu untuk kebutuhan advokasi, melakukan sosialisasi kebijkaan dengan audiensi lingkup kecil. 2.3. Mampu mengidentifikasi posisi dasar dan kebutuhan pemangku kepentingan terkait advokasi kebijakan.
3	Mampu menyelenggarakan advokasi kebijakan keamanan siber.	3.1. Mampu bahan menyusun instrumen dan pelaksanaan advokasi kebijakan pendekatan, melalui bimbingan sosialisasi, teknis, pendampingan, dan *monitoring* evaluasi advokasi kebijakan. 3.2. Mampu mengembangkan serta menjalankan strategi atau intervensi melalui sosialisasi, pendekatan, bimbingan teknis, dan pendampingan dalam mengatasu hambatan sistemis dan resistensi pemangku kepentingan dalam menerapkan kebijakan. 3.3. Mampu mengimplementasikan strategi komunikasi dengan target dan waktu yang terukur dan terencana dengan mendapatkan hasil sesuai yang diharapkan antara lain pemangku kepentingan dapat memahami serta menerapkan kebijakan, *monitoring*, dan evaluasi kebijakan.
4	Mampu mengevaluasi dan menyusun perangkat norma, prosedur, dan instrumen dalam	4.1. Mampu mengevaluasi teknik, metode, dan strategi advokasi yang ada saat ini, menganalisis kelemahan dan kekurangan serta mengembangkan berbagai teknik, metode, dan strategi advokasi

	advokasi kebijakan keamanan siber.	yang lebih efektif dan efisien dari berbagai kondisi pemangku kepentingan. 4.2. Mampu mengembangkan norma standar, kriteria, pedoman, petunjuk teknis strategi komunikasi, dan pelaksanaan advokasi yang efektif serta *monitoring* evaluasi advokasi kebijakan. 4.3. Mampu meyakinkan dan memperoleh dukungan dari pemangku kepentingan, memberikan bimbingan, dan fasilitasi kepada pemangku kepentingan.
5	Mampu mengembangkan, menyinergiskan, dan mengintegrasikan konsep kebijakan advokasi yang berdampak nasional dan/ atau internasional.	5.1. Mampu mengembangkan konsep, kebijakan, teknik metode advokasi kebijakan keamanan siber, *monitoring*, dan evaluasi kebijakan keamanan siber. 5.2. Mampu mengembangkan strategi advokasi kebijakan, sinkronisasi, dan koordinasi implementasi kebijakan yang terintegrasi dan saling melengkapi (komplementer) dengan kebijakan lain yang dapat memberi dampak positif di tingkat nasional atau internasional. 5.3. Mampu menjadi mentor dan rujukan nasional dalam pemecahan masalah advokasi kebijakan.

3. MANAJEMEN RISIKO KEAMANAN SIBER

Nama Kompetensi	:	Manajemen Risiko Keamanan siber
Kode Kompetensi	:	T.KSS-03
Definisi	:	Kemampuan dalam mengidentifikasi, menilai, dan mengelola risiko keamanan

		siber, serta mengevaluasi pelaksanaan manajemen risiko keamanan siber.
Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar dan menguasai teori manajemen risiko keamanan informasi.	1.1. Mampu menjelaskan risiko keamanan informasi. 1.2. Mampu menyebutkan risiko dalam keamanan informasi. 1.3. Mampu menjelaskan konsep dan teori dalam manajemen risiko. 1.4. Mampu mengidentifikasi aset yang terkait dengan keamanan informasi.
2	Mampu mengaplikasikan manajemen risiko keamanan informasi.	2.1. Mampu mengklasifikasikan aset yang terkait keamanan informasi. 2.2. Mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan. 2.3. Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan.
3	Mampu melaksanakan penilaian risiko dan menganalisis penerapan manajemen risiko.	3.1. Mampu mengidentifikasi risiko berdasarkan aset maupun proses bisnis organisasi. 3.2. Mampu menganalisis risiko dalam rangka penilaian risiko. 3.3. Mampu menganalisis metode penanganan risiko dalam bentuk *risk treatment plan* dan/atau *risk register*. 3.4. Mampu memberi pertimbangan dalam penyusunan prosedur dan kebijakan yang diperlukan dalam pelaksanaan manajemen risiko keamanan informasi.
4	Mengevaluasi manajemen risiko.	4.1. Mampu menilai tingkat kematangan manajemen risiko keamanan informasi suatu organisasi.

		4.2. Mampu mengevaluasi efektivitas dan efisiensi pelaksanaan manajemen risiko. 4.3. Mampu mengevaluasi *Risk Treatment Plan* yang sudah ada. 4.4. Mampu mengevaluasi prosedur dan kebijakan manajemen risiko organisasi.
5	Menciptakan dan mengkreasikan sesuatu berhubungan dengan manajemen risiko.	5.1. Mampu menyusun metodologi manajemen risiko keamanan informasi yang tepat dan komprehensif. 5.2. Mampu merancang *framework* manajemen risiko keamanan informasi. 5.3. Mampu merumuskan rekomendasi manajemen risiko keamanan informasi secara nasional baik untuk sektor pemerintah, infrastruktur kritis, mauput privat. 5.4. Mampu merumuskan strategi manajemen risiko keamanan informasi secara nasional.

4. PENILAIAN KEAMANAN TEKNOLOGI INFORMASI

Nama Kompetensi	:	Penilaian Keamanan Teknologi Informasi
Kode Kompetensi	:	T.KSS-04
Definisi	:	Kemampuan dalam menemukan, mengidentifikasi, menganalisis dampak dari sebuah celah keamanan pada sistem informasi serta merumuskan rekomendasi pengamanannya.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik, metode, tata cara, dan prosedur dalam	1.1. Mampu menjelaskan jenis, karakteristik, dan dampak *malware*.

	melakukan penilaian keamanan teknologi informasi.	1.2. Mampu menjelaskan teknik dan metode dalam melakukan analisis *malware*. 1.3. Mampu menjelaskan jenis dan ragam teknologi informasi yang akan dinilai keamanannya. 1.4. Mampu menjelaskan fungsi dan manfaat perangkat penilaian keamanan teknologi informasi.
2	Mampu menerapkan teknik, metode, tata cara, dan prosedur dalam melakukan pengujian keamanan teknologi informasi.	2.1. Mampu menentukan teknik dan metode dalam melakukan pengujian keamanan teknologi informasi. 2.2. Mampu mengoperasikan perangkat pengujian keamanan teknologi informasi. 2.3. Mampu mengilustrasikan hasil pengumpulan aktivitas *malware* pada perangkat teknologi keamanan informasi. 2.4. Mampu mendemonstrasikan pengujian keamanan teknologi informasi. 2.5. Mampu menemukan celah keamanan pada teknologi informasi.
3	Mampu menganalisis hasil pengujian keamanan teknologi informasi.	3.1. Mampu mengidentifikasi teknik dan metode analisis keamanan teknologi informasi yang dibutuhkan. 3.2. Mampu mengkoreksi teknik dan metode analisis keamanan teknologi informasi. 3.3. Mampu menganalisis dampak yang ditimbulkan oleh *malware* pada perangkat teknologi keamanan informasi. 3.4. Mampu mendiagnosis karakteristik *malware* terhadap

		suatu perangkat teknologi keamanan informasi. 3.5. Mampu memvalidasi hasil temuan celah keamanan teknologi informasi.
4	Mampu memberikan pertimbangan pelaksanaan penilaian keamanan teknologi informasi.	4.1. Mampu memberi pertimbangan terhadap tata cara pelaksanaan penilaian keamanan teknologi informasi. 4.2. Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan penilaian keamanan teknologi informasi. 4.3. Mampu menyusun materi diseminasi penilaian keamanan teknologi. 4.4. Mampu meyakinkan pemangku kepentingan terkait manfaat penilaian keamanan teknologi informasi.
5	Mampu merancang pelaksanaan penilaian keamanan teknologi informasi.	5.1. Mampu merumuskan rekomendasi pengamanan teknologi informasi secara nasional. 5.2. Mampu mengembangkan teknik dan metode pelaksanaan penilaian keamanan teknologi informasi. 5.3. Mampu merancang strategi kerja sama pertukaran informasi hasil penilaian keamanan teknologi informasi tingkat nasional, regional, bilateral, atau multilateral.

5. INTELIJEN SIBER

Nama Kompetensi	:	Intelijen Siber
Kode Kompetensi	:	T.KSS-05
Definisi	:	Kemampuan dalam memahami, menerapkan, menganalisis,

		memberikan rekomendasi terkait kegiatan pengumpulan informasi, *profiling*, pembinaan komunitas serta ancaman dan kerawanan siber.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik, metode, tata cara, dan prosedur dalam melakukan intelijen siber.	1.1. Mampu menjelaskan konsep dasar, teknik, metode, tata cara, dan prosedur pengumpulan informasi intelijen. 1.2. Mampu menjelaskan konsep dasar, teknik, metode, tata cara, dan prosedur analisis intelijen siber. 1.3. Mampu memahami konsep dasar, teknik, metode, tata cara, dan prosedur dalam menentukan ruang lingkup target *monitoring*. 1.4. Mampu mengkategorikan sumber data intelijen siber. 1.5. Mampu menggali komunitas keamanan informasi, keamanan siber, dan persandian.
2	Mampu menerapkan konsep dasar, teknik, metode, tata cara, dan prosedur dalam melakukan intelijen siber.	2.1. Mampu menentukan teknik dan metode pengumpulan informasi intelijen yang dibutuhkan. 2.2. Mampu menentukan teknik dan metode pengolahan informasi intelijen yang dibutuhkan. 2.3. Mampu mengoperasikan perangkat pengumpulan dan pengolahan informasi intelijen. 2.4. Mampu mengilustrasikan hasil pengumpulan informasi intelijen.
3	Mampu melakukan analisis informasi intelijen siber.	3.1. Mampu menfidentifikasi teknik dan metode analisis informasi intelijen yang dibutuhkan. 3.2. Mampu mengkorelasikan teknik dan metode analisis informasi intelijen siber.

		3.3. Mampu memberikan bimbingan teknis dan asistensi dalam melakukan analisis informasi intelijen. 3.4. Mampu mengidentifikasi karakteristik dari target *monitoring*. 3.5. Mampu menyimpulkan pola, metode, teknik ancaman keamanan informasi, keamanan siber, dan persandian. 3.6. Mampu mengkorelasikan data hasil pengumpulan informasi intelijen siber. 3.7. Mampu melakukan analisis *profiling* terhadap target pengguna media sosial.
4	Mampu memberikan pertimbangan pelaksanaan intelijen siber.	4.1. Mampu memutuskan analisis ruang lingkup target *monitoring* intelijen siber. 4.2. Mampu memvalidasi target *monitoring*. 4.3. Mampu memprediksi ancaman dan kerawanan siber. 4.4. Mampu memberi pertimbangan terhadap tata cara pelaksanaan intelijen siber. 4.5. Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan intelijen siber.
5	Mampu merancang pelaksanaan intelijen siber.	5.1. Mampu memberikan rekomendasi taktis, operasional dan strategis. 5.2. Mampu mengembangkan teknik dan metode pelaksanaan intelijen siber. 5.3. Mampu merumuskan rekomendasi keamanan informasi, keamanan siber, dan persandian secara nasional.

6. *MONITORING KEAMANAN JARINGAN*

Nama Kompetensi	:	*Monitoring* Keamanan Jaringan
Kode Kompetensi	:	T.KSS-06
Definisi	:	Kemampuan untuk mengimplementasikan, mengumpulkan, menganalisis informasi dan aktivitas data dalam sebuah jaringan sistim informasi dalam rangka pengamanan siber.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik, metode, tata cara, dan prosedur dalam melakukan *monitoring* keamanan jaringan.	1.1. Mampu menjelaskan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan. 1.2. Mampu menjelaskan fungsi dan manfaat perangkat *monitoring* keamanan jaringan. 1.3. Mampu menjelaskan tata cara dalam melakukan konfigurasi perangkat *monitoring* keamanan jaringan.
2	Mampu menerapkan *monitoring* keamanan jaringan.	2.1. Mampu menggunakan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan. 2.2. Mampu mengoperasikan perangkat *monitoring* keamanan jaringan. 2.3. Mampu mengilustrasikan hasil pengumpulan aktivitas data dalam jaringan. 2.4. Mampu mendemonstrasikan *monitoring* lalu lintas jaringan.
3	Mampu melakukan analisis keamanan jaringan.	3.1. Mampu mengidentifikasi teknik dan metode analisis keamanan jaringan yang dibutuhkan. 3.2. Mampu mengkorelasikan teknik dan metode analisis keamanan jaringan.

		3.3.	Mampu mendeteksi adanya anomali pada *log* perangkat *monitoring* keamanan jaringan.
		3.4.	Mampu menganalisis hasil temuan anomali.
4	Mampu memberikan pertimbangan pelaksanaan *monitoring* keamanan jaringan.	3.1.	Mampu memutuskan ruang lingkup target *monitoring* jaringan.
		3.2.	Mampu menyimpulkan pola, metode, dan teknik serangan pada jaringan.
		3.3.	Mampu memprediksi ancaman dan kerawanan jaringan.
		3.4.	Mampu memberi pertimbangan terhadap tata cara pelaksanaan *monitoring* keamanan jaringan.
		3.5.	Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan *monitoring* keamanan jaringan.
		3.6.	Mampu menyusun materi diseminasi keamanan jaringan.
		3.7.	Mampu meyakinkan pemangku kepentingan terkait manfaat *monitoring* keamanan jaringan.
5	Mampu merancang pelaksanaan *monitoring* keamanan jaringan.	5.1.	Mampu merancang implementasi pengamanan jaringan secara nasional.
		5.2.	Mampu merancang strategi kerja sama pertukaran informasi hasil *monitoring* keamanan jaringan tingkat nasional.
		5.3.	Mampu merancang strategi kerja sama pertukaran informasi hasil *monitoring* keamanan jaringan tingkat nasional.
		5.4.	Mampu mengembangkan kebijakan pengamanan jaringan secara nasional.

		5.5. Mampu menilai kebijakan pengamanan jaringan secara nasional.

7. AUDIT KEAMANAN INFORMASI

Nama Kompetensi	:	Audit Keamanan Informasi
Kode Kompetensi	:	T.KSS-07
Definisi	:	Kemampuan mengumpulkan dan mengolah data, mengidentifikasi, menganalisis, merumuskan, menyelenggarakan, membimbing, mengevaluasi, dan mengembangkan teori, konsep, metode, prosedur, peraturan, dan pelaksanaan audit keamanan informasi.

Level	Deskripsi	Indikator Perilaku
1	Mampu menjelaskan konsep audit keamanan informasi, keamanan siber, dan persandian.	1.1. Mampu menjelaskan tahapan audit keamanan informasi, keamanan siber, dan persandian. 1.2. Mampu menjelaskan tujuan dan manfaat audit keamanan informasi, keamanan siber, dan persandian. 1.3. Mampu mengidentifikasi norma, standar, prosedur, dan kriteria audit keamanan informasi lain yang berlaku.
2	Menerapkan konsep audit keamanan informasi, keamanan siber, dan persandian.	2.1. Mampu menentukan standar, prosedur, dan kriteria audit keamanan informasi, keamanan siber, dan persandian. 2.2. Mampu menggunakan instrumen audit keamanan informasi, keamanan siber, dan persandian. 2.3. Mampu menentukan data yang diperlukan untuk kegiatan audit keamanan informasi, keamanan siber, dan persandian.

3	Mengaudit keamanan informasi, keamanan siber, dan persandian sesuai dengan prosedur/petunjuk teknis.	3.1.	Mampu menelaah kesesuaian data pada kegiatan audit keamanan informasi, keamanan siber, dan persandian.
		3.2.	Mampu mengaudit lapangan sesuai norma, standar, prosedur, dan kriteria tentang audit keamanan informasi, keamanan siber, dan persandian.
		3.3.	Mampu mendokumentasikan hasil audit keamanan informasi, keamanan siber, dan persandian.
		3.4.	Mampu memeriksa proses audit keamanan informasi, keamanan siber, dan persandian.
4	Mengevaluasi pelaksanaan audit keamanan informasi, keamanan siber, dan persandian.	4.1.	Mampu mengevaluasi rekomendasi hasil audit keamanan informasi, keamanan siber, dan persandian.
		4.2.	Mampu menilai tindak lanjut implementasi rekomendasi audit keamanan informasi, keamanan siber, dan persandian.
		4.3.	Mampu mengevaluasi instrumen audit keamanan informasi, keamanan siber, dan persandian.
5	Merumuskan konsep kebijakan dan standar sebagai acuan pelaksanaan audit keamanan informasi, keamanan siber, dan persandian.	5.1.	Mampu menyusun kebijakan dan standar audit Keamanan Informasi, keamanan siber, dan persandian.
		5.2.	Mampu merumuskan kajian kebijakan dan standar audit keamanan informasi, keamanan siber, dan persandian.
		5.3.	Mampu menyusun strategi implementasi terkait audit keamanan informasi, keamanan siber, dan persandian.

8. PENYEDIAAN LAYANAN KEAMANAN INFORMASI

Nama Kompetensi	:	Penyediaan Layanan Keamanan Informasi
Kode Kompetensi	:	T.KSS-08
Definisi	:	Kemampuan mengidentifikasi, menyelenggarakan, menganalisis, mengevaluasi, dan merumuskan teori, konsep, metode, prosedur, peraturan, dan pelaksanaan penyediaan layanan keamanan informasi.

Level	**Deskripsi**	**Indikator Perilaku**
1	Memahami konsep dasar, metode, dan peraturan penyediaan layanan keamanan informasi.	1.1. Mampu menjelaskan jenis dan konsep penyediaan layanan keamanan informasi. 1.2. Mampu menjelaskan tahapan penyediaan layanan keamanan informasi. 1.3. Mampu mengidentifikasi norma, standar, prosedur, dan kriteria penyediaan layanan keamanan informasi.
2	Menyelenggarakan penyediaan layanan keamanan informasi sesuai dengan prosedur/petunjuk teknis.	2.1. Mampu menentukan kebutuhan pengguna dan kecukupan sumber daya yang dialokasikan oleh organisasi untuk melaksanakan penyediaan layanan keamanan informasi. 2.2. Mampu melaksanakan layanan keamanan informasi berdasarkan norma, standar, prosedur, dan kriteria yang berlaku. 2.3. Mampu menangani permasalahan teknis saat penyelenggaraan layanan keamanan informasi.
3	Mengelola penyelenggaraan penyediaan layanan keamanan informasi.	3.1. Mampu menganalisis kebutuhan penyelenggaraan layanan keamanan informasi sesuai dengan kebutuhan pengguna dan kecukupan sumber daya yang

		dialokasikan oleh organisasi atau pengguna. 3.2. Mampu menganalisis norma, standar, prosedur, dan kriteria untuk penyelenggaraan layanan keamanan informasi. 3.3. Mampu memberikan bimbingan teknis mengenai layanan keamanan informasi yang akan diterapkan.
4	Mengevaluasi penyelenggaraan penyediaan layanan keamanan informasi.	4.1. Mampu mengevaluasi pelaksanaan layanan keamanan informasi. 4.2. Mampu mengevaluasi standar penyelenggaraan layanan keamanan informasi. 4.3. Mampu memberi rekomendasi perbaikan penyelenggaraan layanan keamanan informasi.
5	Merumuskan kebijakan dan strategi penyediaan layanan keamanan informasi.	5.1. Mampu mengembangkan kebijakan penyelenggaraan layanan keamanan informasi. 5.2. Mampu merumuskan kebijakan penyediaan layanan keamanan informasi. 5.3. Mampu menyusun strategi implementasi layanan keamanan informasi.

9. PENGELOLAAN CSIRT

Nama Kompetensi	:	Pengelolaan CSIRT
Kode Kompetensi	:	T.KSS-09
Definisi	:	Kemampuan untuk melakukan asistensi CSIRT, membangun kapabilitas CSIRT, melakukan penilaian kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber, dan penilaian kematangan CSIRT, serta evaluasi hasil

		penilaian kesiapan dan kematangan CSIRT.
Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar CSIRT dan tahapan penyelenggaraan CSIRT	1.1. Mampu menjelaskan konsep dasar CSIRT, peraturan terkait CSIRT, dan prosedur penyelenggaraan CSIRT, tata cara prosedur untuk asistensi CSIRT. 1.2. Mampu menjelaskan langkah-langkah dalam membangun kapabilitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber. 1.3. Mampu menjelaskan langkah-langkah dalam melakukan penilaian kesiapan CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber. 1.4. Mampu menjelaskan langkah-langkah dalam melakukan penilaian kematangan CSIRT.
2	Mampu melaksanakan pengelolaan CSIRT sesuai prosedur	2.1. Mampu menerapkan prosedur untuk melakukan asistensi CSIRT. 2.2. Mampu menerapkan prosedur pada kegiatan yang terkait pembangunan kapabilitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber, sesuai prosedur. 2.3. Mampu menentukan sumber data yang diperlukan dalam penilaian kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber.

		2.4. Mampu menentukan sumber data yang diperlukan dalam penilaian kematangan CSIRT.
3	Mampu menyusun bahan materi pada kegiatan pengelolaan CSIRT	3.1. Mampu membuat bahan materi pada kegiatan asistensi CSIRT. 3.2. Mampu membuat bahan materi pada pelaksanaan kegiatan pembangunan kapabilitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber. 3.3. Mampu menguji kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber. 3.4. Mampu menguji kematangan CSIRT.
4	Mampu mengevaluasi kegiatan yang terkait dengan pengelolaan CSIRT	4.1. Mampu memberikan pertimbangan dalam rangka evaluasi kegiatan asistensi CSIRT. 4.2. Mampu memberikan pertimbangan dalam rangka evaluasi kegiatan pembangunan kapasitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber. 4.3. Mampu merinci aspek-aspek penilaian kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber. 4.4. Mampu merinci aspek-aspek penilaian kematangan CSIRT. 4.5. Mampu mengevaluasi penilaian kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber.

		4.6. Mampu mengevaluasi instrumen audit keamanan informasi, keamanan siber, dan persandian.
5	Mampu mengembangkan konsep, teori, kebijakan, dan menjadikannya sebagai standar acuan bagi pengelolaan CSIRT	5.1. Mampu mengembangkan konsep, teknik, atau kebijakan baru terkait asistensi CSIRT. 5.2. Mampu mengembangkan konsep, teknik, atau kebijakan baru dalam kegiatan pembangunan kapasitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber. 5.3. Melakukan perumusan rekomendasi atas kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber. 5.4. Melakukan perumusan rekomendasi terhadap kematangan CSIRT.

10. MANAJEMEN INSIDEN SIBER

Nama Kompetensi	:	Manajemen Insiden Siber
Kode Kompetensi	:	T.KSS-10
Definisi	:	Kemampuan untuk mengumpulkan, mengidentifikasi, menilai, memahami, dan mengatasi situasi dari saat pertama kali insiden siber terjadi sampai ke titik pemulihan kembali.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, dan tata cara prosedur manajemen insiden siber.	1.1. Mampu menjelaskan konsep dasar, teknik metode, peraturan dan mekanisme, dan tata cara prosedur manajemen insiden siber. 1.2. Mampu menjelaskan tahapan pelaksanaan manajemen insiden siber.

		1.3.	Mampu menjelaskan berbagai manfaat dari manajemen insiden siber.
2	Mampu melaksanakan manajemen insiden siber sesuai pedoman kerja/petunjuk teknis.	2.1.	Mampu melaksanakan proses manajemen insiden sesuai prosedur yang ditetapkan.
		2.2.	Mampu menggunakan alat, metode, dan teknik untuk melakukan manajemen insiden siber.
		2.3.	Mampu mengidentifikasi permasalahan dasar terkait manajemen insiden siber.
		2.4.	Mampu menggambarkan prosedur pengelolaan data alumni dalam bentuk SOP sederhana dan jadwal kerja.
		2.5.	Mampu mendemonstrasikan prosedur dan teknik pengelolaan.
3	Mampu menyelenggarakan manajemen insiden siber.	3.1.	Mampu melakukan analisis terkait manajemen insiden siber.
		3.2.	Mampu melaksanakan rekomendasi teknis terkait manajemen insiden siber.
		3.3.	Mampu membimbing perbaikan kesalahan prosedur dalam manajemen insiden siber.
		3.4.	Mampu menunjukkan perbandingan antara kedua metode pengelolaan data tersebut, setidaknya dari segi kelebihan dan kekurangan.
		3.5.	Mampu mengomunikasikan hasil analisis melalui lisan dan tulisan.
4	Mampu menganalisis manajemen insiden siber.	4.1.	Mampu melakukan evaluasi implementasi Pengamanan Informasi.
		4.2.	Mampu merancang metode dalam meningkatkan efisiensi dan/atau

		efektivitas manajemen insiden siber pada lingkup instansinya. 4.3. Mampu melakukan penilaian kesiapan manajemen insiden siber pada lingkup instansinya. 4.4. Mampu merancang skenario simulasi kesiapan manajemen insiden siber. 4.5. Mampu melakukan penilaian keamanan informasi dan penentuan insiden keamanan informasi.
5	Mampu mengembangkan konsep, teori, kebijakan, teknik metode, dan analisis manajemen insiden siber.	5.1. Mampu mengembangkan kebijakan, rencana, dan strategi sesuai dengan hukum, peraturan, kebijakan, dan standar manajemen insiden siber. 5.2. Mengidentifikasi, menganalisis teori, konsep, dan kebijakan manajemen insiden siber, serta menemukan kelebihan dan kekurangan perbaikannya. 5.3. Mengembangkan teori, konsep, dan kebijakan terkait manajemen insiden siber, meyakinkan unit kerja terkait dan pemangku kepentingan untuk menerima konsep, teori, dan kebijakan yang dikembangkan. 5.4. Menjadi mentor dan sumber rujukan utama (nasional) dalam implementasi manajemen insiden siber.

11. MANAJEMEN KRISIS SIBER

Nama Kompetensi	:	Manajemen Krisis Siber
Kode Kompetensi	:	T.KSS-11
Definisi	:	Kemampuan untuk mengumpulkan, mengidentifikasi, menilai, memahami, dan mengatasi situasi yang serius

		terutama dari saat pertama kali insiden siber terjadi sampai ke titik pemulihan kembali.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, dan tata cara prosedur manajemen krisis siber.	1.1. Memahami dan mampu menjelaskan konsep dasar manajemen krisis siber. 1.2. Memiliki pengetahuan tentang protokol, proses, dan teknis manajemen krisis. 1.3. Mampu menjelaskan tahapan manajemen krisis siber.
2	Mampu melaksanakan manajemen krisis siber sesuai pedoman kerja/petunjuk teknis.	2.1. Mampu melaksanakan pemberian peringatan/deteksi dari insiden yang tidak biasa. 2.2. Mampu mengklasifikasikan informasi yang relevan terkait kondisi krisis siber. 2.3. Mampu melaksanakan peningkatan pertahanan aset vital.
3	Mampu menyelenggarakan manajemen krisis siber.	3.1. Mampu melakukan penilaian situasional untuk deklarasi kondisi krisis. 3.2. Mampu menjalankan *crisis management plan*. 3.3. Mampu melakukan simulasi krisis siber.
4	Mampu mengevaluasi dan menyusun perangkat norma standar, prosedur, dan instrumen pada manajemen krisis siber	4.1. Mampu menyusun pedoman, petunjuk teknis, cara kerja yang dijadikan norma standar, prosedur, dan instrumen pelaksanaan manajemen krisis siber. 4.2. Mampu melakukan evaluasi terhadap teknis/metode/sistem cara kerja penanganan krisis siber dan melakukan pengembangan

		atau perbaikan cara kerja penanganan insiden. 4.3. Mampu melaksanakan hubungan dan koneksi dengan organisasi internal dan eksternal dalam proses manajemen krisis siber. 4.4. Mampu menyusun dokumen *crisis management plan*. 4.5. Mampu memberikan bimbingan/ asistensi pembuatan kebijakan manajemen krisis Level organisasi.
5	Mampu mengembangkan konsep, teori, kebijakan, teknik metode, dan analisis manajemen krisis siber.	5.1. Mampu mengembangkan kebijakan, rencana, dan strategi sesuai dengan hukum, peraturan, kebijakan, dan standar manajemen krisis siber. 5.2. Mengidentifikasi, meganalisis teori, konsep, dan kebijakan manajemen krisis siber, serta menemukan kelebihan dan kekurangan perbaikannya. 5.3. Mengembangkan teori, konsep, dan kebijakan terkait manajemen krisis siber, meyakinkan unit kerja terkait dan pemangku kepentingan untuk menerima konsep, teori, dan kebijakan yang dikembangkan. 5.4. Menjadi mentor dan sumber rujukan utama (nasional) dalam implementasi manajemen krisis siber.

12. FORENSIK DIGITAL

Nama Kompetensi	:	Forensik Digital
Kode Kompetensi	:	T.KSS-12
Definisi	:	Kemampuan dalam melaksanakan kegiatan forensik digital.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, serta tata cara prosedur forensik digital.	1.1. Mampu memahami konsep dasar forensik digital. 1.2. Mampu memahami prinsip-prinsip terkait forensik digital. 1.3. Mampu memahami prosedur/ petunjuk pelaksanaan forensik digital.
2	Menyelidiki sumber bukti digital.	2.1. Mampu menentukan sumber data (sumber bukti digital, *log* file, dan informasi lainnya) yang potensial terkait keamanan siber. 2.2. Mampu melakukan preservasi sumber bukti digital. 2.3. Mampu menggunakan *tools* forensik digital. 2.4. Mampu menentukan metode-metode forensik digital.
3	Menganalisis sumber bukti digital.	3.1. Mampu menganalisis sumber bukti digital dan informasi lainnya dalam rangka forensik digital. 3.2. Mampu mengkorelasikan hasil analisis dengan bukti-bukti digital lainnya. 3.3. Mampu menganalisis norma, standar, prosedur, dan kriteria di bidang forensik digital.
4	Merekomendasikan hasil forensik digital.	4.1. Mampu merekomendasikan terkait dengan profil hasil forensik digital. 4.2. Mampu mengevaluasi norma, standar, prosedur, kriteria di bidang forensik digital. 4.3. Mampu mengevaluasi tren forensik digital.
5	Merumuskan keterangan ahli, rekomendasi, dan kebijakan di bidang forensik digital.	5.1. Mampu merumuskan keterangan sebagai ahli forensik digital. 5.2. Mampu merumuskan rekomendasi forensik digital.

		5.3. Mampu merumuskan kebijakan di bidang forensik digital.

13. INVESTIGASI SIBER

Nama Kompetensi	:	Investigasi Siber
Kode Kompetensi	:	T.KSS-13
Definisi	:	Kemampuan dalam melaksanakan investigasi siber.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, peraturan, dan prosedur/petunjuk pelaksanaan investigasi siber.	1.1. Mampu memahami konsep dasar investigasi siber. 1.2. Mampu memahami peraturan terkait investigasi siber. 1.3. Mampu memahami prosedur/ petunjuk pelaksanaan investigasi siber.
2	Melakukan investigasi siber.	2.1. Mampu mengklasifikasikan temuan investigasi siber. 2.2. Mampu menentukan sumber daya pelaksanaan investigasi siber. 2.3. Mampu menerapkan metodologi investigasi siber.
3	Menganalisis investigasi siber.	3.1. Mampu menganalisis hasil investigasi siber. 3.2. Mampu menganalisis hasil temuan penyimpangan penyelenggaraan persandian. 3.3. Mampu menganalisis norma, standar, prosedur, dan kriteria investigasi di bidang keamanan siber dan/atau persandian.
4	Mengevaluasi investigasi siber.	4.1. Mampu mengevaluasi hasil investigasi di bidang keamanan siber, dan/atau persandian. 4.2. Mampu mengevaluasi norma, standar, prosedur, kriteria investigasi di bidang keamanan siber dan/atau persandian.

		4.3. Mampu mengevaluasi tren investigasi di bidang keamanan siber dan/atau persandian.
5	Merumuskan strategi, rekomendasi, dan kebijakan investigasi di bidang keamanan siber dan/atau persandian.	5.1. Mampu merumuskan strategi investigasi di bidang keamanan siber dan/atau persandian. 5.2. Mampu merumuskan rekomendasi investigasi di bidang keamanan siber dan/atau persandian. 5.3. Mampu merumuskan kebijakan investigasi di bidang keamanan siber dan/atau persandian.

14. *DATA SCIENCE* KEAMANAN SIBER DAN SANDI NEGARA

Nama Kompetensi	:	*Data Science* Keamanan Siber dan Sandi Negara
Kode Kompetensi	:	T.KSS-14
Definisi	:	Kemampuan dalam melaksanakan kegiatan *data science*.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, serta tata cara prosedur *data science*.	1.1. Mampu memahami konsep dasar *data science*. 1.2. Mampu memahami metode terkait *data science*. 1.3. Mampu memahami perosedur/ petunjuk pelaksanaan *data science*.
2	Menerapkan pengumpulan dan pemetaan serta metode *data science.*	2.1. Mampu melakukan pengumpulan *data science*. 2.2. Mampu melakukan pemetaan *data science*. 2.3. Mampu menerapkan metode *data science*.
3	Menganalisis/ interpretasi *information gathering*.	3.1. Mampu menganalisis hasil pengumpulan *data science*. 3.2. Mampu menganalisis norma, standar, prosedur, dan kriteria

		data science di bidang keamanan siber. 3.3. Mampu menganalisis metode pengumpulan *data science* di bidang keamanan siber.
4	Merekomendasikan hasil *information gathering*.	4.1. Mampu merekomendasikan hasil pengumpulan *data science*. 4.2. Mampu mengevaluasi norma, standar, prosedur, kriteria di bidang *data science* di bidang keamanan siber. 4.3. Mampu menganalisis *data science*.
5	Merumuskan strategi rekomendasi dan kebijakan *data science* di bidang keamanan siber.	5.1. Mampu menyusun strategi implementasi *data science* di bidang keamanan siber. 5.2. Mampu merusumskan rekomendasi *data science* di bidang keamanan siber. 5.3. Mampu merumuskan kebijakan *data science* di bidang keamanan siber.

15. ANALISIS KRIPTO

Nama Kompetensi	:	Analisis Kripto
Kode Kompetensi	:	T.KSS-15
Definisi	:	Kemampuan dalam melaksanakan kegiatan analisis kripto.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, dan tata cara prosedur analisis kripto.	1.1. Mampu memahami konsep dasar analisis kripto. 1.2. Mampu memahami metode-metode analisis kripto. 1.3. Mampu memahami prosedur/ petunjuk pelaksanaan analisis kripto.
2	Menerapkan analisis kripto.	2.1. Mampu menggunakan *tools* analisis kripto.

		2.2. Mampu menerapkan prosedur/ petunjuk pelaksanaan analisis kripto. 2.3. Mampu memperoleh profil target analisis kripto. 2.4. Mampu memcahkan kode (*code breaking*).
3	Mengevaluasi analisis kripto.	3.1. Mampu mengevaluasi algoritma kriptografi target. 3.2. Mampu menganalisis profil target. 3.3. Mampu mengevaluasi metode-metode analisis kripto.
4	Merekomendasikan hasil analisis kripto.	4.1. Mampu menyampaikan hasil analisis kripto. 4.2. Mampu memberikan alternatif prosedur/metode analisis kripto. 4.3. Mampu merekomendasikan tren analisis kripto.
5	Merancang strategi dan metode/*tools* analisis kripto.	5.1. Mampu merancang strategi analisis kripto. 5.2. Mampu memperbaiki metode analisis kripto. 5.3. Mampu mengembangkan metode/*tools* analisis kripto.

16. REKAYASA KRIPTOGRAFI

Nama Kompetensi	:	Rekayasa Kriptografi
Kode Kompetensi	:	T.KSS-16
Definisi	:	Kemampuan dalam melakukan perancangan algoritme, protokol, dan manajemen kunci kriptografi.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar dan prosedur rekayasa kriptografi.	1.1. Mampu mendaftar perangkat yang dibutuhkan dalam rekayasa kriptografi. 1.2. Mampu memahami konsep dan teori dasar terkait pengkajian

		teknologi keamanan siber dan sandi. 1.3. Mampu memahami prosedur kerja atau petunjuk teknis melaksanakan rekayasa kriptografi.
2	Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan perancangan desain rekayasa kriptografi.	2.1. Mampu mengoperasikan prosedur penyalinan/pencadangan data hasil rekayasa kriptografi. 2.2. Mampu menerapkan prosedur kerja atau petunjuk teknis perancangan desain rekayasa kriptografi. 2.3. Mampu menerapkan simulasi rekayasa kriptografi.
3	Menganalisis rancangan rekayasa kriptografi.	3.1. Mampu menguji hasil rekayasa kriptografi. 3.2. Mampu menganalisis kekuatan algoritma, manajemen kunci, dan protokol kriptografi. 3.3. Mampu menganalisis kebutuhan rekayasa kriptografi.
4	Mengevaluasi hasil rekayasa kriptografi.	4.1. Mampu mengevaluasi hasil rekayasa kriptografi. 4.2. Mampu mengevaluasi implementasi hasil rekayasa kriptografi. 4.3. Mampu mengevaluasi desain protokol kriptografi.
5	Membangun dan mengembangkan algoritme/protokol/ manajemen kunci kriptografi.	5.1. Mampu merumuskan *grand design* implementasi hasil pengkajian teknologi keamanan siber dan sandi. 5.2. Mampu merumuskan kebijakan strategis implementasi hasil kajian teknologi keamanan siber dan sandi. 5.3. Mampu merancang desain algoritme/protokol/manajemen kunci kriptografi.

17. RANCANG BANGUN PERANGKAT KEAMANAN TEKNOLOGI INFORMASI

Nama Kompetensi	:	Rancang Bangun Perangkat Keamanan Teknologi Informasi
Kode Kompetensi	:	T.KSS-17
Definisi	:	Kemampuan yang berkaitan dengan pembuatan perangkat keamanan teknologi informasi.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar dan prosedur rancang bangun perangkat keamanan teknologi informasi.	1.1. Mampu mendaftar perangkat yang dibutuhkan dalam rancang bangun keamanan teknologi informasi. 1.2. Mampu memahami konsep dan teori dasar terkait rancang bangun perangkat keamanan teknologi informasi. 1.3. Mampu memasangkan konfigurasi perangkat keamanan teknologi informasi hasil rancang bangun.
2	Menerapkan pedoman kerja/petunjuk teknis dalam melaksanakan perancangan desain perangkat keamanan teknologi informasi.	2.1. Mampu mengoperasikan prosedur penyalinan/pencadangan data hasil pengkajian teknologi keamanan siber dan sandi. 2.2. Mampu menerapkan konsep dan teori terkait pengkajian teknologi keamanan siber dan sandi. 2.3. Mampu menerapkan desain perangkat keamanan teknologi informasi pada suatu *framework* tertentu.
3	Menganalisis perancangan perangkat keamanan teknologi informasi.	3.1. Mampu menemukan pola konfigurasi yang tepat pada perangkat keamanan teknologi informasi hasil rancang bangun. 3.2. Mampu menganalisis hasil pengujian perangkat keamanan

		teknologi informasi hasil rancang bangun. 3.3. Mampu menganalisis kebutuhan rancang bangun perangkat keamanan teknologi informasi. 3.4. Mampu memerinci spesifikasi teknis perangkat keamanan teknologi informasi hasil rancang bangun. 3.5. Mampu menjamin pemberian dukungan pada pengkajian teknologi keamanan siber dan sandi.
4	Mengevaluasi perangkat keamanan teknologi informasi hasil rancang bangun.	4.1. Mampu mengevaluasi hasil rancang bangun perangkat keamanan teknologi informasi. 4.2. Mampu mengevaluasi implementasi hasil rancang bangun perangkat keamanan teknologi informasi. 4.3. Mampu menelaah celah keamanan pada hasil rancang bangun perangkat keamanan teknologi informasi.
5	Membangun perangkat keamanan teknologi informasi.	5.1. Mampu merumuskan *grand design* implementasi hasil pengkajian teknologi keamanan siber dan sandi. 5.2. Mampu merumuskan kebijakan strategis implementasi hasil kajian teknologi keamanan siber dan sandi. 5.3. Mampu merancang desain perangkat keamanan teknologi informasi.

18. PENGKAJIAN TEKNOLOGI KEAMANAN SIBER DAN SANDI

Nama Kompetensi	:	Pengkajian Teknologi Keamanan siber dan Sandi
Kode Kompetensi	:	T.KSS-18

Definisi	:	Kemampuan yang berkaitan dengan pelaksanaan kegiatan pengkajian pada bidang teknologi keamanan siber dan sandi.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar dan prosedur pengkajian teknologi keamanan siber dan sandi.	1.1. Mampu mendaftar perangkat yang dibutuhkan dalam pengkajian. 1.2. Mampu memahami pedoman kerja atau petunjuk teknis dalam pengkajian teknologi keamanan siber dan sandi. 1.3. Mampu memahami konsep dan teori dasar terkait pengkajian teknologi keamanan siber dan sandi.
2	Menerapkan pedoman kerja/petunjuk teknis dalam melaksanakan pengkajian teknologi keamanan siber dan sandi.	2.1. Mampu mengoperasikan prosedur penyalinan/pencadangan data hasil pengkajian teknologi keamanan siber dan sandi. 2.2. Mampu menggali celah keamanan dalam suatu teknologi informasi. 2.3. Mampu menerapkan konsep dan teori terkait pengkajian teknologi keamanan siber dan sandi.
3	Menganalisis pelaksanaan kegiatan pengkajian teknologi keamanan siber dan sandi.	3.1. Mampu menguji celah keamanan teknologi informasi. 3.2. Mampu membuat *blueprint* simulasi perangkat keamanan teknologi informasi. 3.3. Mampu mengklasifikasikan prosedur dalam identifikasi kebutuhan pengkajian teknologi keamanan siber dan sandi. 3.4. Mampu menganalisis kebutuhan pengkajian teknologi keamanan siber dan sandi.

4	Mengevaluasi hasil pengkajian teknologi keamanan siber dan sandi.	4.1. Mampu menganalisis hasil pengkajian teknologi keamanan siber dan sandi. 4.2. Mampu menelaah kekuatan dan kelemahan teknologi keamanan siber dan sandi. 4.3. Mampu merekomendasikan hasil kajian teknologi keamanan siber dan sandi.
5	Mengembangkan hasil pengkajian teknologi keamanan siber dan sandi.	5.1. Mampu merumuskan *grand design* implementasi hasil pengkajian teknologi keamanan siber dan sandi. 5.2. Mampu merumuskan kebijakan strategis implementasi hasil kajian teknologi keamanan siber dan sandi. 5.3. Mampu melakukan penyusunan strategi implementasi Pengamanan Informasi. 5.4. Mampu merekomendasikan strategi kerja sama kemitraan kajian.

19. PENGELOLAAN PENELITIAN TEKNOLOGI KEAMANAN SIBER DAN SANDI NEGARA

Nama Kompetensi	:	Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara
Kode Kompetensi	:	T.KSS-19
Definisi	:	Kemampuan dalam melakukan pengelolaan penelitian teknologi keamanan siber dan sandi negara.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar teknik metode, peraturan, mekanisme, dan tata cara prosedur penelitian terkait	1.1. Mampu mendaftar perangkat yang dibutuhkan dalam rekayasa kriptografi. 1.2. Mampu memahami prosedur kerja atau petunjuk teknis

	teknologi keamanan siber dan sandi.	melaksanakan tahapan penelitian. 1.3. Mampu mengkategorikan jenis penelitian, pemetaan, personil, dan kerja sama yang dibutuhkan dalam penelitian.
2	Menerapkan pedoman kerja/petunjuk teknis dalam melaksanakan penelitian.	2.1. Mampu mengoperasikan prosedur penyalinan/pencadangan data hasil rekayasa kriptografi. 2.2. Mampu menerapkan prosedur kerja atau petunjuk teknis tahapan proses penelitian. 2.3. Mampu menyesuaikan perbedaan dalam prosedur pengelolaan penelitian dengan kondisi penelitian untuk memecahkan permasalahan yang ada.
3	Mengelola dan merencanakan penelitian.	3.1. Mampu menata instrumen untuk kegiatan identifikasi, pengumpulan, pengolahan, dan pelaporan suatu kegiatan penelitian dalam bidang teknologi keamanan siber dan sandi. 3.2. Mampu mengoptimalkan pengetahuan terkait tujuan, metode, teknik analisis, dan kesimpulan suatu penelitian secara teknis maupun operasional melalui bimbingan teknis. 3.3. Mampu memecahkan masalah teknis operasional penelitian.
4	Mengevaluasi kegiatan penelitian.	4.1. Mampu mengevaluasi terhadap teknis/metode/sistem kerja menemukenali kelebihan dan kekurangan melakukan pengembangan atau perbaikan cara kerja dari penelitian terkait teknologi keamanan siber dan sandi.

		4.2. Mampu menyusun pedoman, petunjuk teknis, atau cara kerja yang menjadi operasional standar penelitian. 4.3. Mampu menyusun rekomendasi metode pengelolaan penelitian.
5	Mengembangkan konsep, teori, atau kebijakan terkait penelitian teknologi keamanan siber dan sandi.	5.1. Mampu merekomendasikan strategi kerja sama kemitraan penelitian. 5.2. Mampu mengajar (edukasi/ literasi) keamanan siber dan sandi. 5.3. Mampu merumuskan metode baru atau memodifikasi metode yang ada terkait pengelolaan penelitian.

20. PENGELOLAAN *SECURITY OPERATION CENTER (SOC)*

Nama Kompetensi	:	Pengelolaan *Security Operation Center* (SOC)
Kode Kompetensi	:	T.KSS-20
Definisi	:	Kemampuan mengumpulkan, mengidentifikasi, mengolah, menganalisis, merumuskan, dan melaksanakan asistensi, serta memberikan rekomendasi pengelolaan *Security Operation Center* (SOC) meliputi kebijakan dan prosedur, pengelolaan personil, keberlangsungan layanan SOC, penilaian kepatuhan penyelenggaraan SOC dan maturitas SOC.

Level	Deskripsi	Indikator Perilaku
1	Menjelaskan konsep dasar, teknik, metode, sistem, peraturan, tata cara prosedur pengelolaan SOC.	1.1. Mampu menjelaskan konsep dasar, teknik metode, sistem, peraturan, tata cara prosedur, tujuan dan manfaat pengelolaan SOC.

		1.2. Mampu menjelaskan konsep dasar, teknik metode, kriteria, tujuan, manfaat, dan identifikasi dukungan teknis operasional SOC. 1.3. Mampu mengidentifikasi norma, standar, prosedur dan kriteria pengelolaan SOC yang berlaku.
2	Menerapkan pengelolaan SOC.	2.1. Mampu melaksanakan pengelolaan SOC sesuai prosedur. 2.2. Mampu melatih pemangku kepentingan untuk dapat mengelola SOC. 2.3. Mampu menentukan spesifikasi dukungan teknis operasional SOC. 2.4. Mampu mengklasifikasikan dukungan teknis operasional SOC. 2.5. Mampu menggunakan instrumen penilaian maturitas SOC.
3	Menganalisis keberlangsungan pengelolaan SOC.	3.1. Mampu menelaah norma, standar, prosedur, dan kriteria terkait pengelolaan SOC. 3.2. Mampu memeriksa keberlangsungan layanan pengelolaan SOC. 3.3. Mampu memecahkan masalah teknis operasional yang timbul. 3.4. Mampu membuat instrumen penilaian maturitas SOC. 3.5. Mampu menelaah spesifikasi dukungan teknis operasional SOC.
4	Mengevaluasi pengelolaan SOC.	4.1. Mampu menilai kepatuhan pengelolaan SOC. 4.2. Mampu memberi pertimbangan terhadap tata cara pelaksanaan pengelolaan SOC.

		4.3. Mampu mengevaluasi instrumen penilaian maturitas SOC. 4.4. Mampu mengevaluasi teknik, metode, infrastruktur, perangkat/ *tools engineering* yang digunakan dalam operasional SOC.
5	Mengembangkan pengelolaan SOC.	5.1. Mampu menyusun kebijakan pengelolaan SOC. 5.2. Mampu merumuskan kajian kebijakan pengelolaan SOC. 5.3. Mampu menyusun strategi implementasi terkait pengelolaan SOC. 5.4. Mampu mengembangkan infrastruktur/perangkat/*tools engineering* yang digunakan dalam operasional SOC.

21. PENGELOLAAN PUSAT KONTAK SIBER NASIONAL

Nama Kompetensi	:	Pengelolaan Pusat Kontak Siber Nasional
Kode Kompetensi	:	T.KSS-21
Definisi	:	Kemampuan mengumpulkan/ mengidentifikasi, mengolah, menganalisis dan merumuskan teknis operasional pengelolaan pusat kontak siber nasional untuk merespon aduan siber nasional yang berasal dari publik baik perorangan atau kelompok (K/L/D/I atau komunitas).

Level	Deskripsi	Indikator Perilaku
1	Menjelaskan konsep dasar, teknik metode, peraturan, tata cara prosedur pengelolaan pusat kontak siber nasional.	1.1. Mampu menjelaskan konsep dasar, teknik metode, peraturan dan tata cara prosedur pengelolaan pusat kontak siber nasional. 1.2. Mampu menjelaskan tujuan dan manfaat pengelolaan pusat kontak siber nasional.

		1.3. Mampu mengidentifikasi norma, standar, prosedur dan kriteria pengelolaan pusat kontak siber nasional yang berlaku.
2	Menerapkan konsep pengelolaan pusat kontak siber nasional.	2.1. Mampu menggunakan instrumen pengelolaan pusat kontak siber nasional. 2.2. Mampu melengkapi bukti aduan dan identitas pelapor aduan siber nasional. 2.3. Mampu menentukan aduan siber terverifikasi dan tidak terverifikasi.
3	Menganalisis pelaksanaan pengelolaan pusat kontak siber nasional.	3.1. Mampu memeriksa proses pelaksanaan pengelolaan pusat kontak siber nasional. 3.2. Mampu menganalisis masalah teknis dalam pelaksanaan pengelolaan pusat kontak siber. 3.3. Mampu memecahkan masalah teknis dalam pelaksanaan pengelolaan pusat kontak siber. 3.4. Mampu membuat garis besar instrumen pengelolaan pusat kontak siber.
4	Mengevaluasi pengelolaan pusat kontak siber nasional.	4.1. Mampu mengevaluasi teknis/ metode/sistem cara kerja pengelolaan pusat kontak siber nasional. 4.2. Mampu memberi pertimbangan terhadap tata cara pelaksanaan pengelolaan pusat kontak siber nasional. 4.3. Mampu mengevaluasi instrumen pengelolaan pusat kontak siber nasional.
5	Mengembangkan pengelolaan pusat kontak siber nasoinal.	5.1. Mampu merumuskan kebijakan pengelolaan pusat kontak siber nasional.

		5.2. Mampu menyusun kebijakan pengelolaan pusat kontak siber. 5.3. Mampu menyusun strategi implementasi terkait pengelolaan pusat kontak siber nasional.

22. ANALISIS KELAIKAN SERTIFIKASI ELEKTRONIK

Nama Kompetensi	:	Analisis Kelaikan Sertifikasi Elektronik
Kode Kompetensi	:	T.KSS-22
Definisi	:	Kemampuan mengumpulkan, mengidentifikasi, mengolah, menganalisis dan merumuskan kegiatan, mengkoordinasikan, melakukan dan mengarahkan pelaksanaan tugas penerbitan, pembaruan, dan pencabutan serta pelayanan administratif sertifikat elektronik pemerintah sesuai prosedur dan ketentuan yang berlaku.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep pelayanan sertifikasi elektronik.	1.1. Mampu menjelaskan konsep dasar, teknik, metode, peraturan, dan mekanisme infrastuktur kunci publik. 1.2. Mampu menjelaskan proses dan *life cycle* sertifikat elektronik. 1.3. Mampu menjelaskan manfaat dan penggunaan sertifikat elektronik dengan konsep dasar infrastuktur kunci publik.
2	Menerapkan pelayanan sertifikasi elektronik sesuai dengan prosedur.	2.1. Mampu menangani pelayanan administratif dalam rangka verifikasi terhadap dokumen dan berkas permohonan penerbitan, pembaruan, dan pencabutan sertifikat elektronik. 2.2. Mampu menangani penerbitan, pembaruan, dan pencabutan sertifikat elektronik.

		2.3. Mampu mengklasifikasikan permasalahan dalam proses penerbitan, pembaruan, dan pencabutan sertifikat elektronik. 2.4. Mampu menerapkan sistem manajemen keamanan informasi dan manajemen kunci kriptografi
3	Membimbing penerapan dan manajemen sertifikat elektronik.	3.1. Mampu mengilustrasikan penerapan sertifikat elektronik kepada pemangku kepentingan. 3.2. Mampu mengelola pihak *Registration Authority*/ koordinator penerbitan sertifikat elektronik dalam hal *coaching*, konseling dan *mentoring*. 3.3. Mampu mengidentifikasi permasalahan dalam layanan *helpdesk* sertifikasi elektronik. 3.4. Mampu memecahkan masalah yang timbul dalam proses penerbitan, pembaruan, dan pencabutan sertifikat elektronik.
4	Mengevaluasi pelayanan sertifikat elektronik sesuai peraturan.	4.1. Mampu merekomendasikan perbaikan prosedur pelaksanaan kegiatan terkait penyelenggaraan sertifikasi elektronik. 4.2. Mampu merekomendasikan perbaikan pada *certificate policy* dan *certificate policy statement* dalam penyelenggaraan sertifikasi elektronik. 4.3. Mampu merekomendasikan perbaikan standar teknis penyelenggaraan sertifikasi elektronik.
5	Mengembangkan strategi dan kebijakan dalam pelayanan sertifikat elektronik.	5.1. Mampu menyusun konsep, teori dan kebijakan pelayanan sertifikasi elektronik.

		5.2. Mampu menyusun strategi implementasi pelayanan sertifikat elektronik. 5.3. Mampu merumuskan solusi terhadap permasalahan dalam pelayanan sertifikasi elektronik.

23. PEMENUHAN TEKNIS SISTEM SERTIFIKASI ELEKTRONIK

Nama Kompetensi	:	Pemenuhan Teknis Sistem Sertifikasi Elektronik
Kode Kompetensi	:	T.KSS-23
Definisi	:	Kemampuan mengumpulkan, mengidentifikasi, mengolah, menganalisis, mengoordinasikan, dan mengarahkan pelaksanaan tugas penyiapan pengembangan aplikasi pengguna dan teknologi sertifikasi elektronik pemerintah sesuai dengan prosedur dan peraturan yang berlaku.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep pemenuhan teknis sistem sertifikasi elektronik.	1.1. Mampu menjelaskan konsep dasar, teknik, metode, peraturan, dan mekanisme infrastruktur kunci publik. 1.2. Mampu menjelaskan pemrograman/pengembangan sistem berbasis perangkat lunak atau perangkat keras. 1.3. Mampu menjelaskan manfaat dan penggunaan sertifikat elektronik dengan konsep dasar infrastuktur kunci publik.
2	Menerapkan pemenuhan teknis sistem elektronik.	2.1. Mampu membangun sistem sertifikasi elektronik berdasarkan analisis kebutuhan. 2.2. Mampu menerapkan modul-modul sertifikasi elektronik ke sistem milik pengguna.

		2.3. Mampu menerapkan sistem manajemen keamanan informasi dan manajemen kunci kriptografi. 2.4. Mampu memberikan bimbingan teknis pengimplementasian sistem sertifikasi elektronik kepada pengguna.
3	Membimbing penerapan dan manajemen sertifikat elektronik.	3.1. Mampu menganalisis kebutuhan penerapan teknologi sertifikat elektronik. 3.2. Mampu mengidentifikasi proses bisnis sistem pemangku kepentingan dalam rangka implementasi sertifikat elektronik. 3.3. Mampu menganalisis kebutuhan desain dan perencanaan teknis penerapan sertifikat elektronik pada pemangku kepentingan. 3.4. Mampu menguji hasil penerapan modul-modul sertifikasi elektronik pada aplikasi pengguna.
4	Mengevaluasi penerapan pemenuhan teknis sertifikat elektronik.	4.1. Mampu merekomendasikan konsep norma, standar, prosedur, dan kriteria pelaksanaan kegiatan terkait pengimplementasian sistem sertifikasi elektronik. 4.2. Mampu mengevaluasi tahapan pemenuhan teknis sistem sertifikasi elektronik. 4.3. Mampu merekomendasikan kajian penerapan teknologi sertifikasi elektronik.
5	Mengembangkan strategi dan kebijakan dalam pemenuhan teknis sertifikat elektronik.	5.1. Mampu menyusun konsep kebijakan terkait pemenuhan teknis sertifikat elektronik/ penyelenggaraan sertifikasi elektronik.

		5.2. Mampu menyusun strategi implementasi pemenuhan teknis sertifikasi elektronik. 5.3. Mampu merumuskan solusi terhadap permasalahan pada pemenuhan teknis sertifikasi elektronik.

24. PENGELOLAAN JARINGAN DAN INFRASTRUKTUR SERTIFIKASI ELEKTRONIK

Nama Kompetensi	:	Pengelolaan Jaringan dan Infrastruktur Sertifikasi Elektronik
Kode Kompetensi	:	T.KSS-24
Definisi	:	Kemampuan mengumpulkan, mengidentifikasi, mengolah, menganalisis dan merumuskan dan mengoordinasikan, pemanfaatan jaringan dan infrastruktur serta manajemen kunci sertifikasi elektronik.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep pengelolaan jaringan dan infrastruktur sertifikasi elektronik.	1.1. Mampu menjelaskan konsep dasar, teknik, metode, peraturan, keamanan, dan mekanisme infrastuktur sertifikasi elektronik. 1.2. Mampu menjelaskan konsep dasar, penggunaan, metode, manfaat, keamanan, dan mekanisme jaringan, *application server, database* dan infrastruktur teknologi informasi. 1.3. Mampu menjelaskan langkah-langkah tahapan pelaksanaan perubahan konfigurasi pada jaringan, *application server, database*, dan infrastruktur teknologi informasi.
2	Menerapkan pemenuhan teknis sistem elektronik.	2.1. Mampu melakukan instalasi dan konfigurasi sistem dan perangkat keamanan dalam rangka

		penyelenggaraan sertifikasi elektronik. 2.2. Mampu menentukan rencana pemulihan sistem dari bencana dan pemeliharaan fisik perangkat penyelenggaraan sertifikasi elektronik. 2.3. Mampu melakukan *monitoring* keamanan dan pemeriksaan status sistem agar dapat beroperasi dengan baik. 2.4. Mampu membangun *server* dan jaringan sistem sertifikasi elektronik. 2.5. Mampu melakukan *backup data* dan sistem.
3	Mengelola sistem penyelenggaraan sertifikasi elektronik.	3.1. Mampu mengelola akun pengelola/*administrator* sistem sertifikasi elektronik dalam hal pembuatan, pemeliharaan, dan pencabutan akun. 3.2. Mampu mengelola perangkat dan infrastruktur pengelolaan sistem sertifikasi elektronik (termasuk pemutakhiran). 3.3. Mampu mendeteksi gangguan dan permasalahan dalam operasional pengelolaan sistem elektronik. 3.4. Mampu mengoptimalkan sistem sertifikasi elektronik. 3.5. Mampu mengoptimalkan perangkat keamanan sistem sertifikasi elektronik seperti *Hardware Security Module* (HSM) serta *backup data* dan sistem.
4	Mengevaluasi penerapan pemenuhan teknis sertifikat elektronik.	4.1. Mampu merekomendasikan norma, standar, prosedur, dan kriteria pelaksanaan kegiatan terkait pengelolaan sistem sertifikasi elektronik.

		4.2. Mampu mengidentifikasi permasalahan dalam rangka pelaporan insiden keamanan penyelenggaraan sertifikat elektronik. 4.3. Mampu mengevaluasi pengelolaan jaringan dan infrastruktur sertifikasi elektronik baik internal maupun eksternal. 4.4. Mampu merekomendasikan perbaikan pengelolaan jaringan dan infrastruktur sertifikat elektronik.
5	Mengembangkan strategi dan kebijakan dalam pengelolaan sertifikat elektronik.	5.1. Mampu menyusun konsep kebijakan terkait pengelolaan sertifikasi elektronik. 5.2. Mampu menyusun strategi implementasi pengelolaan sertifikasi elektronik. 5.3. Mampu merumuskan solusi terhadap permasalahan pada pengelolaan sertifikasi elektronik.

25. VERIFIKASI ALGORITMA KRIPTOGRAFI

Nama Kompetensi	:	Verifikasi Algoritma Kriptografi
Kode Kompetensi	:	T.KSS-25
Definisi	:	Kemampuan dalam melakukan verifikasi algoritma kriptografi.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar, teknik metode, dan prosedur verifikasi algoritma kriptografi.	1.1. Mampu menyebutkan dan mencatat perangkat yang dibutuhkan dalam verifikasi algoritma kriptografi. 1.2. Mampu menjelaskan mekanisme verifikasi algoritma kriptografi. 1.3. Mampu menjelaskan ruang lingkup dan *output* verifikasi algoritma kriptografi.

2	Menerapkan pedoman kerja/petunjuk teknis dalam melaksanakan verifikasi algoritma kriptografi.	2.1. Mampu mengurutkan tahapan kegiatan verifikasi algoritma kriptografi berdasarkan pedoman/petunjuk teknis yang berlaku. 2.2. Mampu mendemonstrasikan kegiatan verifikasi algoritma kriptografi berdasarkan pedoman kerja/petunjuk teknis yang berlaku. 2.3. Mampu menyusun laporan pelaksanaan verifikasi algoritma kriptografi.
3	Mengelola verifikasi algoritma kriptografi.	3.1. Mampu menganalisis hasil verifikasi algoritma kriptografi. 3.2. Mampu menguji hasil verifikasi algoritma kriptografi. 3.3. Mampu mendeteksi ketidaksesuaian proses verifikasi algoritma kriptografi.
4	Mengevaluasi kegiatan verifikasi algoritma kriptografi.	4.1. Mampu menilai efektivitas dan efisiensi prosedur dan metode verifikasi algoritma kriptografi. 4.2. Mampu mengarahkan prosedur dan metode verifikasi algoritma kriptografi yang dinilai lebih efektif dan efisien. 4.3. Mampu menyamakan persepsi dan membuat kesepakatan dengan pemangku kepentingan dalam pelaksanaan verifikasi algoritma kriptografi.
5	Mengembangkan konsep, metode, dan kebijakan terkait verifikasi algoritma kriptografi.	5.1. Mampu merencanakan program pengembangan konsep, metode, dan kebijakan verifikasi algoritma kriptografi. 5.2. Mampu membangun konsep, metode, dan kebijakan verifikasi algoritma kriptografi.

		5.3. Mampu membuat regulasi yang menjadi acuan utama verifikasi algoritma kriptografi.

26. *FUNCTIONAL TESTING*

Nama Kompetensi	:	***Functional Testing***
Kode Kompetensi	:	T.KSS-26
Definisi	:	Kemampuan dalam melakukan *functional testing* produk.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar, teknik metode, dan prosedur *functional testing*.	1.1. Mampu mengidentifikasi peralatan *software* ataupun *hardware* yang dibutuhkan dalam melakukan *functional testing*. 1.2. Mampu melakukan instalasi *software* yang dibutuhkan untuk melakukan *functional testing*. 1.3. Mampu melakukan konfigurasi *software* atau *hardware* yang dibutuhkan untuk melakukan *functional testing*. 1.4. Mampu menjelaskan mekanisme *functional testing*.
2	Melaksanakan *functional testing*.	2.1. Mampu menentukan tahapan yang dilakukan dalam pelaksanaan *functional testing*. 2.2. Mampu menyusun rencana uji *functional testing*. 2.3. Mampu menjalanan *functional testing* sesuai *test plan* dan metode yang berlaku.
3	Mengelola *functional testing*.	3.1. Mampu memverifikasi hasil instalasi dan/atau konfigurasi *software* atau *hardware* yang dibutuhkan untuk melakukan *functional testing*. 3.2. Mampu menganalisis hasil *functional testing*.

		3.3. Mampu memecahkan permasalahan yang dihadapi dalam melakukan *functional testing*.
4	Mengevaluasi *test plan* dan pelaksanaan *functional testing*.	4.1. Mampu menilai keabsahan *test plan* yang disusun. 4.2. Mampu menilai efektivitas dan efisiensi prosedur, dan metode yang digunakan dalam *functional testing*. 4.3. Mampu menyusun prosedur, metode, dan standar *functional testing* yang lebih efektif dan efisien.
5	Mampu mengembangkan konsep, teori, kebijakan, dan menjadi acuan bagi implementasi serta solusi dalam pelaksanaan *functional testing*.	5.1. Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan terkait pelaksanaan *functional testing* serta mengupayakan peningkatan kualitasnya. 5.2. Mampu mengembangkan teori, konsep dan kebijakan terkait pelaksanaan *functional testing*. 5.3. Mampu membuat regulasi yang menjadi acuan utama *functional testing*.

27. ANALISIS KERAWANAN PRODUK KEAMANAN SIBER DAN SANDI NEGARA

Nama Kompetensi	:	Analisis Kerawanan Produk Keamanan Siber dan Sandi Negara
Kode Kompetensi	:	T.KSS-27
Definisi	:	Kemampuan dalam melakukan analisis kerawanan produk keamanan siber dan sandi negara.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar, teknik metode,	1.1. Mampu mengidentifikasi peralatan *software* ataupun *hardware* yang dibutuhkan dalam

	dan prosedur analisis kerawanan produk.	melakukan analisis kerawanan produk. 1.2. Mampu melakukan instalasi *software* yang dibutuhkan untuk melakukan analisis kerawanan produk. 1.3. Mampu melakukan konfigurasi *software* atau *hardware* yang dibutuhkan untuk melakukan analisis kerawanan produk. 1.4. Mampu memverifikasi hasil instalasi dan/atau konfigurasi *software* atau *hardware* yang dibutuhkan untuk melakukan analisis kerawanan produk. 1.5. Mampu menjelaskan mekanisme analisis kerawanan produk.
2	Melaksanakan analisis kerawanan produk.	2.1. Mampu menentukan tahapan yang dilakukan dalam pelaksanaan analisis kerawanan produk. 2.2. Mampu menyusun rencana uji analisis kerawanan produk. 2.3. Mampu menjalanan analisis kerawanan produk sesuai *test plan* dan metode yang berlaku.
3	Mengelola analisis kerawanan produk.	3.1. Mampu memverifikasi hasil instalasi dan/atau konfigurasi *software* atau *hardware* yang dibutuhkan untuk melakukan analisis kerawanan produk. 3.2. Mampu menganalisis hasil analisis kerawanan produk. 3.3. Mampu memecahkan permasalahan yang dihadapi dalam melakukan analisis kerawanan produk.
4	Mengevaluasi *test plan* dan pelaksanaan	4.1. Mampu menilai keabsahan *test plan* yang disusun.

	analisis kerawanan produk.	4.2. Mampu menilai efektivitas dan efisiensi prosedur, dan metode yang digunakan dalam analisis kerawanan produk. 4.3. Mampu menyusun prosedur, metode, dan standar analisis kerawanan produk yang lebih efektif dan efisien.
5	Mampu mengembangkan konsep, teori, kebijakan, dan menjadi acuan bagi implementasi serta solusi dalam pelaksanaan analisis kerawanan produk.	5.1. Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan terkait pelaksanaan analisis kerawanan produk serta mengupayakan peningkatan kualitasnya. 5.2. Mampu mengembangkan teori, konsep dan kebijakan terkait pelaksanaan analisis kerawanan produk. 5.3. Mampu membuat regulasi yang menjadi acuan utama analisis kerawanan produk.

28. PENGELOLAAN PENGUJIAN PRODUK KEAMANAN SIBER DAN SANDI NEGARA

Nama Kompetensi	:	Pengelolaan Pengujian Produk Keamanan Siber dan Sandi Negara
Kode Kompetensi	:	T.KSS-28
Definisi	:	Kemampuan dalam melakukan pengelolaan pengujian produk keamanan siber dan sandi negara.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep pengelolaan pengujian produk.	1.1. Mampu menjelaskan konsep, prosedur, metode, serta mengidentifikasi peraturan terkait layanan pengujian produk. 1.2. Mampu menjelaskan tahapan-tahapan layanan pengujian produk.

		1.3.	Mampu menjelaskan ruang lingkup dan *output* pengujian produk.
2	Melaksanakan layanan pengujian produk.	2.1.	Mampu merancang instrumen pengujian dokumen, penyiapan sarana prasarana, dokumen, serta melakukan koordinasi dalam rangka penyelenggaraan layanan sertifikasi produk.
		2.2.	Mampu mensosialisasikan kebijakan, peraturan, tahapan pelaksanaan layanan pengujian keamanan produk.
		2.3.	Mampu memecahkan permasalahan teknis operasional dalam penyelenggaraan layanan pengujian produk.
3	Mengelola pengelolaan pengujian produk.	3.1.	Mampu memverifikasi hasil instalasi dan/atau konfigurasi *software* atau *hardware* yang dibutuhkan untuk melakukan *vulnerability testing assessment*.
		3.2.	Mampu menganalisis hasil *vulnerability testing assessment*.
		3.3.	Mampu memecahkan permasalahan yang dihadapi dalam melakukan *vulnerability testing assessment*.
4	Mengevaluasi kegiatan pengelolaan pengujian produk.	4.1.	Mampu menilai efektivitas dan efisiensi prosedur, metode, dan standar yang digunakan dalam layanan pengujian produk.
		4.2.	Mampu menyusun prosedur, metode, dan standar layanan pengujian produk yang lebih efektif dan efisien.
		4.3.	Mampu menyamakan persepsi dan membuat kesepakatan dengan pemangku kepentingan

		dalam pelaksanaan layanan pengujian produk.
5	Mampu mengembangkan konsep, teori, kebijakan, dan menjadi acuan bagi implementasi serta solusi dalam pelaksanaan layanan pengujian produk.	5.1. Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan terkait pelaksanaan layanan pengujian produk, serta mengupayakan peningkatan kualitasnya. 5.2. Mampu mengembangkan teori, konsep dan kebijakan terkait layanan pengujian produk dengan melibatkan para pemangku kepentingan. 5.3. Mampu membuat regulasi yang menjadi acuan utama layanan pengujian produk.

29. PENGELOLAAN SERTIFIKASI PRODUK KEAMANAN SIBER DAN SANDI NEGARA

Nama Kompetensi	:	Pengelolaan Sertifikasi Produk Keamanan Siber dan Sandi Negara
Kode Kompetensi	:	T.KSS-29
Definisi	:	Kemampuan dalam melakukan pengelolaan sertifikasi produk keamanan siber dan sandi negara.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep pengelolaan sertifikasi produk.	1.1. Mampu menjelaskan konsep, prosedur, metode, serta mengidentifikasi peraturan terkait layanan sertifikasi produk. 1.2. Mampu menjelaskan setiap tahapan layanan sertifikasi produk. 1.3. Mampu menjelaskan ruang lingkup dan *output* sertifikasi produk.
2	Melaksanakan layanan pengujian produk.	2.1. Mampu merancang instrumen pengujian dokumen, penyiapan sarana prasarana, dokumen,

		serta melakukan koordinasi dalam rangka penyelenggaraan layanan sertifikasi produk. 2.2. Mampu mendemonstrasikan tahapan-tahapan sertifikasi produk sesuai pedoman kerja/ petunjuk teknis yang berlaku. 2.3. Mampu menyusun laporan pelaksanaan sertifikasi produk.
3	Mengelola pengelolaan sertifikasi produk.	3.1. Mampu merancang instrumen sertifikasi, penyiapan sarana prasarana, penyusunan dokumen, serta melakukan koordinasi dalam rangka penyelenggaraan layanan sertifikasi produk. 3.2. Mampu mensosialisasikan kebijakan, peraturan, dan tahapan pelaksanaan layanan sertifikasi keamanan produk. 3.3. Mampu memecahkan permasalahan teknis operasional dalam penyelenggaraan layanan sertifikasi produk.
4	Mengevaluasi kegiatan pengelolaan sertifikasi produk.	4.1. Mampu menilai efektivitas dan efisiensi prosedur, metode, dan standar yang digunakan dalam layanan sertifikasi produk. 4.2. Mampu menyusun prosedur, metode, dan standar layanan sertifikasi produk yang lebih efektif dan efisien. 4.3. Mampu menyamakan persepsi dan membuat kesepakatan dengan pemangku kepentingan dalam pelaksanaan layanan sertifikasi produk.
5	Mampu mengembangkan konsep, teori,	5.1. Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan terkait pelaksanaan

	kebijakan, dan menjadi acuan bagi implementasi serta solusi dalam pelaksanaan layanan sertifikasi produk.	layanan sertifikasi produk serta mengupayakan peningkatan kualitasnya. 5.2. Mampu mengembangkan teori, konsep dan kebijakan terkait layanan sertifikasi produk dengan melibatkan para pemangku kepentingan. 5.3. Mampu membuat regulasi yang menjadi acuan utama layanan sertifikasi produk.

30. VALIDASI DOKUMEN SERTIFIKASI

Nama Kompetensi	:	Validasi Dokumen Sertifikasi
Kode Kompetensi	:	T.KSS-30
Definisi	:	Kemampuan dalam melakukan validasi dokumen sertifikasi.

Level	Deskripsi	Indikator Perilaku
1	Mengetahui konsep dasar, teknik, metode, dan prosedur validasi dokumen sertifikasi.	1.1. Mampu mengindentifikasi persyaratan dokumen yang harus dipenuhi pemohon sertifikasi. 1.2. Mampu menjelaskan setiap dokumen yang harus dipenuhi pemohon sertifikasi. 1.3. Mampu menjelaskan ruang lingkup dan *output* validasi dokumen.
2	Melaksanakan validasi dokumen sertifikasi.	2.1. Mampu mengurutkan tahapan validasi dokumen sertifikasi. 2.2. Mampu mendemonstrasikan kegiatan validasi dokumen sertifikasi. 2.3. Mampu membuat laporan hasil validasi dokumen.
3	Mengelola validasi dokumen sertifikasi.	3.1. Mampu merancang instrumen validasi dokumen. 3.2. Mampu menganalisis hasil validasi dokumen sertifikasi.

		3.3. Mampu mendeteksi kekurangan/ ketidaksesuaian hasil validasi dokumen sertifikasi.
4	Mengevaluasi kegiatan validasi dokumen sertifikasi.	4.1. Mampu menilai efektivitas dan efisiensi prosedur dan metode validasi dokumen sertifikasi. 4.2. Mampu mengarahkan prosedur dan metode validasi dokumen sertifikasi yang lebih efektif dan efisien. 4.3. Mampu menyamakan persepsi dan membuat kesepakatan dengan pemangku kepentingan dalam kegiatan validasi dokumen.
5	Mengembangkan konsep, metode, dan kebijakan terkait validasi dokumen kriptografi.	5.1. Mampu merencanakan program pengembangan konsep, metode, dan kebijakan validasi dokumen sertifikasi. 5.2. Mampu membangun konsep, metode, dan kebijakan validasi dokumen sertifikasi. 5.3. Mampu membuat regulasi yang menjadi acuan utama validasi dokumen.

31. DIPLOMASI SIBER

Nama Kompetensi	:	Diplomasi Siber
Kode Kompetensi	:	T.KSS-31
Definisi	:	Kemampuan dalam memahami, melakukan penyiapan bahan, analisis bahan, harmonisasi dan perumusan strategi dan kebijakan keamanan siber melalui diplomasi.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, serta tata	1.1. Mampu memahami konsep dasar diplomasi siber. 1.2. Mampu memahami metode terkait diplomasi siber.

	cara prosedur diplomasi siber.	1.3. Mampu memahami prosedur/ petunjuk pelaksanaan diplomasi siber.
2	Menyiapkan bahan perumusan diplomasi siber.	2.1. Mampu mengolah data dan informasi untuk penyusunan kajian diplomasi siber. 2.2. Mampu menentukan potensi dan tantangan pemanfaatan forum kerja sama nasional dan internasional dalam perumusan bahan diplomasi siber. 2.3. Mampu menentukan keterkaitan antara kebijakan nasional dan internasional dalam rangka penyelenggaraan diplomasi siber.
3	Menganalisis bahan perumusan diplomasi siber.	3.1. Mampu memberikan masukan yang berkontribusi pada pengembangan kerja sama antar lembaga pemerintah atau nonpemerintah pada tingkat nasional atau internasional. 3.2. Mampu merumuskan korelasi hubungan sebab akibat dalam hal perumusan bahan diplomasi siber dengan mempertimbangkan faktor-faktor yang relevan. 3.3. Mampu menganalisis arah dan strategi kebijakan nasional dalam hal keamanan siber dan kaitannya dengan diplomasi siber.
4	Mengharmonisasikan pelaksanaan diplomasi siber.	4.1. Mampu mengkoordinasikan pengembangan kerja sama antara lembaga pemerintah maupun nonpemerintah pada tingkat nasional atau internasional. 4.2. Mampu menyelaraskan arah dan strategi kebijakan keamanan siber nasional dan internasional dengan penyelenggaraan diplomasi siber.

		4.3. Mampu mengevaluasi kebijakan dan strategi keamanan siber nasional.
5	Merumuskan pengembangan strategi dan konsep kebijakan keamanan siber.	5.1. Mampu mengkombinasikan pendekatan interdisipliner dan/atau multidisipliner dalam perumusan diplomasi siber. 5.2. Mampu menyelaraskan arah dan strategi keamanan siber nasional dengan diplomasi siber. 5.3. Mampu merumuskan pengembangan strategi dan kebijakan diplomasi siber di bidang keamanan siber.

32. PENAPISAN KONTEN

Nama Kompetensi	:	Penapisan Konten
Kode Kompetensi	:	T.KSS-32
Definisi	:	Kemampuan dalam memahami, menerapkan, menganalisis, mengevaluasi, dan merumuskan strategi, metode, kebijakan dalam pelaksanaan penapisan konten untuk keamanan siber.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme, serta tata cara prosedur penapisan konten.	1.1. Mampu memahami konsep dasar penapisan konten. 1.2. Mampu memahami metode terkait penapisan konten. 1.3. Mampu memahami prosedur/ petunjuk pelaksanaan penapisan konten.
2	Menerapkan metode, *tools*, dan teknik penapisan konten.	2.1. Mampu mengoperasikan perangkat dan *tools* untuk pelaksanaan penapisan konten. 2.2. Mampu mengkategorikan konten yang perlu ditapiskan. 2.3. Mampu menyusun laporan pelaksanaan penapisan konten.

3	Menganalisis pelaksanaan penapisan konten.	3.1. Mampu merumuskan norma, standar, prosedur, dan kriteria penapisan konten. 3.2. Mampu menganalisis metode, *tools*, dan teknik penapisan konten. 3.3. Mampu menganalisis laporan pelaksanaan penapisan konten.
4	Mengevaluasi pelaksanaan penapisan konten.	4.1. Mampu merekomendasikan metode, *tools*, dan teknis penapisan konten. 4.2. Mampu mengevaluasi norma, standar, prosedur, kriteria serta kebijakan terkait penapisan konten. 4.3. Mampu mengkoordinasikan dan menyelaraskan hasil penapisan konten serta kebijakan keamanan siber dengan pihak terkait
5	Merumuskan strategi, rekomendasi, dan kebijakan penapisan konten di bidang keamanan siber.	5.1. Mampu menyusun strategi implementasi keamanan siber tentang penapisan konten secara nasional. 5.2. Mampu merumuskan kebijakan keamanan siber tentang penapisan konten secara nasional. 5.3. Mampu mengembangkan metode, *tools*, dan teknik penapisan konten.

33. PENYUSUNAN KEBIJAKAN KEAMANAN SIBER

Nama Kompetensi	:	Penyusunan Kebijakan Keamanan Siber
Kode Kompetensi	:	T.KSS-33
Definisi	:	Kemampuan dalam menyusun, menganalisis, mengevaluasi, dan merumuskan kebijakan terkait keamanan siber dalam lingkup institusi, regional, maupun nasional.

Level	Deskripsi	Indikator Perilaku
1	Memahami konsep dasar, teknik metode, peraturan dan mekanisme keamanan siber.	1.1. Mampu memahami konsep dasar keamanan siber. 1.2. Mampu memahami metode terkait keamanan siber. 1.3. Mampu memahami kebijakan keamanan siber.
2	Menyiapkan bahan penyusunan kebijakan keamanan siber.	2.1. Mampu mengolah data dan informasi terkait kebijakan keamanan siber. 2.2. Mampu menentukan potensi dan tantangan di bidang keamanan siber. 2.3. Mampu menyiapkan bahan penyelenggaran kegiatan penyusunan kebijakan keamanan siber.
3	Menganalisis bahan penyusunan kebijakan keamanan siber.	3.1. Mampu menyusun bahan perumusan kebijakan keamanan siber pada tingkat institusi maupun nasional. 3.2. Mampu menganalisis kebijakan yang tersedia di bidang keamanan siber pada tingkat institusi maupun nasional. 3.3. Mampu menganalisis norma, standar, prosedur, dan kriteria yang tersedia di bidang keamanan siber pada tingkat institusi maupun nasional.
4	Mengevaluasi kebijakan keamanan siber.	4.1. Mampu merekomendasikan strategi dan kebijakan keamanan siber pada tingkat institusi maupun nasional. 4.2. Mampu mengevaluasi norma, standar, prosedur, dan kriteria yang tersedia di bidang keamanan siber pada tingkat institusi maupun nasional.

		4.3.	Mampu mengevaluasi kebijakan yang tersedia di bidang keamanan siber pada tingkat institusi maupun nasional.
5	Merumuskan strategi, rekomendasi, dan kebijakan di bidang keamanan siber.	5.1.	Mampu menyusun strategi kebijakan dan implementasi kebijakan di bidang keamanan siber pada tingkat institusi maupun nasional.
		5.2.	Mampu merumuskan rekomendasi kebijakan di bidang keamanan siber.
		5.3.	Mampu merumuskan kebijakan di bidang keamanan siber.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN