PEMERINTAH KABUPATEN PESISIR SELATAN
DINAS KOMUNIKASI DAN INFORMATIKA
Jln. Dr. M. Hatta Painan, Kabupaten Pesisir Selatan, Sumatera barat 25613
Telepon (0756) 231 2227
Laman https://diskominfo.pesisirselatankab.go.id, Pos-el : Kominfo@pesisirselatankab.go.id

KEPUTUSAN

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN PESISIR SELATAN
NOMOR : 500.12/25/KOMINFO/2026

TENTANG

PANDUAN UMUM MANAJEMEN RISIKO KEAMANAN INFORMASI PEMERINTAH KABUPATEN PESISIR SELATAN

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN PESISIR SELATAN,

Menimbang

a. bahwa dalam rangka mengamankan aset informasi dan menjamin keberlangsungan layanan sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Pesisir Selatan, perlu diterapkan manajemen risiko keamanan siber secara terstruktur;

b. bahwa untuk memberikan arah dan pedoman yang jelas dalam pelaksanaan pengamanan aset dan mitigasi risiko, diperlukan sebuah dokumen panduan umum mengenai manajemen risiko keamanan siber;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan tentang Panduan Umum Manajemen Risiko Keamanan Siber Pemerintah Kabupaten Pesisir Selatan;

Mengingat

1. Undang-Undang Nomor 12 Tahun 1956 tentang Pembentukan Daerah Otonom Kabupaten Dalam Lingkungan Daerah Propinsi Sumatera Tengah (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 25), sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 7 Tahun 1965 tentang Pembentukan Daerah Tingkat II Sarolangun- Bangko Dan Daerah Tingkat II Tanjung Jabung Dengan Mengubah Undang-Undang Nomor 12 Tahun 1956 tentang Pembentukan Daerah Otonom Kabupaten Di Propinsi Sumatera Tengah (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 50, Tambahan Lembaran Negara Republik Indonesia Nomor 2755);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587), sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

4. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
5. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215, Tambahan Lembaran Negara Republik Indonesia Nomor 5357);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik;
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Standar Teknis dan Prosedur Keamanan Keamanan Informasi;
9. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
10. Peraturan Daerah Kabupaten Pesisir Selatan Nomor 8 Tahun 2016 tentang Organisasi Perangkat Daerah Kabupaten Pesisir Selatan;
11. Peraturan Daerah Nomor 4 Tahun 2020 tentang Pengelolaan Sistem Pemerintahan Berbasis Elektronik;
12. Peraturan Daerah Nomor 9 Tahun 2025 tentang Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2026;
13. Peraturan Bupati Nomor 12 Tahun 2022 tentang Perubahan atas Peraturan Bupati Nomor 22 Tahun 2021 tentang Pelaksanaan Peraturan Daerah Kabupaten Pesisir Selatan Nomor 4 Tahun 2020 tentang Pengelolaan Sistem Pemerintahan Berbasis Elektronik;
14. Peraturan Bupati Nomor 9 Tahun 2026 tentang Perubahan Kedua Peraturan Bupati Nomor 51 Tahun 2025 tentang Penjabaran Anggaran Pendapatan dan Belanja Daerah Tahun 2026;

MEMUTUSKAN :

Menetapkan : KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN PESISIR SELATAN TENTANG PANDUAN UMUM MANAJEMEN RISIKO KEAMANAN INFORMASI PEMERINTAH KABUPATEN PESISIR SELATAN.

KESATU : Menetapkan Panduan Umum Manajemen Risiko Keamanan Informasi Pemerintah Kabupaten Pesisir Selatan sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Panduan Umum sebagaimana dimaksud pada Diktum KESATU menjadi acuan dan pedoman kerja bagi seluruh aparatur di lingkungan Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan dalam mengelola keamanan sistem informasi.

KETIGA : Keputusan ini mulai berlaku pada tanggal ditetapkan dengan ketentuan apabila di kemudian hari terdapat kekeliruan akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Painan
Pada tanggal 15 Juli 2026

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN PESISIR SELATAN

WENDI, S.H., M.Hum.
Pembina Utama Muda (IV/c)
NIP. 19760407 199803 1 005

LAMPIRAN
KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
NOMOR 500.12/25/KOMINFO/2026
TANGGAL 15 Juli 2026
TENTANG
PANDUAN UMUM MANAJEMEN RISIKO KEAMANAN INFORMASI PEMERINTAH KABUPATEN PESISIR SELATAN

PANDUAN UMUM MANAJEMEN RISIKO KEAMANAN SIBER PEMERINTAH KABUPATEN PESISIR SELATAN

1. TUJUAN DAN SASARAN

Proses Manajemen Risiko Keamanan Siber bertujuan untuk melindungi aset informasi dari ancaman siber, mengendalikan risiko organisasi terkait keamanan siber serta melaksanakan tindakan dalam rangka mengurangi risiko yang diterima dan kemungkinan dampaknya.

Sasaran dalam manajemen risiko di Pemerintah Kabupaten Pesisir Selatan adalah:

- Mengidentifikasi risiko keamanan siber yang mungkin mempengaruhi proses bisnis Pemerintah Kabupaten Pesisir Selatan.
- Melakukan analisis risiko, dampak dan kemungkinan terjadinya risiko keamanan siber di Pemerintah Kabupaten Pesisir Selatan.
- Merencanakan pengendalian risiko yang dibutuhkan dalam rangka melakukan tindakan untuk menangani dan mengeliminasi risiko di Pemerintah Kabupaten Pesisir Selatan.
- Peningkatan efektivitas dan pelaksanaan Manajemen Risiko yang berkelanjutan di Pemerintah Kabupaten Pesisir Selatan.

Pedoman ini memberikan petunjuk mengenai pengelolaan manajemen risiko di Pemerintah Kabupaten Pesisir Selatan dalam menganalisa dan mengontrol risiko yang teridentifikasi terkait dengan pengelolaan sistem informasi sebagai pendukung proses bisnis utama. Selanjutnya pedoman ini juga dijadikan acuan dalam menentukan kontrol pengamanan yang akan dilakukan Pemerintah Kabupaten Pesisir Selatan untuk mengurangi dampak dan kemungkinan risiko terkait sistem informasi dan proses pendukung pengelolaan informasi di Pemerintah Kabupaten Pesisir Selatan.

1.1. Ruang Lingkup

Kebijakan ini berlaku untuk seluruh aset teknologi informasi dan sarana pendukungnya yang digunakan dalam seluruh penyelenggaraan layanan keamanan informasi di lingkungan Pemerintah Kabupaten Pesisir Selatan.

1.2. Referensi

- Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik

- Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Standar Teknis dan Prosedur Keamanan Informasi.

1.3. Definisi

- Aset : Segala sesuatu milik Pemerintah Kabupaten Pesisir Selatan yang bernilai dan perlu dilindungi dari ancaman, meliputi perangkat keras, perangkat lunak, peralatan kantor, data, serta SDM
- Risiko : Efek dari ketidakpastian pada sasaran
- Manajemen Risiko : Aktivitas terkoordinasi untuk mengarahkan dan mengendalikan organisasi dalam kaitannya dengan risiko
- Pemangku Kepentingan : Orang atau organisasi yang dapat memengaruhi atau dipengaruhi atau menganggap dirinya dipengaruhi oleh suatu keputusan atau aktivitas
- Sumber risiko : Elemen yang secara mandiri atau dalam kombinasi memiliki potensi atau menimbulkan risiko
- Peristiwa : Kejadian atau perubahan suatu set dari kondisi
- Konsekuensi : Hasil keluaran suatu peristiwa yang memengaruhi sasaran
- Kemungkinan kejadian : Kemungkinan terjadinya sesuatu
- Pengendalian : Tindakan yang memelihara dan/atau memodifikasi risiko

1.4. Klasifikasi Aset

Aset berupa Data dan Informasi, Perangkat Lunak, Perangkat Keras, dan Sarana Pendukung.

a. Klasifikasi Aset Data dan Informasi

   Klasifikasi Aset Data dan Informasi terbagi menjadi 3 (tiga) kategori, antara lain:

   - Rahasia : Dokumen yang sangat sensitif dan hanya dapat diakses oleh pihak yang berwenang, contohnya: Laporan Monitoring, Laporan Insiden Siber, Laporan Pengembangan Aplikasi atau Dokumen Topologi Jaringan.
   - Terbatas : Dokumen yang hanya dapat diakses oleh pegawai internal organisasi, contohnya: Laporan Penanganan Insiden.
   - Publik : Dokumen yang dapat diakses oleh umum di luar lingkungan organisasi, contohnya: Kebijakan SMKI, Panduan Umum Manajemen Risiko Keamanan Informasi.

b. Klasifikasi Perangkat Lunak

   Klasifikasi Perangkat Lunak dikategorikan antara lain; Sistem Elektronik dengan kategori Strategis, Tinggi, dan Rendah

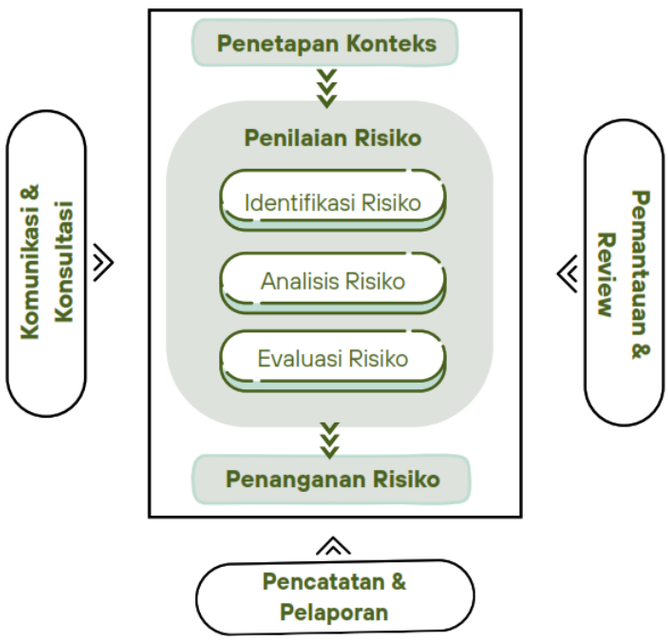
c. Klasifikasi Perangkat Keras dan Sarana Pendukung

   Klasifikasi Perangkat Keras dan Sarana Pendukung dikategorikan, antara lain; Kritikal dan Tidak Kritikal

2. KONSEP MANAJEMEN RISIKO KEAMANAN INFORMASI

Manajemen risiko merupakan proses pengelolaan yang berkesinambungan, mulai dari penetapan ruang lingkup sampai penanganan risiko. Proses ini penting untuk mengidentifikasi, mengevaluasi, dan mengelola risiko terkait dengan keamanan informasi dengan tujuan untuk melindungi aset informasi Pemerintah Kabupaten Pesisir Selatan.

Pelaksanaan Manajemen Risiko Keamanan Siber Pemerintah Kabupaten Pesisir Selatan meliputi beberapa siklus dan tahapan seperti pada Gambar 1 di bawah ini:



Gambar 1 Proses Manajemen Risiko

Secara garis besar, pelaksanaan proses manajemen risiko terbagi menjadi 8 (delapan) tahap yaitu :

- Tahap 1: Komunikasi dan Konsultasi

  Proses berkesinambungan untuk menciptakan dialog dengan para pemangku kepentingan guna meningkatkan kesadaran dan pemahaman mengenai risiko Keamanan Informasi serta mendapatkan umpan balik dan informasi dalam rangka sebagai dukungan dalam pengambilan keputusan.

- Tahap 2: Penetapan Konteks

  Pada proses ini Pemerintah Kabupaten Pesisir Selatan akan melakukan identifikasi parameter dasar dan ruang lingkup penerapan Manajemen Risiko Keamanan Informasi.

- Tahap 3: Identifikasi Risiko

  Proses mengenali seluruh ancaman dan kerentanan pada aset
  Pemerintah Kabupaten Pesisir Selatan serta dampak yang akan mempengaruhi kerahasiaan, integritas dan ketersediaan layanan keamanan informasi.

- Tahap 4: Analisis Risiko

  Proses penilaian potensi dampak dan kemungkinan terjadinya risiko yang sudah diidentifikasi sebelumnya, sehingga dapat terlihat tingkat keparahan risiko atas aset Pemerintah Kabupaten Pesisir Selatan.

- Tahap 5: Evaluasi Risiko

  Proses penentuan tindakan mitigasi risiko yang akan dilakukan terhadap risiko yang telah dianalisis, sehingga Pemerintah Kabupaten Pesisir Selatan dapat menentukan prioritas dalam melakukan pengelolaan risiko.

- Tahap 6: Penanganan Risiko

  Proses pelaksanaan langkah-langkah penanganan sesuai dengan hasil evaluasi risiko untuk menekan risiko yang terkait dengan keamanan informasi Pemerintah Kabupaten Pesisir Selatan.

- Tahap 7: Pemantauan dan Reviu

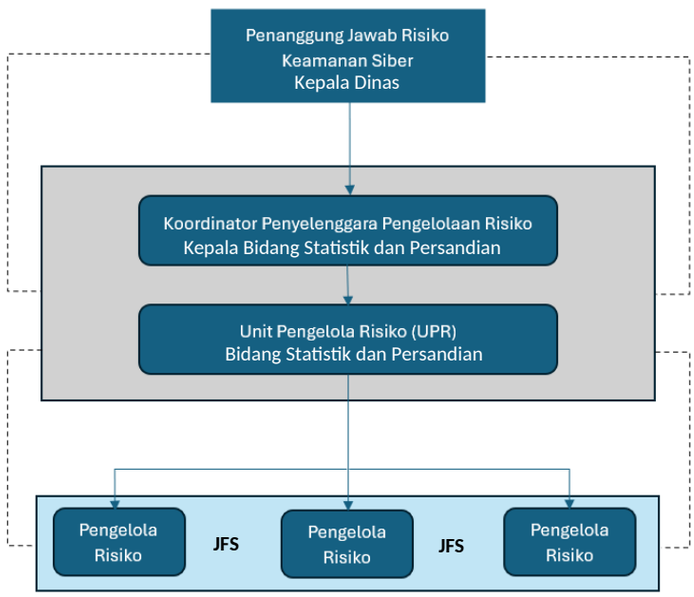
  Proses pemantauan faktor-faktor atau penyebab yang memengaruhi risiko Keamanan Informasi, pelaksanaan rencana aksi penanganan risiko Keamanan Informasi serta mengontrol kesesuaian dan ketepatan proses Manajemen Risiko Keamanan Informasi. Proses ini dilakukan Pemerintah Kabupaten Pesisir Selatan secara berkala dan hasilnya dapat dijadikan dasar dalam melakukan penyesuaian kembali proses Manajemen Risiko Keamanan Informasi.

- Tahap 8: Pencatatan dan Pelaporan

  Proses pendokumentasian akvitas dan penyampaian hal-hal yang berhubungan dengan hasil proses Manajemen Risiko Keamanan Informasi di lingkungan Pemerintah Kabupaten Pesisir Selatan dalam kurun waktu tertentu.

3. ORGANISASI MANAJEMEN RISIKO

Struktur tanggung jawab dalam fungsi manajemen risiko dapat dilihat seperti pada Gambar 2. Struktur Organisasi Manajemen Risiko Keamanan Siber.



Gambar 2 Struktur Organisasi Manajemen Risiko Keamanan Siber

Secara umum, tanggung jawab dalam proses manajemen risiko keamanan siber di Pemerintah Kabupaten Pesisir Selatan adalah sebagai berikut.

- Penanggung Jawab Risiko dari lingkup proses manajemen risiko keamanan siber mempunyai tanggung jawab:
  - Penetapan kerangka kerja dan pedoman pelaksanaan manajemen risiko keamanan siber.
  - Memonitor pelaksanaan proses manajemen risiko.
  - Memastikan pemenuhan sumber daya yang diperlukan dalam proses manajemen risiko.
  - Menentukan selera risiko Keamanan Informasi di Pemerintah Kabupaten Pesisir Selatan.
  - Pelaksanaan komitmen pimpinan dan penerapan budaya sadar Risiko Keamanan Informasi

- Koordinator Penyelenggara Pengelolaan Risiko mempunyai tanggung jawab:
  - Meninjau terhadap profil risiko khususnya pada masing-masing unit untuk memastikan rencana pengendalian sudah dibuat.
  - Memastikan kontrol yang diperlukan dalam meminimalkan risiko yang teridentifikasi.
  - Mengidentifikasi, menganalisis, dan mengevaluasi risiko dan memastikan tindakan pengendalian yang tepat di masing-masing unit.
  - Melaporkan hasil evaluasi risiko terkait dengan nilai risiko yang telah dievaluasi dan di-*review* serta menentukan rencana tindakan pengendalian yang diperlukan kepada Unit Pemilik Risiko (UPR)

- Unit Pemilik Risiko (UPR) mempunyai tanggung jawab:
  - Pelaksanaan pembinaan budaya sadar Risiko Keamanan Informasi melalui sosialisasi, bimbingan, pelatihan dan supervisi penerapan manajemen Risiko Keamanan Informasi.
  - Melaporkan hasil evaluasi risiko dan tindakan pengendalian kepada Sekretaris Utama Pemerintah Kabupaten Pesisir Selatan
  - Memastikan proses Manajemen Risiko TI dilaksanakan sesuai jadwal pelaksanaan secara periodik berdasarkan masing-masing tugas dan tanggung jawabnya
  - Penyusunan dan penetapan penilaian risiko Keamanan Informasi dan rencana pelaksanaan Manajemen Risiko Keamanan Informasi termasuk

- Pengelola Risiko mempunyai tanggung jawab untuk:
  - Mengidentifikasi risiko yang terdapat dalam bagiannya dan melaporkan kepada Koordinator Risiko untuk dapat ditangani.
  - Mengelola risiko termasuk mengendalikan risiko tersebut berdasarkan rencana pengendalian yang telah ditetapkan.

4. KONTEKS MANAJEMEN RISIKO Pemerintah Kabupaten Pesisir Selatan

Dalam hal penetapan konteks, Pemerintah Kabupaten Pesisir Selatan melakukan penetapan konteks terkait informasi organisasi sampai selera risiko manajemen keamanan informasi.

4.1. Penetapan Kategori Risiko

Penetapan kategori risiko bertujuan untuk menjamin agar proses identifikasi, analisis, dan evaluasi risiko dilakukan secara komprehensif. Contoh kategori Risiko Keamanan Informasi Pemerintah Kabupaten Pesisir Selatan dapat dilihat pada Tabel 1 Kategori Risiko

Tabel 1 Kategori Risiko

No	Jenis Risiko	Keterangan
1	Infrastruktur	Risiko yang berkaitan dengan pusat data, jaringan intra pemerintah, dan sistem penghubung layanan termasuk perangkat keras, perangkat lunak, dan fasilitas penunjang utama
2	Bencana Alam	Risiko yang berkaitan dengan peristiwa yang disebabkan oleh alam
3	Sumber Daya Manusia (SDM)	Sumber Daya Manusia (SDM)Risiko yang berkaitan dengan kelalaian, kurangnya kompetensi, ketidaksengajaan, atau tindakan penyalahgunaan wewenang oleh pegawai/pihak yang memiliki akses ke sistem.
4	Serangan Siber (Logik)	Risiko yang berkaitan dengan ancaman digital dari pihak luar maupun dalam seperti peretasan (*hacking*), infeksi *malware/ransomware*, pencurian data, dan gangguan layanan.
5	Kepatuhan dan Hukum	Risiko yang berkaitan dengan pelanggaran terhadap peraturan perundang-undangan (misalnya UU ITE atau Pelindungan Data Pribadi), kebijakan internal, atau standar operasional yang berlaku.

4.2. Area Dampak

Penetapan Area Dampak Risiko bertujuan untuk mengetahui area lingkungan Pemerintah Kabupaten Pesisir Selatan yang terdampak oleh Risiko. Penetapan area diawali dengan melakukan identifikasi dampak Risiko. Contoh Area Dampak dapat dilihat pada Tabel 2 berikut:

Tabel 2 Area Dampak

No	Area Dampak	Keterangan
1	Layanan	Area yang berkaitan dengan pemenuhan

	Organisasi	kebutuhan atau jasa kepada *stakeholder*
2	Operasional dan Aset TIK	Area yang berkaitan dengan kegiatan operasional TIK dan pengelolaan aset TIK
3	Reputasi	Area yang berkaitan dengan menurunnya tingkat kepercayaan publik, opini negatif, atau memburuknya citra instansi di mata stakeholder.
4	Kinerja	Area yang berkaitan dengan kegagalan pencapaian target, sasaran strategis, program, atau kegiatan utama instansi yang telah ditetapkan.
5	SDM	Area yang berkaitan dengan keselamatan jiwa, kesehatan, kecelakaan kerja, atau terganggunya moral dan produktivitas pegawai.
6	Hukum dan Regulasi	Area yang berkaitan dengan tuntutan hukum (pidana/perdata), sanksi administratif, dan tingkat kepatuhan terhadap peraturan perundang-undangan yang berlaku.
7	Finansial	Area yang berkaitan dengan potensi kerugian keuangan negara/daerah, pemborosan anggaran, kehilangan aset, atau denda finansial.

4.3. Kriteria Risiko Keamanan Informasi Pemerintah Kabupaten Pesisir Selatan

Penetapan kriteria risiko Keamanan Informasi di lingkungan Pemerintah Kabupaten Pesisir Selatan merupakan langkah penting dalam proses siklus manajemen risiko yang bertujuan untuk membantu Pemerintah Kabupaten Pesisir Selatan dalam mengidentifikasi, mengukur, dan mengelola risiko yang muncul agar lebih efektif. Kriteria risiko ini ditinjau secara berkala dan perlu dilakukan evaluasi serta penyesuaian dengan perubahan yang terjadi. Dalam penetapan kriteria risiko Keamanan Informasi ini terdiri dari:

4.3.1. Kriteria Kemungkinan

Kriteria kemungkinan risiko Keamanan Informasi di lingkungan Pemerintah Kabupaten Pesisir Selatan dilakukan berdasarkan penetapan level kemungkinan dan penetapan kriteria dari setiap level kemungkinan terhadap risiko keamanan siber. Dalam penentuan level kemungkinan dibagi menjadi 5 (lima) tingkatan sesuai dengan Tabel berikut

Tabel 3 Kriteria Kemungkinan

Kemungkinan		Probabilitas dalam 1 (satu) Periode	
1	Hampir Tidak Terjadi	x <= 5%	< 2 kali dalam 1 tahun
2	Jarang Terjadi	5% < x <= 10%	2-5 kali dalam 1 tahun
3	Kadang-Kadang Terjadi	10% < x <= 20%	6-9 kali dalam 1 tahun
4	Sering Terjadi	20% < x <= 50%	10-12 kali dalam 1 tahun
5	Hampir Pasti Terjadi	x > 50%	> 12 kali dalam 1 tahun

Berdasarkan Tabel 2 di ,atas dari level kemungkinan ditetapkan pendekatan terjadinya dalam periode tertentu dengan pendekatan persentase probabilitas statistik dan jumlah frekuensi terjadinya risiko dalam satuan waktu.

4.3.2. Kriteria Dampak

Penetapan kriteria dampak risiko keamanan siber di lingkungan Pemerintah Kabupaten Pesisir Selatan dilakukan dengan kombinasi antara area dampak risiko Keamanan Informasi dan level dampak. Pengukuran dampak merupakan pengukuran terhadap seberapa besar dampak yang ditimbulkan oleh sebuah risiko apabila risiko tersebut terjadi (tereksploitasi). Untuk level dampak dilingkungan Pemerintah Kabupaten Pesisir Selatan ditetapkan dalam 5 (lima) tingkatan. Pelaksanaan analisa dampak ini mengacu pada tujuan pengamanan terhadap aset yang berkaitan dengan proses bisnis dan akibat yang ditimbulkan berdasarkan kerugian dari aspek kerahasiaan, ketersediaan dan integritas. analisa dampak yang digunakan oleh Pemerintah Kabupaten Pesisir Selatan dapat dilihat pada Tabel 3 berikut.

Tabel 4 Kriteria Dampak

No	Dampak	Finansial	Reputasi	Kinerja	Layanan Organisasi	Operasional TIK	Hukum dan Regulasi
1	Tidak Signifikan	Jumlah kerugian negara ≤ Rp 10 juta	Keluhan stakeholder secara langsung lisan/ tertulis jumlahnya ≤ 3 kali dalam satu periode	Penurunan <20%	Business Process tertunda ≤ 1 hari	Gangguan kecil	Tidak ada pelanggaran hukum

No	Dampak	Finansial	Reputasi	Kinerja	Layanan Organisasi	Operasional TIK	Hukum dan Regulasi
2	Kurang Signifikan	Jumlah kerugian negara lebih dari Rp 10 juta s.d Rp 50 juta	Keluhan stakeholder secara langsung lisan/ tertulis ke organisasi jumlahnya lebih dari 3 kali dalam satu periode	Penurunan 20%<x<=40%	Business Process tertunda di atas 1 hari s.d. 5 hari	Gangguan sporadis	Pelanggaran ringan dengan teguran
3	Cukup Signifikan	Jumlah kerugian negara lebih dari Rp 50 juta s.d Rp 100 juta	Pemberitaan negatif di dalam media massa lokal	Penurunan 40%<x<=60%	Business Process tertunda di atas 5 hari s.d. 15 hari	Terhenti sementara	Pelanggaran ringan dengan surat peringatan
4	Signifikan	Jumlah kerugian negara lebih dari Rp 100 juta s.d Rp 500 juta	Pemberitaan negatif di dalam media massa nasional	Penurunan 60%<x<=80%	Business Process tertunda di atas 15 hari s.d. 30 hari	Terhenti lama	Pelanggaran sedang yang dikenakan sanksi administratif
5	Sangat Signifikan	Jumlah kerugian negara lebih Rp 500 juta	Pemberitaan negatif di dalam media massa internasional	Penurunan >80%	Business Process tertunda di atas 30 hari	Tidak berfungsi	Pelanggaran berat dengan sanksi hukum

4.4. Matriks Analisis dan Level Risiko Keamanan Informasi

Setelah tingkat kecenderungan dan dampak dari tiap risiko diidentifikasi, selanjutnya dilakukan penentuan nilai risiko dasar (*Inherent Risk*) maupun *Residual Risk.* Nilai risiko dasar adalah tingkatan risiko yang timbul apabila tidak adanya kontrol, kemudian *Residual Risk* merupakan risko yang tersisa yang masih ada setelah segala upaya dalam pengelolaan risiko telah diimplementasikan. *Residual risk* ini bukanlah hal yang buruk atau tidak diinginkan dalam suatu kondisi dalam pengelolaan risiko, biasanya terdapat beberapa pertimbangan saat *residual risk* muncul, seperti adanya keterbatasan sumber daya, keputusan pimpinan, risiko yang tidak terduga, dan juga perubahan lingkungan. Dalam konteks *Residual Risk* pada lingkungan Pemerintah Kabupaten Pesisir Selatan juga dilakukan penilaian untuk dapat dilihan kesimpulan atas sisa risiko tersebut diterima (*Acceptable*) atau tidak diterima (*Not Acceptable*). Jika simpulan dari *residual risk* tersebut adalah tidak diterima (*Not Acceptable*) maka perlu bagi Tim Keamanan Informasi dapat menetapkan rencana kontrol tambahan yang dapat kemudian menjadi pertimbangan dalam penyusunan program kerja Pemerintah Kabupaten Pesisir Selatan selanjutnya.

Nilai risiko diperoleh dari hasil perhitungan antara tingkat kemungkinan dan juga dampak dari risiko sebagai berikut ini.

Nilai Risiko = Kemungkinan × Dampak Kriteria nilai risiko

Matriks yang digunakan dalam melihat nilai risiko di lingkungan Pemerintah Kabupaten Pesisir Selatan seperti pada Tabel 5 berikut ini.

Tabel 5 Level Dampak

Matriks Analisis Risiko 5X5			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	1	Hampir Tidak Terjadi	1	3	5	8	20
	2	Jarang Terjadi	2	7	11	13	21
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	4	Sering Terjadi	6	12	16	19	24
	5	Hampir Pasti Terjadi	9	15	18	23	25

Kemudian besaran nilai risiko sebagai mana Tabel 5. Selanjutnya dikelompokkan ke dalam level risiko yang memiliki 5 rentang nilai besaran, yang mana dipetakan pada Tabel 6 berikut ini:

Tabel 6 Peta Level Risiko Keamanan Siber

Matriks Analisis Risiko 5X5			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	1	Hampir Tidak Terjadi	Sangat Rendah	Rendah	Sedang	Sedang	Tinggi
	2	Jarang Terjadi	Sangat Rendah	Rendah	Sedang	Sedang	Sangat Tinggi
	3	Kadang-Kadang Terjadi	Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
	4	Sering Terjadi	Rendah	Sedang	Tinggi	Tinggi	Sangat Tinggi
	5	Hampir Pasti Terjadi	Rendah	Sedang	Tinggi	Sangat Tinggi	Sangat Tinggi

Kemudian kriteria yang dijadikan rujukan dalam penentuan leveling risiko dapat dilihat pada Error: Reference source not found.

Tabel 7 Kriteria Pertimbangan Level Risiko

Level Risiko		Rentang Besaran Risiko	Keterangan Warna
1	Sangat Rendah	1-5	
2	Rendah	6-10	
3	Sedang	11-15	
4	Tinggi	16-20	
5	Sangat Tinggi	21-25	

4.5. Selera Risiko Keamanan Informasi

Selera risiko keamanan informasi digunakan sebagai acuan dalam penentuan ambang batas minimum terhadap Besaran Risiko yang harus ditangani untuk setiap kategori risiko. Besaran Risiko yang ditangani oleh Pemerintah Kabupaten Tanah Datar Adalah risiko dengan besaran lebih dari 10 atau Risiko yang berada pada level sedang.

5. IDENTIFIKASI RISIKO

5.1. Jenis Risiko

Jenis risiko secara umum dibedakan menjadi 2 (dua), yaitu Risiko Positif dan Risiko Negatif. Kedua jenis risiko ini dapat mempengaruhi dan berimplikasi pada proses bisnis atas pelaksanaan penerapan keamanan siber khususnya terkait keamanan informasi di lingkungan Pemerintah Kabupaten Pesisir Selatan. Penentuan dari jenis risiko ini adalah:

- **Risiko Positif** adalah risiko yang muncul sebagai “peluang risiko” dimana terdapat potensi kejadian atau perubahan yang dapat memberikan dampak positif bagi Pemerintah Kabupaten Pesisir Selatan atau bagi proyek/kinerja yang sedang berlangsung. Misalnya peluang untuk adanya inovasi baru atas risiko yang muncul, atau peluang yang menguntungkan dari adanya fluktuasi mata uang terhadap risiko yang muncul.
- **Risiko Negatif** adalah risiko yang muncul sebagai “ancaman risiko” dimana terdapat potensi kejadian atau perubahan yang dapat memberikan dampak negatif/kerugian jika tidak diberikan opsi penanganan.

Dalam konteks keamanan yang muncul biasanya lebih kepada risiko negatif namun tidak menutup kemungkinan adanya risiko positif pada konteks keamanan.

5.2. Identifikasi Ancaman dan Kerawanan dari Risiko

Proses identifikasi kecenderungan dan dampak risiko ini dilakukan untuk seluruh proses bisnis di lingkungan Pemerintah Kabupaten Pesisir Selatan, sehingga seluruh pegawai dapat memahami kondisi risiko yang dapat terjadi dalam pelaksanaan proses bisnis di lingkungan Pemerintah Kabupaten Pesisir Selatan. Proses identifikasi kecenderungan dan dampak risiko berdasarkan kategori kritikalitas aset.

Identifikasi kerawanan adalah proses untuk mengidentifikasi kelemahan dalam prosedur, sistem pengamanan TI, desain dan implementasi sistem, dan kontrol internal yang memiliki kemungkinan untuk dimanfaatkan dalam menyerang sistem. Sedangkan dalam identifikasi ancaman, pengelola risiko perlu mengidentifikasi potensi bahaya yang dapat mengeksploitasi kerentanan. Suatu ancaman belum dapat dikatakan sebagai risiko jika tidak disertai dengan kerawanan risiko yang memungkinkan ancaman terjadi.

6. ANALISIS DAN EVALUASI RISIKO

Analisis dan evaluasi risiko dilakukan dengan menilai tingkat nilai kecenderungan dan kelemahan terhadap proses bisnis dari terjadinya risiko yang telah teridentifikasi. Dalam melakukan analisis risiko mengacu kepada:

- Kontrol yang ada, meliputi: proses dan prosedur, alat, dan kontrol lain yang telah ada dan dilakukan saat ini oleh organisasi untuk meminimalkan kecenderungan.
- Kemungkinan, yaitu suatu gambaran probabilitas terjadinya risiko pada organisasi.
- Dampak, yaitu suatu gambaran akibat dari risiko yang mengindikasikan kerugian yang dialami, baik secara finansial maupun operasional ketika risiko tersebut terjadi.

6.1. Praktik Pengendalian Terbaik

Kontrol/pengendalian dalam keamanan informasi merupakan proses atau alat yang digunakan pada sistem yang berjalan pada saat ini yang meliputi keberadaan proses dan prosedur, perangkat TI, dan sumber daya TI lainnya. Contoh kontrol yang telah diimplementasikan di Pemerintah Kabupaten Pesisir Selatan antara lain:

- Pemeliharaan rutin pada perangkat
- Penggunaan antivirus pada PC/Notebook
- Akses kontrol ke ruang kerja

Kontrol tersebut dinyatakan efektif apabila dapat mencegah atau meminimalkan terjadinya risiko di lingkungan Pemerintah Kabupaten Pesisir Selatan. Kemudian juga dilakukan identifikasi praktik terbaik pengendalian/kontrol yang dapat diterapkan pada risiko yang muncul.

7. RENCANA PENANGANAN RISIKO (*RISK TREATMENT PLAN*)

Pemerintah Kabupaten Pesisir Selatan harus memprioritaskan pengendalian risiko berdasarkan ketersediaan dan keterbatasan sumber daya, baik teknologi, uang, maupun dokumen serta dampak secara proses bisnis. Dalam pembuatan *risk treatment plan* terdapat 5 (lima) jenis pengendalian risiko, yaitu Eskalasi Risiko, Mitigasi Risiko, Transfer Risiko, Penghindaran/transfer Risiko, dan Penerimaan Risiko.

Tahapan yang dilakukan dalam *risk treatment plan* meliputi hal-hal berikut:

1) Penentuan Penerimaan Risiko

Proses ini bertujuan untuk menentukan apakah suatu risiko akan diterima atau tidak.

Suatu risiko dapat diterima apabila Nilai Risiko (NR) adalah “Rendah” dan “Sangat Rendah”.

Penerimaan risiko juga dapat dilakukan apabila NR dari suatu risiko bernilai “Sedang” atau “Tinggi” dan sudah tidak dapat dikontrol lagi. Penentuan penerimaan risiko dengan NR bernilai “Sedang” atau “Tinggi” harus diketahui dan disetujui oleh Komite Manajemen Risiko.

2) Penentuan Pengendalian Risiko

Untuk risiko yang memiliki dampak di luar dari batas penerimaan risiko, perlu dilaksanakan tindakan pengendalian risiko sebagai berikut:

- ***Eskalasi Risiko*** merupakan tindakan pengendalian risiko yang diidentifikasi melewati tingkat tanggung jawab atau kewenangan Tim Keamanan Informasi dan bahkan ANRI sebagai Instansi.
- ***Control*** atau ***Mitigasi Risiko*** merupakan tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem praktik terbaik atau aturan.
- ***Transfer*** merupakan tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.
- ***Penghindaran Risiko*** merupakan strategi yang melibatkan Tindakan untuk sepenuhnya menghindari atau menghentikan aktifitas situasi yang berpotensi menimbulkan risiko/ risiko baru karena tidak dapat terelakkan.
- ***Penerimaan Risiko*** adalah Pemerintah Kabupaten Pesisir Selatan memilih untuk menerima risiko yang telah diidentifikasi tanpa melakukan Tindakan pengelolaan risiko

tambahan, hal ini memungkinkan jika risiko mau pada selera risiko instansi / penerimaan risiko atau jika biaya mengurangi risiko tersebut terlalu tinggi dibandingkan dengan potensi kerugiannya.

3) Penentuan Nilai Risiko Akhir

Proses ini bertujuan untuk memperkirakan perubahan nilai risiko jika rencana pengendalian risiko telah diterapkan. Dari proses ini dapat dilihat apakah rencana pengendalian risiko bersifat responsif dengan menurunkan dampak risiko atau bersifat preventif dengan mengurangi kemungkinan risiko terjadi.

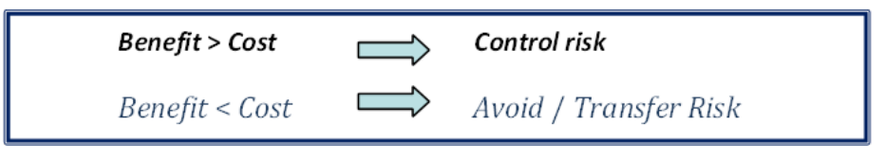
Penentuan ekspektasi nilai risiko akhir dilakukan dengan memperkirakan nilai kecenderungan akhir dan nilai dampak akhir yang diharapkan jika rencana pengendalian risiko telah diterapkan. Kriteria penentuan nilai risiko akhir menggunakan kriteria dan matriks yang sama dengan proses penentuan nilai risiko dasar.

7.1. Penentuan Rencana Penanganan Risiko, PIC, Target Waktu

Langkah-langkah yang harus dilakukan pada penentuan rencana penanganan risiko adalah:

- Menyusun rencana tindak lanjut untuk mengurangi nilai risiko.
- 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*).



7.2. 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:

- waktu implementasi kontrol;
- aktivitas detail dalam implementasi kontrol termasuk penyediaan sumber daya untuk mendukung terlaksananya aktivitas tersebut;
- pegawai/staff yang bertanggung jawab dalam implementasi kontrol

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

8. PEMANTAUAN DAN REVIU

Proses manajemen risiko keamanan siber 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 keamanan siber di Pemerintah Kabupaten Pesisir Selatan mengacu pada berikut:

Tabel 8 Tabel Monitoring Rencana Aksi Penanganan Risiko

Level	Review Risk Register (Monitoring)	Pelaporan Risiko
Koordinator Penyelenggara Pengelolaan Risiko	Setiap 6 bulan	-
Penanggung Jawab	Setiap Tahun	Setiap Tahun

9. PENCATATAN DAN PELAPORAN

Hasil dari pelaksanaan manajemen risiko yang dilaporkan kepada Penanggung Jawab Risiko Keamanan Siber 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:

- Proses pelaksanaan *risk assessment*
- Identifikasi risiko pada Pemerintah Kabupaten Pesisir Selatan
- Evaluasi dan analisis risiko
- *Risk Acceptance* yang terdapat pada registrasi risiko Pemerintah Kabupaten Pesisir Selatan
- Rencana penanganan risiko

Proses manajemen risiko dalam kegiatan *review risk assessment* harus dievaluasi secara berkala, yaitu satu tahun sekali. Pengkajian ulang proses *risk assessment* juga dilakukan apabila terjadi perubahan pada:

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

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN PESISIR SELATAN

WENDI, S.H., M.Hum.
Pembina Utama Muda (IV/c)
NIP. 19760407 199803 1 005