



PEMERINTAH PROVINSI JAWA TENGAH

STANDARD OPERATING PROCEDURE

TATA CARA PENGELOLAAN RISIKO

LAYANAN PENGADAAN SECARA ELEKTRONIK (LPSE)



PROVINSI JAWA TENGAH

2018

Daftar Isi

Daftar Istilah.....	3
1. Metode Penilaian Risiko.....	4
1.1. Penilaian Dampak	4
1.2. Penilaian Pengancam	4
1.3. Penilaian Kerentanan	5
1.4. Penilaian Paparan	5
1.5. Penilaian Risiko	6
1.6. Klasifikasi Risiko	7
2. Prosedur Pengelolaan Risiko.....	8

Daftar Istilah

1. **Risiko** adalah segala sesuatu yang dapat memberikan gangguan terhadap suatu proses, output, maupun kegiatan. Dalam melaksanakan penilaian risiko dapat menggabungkan dari beberapa jenis risiko, yaitu: Risiko Operasional, Risiko Finansial, Risiko Kepatuhan, Risiko Turunan (*Inherent Risk*) dan Risiko Sisa (*Residual Risk*).
 - a. **Risiko Operasional** adalah risiko yang diakibatkan oleh kegagalan dari Pedoman & prosedur, proses, sistem, personil, atau kejadian eksternal. Hal ini termasuk risiko dari kesalahan operasional pada aktivitas bisnis atau kesalahan dalam pengelolaan dan sistem manajemen.
 - b. **Risiko Finansial** adalah risiko yang diakibatkan antara lain oleh risiko pasar, yaitu akibat dari pergerakan negatif komponen-komponen pasar, seperti nilai valas, suku bunga, ekuitas dan komoditas.
 - c. **Risiko Kepatuhan** adalah risiko yang diakibatkan oleh keterlambatan, pelanggaran atau ketidaksesuaian dengan hukum yang berlaku, pelanggaran atau ketidaksesuaian perjanjian pihak ketiga (kontrak) dan pelanggaran atau ketidaksesuaian dengan regulasi eksternal/internal.
 - d. **Risiko Turunan** adalah risiko yang diakibatkan oleh kegagalan atau tidak adanya pengendalian (kontrol) internal.
 - e. **Risiko Sisa** adalah risiko yang masih muncul setelah dilakukannya pengendalian (kontrol). Risiko sisa juga harus dikendalikan hingga mencapai tingkat risiko yang dapat diterima.
2. **Dampak** adalah pengaruh atau akibat yang muncul dari suatu risiko yang ada.
3. **Pengancam** adalah pihak yang membawa akibat potensial dari suatu insiden yang tidak dikehendaki dikarenakan adanya kelemahan yang dapat membahayakan system atau organisasi.
4. **Kerentanan** adalah kerawanan dari aset yang dapat dieksploitasi dan menimbulkan ancaman.
5. **Paparan** adalah tingkat keterpengaruhan aset dari suatu risiko.
6. **Kontrol** adalah alat untuk mengendalikan risiko, dapat merupakan kebijakan, prosedur, standard, tindakan, struktur, organisasi atau teknologi yang dapat bersifat administrative, pengelolaan, teknis atau hukum.

1. Metode Penilaian Risiko

1.1. Penilaian Dampak

Pemberian nilai dampak diidentifikasi dari beberapa aspek berikut:

Nilai	Ekonomi	Reputasi	Pidana	Kinerja
4	Menghambat penyerapan anggaran	Pembubaran LPSE	Personil LPSE terancam hukuman pidana lebih dari 5 tahun	Menghentikan pelayanan kepada pengguna
3	Mengganggu penerapan anggaran	Pengalihan pengelolaan LPSE kepada pihak/unit kerja lain	Personil LPSE terancam hukuman pidana kurang dari 5 tahun	Mengganggu pelayanan kepada pengguna
2	Potensi mengganggu penyerapan anggaran	Kehilangan kepercayaan pengguna	Tidak ada	Meyulitkan pelaksanaan pemberian layanan
1	Tidak ada	Tidak ada	Tidak ada	Tidak ada

1.2. Penilaian Pengancam

Pemberian nilai pengancam diidentifikasi dari profil pengancam berikut:

Nilai	Tingkat	Profil
4	Sangat Tinggi	<ul style="list-style-type: none">- Kejahatan terorganisir- Pemerintah Negara lain- Pemilik dana lebih dari Rp. 1 Miliar
3	Tinggi	<ul style="list-style-type: none">- Operator atau Administrator- Pemilik dana antara Rp. 100 Juta sampai Rp. 1 Miliar
2	Sedang	<ul style="list-style-type: none">- Pengguna yang sah- Peretas senior- Pemilik dana antara Rp. 10 Juta sampai Rp. 100 Juta
1	Rendah	<ul style="list-style-type: none">- Pengguna yang tidak sah- Peretas pemula- Pemilik dana sampai dengan Rp. 10 Juta

1.3. Penilaian Kerentanan

Pemberian nilai kerentanan diidentifikasi dari 4 (empat) aspek, sebagai berikut

Kerentanan	Aspek Penilaian
Orang	<ul style="list-style-type: none">- Latar belakang- Tingkah laku- Ketaatan prosedur- Kompetensi
Administratif	<ul style="list-style-type: none">- Kebijakan- Prosedur- Efektifitas implementasi kebijakan dan prosedur
Logis	<ul style="list-style-type: none">- Arsitektur system- Pengendalian akses- Konfigurasi system
Fisik	<ul style="list-style-type: none">- Pengendalian akses- Daya tahan terhadap serangan fisik- Perlindungan fisik

Berdasarkan identifikasi diatas, kerentanan diberikan nilai:

Nilai	Tingkat Kerentanan
4	Sangat Tinggi
3	Tinggi
2	Sedang
1	Rendah

1.4. Penilaian Paparan

Pemberian nilai paparan berdasarkan tingkatan berikut:

Nilai	Tingkat Paparan	Contoh
3	Tinggi	Tidak ada antivirus
2	Sedang	Antivirus terinstal namun tidak update
1	Rendah	Antivirus bekerja dengan baik

1.5. Penilaian Risiko

Penilaian risiko didapat dari perhitungan berikut:

Risiko Turunan (tanpa kontrol) = Dampak x Pengancam x Kerentanan x paparan

Risiko Sisa (dengan kontrol) = Dampak x Pengancam x Kerentanan x paparan

Tabel Keparahan

Pengancam	1				2				3				4				
Kerentanan	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
Dampak	1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Tabel Risiko

paparan	1	2	3
Keparahan	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9
4	4	8	12
6	6	12	18
8	8	16	24
9	9	18	27
12	12	24	36
16	16	32	48
18	18	36	54
24	24	48	72
27	27	54	81
32	32	64	96
36	36	72	108
48	48	96	144
64	64	128	192

1.6. Klasifikasi Risiko

Berdasarkan tabel penilaian risiko, risiko dikelompokkan sebagai berikut:

Risiko	Nilai Risiko	Tindakan
Rendah	≤ 24	Risiko diterima
Sedang	> 24 dan ≤ 64	Dilakukan mitigasi
Tinggi	> 64	Dilakukan mitigasi dengan prioritas tinggi

paparan Keparahan	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9
4	4	8	12
6	6	12	18
8	8	16	24
9	9	18	27
12	12	24	36
16	16	32	48
18	18	36	54
24	24	48	72
27	27	54	81
32	32	64	96
36	36	72	108
48	48	96	144
64	64	128	192

2. Prosedur Pengelolaan Risiko

Risiko dikelola dengan cara didaftarkan dengan menggunakan daftar yang terus diperbaharui. Pendaftaran risiko dibuat berdasarkan pengelompokan dari klasifikasi dan sub klasifikasi aset, adapun isi daftar risiko sebagai berikut:

- 1) No., adalah nomor urut risiko atau dapat juga dengan kombinasi huruf dan angka, tanggal atau kode lainnya jika dibutuhkan;
- 2) Sub Klasifikasi, adalah Sub Klasifikasi aset yang sudah didaftarkan pada Form Daftar Aset;
- 3) Dampak, adalah penjelasan dampak dari risiko beserta penilaian yang sesuai dengan Metode Penilaian Risiko (poin 1.1);
- 4) Pengancam, adalah penjelasan pengancam dari risiko beserta penilaian yang sesuai dengan Metode, Penilaian Risiko (poin 1.2);
- 5) Kerentanan, adalah penjelasan kerentanan dari aset beserta penilaian yang sesuai dengan Metode Penilaian Risiko (poin 1.3);
- 6) Paparan, adalah penjelasan paparan risiko terhadap aset beserta penilaian yang sesuai dengan Metode Penilaian Risiko (poin 1.4);
- 7) Jenis Risiko, merupakan aspek Kerahasiaan, Integritas dan Ketersediaan yang melekat pada aset yang terpapar risiko;
- 8) Nilai Risiko, merupakan hasil perhitungan risiko yang sesuai dengan Metode Penilaian Risiko (poin 1.5);
- 9) Kontrol, merupakan tindakan-tindakan pengendalian yang diambil yang bertujuan untuk menurunkan nilai kerentanan atau paparan;
- 10) Mitigasi, adalah informasi kontrol yang akan diterapkan, PIC yang melaksanakan dan target penyelesaian proses mitigasi. Tindakan mitigasi diambil berdasarkan klasifikasi risiko yang sesuai dengan Metode Penilaian Risiko (poin 1.6).

3. Formulir Pengelolaan Risiko Layanan