KERANGKA KUALIFIKASI NASIONAL INDONESIA

KEAMANAN INFORMASI

LEMBAR PENGESAHAN

TIM PERUMUS		
No.	**Nama**	**Keterangan**
1.	Prof. Teddy Mantoro	APTIKOM
2.	Andika Triwidada	ID-CERT
3.	Ferry Astika Saputra, ST.,M.Sc	Politeknik Elektronika Negeri Surabaya
4.	Andy Minar Widjaya	KKI, CSCP
5.	Drs. Agus Wardjito, M.M	Praktisi skema

TIM VERIFIKASI		
No.	**Nama**	**Keterangan**
1.		Kominfo
2.		Kemenaker
3.		BNSP

PERSETUJUAN	
Kementerian Komunikasi dan Informatika	Badan Nasional Sertifikasi Profesi
Nama:	Nama:
Jabatan:	Jabatan:

KERANGKA KUALIFIKASI NASIONAL INDONESIA
KEAMANAN INFORMASI

BAB I
PENDAHULUAN

LATAR BELAKANG

Selama beberapa dekade terakhir, evolusi teknologi yang cepat telah turut pula mempercepat transformasi masyarakat terhadap budaya digital. Kecepatan perubahan ini telah menyebabkan perbedaan dalam komposisi teknologi informasi dan komunikasi (TIK) khususnya tenaga kerja keamanan teknologi informasi (TI). Variasi dalam pelatihan, keahlian, dan pengalaman merupakan konsekuensi wajar dari evolusi ini, dan tercermin dalam semakin melimpahnya kegiatan perekrutan, pendidikan, dan praktek retensi antara organisasi/perusahaan. Dari awal revolusi digital, organisasi publik, swasta, dan akademis memiliki semua sumber daya yang berdedikasi untuk mengembangkan bidang keamanan TI praktis dan telah membuat kemajuan yang signifikan.

Hal ini semakin penting untuk profesional/tenaga kerja bidang teknologi informasi dan komunikasi, khususnya sub-bidang keamanan TI untuk memenuhi tantangan hari ini, dan secara proaktif menggapai tujuan mereka di masa depan. Keterbukaan dan meningkatnya kuantitas sistem yang terhubung ke Internet, konvergensi sistem gambar, suara dan komunikasi data, piranti bergerak ditambah dengan ancaman keamanan yang muncul dari internal dari eksternal organisasi yang berusaha untuk ‘mengganggu’ sistem membuka peluang kebutuhan spesialis keamanan TI yang terlatih dan memiliki perangkat yang mencukup (well-equipped). Pelayanan bersama infrastruktur serta informasi antara pemerintah dan industri menunjukkan perlunya model inovatif peran, tanggung jawab, dan kompetensi yang dibutuhkan untuk tenaga kerja bidang teknologi informasi dan komunikasi khususnya sub-bidang keamanan TI.

Untuk membantu organisasi dan anggota saat ini dan masa depan tenaga kerja ini, Kementerian Komunikasi dan Informatika (KemKominfo) bekerja dengan para ahli dari akademisi, pemerintah, dan sektor swasta mengembangkan sebuah kerangka tingkat tinggi yang menetapkan standar nasional mewakili pengetahuan dan keterampilan penting yang harus dimiliki oleh praktisi keamanan TI.

Atas dasar pertimbangan tersebut diatas, KemKominfo mendorong upaya-upaya yang diperlukan untuk membangun dasar bagi pengembangan program sertifikasi keamanan yang akan diterima secara luas oleh sektor publik dan swasta. Kementerian Kominfo, Kementerian Tenaga Kerja dan lembaga pemerintah lainnya dapat membantu upaya-upaya ini dengan efektif mengartikulasikan kebutuhan masyarakat keamanan TI. Sebagai tindak lanjut dari upaya ini adalah program Pelatihan dan Pendidikan di bidang teknologi informasi dan komunikasi sub-bidang keamanan TI untuk pembangunan angkatan kerja yang dapat mencukupi kebutuhan industri nasional.

Sebagai acuan maka dibutuhkan sebuah kerangka standar bidang keamanan informasi yang menitikberatkan kepada kompetensi yang harus dimiliki oleh tiap individu yang melakukan fungsi-fungsi keamanan informasi. Atas dasar kebutuhan inilah disusun Kerangka Kualifikasi Nasional Indonesia (KKNI) bidang Teknologi Informasi dan Komunikasi sub-bidang Keamanan Informasi.

KKNI bidang Teknologi Informasi dan Komunikasi sub-bidang Keamanan Informasi digunakan untuk memberikan panduan untuk identifikasi dan kategorisasi posisi dan sertifikasi personil yang melakukan fungsi keamanan informasi yang mendukung implementasi keamanan informasi organisasi. Tenaga kerja bidang keamanan informasi termasuk, namun tidak terbatas pada, semua individu yang melakukan salah satu fungsi keamanan informasi dalam organisasi sesuai dengan kebijakan, prosedur dan peraturan yang berlaku.

Standar ini dirumuskan dengan menggunakan acuan sebagai berikut :

1. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan;
2. Peraturan Pemerintah Nomor 23 Tahun 2004 tentang Badan Nasional Sertifikasi Profesi;
3. Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor 5 Tahun 2012 tentang Sistem Standarisasi Kompetensi Kerja Nasional;
4. Peraturan Menteri Tenaga Kerja dan Transmigrasi Nomor 8 Tahun 2012 tentang Tata Cara Penetapan Standar Kompetensi Kerja Nasional Indonesia;
5. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
6. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik;
7. ICA11 - Information and Communications Technology Training Package (Release 2.0) tahun 2013

Penyusunan Kerangka Kualifikasi Nasional Indonesia Bidang Teknologi Informasi dan Komputer Subbidang Keamanan Informasi mempunyai tujuan sebagai berikut:

1. Menetapkan dasar (baseline) keterampilan teknis dan manajemen keamanan informasi di antara SDM yang melaksanakan fungsi keamanan informasi dalam organisasi.
2. Mengembangkan dan meremajakan keterampilan secara formal untuk tenaga kerja bidang keamanan informasi yang terdiri dari beragam model pelatihan, program magang (on-the-job training), praktek-praktek dan sertifikasi/re-sertifikasi.
3. Melakukan verifikasi pengetahuan dan keterampilan tenaga kerja bidang keamanan informasi melalui pengujian sertifikasi standar.

B. KEAMANAN INFORMASI

1. Pengertian Keamanan Informasi

   Berdasarkan SANS Institute Information Security Resources, keamanan Informasi mengacu pada proses dan metodologi yang dirancang dan dilaksanakan untuk melindungi cetak, elektronik, atau bentuk lain dari informasi rahasia, pribadi dan sensitif atau data dari akses yang tidak sah, penggunaan, penyalahgunaan, pengungkapan, kehancuran, modifikasi, atau gangguan.
2. Pengertian Perlindungan Informasi

   Berdasarkan pasal 26 ayat 1 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa “kecuali ditentukan oleh Peraturan Perundang-undangan, penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan”.
3. Manajemen Risiko Keamanan Informasi

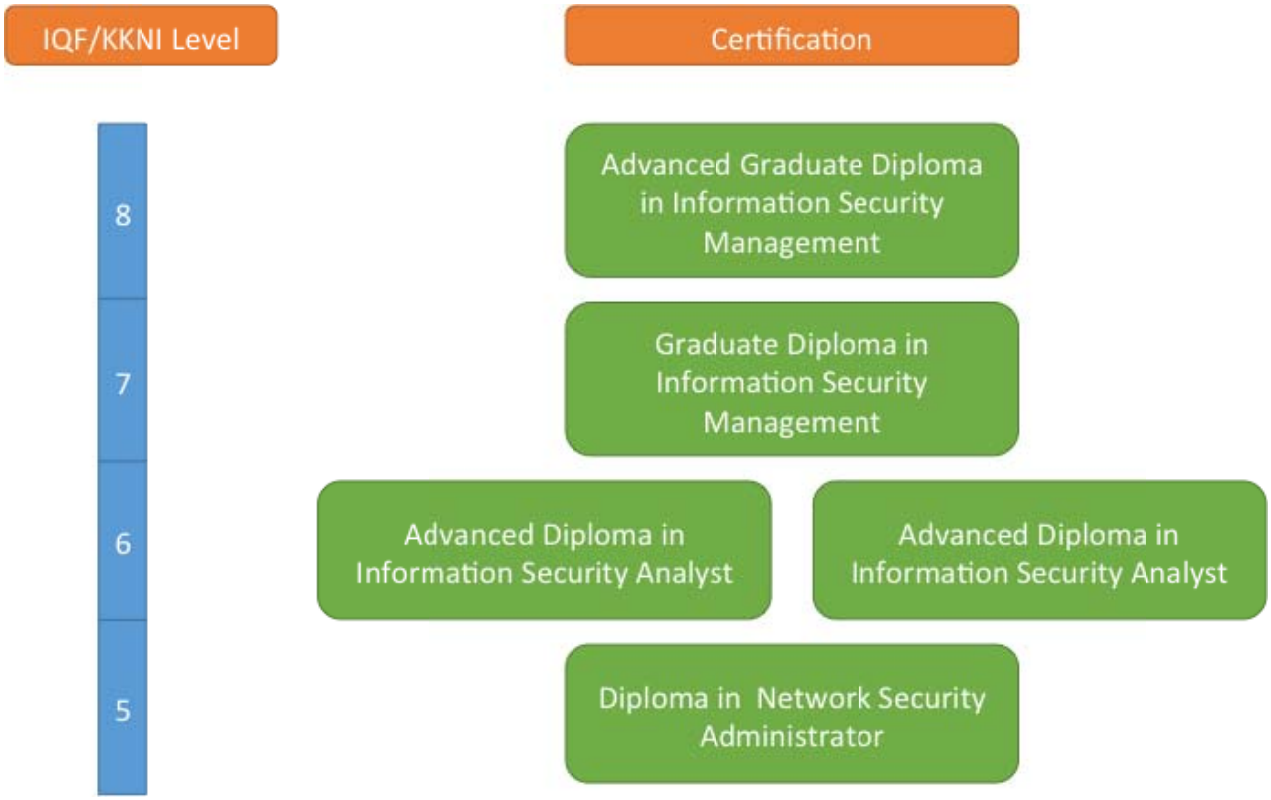
   Menurut ISO/IEC 27001 dan ISO/IEC 27002, istilah risiko keamanan informasi adalah potensi ancaman yang ada akan mengeksploitasi kerentanan aset atau kelompok aset sehingga dapat menyebabkan kerugian pada suatu organisasi. Berdasarkan hal ini maka ISO/IEC 27005 menyadari perlunya manajemen risiko keamanan informasi untuk mengidentifikasi kebutuhan organisasi mengenai persyaratan keamanan informasi dan menciptakan sistem manajemen keamanan informasi yang efektif. Pendekatan ini secara umum harus sesuai untuk lingkungan organisasi dan secara khusus harus diselaraskan dengan manajemen

risiko organisasi secara keseluruhan. Upaya keamanan harus menangani risiko secara efektif dan tepat waktu dimanapun dan kapanpun dibutuhkan.

BAB II
PENJENJANGAN KKNI KEAMANAN INFORMASI

PENJENJANGAN KKNI KEAMANAN INFORMASI

Sertifikasi di bidang Keamanan Informasi diberikan dalam berbagai jenjang KKNI yang meliputi jenjang KKNI 5 sampai 8. Jenis sertifikasi dan ekuivalensinya dengan jenjang KKNI dapat dilihat pada diagram yang disajikan pada Gambar 1.



Gambar 1. Jenis sertifikasi di bidang Keamanan Informasi

Berikut adalah ringkasan skema KKNI – *Keamanan Informasi* yang terdiri dari pemaketan nama packaging/sertifikasi, level KKNI (IQF) dan kesetaraannya pada *Australian Qualification Framework* (AQF) beserta kemungkinan Jabatan (*Job Roles*):

NO	Packaging	Level IQF/KKNI	Job Roles
1	J.62090.01.KUALIFIKASI .5.Sertifikat Administrator Keamanan Jaringan Diploma in Network Security Administrator	5	✓ Network Security Administrator ✓ IT security administrator ✓ systems/network administrator ✓ senior network administrator
2	J.62090.01.KUALIFIKASI .6.Advanced Diploma in Information Security Analyst Advanced Diploma in Information Security Analyst	6	✓ network security analyst ✓ systems security analyst ✓ IT security analyst
3	J.62090.01.KUALIFIKASI .6.Advanced Diploma in Information Security Specialist Advanced Diploma in Information Security Specialist	6	✓ network security specialist ✓ IT security specialist ✓ e-security specialist ✓ ICT security specialist
4	J.62090.01.KUALIFIKASI .7. Graduate Diploma in Information Security Management Graduate Diploma in Information Security Management	7	✓ Information System Security Manager ✓ Information Security Audit Manager
5	J.62090.01.KUALIFIKASI .8.Advanced Graduate Diploma in Information Security Management	8	✓ Senior Information Security Manager

NO	Packaging	Level IQF/KKNI	Job Roles
	Advanced Graduate Diploma in Information Security Management		✓ Information technology director ✓ Chief Information Security Officer ✓ Information Security Director

BAB III
PENGEMASAN KKNI KEAMANAN INFORMASI

B.1 PENGEMASAN KKNI LEVEL 5 CERTIFICATION IN NETWORK SECURITY ADMINISTRATOR

Diploma in Network Security Administrator

J.62090.01.KUALIFIKASI.5.Sertifikat Administrator Keamanan Jaringan

Deskripsi

Program sertifikasi ini bertujuan untuk menunjukkan tingkat keterampilan dan pengetahuan dalam mengembangkan dasar-dasar keterampilan KKNI level 5 - Sertifikat Administrator Keamanan Jaringan.

Peserta dengan kualifikasi ini dapat bekerja sebagai network security administrator dalam suatu tim *network security* atau sebagai pendukung *network security analyst*.

Sikap Kerja

Sikap kerja yang dimiliki oleh yang memenuhi kualifikasi KKNI level 5 dengan Sertifikat Administrator Keamanan Jaringan:

1. Sikap kerja umum (berdasarkan KKNI):
   a) Bertaqwa kepada Tuhan Yang Maha Esa.
   b) Memiliki moral, etika dan kepribadian yang baik di dalam menyelesaikan tugasnya.
   c) Berperan sebagai warga negara yang bangga dan cinta tanah air serta mendukung perdamaian dunia.
   d) Mampu bekerjasama dan memiliki kepekaan sosial dan kepedulian yang tinggi terhadap masyarakat dan lingkungannya.
   e) Menghargai keanekaragaman budaya, pandangan, kepercayaan, dan agama serta pendapat/temuan original orang lain.
   f) Menjunjung tinggi penegakan hukum serta memiliki semangat untuk mendahulukan kepentingan bangsa serta masyarakat luas
2. Sikap kerja khusus:
   a) Menjalankan tanggung jawab dan wewenang sesuai dengan perannya sebagai seseorang yang memiliki kualifikasi KKNI level 5 dengan Sertifikat Administrator Keamanan Jaringan

b) Disiplin, teliti dan objektif dalam menjalankan tugasnya dan dapat diberitanggung jawab atas hasil kerja orang lain.

Peran Kerja

Peran kerja dari individu dengan kualifikasi KKNI level 5 dengan Sertifikat Administrator Keamanan Jaringan adalah melaksanakan tugas yang berkaitan dengan lingkup tanggung jawab dan kewenangannya pada pengelolaan perangkat keamanan jaringan.

Berperan dalam menyelesaikan pekerjaan yang luas dalam bidang Keamanan Informasi dan memilih metoda yang sesuai dan berperan dalam menerapkan kebijakan dan/atau standar keamanan informasi, serta mampu menunjukkan kinerja dengan mutu dan kuantitas yang terukur.

Kemungkinan Jabatan

Kemungkinan jabatan yang relevan dengan kualifikasi, diantaranya:

- ✓ Network Security Administrator
- ✓ IT security administrator
- ✓ Systems/network administrator
- ✓ Senior network administrator

Aturan Pengemasan

25 unit kompetensi yang harus diselesaikan/dipenuhi, dengan perincian:

17 unit kompetensi inti

8 unit kompetensi pilihan

Daftar Unit **Kompetensi Inti:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2.	J.62090.006.01	Melaksanakan kebijakan keamanan informasi
3.	J.62090.023.01	Mengelola Keamanan Fisik
4.	J.62090.024.01	Melaksanakan Pencatatan Asset
5.	J.62090.028.01	Mengelola Script Keamanan Informasi
6.	J.62090.029.01	Mengelola perimeter keamanan
7.	J.62090.030.01	Melakukan Instalasi Piranti Lunak
8.	J.62090.032.01	Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan

9.	J.62090.037.01	Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
10.	J.62090.039.01	Mengimplementasikan koreksi atas kerentanan keamanan informasi
11.	J.62090.041.01	Menyediakan dukungan keamanan untuk permasalahan perangkat keras dan piranti lunak
12.	J.62090.042.01	Melakukan aktifitas penghapusan hak akses
13.	J.62090.044.01	Mengaplikasikan Patch Keamanan
14.	J.62090.048.01	Melaksanakan Kegiatan Pemulihan Data
15.	TIK.JK05.005.01	Melakukan Deteksi Dan Mengatasi Masalah Di Jaringan
16.	TIK.OP02.014.01	Mempergunakan Piranti lunak Anti Virus
17.	TIK.OP02.018.01	Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery

Daftar Unit **Kompetensi Pilihan:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.003.01	Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet
2.	J.62090.004.01	Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik
3.	J.62090.020.01	Mengelola log
4.	J.62090.026.01	Menyediakan dukungan keamanan bagi pengguna
5.	J.62090.027.01	Mengimplementasikan konfigurasi keamanan informasi
6.	J.62090.035.01	Mengelola siklus pemberian akses
7.	J.62090.036.01	Melaksanakan uji coba sistem pertahanan keamanan informasi
8.	J.62090.040.01	Mengelola insiden keamanan informasi
9.	J.62090.045.01	Mengelola integritas informasi
10.	TIK.CS02.041.01	Mengembalikan File pada Hard Disk yang Terhapus atau Data Hilang
11.	TIK.CS02.042.01	Mencegah Komputer dari serangan berbagai Jenis Virus
12.	TIK.CS02.043.01	Melakukan instalasi software anti Virus
13.	TIK.CS02.044.01	Melakukan Tindakan Ketika Virus Ditemukan
14.	TIK.CS02.045.01	Memperbaiki komputer yang terinfeksi Virus
15.	TIK.CS02.046.01	Membuat Rescue Disk
16.	TIK.CS02.047.01	Membersihkan Virus Jaringan
17.	TIK.JK02.022.01	Melakukan Back Up Dan Restore Basis Data Pengguna
18.	TIK.JK02.023.01	Menyelenggarakan Administrasi Sistem Jaringan
19.	TIK.JK04.004.01	Memonitor Dan Mengadministrasi Keamanan Sistem
20.	TIK.JK04.005.01	Menginstal Dan Memelihara Proses Pembuktian Keaslian (Authentication)
21.	TIK.JK04.017.01	Menginstal Dan Mengkonfigurasi Firewall Pada Server

22.	TIK.JK05.001.01	Mengelola Keamanan Sistem Jaringan
23.	TIK.JK05.004.01	Memelihara Sistem Jaringan Agar Up To Date
24.	TIK.JK05.005.01	Melakukan Deteksi Dan Mengatasi Masalah Di Jaringan
25.	TIK.JK05.006.01	Memberi Petunjuk Atau Saran Permasalahan Jaringan
26.	TIK.JK05.011.01	Memonitor Dan Mengadministrasi Keamanan Jaringan
27.	TIK.OP01.003.01	Mendeskripsikan kewaspasdaan terhadap keamanan informasi
28.	TIK.OP01.005.01	Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer
29.	TIK.PR01.013.01	Mengelola Manajemen Resiko
30.	TIK.SM03.005.01	Menetapkan Manajemen Eskalasi terhadap Permasalahan

Soft skill

Berikut ini adalah Soft –Skill yang harus dimiliki:

Komunikasi	1. Mendokumentasikan dokumen teknis dalam Bahasa Indonesia yang baik dan benar 2. Memahami petunjuk pelaksanaan kebijakan keamanan jaringan
Kerjasama	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Membangun dan mengembangkan kerjasama anggota tim dalam lingkungan Keamanan Informasi
Pemecahan Masalah	1. Menemukan dan mengatasi gangguan peralatan, sistem dan perangkat keamanan jaringan 2. Mengidentifikasi, menguji dan menyelesaikan gangguan sistem dan perangkat keamanan jaringan 3. Melakukan *debugging* dan pembuatan *script* untuk menyelesaikan masalah-masalah pada bidang keamanan jaringan 4. Menangani gangguan teknis, mengembangkan kendali keamanan dan rencana kontijensi untuk menurunkan ancaman dan dampak gangguan keamanan

Inisiatif	1. Responsif terhadap masalah keamanan yang ditemui di lingkungan kerjanya 2. Menginvestigasi dan mendokumentasikan solusi keamanan untuk menangani permasalahan keamanan jaringan
Perencanaan dan pengelolaan	Mengelola perangkat keamanan jaringan sesuai dengan aturan keamanan yang berlaku pada lingkungan kerja
Pengendalian diri	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Memiliki tanggungjawab terhadap hasil kerja anggota/individu sesuai dengan standar kualitas yang telah ditentukan 3. Memiliki tanggungjawab dan otonomi dalam menjalankan teknis operasional yang kompleks dalam tim 4. Bekerja dengan memperhatikan hak cipta, standar kode etik dan privasi pada area keamanan, hukum, moral dan etika yang berlaku di Indonesia
Pembelajaran	1. Mengadopsi dan mengaplikasikan teori, konsep, teknik dan kemampuan kreatif dalam berbagai situasi kerja 2. Mengikuti perkembangan tentang perangkat jaringan yang diterima industri IT saat ini 3. Senantiasa memperbaharui pengetahuan terhadap *tools* dan aplikasi perangkat IT terkait keamanan 4. Berpartisipasi dalam program belajar dan pengembangan kemampuan secara berkesinambungan
Pemahaman Teknologi	1. Memiliki pengetahuan tentang jaringan, protokol komunikasi data, perangkat keamanan jaringan 2. Mampu melakukan instalasi, konfigurasi dan pengujian fungsi dasar perangkat keamanan jaringan

Prasyarat

- ✓ Memiliki kemampuan yang setara dengan KKNI level 4 di bidang *Jaringan Komputer* yang dapat dibuktikan dengan ijazah Diploma 2 bidang Informatika dengan pengalaman kerja minimal 2 tahun di bidang jaringan komputer.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 4 di bidang *Jaringan Komputer* yang dapat dibuktikan dengan ijazah Diploma 2 Non Informatika dengan pengalaman kerja minimal 4 tahun dan lulus uji penempatan kompetensi.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 4 dibidang Jaringan Komputer yang dapat dibuktikan dengan ijazah SMK bidang Informatika dengan pengalaman kerja minimal 4 tahun.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 4 di bidang Jaringan Komputer yang dapat dibuktikan dengan ijazah SMA dengan pengalaman kerja minimal 6 tahun dan lulus uji penempatan kompetensi.

Kesetaraan/Kualifikasi Profesi

Lulusan dari program sertifikasi ini dapat disetarakan dengan program diploma tiga (D3) pada rumpun bidang ilmu Informatika (Rekayasa Perangkat Lunak Aplikasi, Teknologi Informasi, Manajemen Informatika/Sistem Informasi) atau rumpun bidang ilmu Teknik (Teknik Komputer/Sistem Komputer).

B.2 PENGEMASAN KKNI LEVEL 6 ADVANCED DIPLOMA IN INFORMATION SECURITY ANALYST

J.62090.01.KUALIFIKASI.6.Advanced Diploma in Analis Keamanan Informasi

Deskripsi

Program sertifikasi ini bertujuan untuk menunjukkan tingkat keterampilan dan pengetahuan dalam mengembangkan dasar-dasar keterampilan KKNI level 6 Advanced Diploma in Analis Keamanan Informasi.

Peserta dengan kualifikasi ini dapat bekerja sebagai analis keamanan informasi dalam suatu tim manajemen keamanan informasi.

Sikap Kerja

Sikap kerja yang dimiliki oleh yang memenuhi kualifikasi KKNI level 6 Advanced Diploma in Analis Keamanan Informasi:

1. Sikap kerja umum (berdasarkan KKNI):
   a) Bertaqwa kepada Tuhan Yang Maha Esa.
   b) Memiliki moral, etika dan kepribadian yang baik di dalam menyelesaikan tugasnya.
   c) Berperan sebagai warga negara yang bangga dan cinta tanah air serta mendukung perdamaian dunia.
   d) Mampu bekerjasama dan memiliki kepekaan sosial dan kepedulian yang tinggi terhadap masyarakat dan lingkungannya.
   e) Menghargai keanekaragaman budaya, pandangan, kepercayaan, dan agama serta pendapat/temuan original orang lain.
   f) Menjunjung tinggi penegakan hukum serta memiliki semangat untuk mendahulukan kepentingan bangsa serta masyarakat luas
2. Sikap kerja khusus:
   a) Menjalankan tanggung jawab dan wewenang sesuai dengan perannya sebagai seseorang yang memiliki kualifikasi KKNI level 6 Advanced Diploma in Information Security Analyst

b) Mampu memecahkan masalah dalam bidang Keamanan Informasi melalui pendekatan inter atau multidisipliner

c) Dapat memimpin bila bekerjasama dalam suatu tim.

Peran Kerja

Peran kerja dari individu dengan kualifikasi KKNI level 6 dengan Advanced Diploma in Information Security Analyst adalah melaksanakan tugas yang berkaitan dengan lingkup tanggung jawab dan kewenangannya pada pengelolaan dan pengembangan keamanan informasi.

Berperan dalam menyelesaikan pekerjaan yang luas dalam bidang Keamanan Informasi dan memilih metoda yang sesuai dan berperan dalam menerapkan kebijakan dan/atau standar keamanan informasi, serta mampu menunjukkan kinerja dengan mutu dan kuantitas yang terukur.

Kemungkinan Jabatan

Kemungkinan jabatan yang relevan dengan kualifikasi, diantaranya:

- ✓ Network security analyst
- ✓ Systems security analyst
- ✓ IT security analyst

Aturan Pengemasan

20 unit kompetensi yang harus diselesaikan/dipenuhi, dengan perincian:

14 unit kompetensi inti

6 unit kompetensi pilihan

Daftar Unit **Kompetensi Inti:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2.	J.62090.006.01	Melaksanakan kebijakan keamanan informasi
3.	J.62090.011.01	Menerapkan Standar-Standar Keamanan Informasi yang Berlaku
4.	J.62090.014.01	Melaksanakan Alokasi Pemisahan Tugas-tugas
5.	J.62090.023.01	Mengelola Keamanan Fisik
6.	J.62090.024.01	Melaksanakan Pencatatan Asset
7.	J.62090.028.01	Mengelola Script Keamanan Informasi

8.	J.62090.030.01	Melakukan Instalasi Piranti Lunak
9.	J.62090.037.01	Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
10.	J.62090.038.01	Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan
11.	J.62090.044.01	Mengaplikasikan Patch Keamanan
12.	J.62090.048.01	Melaksanakan Kegiatan Pemulihan Data
13.	TIK.JK04.004.01	Memonitor Dan Mengadministrasi Keamanan Sistem
14.	TIK.JK05.011.01	Memonitor Dan Mengadministrasi Keamanan Jaringan

Daftar Unit **Kompetensi Pilihan:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.003.01	Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet
2.	J.62090.004.01	Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik
3.	J.62090.013.01	Mengelola Proses Sertifikasi dan Akreditasi untuk Keamanan Informasi
4.	J.62090.020.01	Mengelola log
5.	J.62090.025.01	Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi
6.	J.62090.036.01	Melaksanakan uji coba sistem pertahanan keamanan informasi
7.	J.62090.043.01	Mengimplementasikan Manajemen Perbaikan/Respon yang Terkait dengan Keamanan Informasi
8.	J.62090.046.01	Mengelola Penggunakan Media Penyimpanan Sementara (Removable Media)
9.	J.62090.047.01	Merancang dan Mengelola Sistem Backup
10.	J.631100.010.01	Mengelola Keamanan Fisik Pusat Data
11.	J.631100.015.01	Melakukan Pengawasan Pusat Data
12.	TIK.JK03.009.01	Melakukan Analisis Teknologi Baru
13.	TIK.JK03.010.01	Melakukan Migrasi Ke Teknologi Baru
14.	TIK.JK03.012.01	Melakukan Audit Pre-Instalasi Untuk Instalasi Perangkat Lunak
15.	TIK.JK04.005.01	Menginstal Dan Memelihara Proses Pembuktian Keaslian (Authentication)
16.	TIK.JK04.017.01	Menginstal Dan Mengkonfigurasi Firewall Pada Server
17.	TIK.JK05.001.01	Mengelola Keamanan Sistem Jaringan
18.	TIK.JK05.006.01	Memberi Petunjuk Atau Saran Permasalahan Jaringan
19.	TIK.JK05.007.01	Menyiapkan Rencana Pemulihan Pada Saat Ada Kerusakan Fatal
20.	TIK.JK05.008.01	Mengelola Keamanan Sistem
21.	TIK.OP01.003.01	Mendeskripsikan kewaspasdaan terhadap keamanan informasi
22.	TIK.OP01.005.01	Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer
23.	TIK.OP02.014.01	Mempergunakan Piranti lunak Anti Virus
24.	TIK.OP02.018.01	Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery
25.	TIK.PR01.013.01	Mengelola Manajemen Resiko
26.	TIK.SM03.005.01	Menetapkan Manajemen Eskalasi terhadap Permasalahan

Soft skill

Berikut ini adalah Soft –Skill yang harus dimiliki:

Komunikasi	1. Mendokumentasikan dokumen teknis dalam Bahasa Indonesia yang baik dan benar 2. Memahami petunjuk pelaksanaan kebijakan keamanan jaringan
Kerjasama	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Membangun dan mengembangkan kerjasama anggota tim dalam lingkungan Keamanan Informasi
Pemecahan Masalah	1. Menemukan dan mengatasi gangguan peralatan, sistem dan perangkat keamanan jaringan 2. Mengidentifikasi, menguji dan menyelesaikan gangguan sistem dan perangkat keamanan jaringan 3. Melakukan *debugging* dan pembuatan *script* untuk menyelesaikan masalah-masalah pada bidang keamanan jaringan 4. Menangani gangguan teknis, mengembangkan kendali keamanan dan rencana kontijensi untuk menurunkan ancaman dan dampak gangguan keamanan
Inisiatif	1. Responsif terhadap masalah keamanan yang ditemui di lingkungan kerjanya 2. Menginvestigasi dan mendokumentasikan solusi keamanan untuk menangani permasalahan keamanan jaringan
Perencanaan dan pengelolaan	Mengelola perangkat keamanan jaringan sesuai dengan aturan keamanan yang berlaku pada lingkungan kerja
Pengendalian	1. Membangun lingkungan kerja yang aman dan berkesinambungan

diri	2. Memiliki tanggungjawab terhadap hasil kerja anggota/individu sesuai dengan standar kualitas yang telah ditentukan 3. Memiliki tanggungjawab dan otonomi dalam menjalankan teknis operasional yang kompleks dalam tim 4. Bekerja dengan memperhatikan hak cipta, standar kode etik dan privasi pada area keamanan, hukum, moral dan etika yang berlaku di Indonesia
Pembelajaran	1. Mengadopsi dan mengaplikasikan teori, konsep, teknik dan kemampuan kreatif dalam berbagai situasi kerja 2. Mengikuti perkembangan tentang perangkat jaringan yang diterima industri IT saat ini 3. Senantiasa memperbaharui pengetahuan terhadap *tools* dan aplikasi perangkat IT terkait keamanan 4. Berpartisipasi dalam program belajar dan pengembangan kemampuan secara berkesinambungan
Pemahaman Teknologi	Memiliki pengetahuan tentang jaringan, protokol komunikasi data, perangkat keamanan jaringan Mampu melakukan instalasi, konfigurasi dan pengujian fungsi dasar perangkat keamanan jaringan

Prasyarat

- ✓ Memiliki kemampuan yang setara dengan KKNI level 5 di bidang Keamanan Informasi yang dapat dibuktikan dengan ijazah Diploma 3 bidang Informatika dengan pengalaman kerja minimal 2 tahun di bidang Keamanan Informasi.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 5 di bidang Keamanan Informasi yang dapat dibuktikan dengan ijazah Diploma 3 Non Informatika dengan pengalaman kerja minimal 4 tahun dan lulus uji penempatan kompetensi.

Kesetaraan/Kualifikasi Profesi

Lulusan dari program sertifikasi ini dapat disetarakan dengan program sarjana (S1) pada rumpun bidang ilmu Informatika (Rekayasa Perangkat Lunak, Teknologi Informasi, Manajemen Informatika/Sistem Informasi) atau rumpun bidang ilmu Teknik (Teknik Komputer/Sistem Komputer) dengan konsentrasi Keamanan Informasi.

B.3 PENGEMASAN KKNI LEVEL 6 ADVANCED DIPLOMA IN INFORMATION SECURITY SPECIALIST

Advanced Diploma in Information Security Specialist

J.62090.01.KUALIFIKASI.6.Sertifikat Spesialis Keamanan Informasi

Deskripsi

Program sertifikasi ini bertujuan untuk menunjukkan tingkat keterampilan dan pengetahuan dalam mengembangkan dasar-dasar keterampilan KKNI level 6 - Sertifikat Spesialis Keamanan Informasi.

Peserta dengan kualifikasi ini dapat bekerja sebagai spesialis keamanan informasi dalam suatu tim manajemen keamanan informasi.

Sikap Kerja

Sikap kerja yang dimiliki oleh yang memenuhi kualifikasi KKNI level 6 dengan Sertifikat Spesialis Keamanan Informasi:

1. Sikap kerja umum (berdasarkan KKNI):
   a) Bertaqwa kepada Tuhan Yang Maha Esa.
   b) Memiliki moral, etika, dan kepribadian yang baik di dalam menyelesaikan tugasnya.
   c) Berperan sebagai warga negara yang bangga dan cinta tanah air serta mendukung perdamaian dunia.
   d) Mampu bekerjasama dan memiliki kepekaan sosial dan kepedulian yang tinggi terhadap masyarakat dan lingkungannya.
   e) Menghargai keanekaragaman budaya, pandangan, kepercayaan, dan agama serta pendapat/temuan original orang lain.
   f) Menjunjung tinggi penegakan hukum serta memiliki semangat untuk mendahulukan kepentingan bangsa serta masyarakat luas
2. Sikap kerja khusus:
   a) Menjalankan tanggung jawab dan wewenang sesuai dengan perannya sebagai seseorang yang memiliki kualifikasi KKNI level 6 dengan Sertifikat Spesialis Keamanan Informasi.
   b) Disiplin, teliti, dan objektif dalam menjalankan tugasnya dan dapat diberi tanggung jawab atas hasil kerja orang lain.
   c) Dapat memimpin bila bekerjasama dalam suatu tim.

Peran Kerja

Peran kerja dari individu dengan kualifikasi KKNI level 6 dengan Sertifikat Spesialis Keamanan Informasi adalah melaksanakan tugas yang berkaitan dengan lingkup tanggung jawab dan kewenangannya pada pengelolaan keamanan informasi.

Berperan dalam menyelesaikan pekerjaan yang luas dalam bidang Keamanan Informasi dan memilih metoda yang sesuai dan berperan dalam menerapkan kebijakan dan/atau standar keamanan informasi, serta mampu menunjukkan kinerja dengan mutu dan kuantitas yang terukur.

Kemungkinan Jabatan

Kemungkinan jabatan yang relevan dengan kualifikasi, diantaranya:

- ✓ Network security specialist
- ✓ IT security specialist
- ✓ e-security specialist
- ✓ ICT security specialist
- ✓ IT security architect
- ✓ Network security architect

Aturan Pengemasan

18 unit kompetensi yang harus diselesaikan/dipenuhi, dengan perincian:

12 unit kompetensi inti

6 unit kompetensi pilihan

Daftar Unit **Kompetensi Inti:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2.	J.62090.006.01	Melaksanakan kebijakan keamanan informasi
3.	J.62090.011.01	Menerapkan Standar-Standar Keamanan Informasi yang Berlaku
4.	J.62090.014.01	Melaksanakan Alokasi Pemisahan Tugas-tugas
5.	J.62090.023.01	Mengelola Keamanan Fisik
6.	J.62090.024.01	Melaksanakan Pencatatan Asset
7.	J.62090.028.01	Mengelola Script Keamanan Informasi

8.	J.62090.030.01	Melakukan Instalasi Piranti Lunak
9.	J.62090.037.01	Mendeteksi Kerentanan (Vulnerabilitas) Keamanan dan Potensi Pelanggaran
10.	J.62090.038.01	Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan
11.	J.62090.044.01	Mengaplikasikan Patch Keamanan
12.	J.62090.048.01	Melaksanakan Kegiatan Pemulihan Data

Daftar Unit **Kompetensi Pilihan:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.003.01	Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet
2.	J.62090.004.01	Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik
3.	J.62090.013.01	Mengelola Proses Sertifikasi dan Akreditasi untuk Keamanan Informasi
4.	J.62090.020.01	Mengelola log
5.	J.62090.025.01	Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi
6.	J.62090.036.01	Melaksanakan uji coba sistem pertahanan keamanan informasi
7.	J.62090.043.01	Mengimplementasikan Manajemen Perbaikan/Respon yang Terkait dengan Keamanan Informasi
8.	J.62090.046.01	Mengelola Penggunakan Media Penyimpanan Sementara (Removable Media)
9.	J.62090.047.01	Merancang dan Mengelola Sistem Backup
10.	J.631100.010.01	Mengelola Keamanan Fisik Pusat Data
11.	J.631100.015.01	Melakukan Pengawasan Pusat Data
12.	TIK.JK03.009.01	Melakukan Analisis Teknologi Baru
13.	TIK.JK03.010.01	Melakukan Migrasi Ke Teknologi Baru
14.	TIK.JK03.012.01	Melakukan Audit Pre-Instalasi Untuk Instalasi Perangkat Lunak
15.	TIK.JK05.006.01	Memberi Petunjuk Atau Saran Permasalahan Jaringan
16.	TIK.JK05.007.01	Menyiapkan Rencana Pemulihan Pada Saat Ada Kerusakan Fatal
17.	TIK.JK05.008.01	Mengelola Keamanan Sistem
18.	TIK.OP01.003.01	Mendeskripsikan kewaspasdaan terhadap keamanan informasi
19.	TIK.OP01.005.01	Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer
20.	TIK.OP02.014.01	Mempergunakan Piranti lunak Anti Virus
21.	TIK.OP02.018.01	Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery
22.	TIK.PR01.013.01	Mengelola Manajemen Resiko
23.	TIK.SM03.005.01	Menetapkan Manajemen Eskalasi terhadap Permasalahan

Soft skill

Berikut ini adalah Soft –Skill yang harus dimiliki:

Komunikasi	1. Mendokumentasikan dokumen teknis dalam Bahasa Indonesia yang baik dan benar 2. Memahami petunjuk pelaksanaan kebijakan keamanan jaringan
Kerjasama	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Membangun dan mengembangkan kerjasama anggota tim dalam lingkungan Keamanan Informasi
Pemecahan Masalah	1. Menemukan dan mengatasi gangguan peralatan, sistem dan perangkat keamanan jaringan 2. Mengidentifikasi, menguji dan menyelesaikan gangguan sistem dan perangkat keamanan jaringan 3. Melakukan *debugging* dan pembuatan *script* untuk menyelesaikan masalah-masalah pada bidang keamanan jaringan 4. Menangani gangguan teknis, mengembangkan kendali keamanan dan rencana kontijensi untuk menurunkan ancaman dan dampak gangguan keamanan
Inisiatif	1. Responsif terhadap masalah keamanan yang ditemui di lingkungan kerjanya 2. Menginvestigasi dan mendokumentasikan solusi keamanan untuk menangani permasalahan keamanan jaringan
Perencanaan dan pengelolaan	Mengelola perangkat keamanan jaringan sesuai dengan aturan keamanan yang berlaku pada lingkungan kerja
Pengendalian diri	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Memiliki tanggungjawab terhadap hasil kerja anggota/individu sesuai dengan standar kualitas yang telah ditentukan

	3. Memiliki tanggungjawab dan otonomi dalam menjalankan teknis operasional yang kompleks dalam tim 4. Bekerja dengan memperhatikan hak cipta, standar kode etik dan privasi pada area keamanan, hukum, moral dan etika yang berlaku di Indonesia
Pembelajaran	1. Mengadopsi dan mengaplikasikan teori, konsep, teknik dan kemampuan kreatif dalam berbagai situasi kerja 2. Mengikuti perkembangan tentang perangkat jaringan yang diterima industri IT saat ini 3. Senantiasa memperbaharui pengetahuan terhadap *tools* dan aplikasi perangkat IT terkait keamanan 4. Berpartisipasi dalam program belajar dan pengembangan kemampuan secara berkesinambungan
Pemahaman Teknologi	1. Memiliki pengetahuan tentang jaringan, protokol komunikasi data, perangkat keamanan jaringan 2. Mampu melakukan instalasi, konfigurasi dan pengujian fungsi dasar perangkat keamanan jaringan

Prasyarat

- ✓ Memiliki kemampuan yang setara dengan KKNI level 5 di bidang Keamanan Informasi yang dapat dibuktikan dengan ijazah Diploma 3 bidang Informatika dengan pengalaman kerja minimal 2 tahun di bidang Keamanan Informasi.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 5 di bidang Keamanan Informasi yang dapat dibuktikan dengan ijazah Diploma 3 Non Informatika dengan pengalaman kerja minimal 4 tahun dan lulus uji penempatan kompetensi.

Kesetaraan/Kualifikasi Profesi

Lulusan dari program sertifikasi ini dapat disetarakan dengan program sarjana (S1) pada rumpun bidang ilmu Informatika (Rekayasa Perangkat Lunak, Teknologi Informasi, Manajemen Informatika/Sistem Informasi) atau rumpun bidang ilmu Teknik (Teknik Komputer/Sistem Komputer) dengan konsentrasi Keamanan Informasi.

B.4 PENGEMASAN KKNI LEVEL 7 GRADUATE DIPLOMA IN INFORMATION SECURITY MANAGEMENT

J.62090.01.KUALIFIKASI.7. Graduate Diploma in Information Security Management

Deskripsi

Program sertifikasi ini bertujuan untuk menunjukkan tingkat keterampilan dan pengetahuan dalam mengembangkan dasar-dasar keterampilan KKNI level 7 Graduate Diploma in Information Security Management.

Peserta dengan kualifikasi ini dapat bekerja sebagai Information System Security Manager dalam suatu tim Keamanan Informasi.

Sikap Kerja

Sikap kerja yang dimiliki oleh yang memenuhi kualifikasi KKNI level 7 Graduate Diploma in Information Security Management:

1. Sikap kerja umum (berdasarkan KKNI):
   a) Bertaqwa kepada Tuhan Yang Maha Esa.
   b) Memiliki moral, etika dan kepribadian yang baik di dalam menyelesaikan tugasnya.
   c) Berperan sebagai warga negara yang bangga dan cinta tanah air serta mendukung perdamaian dunia.
   d) Mampu bekerjasama dan memiliki kepekaan sosial dan kepedulian yang tinggi terhadap masyarakat dan lingkungannya.
   e) Menghargai keanekaragaman budaya, pandangan, kepercayaan, dan agama serta pendapat/temuan original orang lain.
   f) Menjunjung tinggi penegakan hukum serta memiliki semangat untuk mendahulukan kepentingan bangsa serta masyarakat luas
2. Sikap kerja khusus:
   a) Menjalankan tanggung jawab dan wewenang sesuai dengan perannya sebagai seseorang yang memiliki kualifikasi KKNI level 7 Graduate Diploma in Information Security Management
   b) Mampu memecahkan masalah dalam bidang Keamanan Informasi melalui pendekatan inter atau multidisipliner

c) Disiplin, teliti dan objektif dalam menjalankan tugasnya

Peran Kerja

Peran kerja dari individu dengan kualifikasi KKNI level 7 dengan Graduate Diploma in Information Security Management adalah melaksanakan tugas yang berkaitan dengan lingkup tanggung jawab dan kewenangannya pada pengelolaan dan pengembangan keamanan informasi.

Berperan dalam menyelesaikan pekerjaan yang luas dalam bidang Keamanan Informasi dan memilih metoda yang sesuai dan berperan dalam menerapkan kebijakan dan/atau standar keamanan informasi, serta mampu menunjukkan kinerja dengan mutu dan kuantitas yang terukur.

Kemungkinan Jabatan

Kemungkinan jabatan yang relevan dengan kualifikasi, diantaranya:

- ✓ Information System Security Manager
- ✓ Information Security Audit Manager

Aturan Pengemasan

32 unit kompetensi yang harus diselesaikan/dipenuhi, dengan perincian:

22 unit kompetensi inti

10 unit kompetensi pilihan

Daftar Unit **Kompetensi Inti:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2.	J.62090.002.01	Menyelaraskan Penerapan Prinsip Perlindungan Informasi dengan Misi dan Tujuan Organisasi
3.	J.62090.005.01	Menyusun Dokumen Kebijakan Keamanan Informasi
4.	J.62090.006.01	Melaksanakan kebijakan keamanan informasi
5.	J.62090.007.01	Mengelola Siklus Informasi (Klasifikasi, Kategorisasi, Penanggung-Jawab)
6.	J.62090.009.01	Mengelola Prosedur Keamanan Informasi
7.	J.62090.010.01	Mengimplementasikan Prosedur Keamanan Informasi Dalam Kegiatan Pengadaan
8.	J.62090.012.01	Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi
9.	J.62090.013.01	Mengelola Proses Sertifikasi dan Akreditasi untuk Keamanan Informasi
10.	J.62090.014.01	Melaksanakan Alokasi Pemisahan Tugas-tugas

11.	J.62090.015.01	Melaksanakan Koordinasi dan Pengarahan Pelaksanaan Tugas-Tugas Keamanan Informasi
12.	J.62090.016.01	Mengelola Sdm yang Terkait dengan Tugas-Tugas Keamanan Informasi
13.	J.62090.021.01	Mengelola Audit Keamanan Informasi
14.	J.62090.025.01	Mengelola Sistem Pertahanan dan Perlindungan Keamanan Informasi
15.	J.62090.026.01	Menyediakan dukungan keamanan bagi pengguna
16.	J.62090.033.01	Mengidentifikasi Serangan-Serangan Terhadap Kontrol Akses
17.	J.62090.038.01	Melaksanakan Evaluasi Kelemahan (Vulnerabilitas) Keamanan
18.	J.62090.043.01	Mengimplementasikan Manajemen Perbaikan/Respon yang Terkait dengan Keamanan Informasi
19.	M.702000.001.01	Menganalisis Risiko Audit Teknologi Informasi
20.	TIK.SM01.010.01	Menjamin Integritas Informasi
21.	TIK.SM02.007.01	Mengatur Otorisasi Akses Teknologi Informasi
22.	TIK.SM03.004.01	Menetapkan Standar Otorisasi Akses di dalam Organisasi

Daftar Unit **Kompetensi Pilihan:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.017.01	Mengelola Program Peningkatan Kepedulian dan Pelatihan Terkait dengan Keamanan Informasi
2.	J.62090.018.01	Mengelola Risiko Keamanan Informasi
3.	J.62090.019.01	Melakukan Kajian Keamanan Informasi
4.	J.62090.022.01	Melakukan Evaluasi Kinerja Keamanan Informasi
5.	J.62090.029.01	Mengelola perimeter keamanan
6.	J.62090.031.01	Mengelola Aspek Keamanan Sistem Informasi pada Setiap Kegiatan Upgrade/Peremajaan Sistem Informasi
7.	J.62090.032.01	Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan
8.	J.62090.034.01	Mengkaji Efektivitas Penerapan Kontrol Akses
9.	J.62090.039.01	Mengimplementasikan koreksi atas kerentanan keamanan informasi
10.	J.62090.040.01	Mengelola insiden keamanan informasi
11.	J.62090.047.01	Merancang dan Mengelola Sistem Backup
12.	J.620200.001.01	Menentukan Metode Pemodelan Arsitektur Bisnis dan Business Building Block yang Diperlukan
13.	J.620200.002.01	Menetapkan Matriks, Diagram, dan Jenis Kebutuhan (Requirements) yang Diperlukan pada Arsitektur Bisnis
14.	J.620200.004.01	Menyusun Roadmap Arsitektur Bisnis
15.	M.702090.001.01	Mengelola Proyek Secara Terintegrasi (Project Integration Management)
16.	TIK.JK05.008.01	Mengelola Keamanan Sistem
17.	TIK.JK05.010.01	Menjamin Privacy (Kerahasiaan) Pengguna
18.	TIK.OP01.003.01	Mendeskripsikan kewaspasdaan terhadap keamanan informasi
19.	TIK.OP01.005.01	Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer

20.	TIK.OP02.014.01	Mempergunakan Piranti lunak Anti Virus
21.	TIK.OP02.018.01	Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery
22.	TIK.PR01.013.01	Mengelola Manajemen Resiko
23.	TIK.SM03.005.01	Menetapkan Manajemen Eskalasi terhadap Permasalahan

Soft skill

Berikut ini adalah Soft –Skill yang harus dimiliki:

Komunikasi	1. Memberikan solusi dan alternatifnya dalam berdiskusi dengan pemangku kepentingan sarana prasarana Keamanan Informasi. 2. Secara ringkas menuliskan dan menjelaskan sarana prasarana Keamanan Informasi kepada seluruh jajaran internal organisasi 3. Menyusun dan mempresentasikan laporan yang kompleks untuk maksud dan tujuan khusus dengan mempergunakan berbagai metodologi yang media yang sesuai. 4. Memberikan dan menyakinkan informasi kepada pelanggan, rekan sejawat, dan personil unit organisasi terkait. 5. Memiliki kemampuan komunikasi dan literasi menggunakan Bahasa Indonesia, Bahasa Inggris dan/atau bahasa lainnya dalam kegiatan analisis, evaluasi, dan penyampaian informasi.
Kerjasama	1. Memimpin dan membagi peran anggota tim, serta mengarahkan tugas setiap anggota guna mencapai sasaran yang telah ditetapkan. 2. Kerja sama membangun lingkungan kerja yang aman dan berkesinambungan 3. Membangun dan mengembangkan kerjasama anggota tim dalam lingkungan Keamanan Informasi

Pemecahan Masalah	1. Analisis dan mencari solusi masalah yang terkait dengan Keamanan Informasi 2. Mencari akar masalah baik yang berdampak luas maupun khusus, serta melakukan pemeringkatan masalah 3. Membantu mengembangkan strategi pembangunan sarana prasarana Keamanan Informasi guna mengatasi hambatan pembangunan dalam batasan waktu dan biaya yang telah ditetapkan 4. Mengantisipasi permasalahan yang kemungkinan terjadi pada pembangunan sarana prasarana Keamanan Informasi dan mencari solusi untuk mengatasi masalah dan kondisi darurat yang perlu dilakukan
Inisiatif	1. Mengembangkan kriteria baru dan prosedur untuk mewujudkan *best-practice* dalam penyusunan arsitektur sarana dan prasaran Keamanan Informasi 2. Mengidentifikasi kendala dalam perancangan instalasi dan pengembangan strategi Keamanan Informasi sesuai dengan batasan waktu dan biaya 3. Memprioritaskan permintaan yang mendesak
Perencanaan dan pengelolaan	1. Membantu merencanakan, menyusun prioritas dan memantau kegiatan penyusunan arsitektur sarana dan prasarana Keamanan Informasi 2. Membantu menyelaraskan arsitektur sarana dan prasarana Keamanan Informasi dengan rencana bisnis perusahaan 3. Membantu menyusun rencana pengelolaan risiko dan menjalankan implementasi yang telah disepakati

Pengendalian diri	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Memiliki tanggungjawab terhadap hasil kerja diri sendiri sesuai dengan standar kualitas yang telah ditentukan 3. Bekerja dengan memperhatikan hak cipta, standar kode etik dan privasi pada area keamanan, hukum, moral dan etika yang berlaku di Indonesia
Pembelajaran	1. Memberikan dan menerima umpan balik guna tercapainya sasaran organisasi 2. Mengelola pelatihan bagi anggota tim Keamanan Informasi 3. Berpartisipasi dalam program belajar dan pengembangan kemampuan secara berkesinambungan
Pemahaman Teknologi	1. Memiliki pengetahuan untuk membantu fungsi-fungsi pengadaan 2. Membantu membuat keputusan pemilihan teknologi pada area Keamanan Informasi 3. Mengikuti perkembangan tentang perangkat keras ataupun perangkat lunak dalam industri Keamanan Informasi 4. Berperan aktif dalam mengkaji risiko yang mungkin timbul dalam penerapan teknologi baru

Prasyarat

- ✓ Memiliki kemampuan yang setara dengan KKNI level 6 di bidang Keamanan Informasi yang dapat dibuktikan dengan ijazah sarjana (S1/D4) bidang Informatika dengan pengalaman kerja minimal 2 tahun di bidang Keamanan Informasi.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 6 di bidang Keamanan Informasi yang dapat dibuktikan dengan ijazah sarjana

(S1/D4) Non Informatika dengan pengalaman kerja minimal 4 tahun dan lulus uji penempatan kompetensi.

Kesetaraan/Kualifikasi Profesi

Lulusan dari program sertifikasi ini dapat disetarakan dengan program Profesi (Level 7) pada bidang ilmu Informatika (Rekayasa Perangkat Lunak Aplikasi, Teknologi Informasi, Manajemen Informatika/Sistem Informasi), rumpun bidang ilmu Teknik (Teknik Komputer/Sistem Komputer)

B.5 PENGEMASAN KKNI LEVEL 8 ADVANCED GRADUATE DIPLOMA IN INFORMATION SECURITY MANAGEMENT

J.62090.01.KUALIFIKASI.8.Advanced Graduate Diploma in Information Security Management

Deskripsi

Program sertifikasi ini bertujuan untuk menunjukkan tingkat keterampilan dan pengetahuan dalam mengembangkan dasar-dasar keterampilan KKNI level 8 Advanced Graduate Diploma in Information Security Management.

Peserta dengan kualifikasi ini dapat bekerja pada level Chief of Information Security Officer.

Sikap Kerja

Sikap kerja yang dimiliki oleh yang memenuhi kualifikasi KKNI level 8 Advanced Graduate Diploma in Information Security Management:

3. Sikap kerja umum (berdasarkan KKNI):
   a) Bertaqwa kepada Tuhan Yang Maha Esa.
   b) Memiliki moral, etika dan kepribadian yang baik di dalam menyelesaikan tugasnya.
   c) Berperan sebagai warga negara yang bangga dan cinta tanah air serta mendukung perdamaian dunia.
   d) Mampu bekerjasama dan memiliki kepekaan sosial dan kepedulian yang tinggi terhadap masyarakat dan lingkungannya.
   e) Menghargai keanekaragaman budaya, pandangan, kepercayaan, dan agama serta pendapat/temuan original orang lain.
   f) Menjunjung tinggi penegakan hukum serta memiliki semangat untuk mendahulukan kepentingan bangsa serta masyarakat luas
4. Sikap kerja khusus:
   a) Menjalankan tanggung jawab dan wewenang sesuai dengan perannya sebagai seseorang yang memiliki kualifikasi KKNI level 8 Advanced Graduate Diploma in Information Security Management
   b) Mampu memecahkan masalah dalam bidang Keamanan Informasi melalui pendekatan inter atau multidisipliner

Peran Kerja

Peran kerja dari individu dengan kualifikasi KKNI level 8 dengan Advanced Graduate Diploma in Information Security Management adalah melaksanakan tugas yang berkaitan dengan lingkup tanggung jawab dan kewenangannya pada pengelolaan dan pengembangan keamanan informasi.

Berperan dalam menyelesaikan pekerjaan yang luas dalam bidang Keamanan Informasi dan memilih metoda yang sesuai dan berperan dalam menerapkan kebijakan dan/atau standar keamanan informasi, serta mampu menunjukkan kinerja dengan mutu dan kuantitas yang terukur.

Kemungkinan Jabatan

Kemungkinan jabatan yang relevan dengan kualifikasi, diantaranya:

- ✓ Senior Information Security Manager
- ✓ Information Technology Director
- ✓ Chief Information Security Officer
- ✓ Information Security Director

Aturan Pengemasan

33 unit kompetensi yang harus diselesaikan/dipenuhi, dengan perincian:

23 unit kompetensi inti

10 unit kompetensi pilihan

Daftar Unit **Kompetensi Inti:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.001.01	Menerapkan Prinsip Perlindungan Informasi
2.	J.62090.002.01	Menyelaraskan Penerapan Prinsip Perlindungan Informasi dengan Misi dan Tujuan Organisasi

3.	J.62090.005.01	Menyusun Dokumen Kebijakan Keamanan Informasi
4.	J.62090.008.01	Melaksanakan Ketentuan Hukum yang Berlaku tentang Keamanan Informasi
5.	J.62090.009.01	Mengelola Prosedur Keamanan Informasi
6.	J.62090.010.01	Mengimplementasikan Prosedur Keamanan Informasi Dalam Kegiatan Pengadaan
7.	J.62090.012.01	Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi
8.	J.62090.013.01	Mengelola Proses Sertifikasi dan Akreditasi untuk Keamanan Informasi
9.	J.62090.015.01	Melaksanakan Koordinasi dan Pengarahan Pelaksanaan Tugas-Tugas Keamanan Informasi
10.	J.62090.017.01	Mengelola Program Peningkatan Kepedulian dan Pelatihan Terkait dengan Keamanan Informasi
11.	J.62090.018.01	Mengelola Risiko Keamanan Informasi
12.	J.62090.019.01	Melakukan Kajian Keamanan Informasi
13.	J.62090.022.01	Melakukan Evaluasi Kinerja Keamanan Informasi
14.	J.62090.043.01	Mengimplementasikan Manajemen Perbaikan/Respon yang Terkait dengan Keamanan Informasi
15.	M.702090.007.01	Mengelola Komunikasi Proyek (Project Communication Management)
16.	M.702090.008.01	Mengelola Risiko Proyek (Project Risk Management)
17.	MBP.MB04.001.01	Menyusun Perencanaan Anggaran
18.	MBP.MB04.002.01	Mengendalikan Anggaran
19.	TIK.JK05.010.01	Menjamin Privacy (Kerahasiaan) Pengguna
20.	TIK.PR01.013.01	Mengelola Manajemen Resiko
21.	TIK.SM01.010.01	Menjamin Integritas Informasi
22.	TIK.SM02.007.01	Mengatur Otorisasi Akses Teknologi Informasi
23.	TIK.SM03.004.01	Menetapkan Standar Otorisasi Akses di dalam Organisasi

Daftar Unit **Kompetensi Pilihan:**

No	Kode Unit	Judul Unit Kompetensi
1.	J.62090.007.01	Mengelola Siklus Informasi (Klasifikasi, Kategorisasi, Penanggung-Jawab)
2.	J.62090.016.01	Mengelola SDM yang Terkait dengan Tugas-Tugas Keamanan Informasi
3.	J.62090.021.01	Mengelola Audit Keamanan Informasi
4.	J.620200.001.01	Menentukan Metode Pemodelan Arsitektur Bisnis dan Business Building Block yang Diperlukan
5.	J.620200.002.01	Menetapkan Matriks, Diagram, dan Jenis Kebutuhan (Requirements) yang Diperlukan pada Arsitektur Bisnis
6.	J.620200.004.01	Menyusun Roadmap Arsitektur Bisnis
7.	M.702090.001.01	Mengelola Proyek Secara Terintegrasi (Project Integration Management)
8.	M.702090.002.01	Mengelola Ruang Lingkup Proyek (Project Scope Management)
9.	M.702090.003.01	Mengelola Jadwal Waktu Proyek (Project Time Management)
10.	M.702090.004.01	Mengelola Biaya Proyek (Project Cost Management)
11.	M.702090.005.01	Mengelola Kualitas Proyek (Project Quality Management)
12.	M.702090.006.01	Mengelola Sumberdaya Manusia Proyek (Project Human Resource Managment)

13.	M.702090.009.01	Mengelola Pengadaan-pengadaan Proyek (Project Procurement Management)
14.	M.702090.010.01	Mengelola Stakeholder Proyek (Project Stakeholder Management)
15.	TIK.JK02.004.01	Mendisain Sistem Keamanan Jaringan
16.	TIK.OP01.003.01	Mendeskripsikan kewaspasdaan terhadap keamanan informasi
17.	TIK.OP01.005.01	Mengimplementasikan sistem keamanan dan keselamatan pada pengoperasian komputer
18.	TIK.OP02.014.01	Mempergunakan Piranti lunak Anti Virus
19.	TIK.OP02.018.01	Mengoperasikan utilitas dasar untuk Backup, Restore, Data Recovery
20.	TIK.SM03.005.01	Menetapkan Manajemen Eskalasi terhadap Permasalahan

Soft skill

Berikut ini adalah Soft –Skill yang harus dimiliki:

Komunikasi	1. Memberikan solusi dan alternatifnya dalam berdiskusi dengan pemangku kepentingan sarana prasarana Keamanan Informasi. 2. Secara ringkas menuliskan dan menjelaskan sarana prasarana Keamanan Informasi kepada seluruh jajaran internal organisasi 3. Menyusun dan mempresentasikan laporan yang kompleks untuk maksud dan tujuan khusus dengan mempergunakan berbagai metodologi yang media yang sesuai. 4. Memberikan dan menyakinkan informasi kepada pelanggan, rekan sejawat, dan personil unit organisasi terkait. 5. Memiliki kemampuan komunikasi dan literasi menggunakan Bahasa Indonesia, Bahasa Inggris dan/atau bahasa lainnya dalam kegiatan analisis, evaluasi, dan penyampaian informasi.

Kerjasama	1. Memimpin dan membagi peran anggota tim, serta mengarahkan tugas setiap anggota guna mencapai sasaran yang telah ditetapkan. 2. Menjembatani hubungan dengan setiap bagian dari organisasi maupun vendor
Pemecahan Masalah	1. Analisis dan mencari solusi masalah yang terkait dengan Keamanan Informasi 2. Mencari akar masalah baik yang berdampak luas maupun khusus, serta melakukan pemeringkatan masalah 3. Mengembangkan strategi pembangunan sarana prasarana Keamanan Informasi guna mengatasi hambatan pembangunan dalam batasan waktu dan biaya yang telah ditetapkan 4. Mengantisipasi permasalahan yang kemungkinan terjadi pada pembangunan sarana prasarana Keamanan Informasi dan mencari solusi untuk mengatasi masalah dan kondisi darurat yang perlu dilakukan 5. Pemecahan masalah dengan melibatkan tenaga ahli dari luar unit organisasinya.
Inisiatif	1. Mengembangkan kriteria baru dan prosedur untuk mewujudkan *best-practice* dalam penyusunan arsitektur sarana dan prasaran Keamanan Informasi 2. Mengidentifikasi kendala dalam perancangan instalasi dan pengembangan strategi Keamanan Informasi sesuai dengan batasan waktu dan biaya 3. Aktif mendorong terbentuknya manajemen risiko

Perencanaan dan pengelolaan	1. Merencanakan, menyusun prioritas dan memantau kegiatan penyusunan arsitektur sarana dan prasarana Keamanan Informasi 2. Menyelaraskan arsitektur sarana dan prasarana Keamanan Informasi dengan rencana bisnis perusahaan 3. Menyusun rencana pengelolaan risiko dan menjalankan implementasi yang telah disepakati
Pengendalian diri	1. Membangun lingkungan kerja yang aman dan berkesinambungan 2. Memiliki tanggungjawab terhadap hasil kerja diri sendiri sesuai dengan standar kualitas yang telah ditentukan 3. Bekerja dengan memperhatikan hak cipta, standar kode etik dan privasi pada area keamanan, hukum, moral dan etika yang berlaku di Indonesia
Pembelajaran	1. Memberikan dan menerima umpan balik guna tercapainya sasaran organisasi 2. Memberikan kajian dan pelatihan bagi anggota tim penyusun strategi Keamanan Informasi 3. Berpartisipasi dalam program belajar dan pengembangan kemampuan secara berkesinambungan
Pemahaman Teknologi	1. Memiliki pengetahuan untuk membantu fungsi-fungsi pengadaan 2. Membuat keputusan pemilihan teknologi pada area Keamanan Informasi 3. Mengikuti perkembangan tentang perangkat keras ataupun perangkat lunak dalam industri Keamanan Informasi

Prasyarat

- ✓ Memiliki kemampuan yang setara dengan KKNI level 7 di bidang *Audit TI, Manajemen Layanan TI, Enterprise Architecture* dengan pengalaman kerja minimal 5 tahun di bidang Keamanan Informasi.
- ✓ Memiliki kemampuan yang setara dengan KKNI level 6 di bidang *Audit TI, Manajemen Layanan TI, Enterprise Architecture* yang dibuktikan dengan ijazah sarjana (S1/D4) dengan pengalaman kerja di bidang keamanan informasi minimal 10 tahun dan lulus uji penempatan kompetensi.

Kesetaraan/Kualifikasi Profesi

Lulusan dari program sertifikasi ini dapat disetarakan dengan program magister (S2) pada rumpun bidang ilmu Informatika (Rekayasa Perangkat Lunak Aplikasi, Teknologi Informasi, Manajemen Informatika/Sistem Informasi) dengan spesialisasi Keamanan Informasi.