DIGITAL TALENT SCHOLARSHIP

PEMAHAMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS SNI ISO/IEC 27001:2013

Materi 4 – Klausul 6 Perencanaan

KOMINFO Badan Penelitian dan Pengembangan Sumber Daya Manusia

#JADIJAGOANDIGITAL

Profil Pengajar

AKBAR ARYANTO

- Join BSN 2005
- Koordinator Kelompok Substansi Infrastruktur dan Keamanan Informasi PUSDATIN – BSN
- Universitas Gunadarma 1998
- University of Twente – Netherlands 2016
- Universitas Gunadarma 2021
- Assesor SMKI 27001:2013 – KAN
- Lead Auditor SMKI 27001:2013
- akbar@bsn.go.id

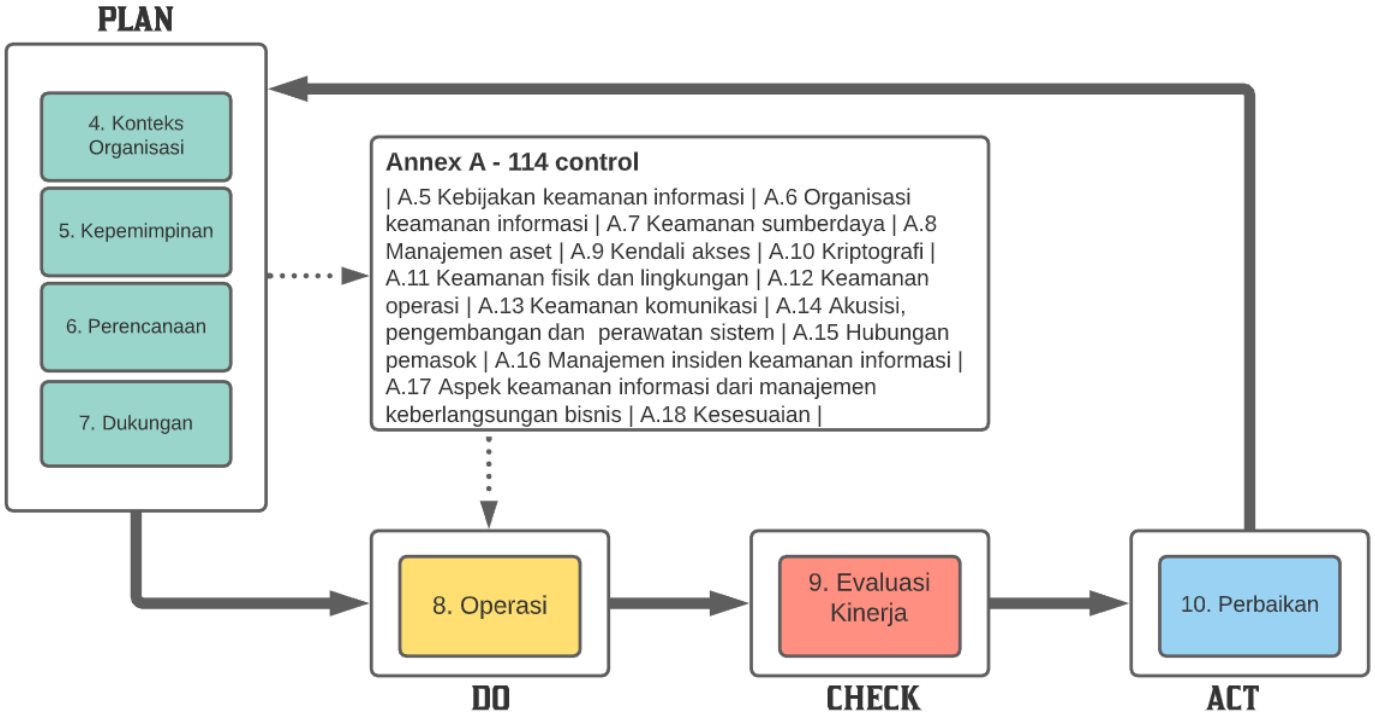
Indra Hikmawan

- S1 Sistem Informasi Universitas Gunadarma
- Pranata Komputer Ahli Pertama Pusat Data dan Sistem Informasi BSN
- Auditor & Implementer SNI ISO/IEC 27001:2013
- Indra.hikmawan@bsn.go.id

Tujuan Pembelajaran

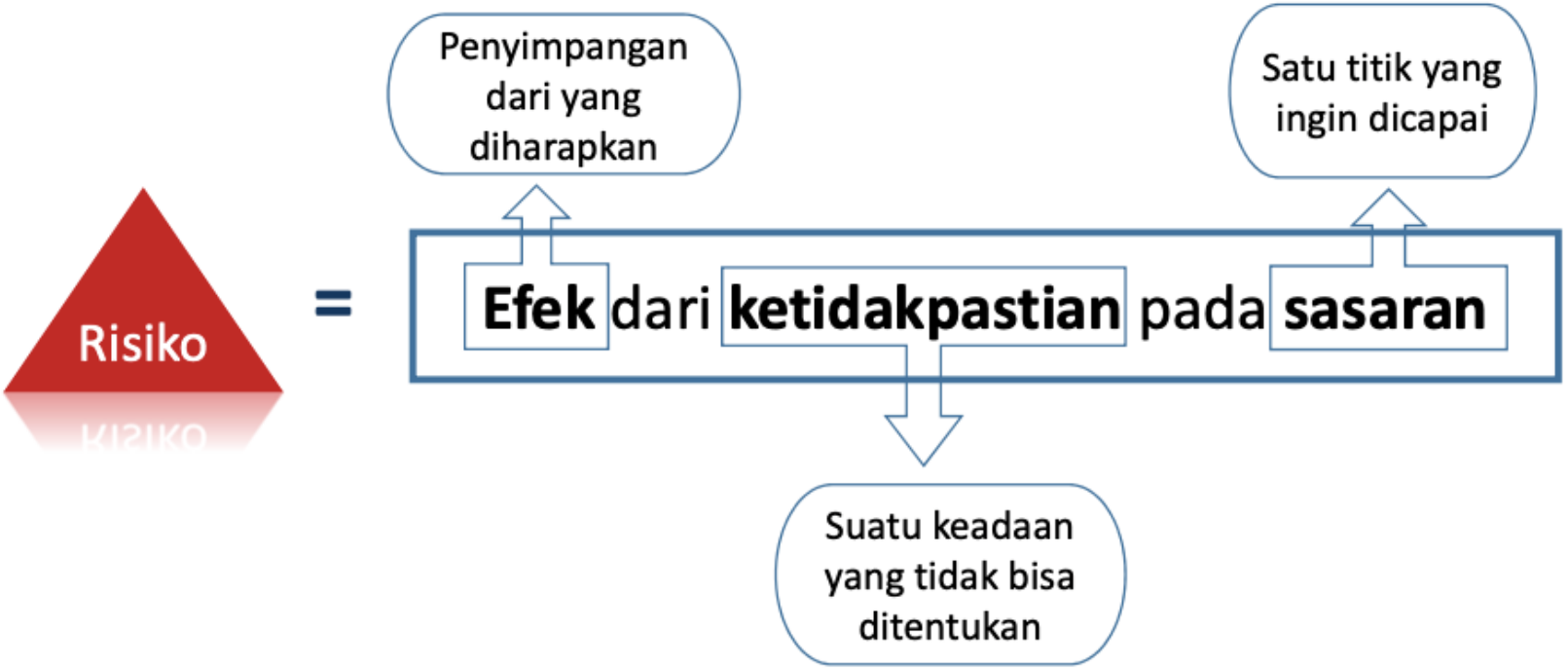
Setelah mengikuti pelatihan modul ini, peserta diharapkan mampu menganalisis Tindakan untuk menangani risiko dan peluang serta sasaran manajemen keamanan informasi dan perencanaan untuk mencapainya.

STRUKTUR SNI ISO/IEC 27001:2013



Konsep Utama SMKI

- Definisi Risiko



(*Effect of uncertainty on objectives* – ISO 31000)

Klausul 6 - Perencanaan

Sub Klausul

- 6.1 Tindakan untuk menangani risiko dan peluang
- 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

6.1 Tindakan untuk Menangani Risiko dan Peluang

Catatan : Proses penilaian dan penanganan risiko keamanan informasi dalam Standar ini sejalan dengan prinsip-prinsip dan pedoman umum yang tersedia dalam ISO 31000

6.1.1 Saat Merencanakan SMKI, organisasi harus mempertimbangkan permasalahan yang dimaksud dalam 4.1 dan persyaratan dalam 4.2, serta menentukan risiko dan peluang yang harus ditangani untuk:

a) memastikan SMKI dapat mencapai manfaat yang diinginkan;

b) mencegah, atau mengurangi, efek yang tidak diinginkan;

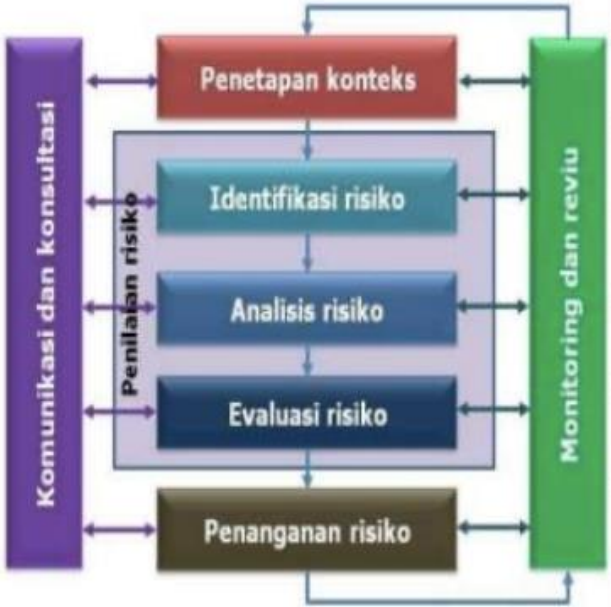
c) mencapai perbaikan yang berkelanjutan

Organisasi harus merencanakan :

d) tindakan untuk menangani risiko dan peluang; dan

e) bagaimana cara:

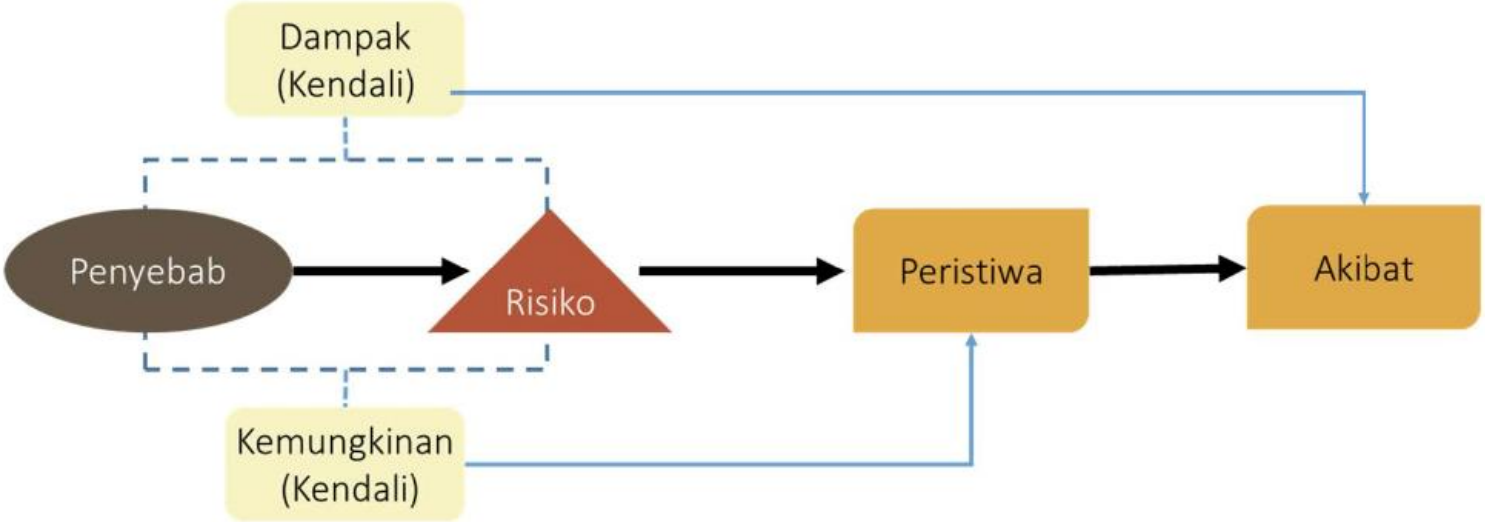
1. Mengintegrasikan dan menerapkan tindakan ke dalam proses SMKI
2. Mengevaluasi efektifitas tindakan tersebut



Proses Manajemen Risiko

1. **Penetapan Konteks**
   latar belakang, ruang lingkup, tujuan, dan lingkungan pengendalian
2. **Identifikasi Risiko**
   mengidentifikasi risiko, waktu, sebab, dan proses terjadinya peristiwa risiko
3. **Analisis risiko**
   mencermati risiko dan tingkat pengendalian serta menilai risiko
4. **Evaluasi risiko**
   dilakukan untuk pengambilan keputusan mengenai penanganan risiko
5. **Penanganan risiko**
   mengidentifikasi opsi penanganan risiko dan memilih opsi terbaik
6. **Monitoring dan reviu**
   memastikan penanganan dan langkah-langkah lanjutan yang diperlukan
7. **Komunikasi dan konsultasi**
   dilakukan terus menerus dengan cara mengembangkan metode komunikasi dan pelaporan kepada *stakeholder* internal maupun eksternal

Memahami Risiko



Klausul 6.1.2 Penilaian risiko keamanan infromasi

Informasi terdokumentasi dipelihara

Kemungkinan Terjadinya Resiko

Kriteria kemungkinan terjadinya Risiko (likelihood/ frequency), yaitu besarnya peluang atau frekuensi suatu Risiko akan terjadi. Pengukurannya bisa menggunakan pendekatan statistik (probability), frekuensi kejadian persatuan waktu (hari, minggu, bulan, tahun) , atau dengan expert judgement

Dampak Terjadinya Risiko

Dampak dan probabilitas risiko-risiko ini ditentukan karena berkaitan dengan Keamanan Informasi (CIA). Berdasarkan kriteria penerimaan risiko organisasi, yang merupakan fungsi dari selera terhadap risiko organisasi, organisasi menentukan pendekatan untuk menangani risiko ini.

Tabel Kategori Resiko

NO	Kategori Risiko	Definisi
1	Reputasi	Risiko yang disebabkan oleh menurunnya tingkat kepercayaan pemangku kepentingan eksternal yang bersumber dari persepsi negatif terhadap organisasi.
2	Finansial	Risiko yang disebabkan kerugian berupa sejumlah biaya yang harus di keluarkan, di tanggung,atau yang hilang dalam bentuk rupiah.
3	Operasional	Risiko yang disebabkan: - ketidakcukupan dan/atau tidak berfungsinya proses internal, kesalahan manusia, dan kegagalan sistem. - adanya kejadian ekstemal yang mempengaruhi operasional organisasi. - adanya tuntutan hukum dari luar kepada organisasi
4	Kinerja	Risiko yang di sebabkan tertunda nya aktifitas kerja dalam suatu ketetapan waktu.

Tabel Dampak Terjadinya Risiko

Tingkat Dampak	Reputasi	Finansial	Operasional	Kinerja
1 (Tidak Signifikan)	Terdapat pemberitaan negatif namun tidak mengakibat penurunan kepercayaan	Tidak terdapat kerugian finansial	Terdapat gangguan namun tidak mengakibatkan proses bisnis teraganggu	Menimbulkan penundaan aktifitas maksimal 24 Jam
2 (Kurang Signifikan)	Terdapat pemberitaan negatif yang dapat mempengaruhi tingkat kepercayaan stakeholder	terdapat kerugian/biaya yang harus dikeluarkan hingga Rp. 50.000.000,-	terdapat gangguan yang menyebabkan 1 mata rantai proses bisnis terganggu	Menimbulkan penundaan aktifitas maksimal 2 x 24 Jam
3 (Cukup Signifikan)	terdapat pemberitaan negatif yang terus menurunkan kepercayaan stakeholder	terdapat kerugian/biaya yang harus dikeluarkan Rp. 50.000.000,- hingga Rp. 250.000.000,-	terdapat gangguan yang menyebabkan lebih dari satu proses bisnis terganggu	Menimbulkan penundaan aktifitas maksimal 7 x 24 Jam
4 (Signifikan)	hilangnya kepercayaan stakeholder	terdapat kerugian/biaya yang harus dikeluarkan Rp. 250.000.000,- hingga 500.000.000,-	terdapat gangguan yang menyebabkan seluruh proses bisnis terganggu	Menimbulkan penundaan aktifitas maksimal 14 x 24 Jam
5 (Sangat Signifikan)	hilangnya kepercayaan stakeholder	terdapat kerugian/biaya yang harus dikeluarkan lebih dari Rp. 500.000.000,-	terjadi kelumpuhan pada proses bisnis	Menimbulkan penundaan aktifitas maksimal lebih dari 14 x 24 Jam

Tabel Peluang / Kemungkinan Terjadinya Risiko

Kemungkinan	Nilai	Uraian
Hampir tidak terjadi	1	Risiko terjadi sekali dalam waktu > 5 Tahun
Jarang Terjadi	2	Risiko dapat terjadi sekali antara 1 – 5 Tahun
Kadang Terjadi	3	Risiko mungkin terjadi 1 – 6 kali setahun
Sering Terjadi	4	Risiko mungkin terjadi rata-rata 1 kali setiap bulan
Hampir Pasti Terjadi	5	Risiko terjadi minimum seminggu 1 kali

MATRIKS ANALISIS RISIKO & LEVEL RISIKO

Nilai Risiko

Nilai Risiko merupakan kombinasi antara tingkat kemungkinan terjadinya risiko dan tingkat dampak yang direpresentasikan dengan angka , yang dirumuskan sebagai berikut :

Nilai Risiko = Level Kemungkinan x Level Dampak

Nilai resiko selanjutnya dikelompokkan dalam rentang nilai tertentu untuk memudahkan saat dilakukan seleksi prioritas penanganan risiko

Matrik Analisis Resiko

Matriks Analisis Risiko 5 x 5			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Level Risiko

Level Risiko SPBE

Level Risiko	Rentang Besaran Risiko	Simbol Warna
Sangat Rendah	1 - 5	Biru
Rendah	6 - 10	Hijau
Sedang	11 – 15	Kuning
Tinggi	16 – 20	Jingga
Sangat Tinggi	21 - 25	Merah

Rentang Nilai Risiko	Pernyataan Rentang Nilai Risiko	Simbol Warna	Tindakan yang diambil
1 - 5	Sangat Rendah	Biru	Tidak diperlukan tindakan
6 - 10	Rendah	Hijau	Diambil tindakan jika diperlukan
11 – 15	Sedang	Kuning	Diambil tindakan jika sumber daya tersedia
16 – 20	Tinggi	Jingga	Diperlukan tindakan untuk mengelola risiko
21 - 25	Sangat Tinggi	Merah	Diperlukan tindakan segera untuk mengelola risiko

Selera Resiko

NO	Kategori Risiko	Besaran Risiko yang harus di tindak lanjuti
1	Reputasi	> 10
2	Finansial	> 8
3	Operasional	> 12
4	Kinerja	> 10

Risk Register

Risk Register

- Eskalasi Risiko

  Eskalasi risiko dipilih jika Risiko berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko ke unit kerja yang lebih tinggi.

- Mitigasi Risiko

  Mitigasi risiko dilakukan dengan cara mengurangi level kemungkinan dan/atau level dampak dari Risiko

- Transfer Risiko

  Transfer risiko dipilih jika terdapat kekurangan sumber daya untuk mengelola Risiko. Opsi ini dilakukan dengan cara mengalihkan kepemilikan risiko kepada pihak lain untuk melakukan pengelolaan dan pertanggungjawaban terhadap Risiko.

- Penghindaran Risiko

  Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SMKI.

- Penerimaan Risiko

Klausul 6.1.3 Penanganan risiko keamanan informasi

Informasi terdokumentasi dipelihara

Statement of Applicability (SOA)

Pernyataan Pemberlakuan

Versi
Tanggal

PERNYATAAN PEMBERLAKUAN / STATEMENT OF APPLICABILITY
(Nama Organisasi)
(Lingkup)

Klausul	Judul	Ya / Tidak	Justifikasi
4	Konteks Organisasi		
4.1	Konteks Organisasi untuk Keamanan Informasi		
4.1.1	Identifikasi Isu Eksternal / Internal	Ya	(Isikan alasan memenuhi/tidaknya klasul / annex tsb)
..			
..			
Annex			
A5	Information Security Policies		
A.5.1	Management Direction for Information Security		
A.5.1.1	Policies for Information Security	Ya	(Isikan alasan memenuhi/tidaknya klasul / annex tsb)
..			
..			

Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Informasi terdokumentasi dipelihara

Klausul 6.2 Sasaran keamanan informasi dan perencanaan untuk mencapainya

Informasi terdokumentasi dipelihara

Sasaran Keamanan Informasi

SASARAN
SISTEM MANAJEMEN KEAMANAN INFORMASI

No	Sasaran	KPI	Aktivitas Pencapaian Kinerja	Indikator Pencapaian	Kebutuhan Sumber Daya	PIC	Jangka Waktu	Evaluasi
1								
2								
...								
...								

Tugas

1. Buatlah Dokumen Risk Register dengan jumlah risiko minimal 5
2. Buatlah Dokumen Sasaran SMKI

#JADIJAGOANDIGITAL

TERIMA KASIH

digitalent.kominfo

DTS_kominfo

digitalent.kominfo

digital talent scholarship