
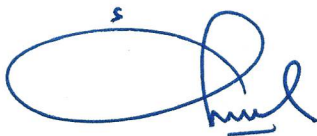




PT Infomedia Nusantara

# Prosedur Pengelolaan Risiko

No. Dokumen	IN.PRO-03
Versi	1.0
Klasifikasi	Terbatas
Tanggal Efektif	08 September 2021
Tanggal Peninjauan	-
Jenis Dokumentasi	Pedoman / Prosedur
Pemilik Dokumen	Koordinator Pengelolaan Risiko


PERSETUJUAN:

DISUSUN:	MENGETAHUI:	DISETUJUI:
		
<u>Firdiansyah</u> Pengendali Dokumen	<u>Samudra Prasetyo</u> Wakil Manajemen	<u>Agus Winarno</u> Manajemen Puncak

	<b>Prosedur Pengelolaan Risiko</b>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	2


## RIWAYAT PERUBAHAN

Versi	Penyusun / Pelaksana Revisi	Tanggal Revisi	Keterangan Perubahan	Bab	Hal
1.0	Pengendali Dokumen	08 September 2021	Versi pertama	-	-

	<b>Prosedur Pengelolaan Risiko</b>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	3

## DAFTAR ISI

	<b>Hal.</b>
<b>RIWAYAT PERUBAHAN</b>	<b>2</b>
<b>DAFTAR ISI</b>	<b>3</b>
<b>TUJUAN</b>	<b>1</b>
<b>REFERENSI</b>	<b>1</b>
<b>PENGKAJIAN DOKUMEN</b>	<b>5</b>
<b>LAMPIRAN</b>	<b>5</b>

	<p style="text-align: center;"><b>Prosedur Pengelolaan Risiko</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	1

## 1. TUJUAN

Kebijakan dan Prosedur ini bertujuan untuk mengelola risiko keamanan informasi yang dihadapi oleh organisasi dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

## 2. REFERENSI

- 00189/KPTS/INF2020\_O\_1/21/D Penerapan Manajemen Risiko Perusahaan
- SNI ISO/IEC 27001:2013 - Klausul 6.1: Tindakan untuk menangani risiko dan peluang
- SNI ISO/IEC 27001:2013 - Klausul 8.2: Penilaian risiko keamanan informasi
- SNI ISO/IEC 27001:2013 - Klausul 8.3: Penanganan risiko keamanan informasi

## 3. Penetapan Konteks


Kondisi organisasi – baik internal maupun eksternal – yang terkait dengan keamanan informasi harus diidentifikasi dan ditetapkan berdasarkan potensi kendala yang akan dihadapi oleh organisasi. Penetapan hal ini selaras dengan identifikasi konteks organisasi berdasarkan persyaratan klausul 4.1 SNI ISO/IEC 27001:2013.

## 4. Tujuan dari Identifikasi Risiko

Tujuan utama dari Risk Assessment adalah untuk memperkirakan Risiko yang mempengaruhi aset di lingkungan PT. Infomedia Nusantara sebagai berikut :

- a. Mengidentifikasi aset, dan menentukan nilainya sesuai dengan persyaratan Kerahasiaan, Integritas dan Ketersediaan.
- b. Mengidentifikasi Kerentanan dalam sistem dan nilainya.
- c. Mengidentifikasi Ancaman yang dapat mengeksploitasi Kerentanan ini.
- d. Memperkirakan probabilitas Ancaman.
- e. Menghitung Risiko dan kemudian mengurutkannya sesuai dengan signifikansi relatifnya.
- f. Menafsirkan hasil.

Tingkat risiko yang ada ini akan memungkinkan PT. Infomedia Nusantara untuk memfokuskan tindakan korektif mereka terhadap kerentanan yang terkait dengan risiko tertinggi.


	<b>Prosedur Pengelolaan Risiko</b>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	2

## 5. Penilaian Risiko


Penilaian risiko (*risk assessment*) merupakan aktivitas untuk melakukan penilaian terhadap risiko-risiko yang telah diidentifikasi dengan mengacu pada kriteria penilaian yang telah ditetapkan. Penilaian risiko mencakup proses-proses sebagai berikut.

**Tabel 1.1 Definisi Kolom Penilaian Risiko**

No	No Kolom Risk Register	Nama Kolom	Deskripsi
1	2	<b>Objective / Scope</b>	Diisi dengan Objective Unit, referensi : - Kontrak Manajemen (Target Unit) - PD Organisasi (Tugas dan Tanggung Jawab) - Master Plan (Sasaran Tahun Berjalan) - 10 Strategic Initiative (yang terkait dengan masing2 unit)
2	3	<b>Nama Risiko</b>	- Diisi dengan hal-hal yang dapat menghambat pencapaian objective unit - Untuk satu objective, risiko (hal yang dapat menghambat pencapaian objective) bisa lebih dari satu.
3	4	<b>Deskripsi Risiko</b>	Diisi dengan penjelasan lebih detail risiko (bagaimana risiko tersebut dapat menghambat pencapaian objective).
4	5	<b>Kategori Risiko</b>	Diisi dengan (pilih salah satu) : 1. Compliance 2. Strategic 3. Financial 4. Operation
5	6	<b>Sumber Risiko</b>	Diisi dengan (pilih salah satu) : 1. Eksternal 2. Internal 3. Internal dan Eksternal  *)Eksternal, apabila sumber risikonya dari luar TELKOM  **)Internal, apabila sumber risikonya dari internal TELKOM
6	7	<b>Akar Penyebab</b>	Diisi dengan penyebab risiko. Untuk mengetahui akar permasalahan utama, metodologinya dapat menggunakan pertanyaan 'Mengapa/WHY' . Atas jawaban tersebut, dilakukan pertanyaan 'Mengapa/WHY' lagi sampai tidak mendapatkan jawaban lagi. Jawaban terakhir ini dianggap sebagai root cause / akar permasalahan.

	<b>Prosedur Pengelolaan Risiko</b>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	3

7	8	<b>Indikator Risiko</b>	Diisi dengan indikator risiko yang dapat diukur Bisa juga diambil pendekatan indikator dari akar penyebab, misal akar penyebabnya "kurangnya kompetensi sales", maka indikatornya "produktivitas sales"
8	9	<b>Mitigasi Eksisting</b>	Diisi dengan kegiatan mitigasi risiko tersebut yang telah/sedang dilakukan oleh unit (apabila ada), dan menjawab setiap akar penyebab
9	10	<b>Dampak Kualitatif (Aspect Risiko C;I;A)</b>	Diisi dengan dampak yang bersifat kualitatif atas risk yang terjadi  Menambahkan aspek Confidentiality, Integrity, Availability)
10	11	<b>Inherent Risk</b>	Diisi levelnya berdasarkan pemetaan risk map / risk appetite berdasarkan likelihood x impact pada tabel setelah mitigasi eksisting
11	14	<b>Justifikasi Likelihood</b>	Diisi dengan penjelasan peluang terjadinya risiko sesuai dengan level yang dipilih pada kolom 11
12	15	<b>Justifikasi Impact</b>	Diisi dengan penjelasan besarnya dampak akibat risiko sesuai dengan level yang dipilih pada kolom 12
13	16	<b>Strategi Response</b>	Diisi dengan strategi perusahaan dalam merespons risiko
14	17	<b>Risk Treatment</b>	Diisi dengan rencana mitigasi /risk response yang akan dilakukan untuk menurunkan level risiko. Risk Treatment / Mitigasi plan harus menjawab setiap akar penyebab yang ada
15	18	<b>Activity Treatment</b>	Diisi dengan aktivitas-aktivitas yang akan dilakukan berkaitan dengan Risk Treatment
16	19	<b>Risk Owner</b>	Diisi dengan pejabat satu level di bawah kepala unit, yang merupakan PIC dari program mitigasi yg dilakukan
17	20	<b>Budget Plan</b>	Diisi dengan kebutuhan anggaran yang diperlukan untuk melaksanakan mitigasi
18	21	<b>Time Plan</b>	Diisi dengan target waktu pelaksanaan setiap aktivitas mitigasi pada kolom 18
19	22	<b>Related Unit</b>	Diisi dengan unit terkait untuk penanganan risiko
20	23	<b>Residual Risk</b>	Diisi levelnya berdasarkan pemetaan risk map / risk appetite berdasarkan likelihood dan impact pada akhir tahun setelah dilakukan rencana mitigasi
21	26	<b>Annex</b>	Diisi dengan referensi Annex control berdasarkan ISO 27001:2013
22	27	<b>Business Process</b>	Diisi dengan proses yang berkaitan dengan risiko yang terjadi
23	28	<b>Asset</b>	Diisi dengan aset yang berhubungan dengan kategori risiko (aset fisik, aset perangkat lunak, jaringan, personel, informasi, cloud server, dll)

	<p style="text-align: center;"><b>Prosedur Pengelolaan Risiko</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	4

## 6. Pedoman untuk Mengidentifikasi Aset

Daftar aset kemudian dilakukan dengan menggunakan informasi yang dikumpulkan dari pemilik aset. Pemilik aset diminta untuk melakukan perincian aset yang mereka menggunakan :

- Meminta untuk pemilik aset memberikan rincian aset fisik, perangkat lunak, Infrastruktur TI, dll dan membuat daftar aset kritis dan tingkat tinggi
- Meminta untuk dapat di jelaskan acuan dari kebijakan dan prosedur terkait aset yang digunakan saat ini.
- Selain itu melakukan wawancara dengan Staf Teknis untuk perincian perangkat keras mereka saat ini dan konfigurasinya, perangkat lunak dan nya konfigurasi, pengaturan Keamanan TI, Infrastruktur TI, kebijakan dan prosedur yang digunakan saat ini.
- Penilaian dilakukan untuk melakukan verifikasi dari kebenaran informasi.
- Aset-aset ini kemudian dikumpulkan dan didaftarkan ke dalam daftar aset untuk dapat dipelihara oleh Pemilik Aset sebagai tindakan pencegahan terhadap risiko yang akan timbul.


## 7. Pedoman untuk Mengevaluasi Aset

Setelah diidentifikasi, aset selanjutnya akan dikenakan penilaian Aset. Nilai-nilai ini mewakili pentingnya aset untuk bisnis organisasi. Nilai aset digunakan untuk mengidentifikasi perlindungan yang tepat untuk aset dan untuk menentukan pentingnya aset bagi organisasi. Nilai-nilai ini dapat dinyatakan dalam dampak bisnis potensial dari peristiwa yang tidak diinginkan yang mempengaruhi hilangnya kerahasiaan, integritas dan/atau ketersediaan. Potensi dampak antara lain terganggunya kegiatan usaha, kerugian finansial, kehilangan pendapatan, pangsa pasar atau citra. Berdasarkan kategori berikut :

- **Confidentiality** adalah Nilai aset berdasarkan Kerahasiaan
- **Integrity** adalah Nilai aset berdasarkan Integritas
- **Availability** adalah Nilai aset berdasarkan Ketersediaan

## 8. Pemantauan Risiko

Risiko tidak bersifat statis, dikarenakan ancaman dan kerentanan dapat berubah tiba-tiba tanpa ada indikasi. Oleh karena itu pemantauan dan peninjauan yang konsisten diperlukan untuk mendeteksi perubahan ini. Proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan berkala minimal 1 tahun sekali. Untuk pemantauan dari penanganan risiko (*risk treatment*) mengikuti tanggal jatuh tempo yang sudah disepakati.

	<b>Prosedur Pengelolaan Risiko</b>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-03
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	5

## 9. PENGKAJIAN DOKUMEN

Dokumen ini dikelola oleh Pengendali Dokumen. Setiap masukan perubahan terhadap prosedur ini harus diajukan kepada Pengendali Dokumen. Perubahannya disetujui oleh Manajemen Puncak sesuai ketentuan yang berlaku di PT Infomedia Nusantara.

Dokumen ini harus ditinjau ulang secara berkala oleh Pengendali Dokumen paling sedikit 1 (satu) kali dalam setahun untuk memastikan kesesuaiannya dengan kondisi organisasi.

## 10. LAMPIRAN

-