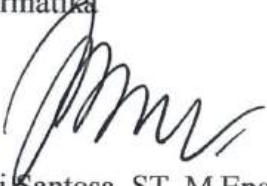




DINAS KOMUNIKASI DAN INFORMATIKA
PEMERINTAH DAERAH KABUPATEN SLEMAN

PROSEDUR PENGELOLAAN MANAJEMEN RISIKO

Nomor	:	T/P.001/SMKI/2025
Tanggal Pembuatan	:	5 Mei 2025
Tanggal Revisi	:	5 Mei 2025
Tanggal Pengesahan	:	5 Mei 2025
Disahkan Oleh	:	Plt. Kepala Dinas Komunikasi dan Informatika  Budi Santosa, ST, M.Eng, M.Eng NIP : 197509021996031001

Catatan Revisi

Versi	Tanggal	Diusulkan Oleh	Deskripsi dan Riwayat Perubahan
1.0	5 Mei 2025	Koor. Manajemen Risiko	Dokumen Baru

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

DAFTAR ISI

DAFTAR ISI	2
1. TUJUAN DAN SASARAN	3
2. KONSEP MANAJEMEN RISIKO	3
3. ORGANISASI MANAJEMEN RISIKO	5
4. IDENTIFIKASI RISIKO	6
5. PENILAIAN RISIKO	6
6. PEMANTAUAN RISIKO	12

	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

1. TUJUAN DAN SASARAN

Proses Manajemen Risiko dimaksudkan untuk mengendalikan risiko berdasarkan proses menentukan aset kritikal, mendeskripsikan risiko, menilai risiko, mengontrol risiko dan melaksanakan tindakan dalam rangka mengurangi tingkat risiko hingga pada tingkatan yang yang dapat diterima.

Sasaran dalam manajemen risiko di Dinas Komunikasi dan Informatika Kabupaten Sleman adalah untuk mengidentifikasi risiko yang mungkin terjadi terhadap proses bisnis Dinas Komunikasi dan Informatika Kabupaten Sleman dalam aktivitas pekerjaan, untuk merencanakan pengendalian risiko yang dibutuhkan dalam rangka melakukan tindakan untuk menangani dan mengeliminasi risiko, dan peningkatan efektivitas dan pelaksanaan Manajemen Risiko yang berkelanjutan.

Pedoman ini memberikan petunjuk mengenai pengembangan manajemen risiko di Dinas Komunikasi dan Informatika Kabupaten Sleman yang meliputi panduan dalam menganalisa dan mengontrol risiko yang teridentifikasi yang terkait dengan pengelolaan sistem informasi sebagai pendukung proses bisnis utama. Selanjutnya manual ini memberikan arahan dalam menentukan kontrol pengamanan yang akan dilakukan untuk mengurangi dampak risiko untuk melindungi informasi kritikal dan proses pendukung pengelolaan informasi terkait kepersonilan dan organisasi.

1.1. Ruang Lingkup

Ruang lingkup dalam proses Manajemen Risiko ini adalah seluruh kegiatan yang dilaksanakan di lingkungan Dinas Komunikasi dan Informatika Kabupaten Sleman.

1.2. Referensi

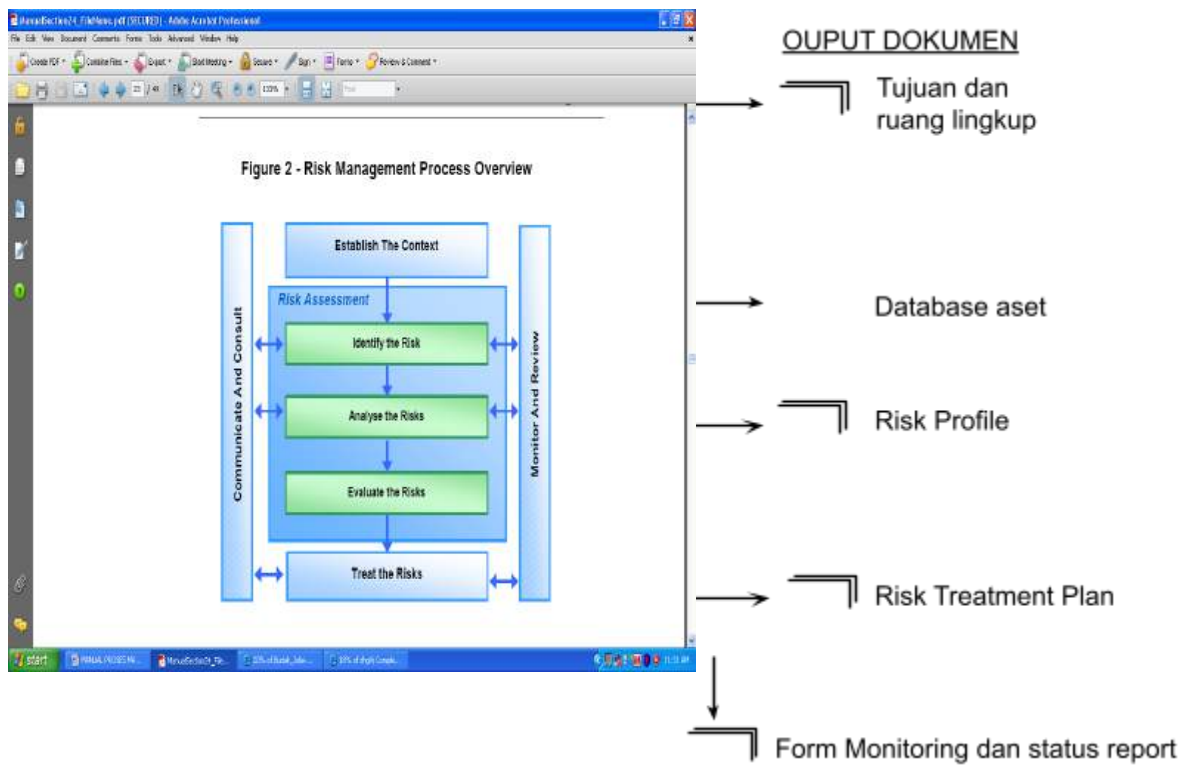
- a. ISO 31000 – Manajemen Risiko
- b. ISO/IEC 27001:2022, C.6.1 – Tindakan Untuk Menangani Risiko dan Peluang
- c. ISO/IEC 27001:2022, C.8.2 – Penilaian Risiko Keamanan Informasi
- d. ISO/IEC 27001:2022, C.8.3 – Penanganan Risiko Keamanan Informasi

2. KONSEP MANAJEMEN RISIKO

Aktivitas dalam proses pengelolaan risiko meliputi registrasi risiko dan rencana pengendalian risiko. Registrasi risiko dilakukan untuk mencatat informasi mengenai risiko-risiko yang teridentifikasi, yang dapat mengganggu proses bisnis. Registrasi risiko ini merupakan suatu daftar risiko yang harus ditinjau dan di-update secara periodik. Sedangkan rencana pengendalian risiko merupakan suatu tindakan penanganan untuk mengurangi tingkat dari risiko.

Pelaksanaan Manajemen Risiko meliputi beberapa siklus dan tahapan seperti pada gambar 1 berikut ini:

	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0



Gambar 1. Proses Manajemen Risiko

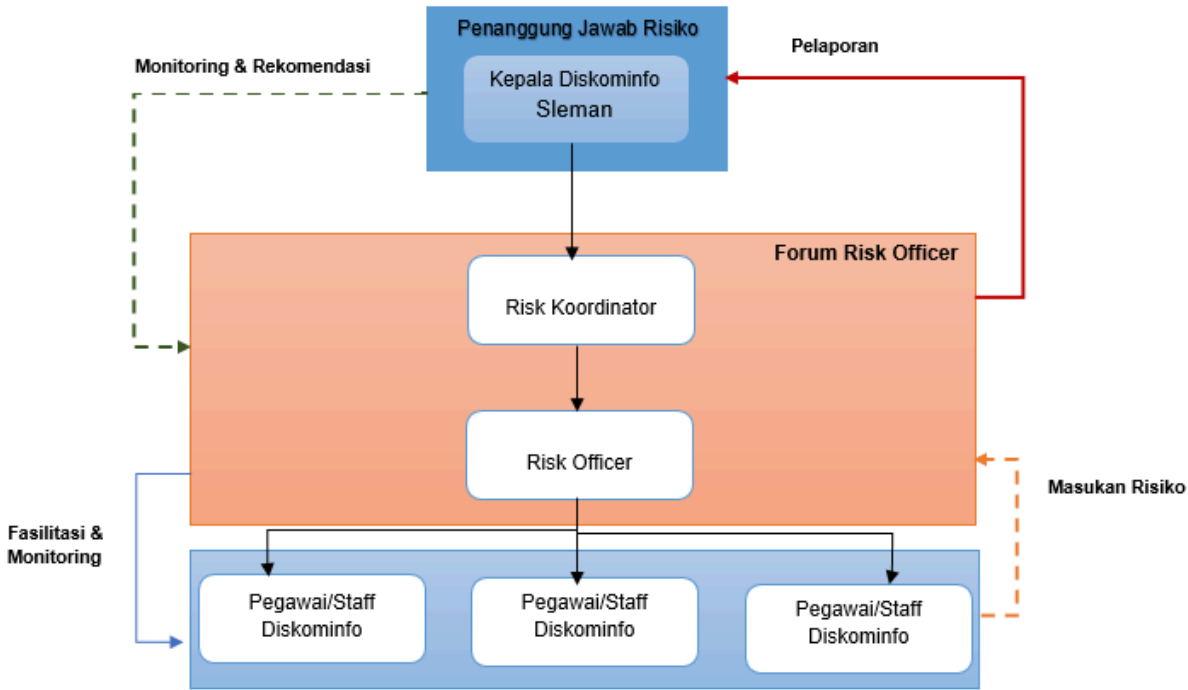
Secara garis besar, pelaksanaan proses manajemen risiko terbagi menjadi 4 tahap yaitu :

- 2.1. Tahap 1: Identifikasi Risiko
Proses penentuan kapan dan bagaimana terjadinya risiko-risiko yang mungkin terjadi sehingga berdampak pada tugas pokok organisasi.
- 2.2. Tahap 2: Penilaian Risiko
Proses analisa kontrol-kontrol yang sudah diterapkan oleh organisasi, menentukan nilai risiko berdasarkan ancaman dan kerawanan yang mungkin terjadi, dan melakukan pengendalian risiko.
- 2.3. Tahap 3: Pemeliharaan Risiko
Proses perumusan rencana tindak lanjut hasil identifikasi risiko dan pemantauan pelaksanaan mitigasi risiko.
- 2.4. Tahap 4: Monitoring Risiko
Proses monitoring kesesuaian pendekatan manajemen risiko yang diterapkan organisasi terhadap kondisi aktual dan efektivitas kontrol – kontrol yang diterapkan secara berkala

	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

3. ORGANISASI MANAJEMEN RISIKO

Struktur tanggung jawab dalam fungsi manajemen risiko dapat dilihat seperti pada gambar 2 berikut.



Gambar 2. Struktur Tanggung Jawab Pemantauan dan Pelaporan Risiko Layanan Dinas Komunikasi dan Informatika Kabupaten Sleman

Secara umum, tanggung jawab dalam proses manajemen risiko di Dinas Komunikasi dan Informatika Kabupaten Sleman adalah sebagai berikut.

- 3.1. Kepala Dinas Komunikasi dan Informatika Kabupaten Sleman sebagai Penanggung Jawab Risiko (*Risk Owner*) dari lingkup proses manajemen risiko di Dinas Komunikasi dan Informatika Kabupaten Sleman mempunyai tanggung jawab:
 - a. Memonitor pelaksanaan proses manajemen risiko.
 - b. Memastikan sumber daya yang diperlukan dalam proses manajemen risiko.
- 3.2. *Risk Coordinator* di Dinas Komunikasi dan Informatika Kabupaten Sleman mempunyai tanggung jawab:
 - a. Meninjau terhadap profil risiko khususnya pada masing-masing unit untuk memastikan rencana pengendalian sudah dibuat.
 - b. Memastikan kontrol yang diperlukan dalam meminimalkan risiko yang teridentifikasi.
 - c. Mengidentifikasi, menganalisis, dan mengevaluasi risiko dan memastikan tindakan pengendalian yang tepat di masing-masing unit.

	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

- d. Melaporkan hasil evaluasi risiko terkait dengan nilai risiko yang telah dievaluasi dan di-review serta menentukan rencana tindakan pengendalian yang diperlukan.
- e. Memastikan proses Manajemen Risiko TI dilaksanakan sesuai jadwal pelaksanaan secara periodik berdasarkan masing-masing tugas dan tanggung jawabnya.

- 3.3. Pegawai Dinas Komunikasi dan Informatika Kabupaten Sleman mempunyai tanggung jawab untuk:
- a. Mengidentifikasi risiko yang terdapat dalam bagiannya dan melaporkan kepada *Risk Coordinator* untuk dapat ditangani.
 - b. Mengelola risiko termasuk mengendalikan risiko tersebut berdasarkan rencana pengendalian yang telah ditetapkan.

4. IDENTIFIKASI RISIKO

Proses identifikasi risiko dilakukan dengan menganalisa sumber ancaman dan kerawanan yang dapat terjadi terhadap setiap aset kritikal berdasarkan metodologi yang digunakan. Selain itu, perlu dipastikan bahwa penilaian risiko yang dilakukan secara berulang dapat menghasilkan hasil yang konsisten, valid, dan dapat diperbandingkan.

5. PENILAIAN RISIKO

Tujuan dari penilaian risiko adalah untuk menghitung nilai risiko bawaan yang didapat dari hasil perkalian nilai dampak (*impact*) dan kemungkinan (*likelihood*). Nilai dampak dari sebuah risiko didefinisikan dari tabel berikut:

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

Level Dampak	Operasional dan Aset TIK	Peraturan / Hukum	Aset Informasi (khusus keamanan informasi)	Reputasi	Sumber Daya Manusia	Finansial	Layanan Organisasi	Kinerja
Tidak Signifikan (1)	Penundaan proses < 30 menit	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan aset informasi.	Tidak ada dampak terhadap reputasi institusi	Tidak memerlukan tambahan SDM	Tidak ada kerugian finansial	Tidak ada pengguna layanan yang terdampak	Tidak ada deviasi terhadap target uptime
Kurang Signifikan (2)	Penundaan proses 30 - 60 menit	Pelanggaran ringan dengan Teguran lisan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat PUBLIK.	Mengganggu kepercayaan sebagian kecil pihak eksternal bidang. Berdampak pada reputasi institusi namun reputasi dapat dipulihkan dalam waktu tidak terlalu lama.	Memerlukan kerjasama dengan kelompok substansi	Kerugian finansial dengan nilai < 5% dari anggaran tahunan atau kerugian terkait aset dengan nilai 5% dari total nilai aset yang dikelola	Layanan yang terdampak bukan layanan kritikal	Deviasi terhadap target uptime < 5%
Cukup Signifikan (3)	Penundaan proses 60 - 180 menit	Pelanggaran sedang yang dikenakan Surat peringatan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat TERBATAS.	Mengganggu kepercayaan sebagian besar pihak eksternal bidang. Berdampak pada reputasi institusi dan pemulihan reputasi membutuhkan waktu yang lama.	Memerlukan kerjasama dengan SDM dari bidang lain	Kerugian finansial dengan nilai 5% - 10 % dari anggaran tahunan atau kerugian terkait aset dengan nilai 5% - 10 % dari	Sudah ada layanan kritikal yang terdampak sebesar < 15% dari total layanan kritikal	Deviasi terhadap target uptime 5% - 10%

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

						total nilai aset yang dikelola		
Signifikan (4)	Penundaan proses dari 180 - 300 menit	Pelanggaran berat dengan sanksi hukum internal	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA.	Mengganggu kepercayaan sebagian besar pihak eksternal OPD, Berdampak pada reputasi institusi dan pemulihan reputasi membutuhkan waktu yang lama.	Memerlukan kerjasama dengan SDM seluruh Dinas Komunikasi dan Informatika Kabupaten Sleman	Kerugian finansial dengan nilai 10% - 15% dari anggaran tahunan atau kerugian terkait aset dengan nilai 10% - 15% dari total nilai aset yang dikelola	Sudah ada layanan kritikal yang terdampak sebesar 15% - 50% dari total layanan kritikal	Deviasi terhadap target uptime 10% - 15%
Sangat Signifikan (5)	Penundaan proses lebih dari 300 menit	Pelanggaran berat dengan sanksi hukum dan peraturan perundang undangan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat SANGAT RAHASIA.	Mengganggu kepercayaan pihak eksternal masyarakat, Berdampak pada reputasi institusi dan sangat sulit dilakukan pemulihan reputasi.	Memerlukan SDM dari eksternal	Kerugian finansial dengan nilai > 15% dari anggaran tahunan atau kerugian terkait aset dengan nilai > 15% dari total nilai aset yang dikelola	Sudah ada layanan kritikal yang terdampak > 50% dari total layanan kritikal	Deviasi terhadap target uptime > 15%

Tabel 1. Kriteria Risiko

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

Nilai	Tingkat	Kriteria Kecenderungan
		Frekuensi terjadinya
1	Hampir Tidak Terjadi	terjadi 1 kali dalam setahun
2	Jarang Terjadi	terjadi antara 2 – 5 kali dalam setahun
3	Kadang – kadang Terjadi	terjadi antara 6 – 9 kali dalam setahun
4	Sering Terjadi	terjadi antara 10 – 12 kali dalam setahun
5	Hampir Pasti Terjadi	terjadi lebih dari 12 kali dalam setahun

Tabel 2. Penilaian Risiko – Kriteria Kecenderungan

NILAI KEMUNGKINAN	Hampir Pasti Terjadi	5	9	15	18	23	25
	Sering Terjadi	4	6	12	16	19	24
	Kadang-Kadang terjadi	3	4	10	14	17	22
	Jarang Terjadi	2	2	7	11	13	21
	Hampir Tidak Terjadi	1	1	3	5	8	20
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan

NILAI DAMPAK

Tabel 3. Penilaian – Matriks Risiko

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

Level Risiko		Nilai Risiko	Keterangan Warna
1	Sangat Rendah	1 – 5	Biru
2	Rendah	6 – 10	Hijau
3	Sedang	11 – 15	Kuning
4	Tinggi	16 – 20	Jingga
5	Sangat Tinggi	21 – 25	Merah

Tabel 4. Kriteria Penilaian Risiko

5.1. Pengelolaan Risiko

Setelah penilaian risiko dilakukan maka kita akan mendapatkan nilai risiko bawaan (*inherent risk*) yang merupakan perkalian dari dampak dan kemungkinan. Selanjutnya kita menentukan penerimaan risiko dari kriteria risiko yang kita buat untuk menentukan keputusan selanjutnya yakni untuk melakukan mitigasi atau menerima risiko tersebut apa adanya berikut dengan prioritas penanganannya.

Risiko dengan klasifikasi tinggi dan menengah harus dikendalikan untuk memitigasi terjadinya risiko tersebut di masa datang atau mengurangi dampak yang terjadi. Pengendalian risiko akan merujuk pada kontrol ISO/IEC 27001:2022 Annex A. Pemilik risiko harus senantiasa memastikan bahwa pengendalian risiko yang dilakukan sudah memadai sehingga risiko yang tersisa (*residual risk*) dapat diterima, berikut adalah tabel klasifikasi risiko.

Klasifikasi Risiko	Keputusan Risiko	Due Date
Sangat Rendah	Terima	N/A
Rendah	Terima	N/A
Sedang	Mitigasi	12 bulan
Tinggi	Mitigasi	6 bulan
Sangat Tinggi	Mitigasi	3 bulan

Tabel 5. Klasifikasi Risiko

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

Selanjutnya perlu dilakukan pemantauan risiko secara berkala dengan memperhatikan beberapa faktor yang mungkin berkontribusi pada perubahan profil risiko yakni:

- a. Perubahan pada proses bisnis
- b. Perubahan ekosistem industri secara luas
- c. Kerentanan baru yang mungkin timbul sebagai akibat pengendalian risiko sebelumnya;
- d. Ancaman baru baik yang berasal dari dalam maupun dari luar yang belum dikenali sebelumnya;
- e. Terjadinya insiden keamanan informasi.

Oleh karena itu, proses pengenalan risiko hendaknya dilakukan secara berkala minimum satu kali dalam satu tahun atau setiap ada perubahan besar dalam bisnis. Seluruh proses penilaian risiko pada sistem manajemen keamanan informasi harus dikomunikasikan kepada para pemangku kepentingan. Metode, proses, dan hasil manajemen risiko harus tersedia dalam informasi terdokumentasi.

5.2. Penentuan Rencana Penanganan Risiko, PIC, Target Waktu

- Langkah-langkah yang harus dilakukan pada penentuan rencana penanganan risiko adalah:
- a. Menyusun rencana tindak lanjut untuk mengurangi nilai risiko.
 - b. Menetapkan pegawai/staff yang bertanggung jawab dalam tenggat waktu pelaksanaan penanganan risiko tersebut.

Rencana penanganan risiko dapat berupa penentuan kebijakan, prosedur dan pedoman, pengadaan teknologi, pengadaan sumber daya, dan pelaksanaan proses dideskripsikan dalam dokumen kebijakan, prosedur dan pedoman. Rencana penanganan harus *feasible* dan *cost-effective*, membandingkan keuntungan dan biaya dari implementasi rencana penanganan (*benefit-cost analysis*).

5.3. Pembuatan Jadwal Detail Rencana Penanganan Risiko

- Berdasarkan hasil rencana pengendalian risiko, dapat dibuat jadwal detail implementasi kontrol yang telah ditentukan pada rencana pengendalian risiko. Implementasi kontrol tersebut dapat dilakukan secara bertahap dimana perlu dideskripsikan:
- a. waktu implementasi kontrol;
 - b. aktivitas detail dalam implementasi kontrol termasuk penyediaan sumber daya untuk mendukung terlaksananya aktivitas tersebut;
 - c. pegawai/staff yang bertanggung jawab dalam implementasi kontrol

Hasil dari finalisasi *risk assessment* dan *risk treatment plan* harus disetujui oleh pemilik risiko. Status progress dari pelaksanaan RTP harus dimonitor dan dicatat secara berkelanjutan.

 DISKOMINFO SLEMAN	PROSEDUR PENGELOLAAN MANAJEMEN RISIKO	No.Dok : T/P.001/SMKI/2025
		Tanggal : 5 Mei 2025
		Rev. : 1.0

6. PEMANTAUAN RISIKO

Proses manajemen risiko SMKI harus terus menerus dimonitor dan dievaluasi untuk memastikan bahwa proses pengamanan informasi masih sejalan dengan strategi dan sasaran perusahaan. Proses monitoring dan evaluasi ini dilakukan secara berkala. Frekuensi pelaporan aktivitas manajemen risiko SMKI di Dinas Komunikasi dan Informatika Kabupaten Sleman mengacu pada tabel berikut:

Level	Review Risk Register (Monitoring)	Pelaporan Risiko
Koordinator Risiko	1 kali dalam setahun	Setiap Tahun

Tabel 6. Frekuensi Pelaporan dan Monitoring terhadap Risiko

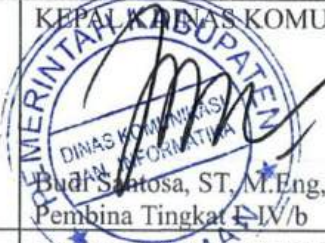
Hasil dari pelaksanaan manajemen risiko yang dilaporkan kepada Kepala Dinas Komunikasi dan Informatika Kabupaten Sleman sebagai tindak lanjut proses pengendalian risiko, dalam bentuk laporan Profil Risiko. Profil Risiko ini menggambarkan proses identifikasi dan analisa risiko serta rencana tindakan penanganan risiko. Bagian-bagian yang terdapat dalam laporan Profil Risiko meliputi:

- a. Proses pelaksanaan *risk assessment*
- b. Identifikasi risiko pada Dinas Komunikasi dan Informatika Kabupaten Sleman.
- c. Evaluasi dan analisis risiko
- d. *Risk Acceptance* yang terdapat pada registrasi risiko Dinas Komunikasi dan Informatika Kabupaten Sleman.
- e. Rencana penanganan risiko

Proses manajemen risiko dalam kegiatan *review risk assessment* harus dievaluasi secara berkala, yaitu satu tahun sekali oleh seluruh pegawai Dinas Komunikasi dan Informatika Kabupaten Sleman. Pengkajian ulang proses *risk assessment* juga dilakukan apabila terjadi perubahan pada:

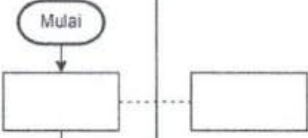
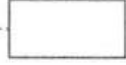
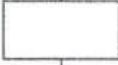
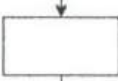
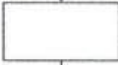
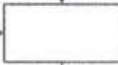
- a. Organisasi
- b. Teknologi
- c. Objektif dan proses bisnis
- d. Ancaman yang teridentifikasi
- e. Efektivitas dari kontrol yang telah diimplementasikan
- f. Kejadian eksternal, seperti perubahan dari lingkungan hukum dan peraturan, perubahan obligasi kontraktual, dan perubahan dari lingkungan sosial.

Bentuk *monitoring* terhadap pelaksanaan pengendalian risiko yang dilaksanakan berdasarkan progress status yang dilakukan dalam melaksanakan kontrol yang telah ditetapkan.

	PEMERINTAH KABUPATEN SLEMAN DINAS KOMUNIKASI DAN INFORMATIKA Jalan Parasamya, Beran, Tridadi, Sleman, Yogyakarta, 55511 Telepon (0274) 868405, Faksimile (0274) 868945 Laman: kominfo.slemankab.go.id, Surel: kominfo@slemankab.go.id	Nomor SOP	T/P.001/SMKI/2025
		Klasifikasi	Terbatas
		Tanggal Pembuatan	5 Mei 2025
		Versi Dokumen	2.0
		Tanggal Revisi	4 Juni 2026
		Tanggal Efektif	4 Juni 2026
		Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA  Budhi Santosa, ST, M.Eng, M.Eng Pembina Tingkat IV/b
		Nama SOP	PROSEDUR MANAJEMEN RISIKO

Dasar Hukum :	Kualifikasi Pelaksana :
1. ISO 31000 – Manajemen Risiko 2. ISO/IEC 27001:2022, C.6.1 – Tindakan Untuk Menangani Risiko dan Peluang 3. ISO/IEC 27001:2022, C.8.2 – Penilaian Risiko Keamanan Informasi 4. ISO/IEC 27001:2022, C.8.3 – Penanganan Risiko Keamanan Informasi	1. Memahami manajemen risiko beserta dengan proses dan kegiatan terkait yang dijabarkan pada dokumen ini dan pada tabel risiko. 2. Mengkoordinasikan, memantau serta mendokumentasikan seluruh proses yang terkait dengan manajemen risiko. 3. Mampu memastikan proses pengkinian dan pengelolaan dari dokumen dan tabel risiko. 4. Mampu mendokumentasikan setiap perubahan dan hasil tinjauan perubahan.
Keterkaitan SOP :	Peralatan/Perlengkapan :
1. Kebijakan Keamanan Informasi 2. Kebijakan Umum Sistem Manajemen Keamanan Informasi 3. Tabel Risiko	1. Komputer PC/Laptop 2. ATK 3. Catatan/Note
Peringatan :	Pencatatan dan Pendataan :
1. Apabila prosedur ini dilaksanakan dapat menjadi panduan proses perubahan pada sistem pengelolaan informasi dan bagian-bagian terkait dengan perubahan yang terjadi, sehingga proses perubahan tidak mempengaruhi sistem informasi di organisasi secara luas. 2. Apabila prosedur ini tidak dijalankan, maka tidak adanya prosedur yang baku apabila adanya perubahan pada proses pengelolaan informasi.	1. Mencatat secara detail pengukuran dan evaluasi implementasi

A. Prosedur Manajemen Risiko

No	Aktivitas	Pelaksana		Mutu Baku			Ket
		Risk Owner	Koordinator Manajemen Risiko	Persyaratan/ Kelengkapan	Waktu	Output	
1	Penerapan Konteks			1. Ruang lingkup 2. kriteria risiko 3. proses bisnis	1 Hari	Konteks manajemen risiko	
2	Menentukan identifikasi risiko			1. Tabel risiko 2. data aset/proses	1 Hari	Daftar risiko	
3	Menetapkan nilai dan level inherent risk berdasarkan analisis dampak & kecenderungan			1. Tabel risiko 2. analisis dampak & kemungkinan	1 Hari	Nilai inherent risk	
4	Merencanakan dan implementasi risk control			1. Daftar risiko 2. rencana pengendalian	1 Hari	Pengendalian risiko diterapkan	
5	Evaluasi tindakan pengendalian risiko			1. Tabel risiko 2. hasil pengendalian	Sesuai dengan SLA	Hasil evaluasi pengendalian	
6	Evaluasi nilai dan level residual risk berdasarkan hasil pengendalian risiko terhadap aspek dampak dan kecenderungan			1. Tabel risiko 2. hasil evaluasi pengendalian	Sesuai dengan SLA	Nilai residual risk	
7	Menjalankan dan implementasi risk treatment			1. Tabel risiko 2. rencana treatment	Sesuai dengan SLA	Risk treatment diterapkan	
8	Evaluasi nilai dan level residual risk berdasarkan hasil treatment terhadap aspek dampak dan kecenderungan			1. Tabel risiko 2. hasil treatment	Sesuai dengan SLA	Nilai residual risk akhir	

B. Prosedur Manajemen Risiko

No	Tanggal	No Revisi	Bagian yang Direvisi
1	5 Mei 2025	1.0	Dokumen Pertama Kali Terbit
2	4 Juni 2026	2.0	Perubahan Format Standar Operasional Prosedur Administrasi Pemerintahan