Panduan Manajemen Risiko TI pada penyusunan standar satuan harga barang dan jasa Pemerintah Provinsi Lampung.

Manajemen risiko IT untuk penyusunan standar satuan harga barang dan jasa Pemerintah Provinsi Lampung merupakan serangkaian proses untuk mengelola risiko terkait IT dalam penggunaan aplikasi e-ssh. Prosesnya meliputi perencanaan, identifikasi, analisis, respon (penanganan), pemantauan dan pengendalian serta pengkomunikasian risiko dari setiap aktivitas IT yang dilaksanakan oleh BPKAD Provinsi Lampung. Dalam upaya mewujudkan kelancaran penyusunan standar satuan harga menggunakan aplikasi e-ssh yang dijalankan, maka divisi / unit kerja IT perlu menerapkan manajemen risiko sebagai sistem peringatan dini (early warning system) dan untuk mendukung penuh keberhasilan penyusunan standar satuan harga yang sedang ditangani oleh BPKAD Provinsi Lampung. Pelaku yang terlibat dalam pembuatan dan pengecekan dokumen adalah Kepala Badan, Kepala Bidang Aset, Kepala Sub Bidang Analisa Kebutuhan Aset, Kepala Sub Bagian Data dan Teknologi Informasi dan unit kerja/divisi IT.

1. Perencanaan Manajemen Risiko

Pada tahap ini dasar yang dipakai adalah dari PMBOK dan. Berdasar PMBOK tahap perencanaan manajemen risiko berisi rencana dasar untuk menghadapi risiko. Yang dijadikan input atau landasan/pijakan pada tahap ini adalah rencana manajemen penyusunan standar satuan harga menggunakan aplikasi e-ssh, , kondisi lingkungan BPKAD, dan proses organisasi. Dimana outputnya adalah berupa rencana manajemen risiko. Hal ini bisa dilakukan melalui rapat perencanaan dan analisis. Template berupa tabel untuk mendefinisikan level risiko, kemungkinan (probability), dampak (impact), dan matrik perkalian probability dan impact dibuat untuk diisikan nanti pada tahap analisis risiko.

Tabel Ukur Dampak

NO	KEMUNGKINAN	URAIAN
1	Jarang	Probabilitas Kejadian ≤ 20%
2	Kemungkinan Kecil	Probabilitas Kejadian ≤ 20% x ≤ 40%
3	Kemungkinan Sedang	Probabilitas Kejadian ≤ 40% x ≤ 60%
4	Kemungkinan Besar	Probabilitas Kejadian ≤ 60% x ≤ 80%
5	Hampir Pasti	Probabilitas Kejadian ≤ 80% x ≤ 100%

Di atas adalah tabel ukuran dampak untuk menentukan standar dampak dari akibat timbulnya risiko TI yang terjadi.

Perencanaan manajemen risiko PMBOK mengaitkan risiko pada IT dengan alur hidup Penyusunan Standar Satuan Harga menggunakan aplikasi e-ssh mulai dari penyesuaian user, jumlah sumber daya, dan sebagainya. Untuk perencanaan manajemen risiko PMBOK dimulai dengan mempelajari kondisi eksternal, penetapan ruang lingkup proses manajemen risiko, dan membangun kriteria risiko. Jadi, yang perlu dilakukan pada tahap ini adalah sebagai berikut :

1. Membuat rencana manajemen risiko penyusunan standar satuan harga yang memuat metodologi, peran dan tanggung jawab, keuangan, jadwal, kategori risiko, definisi kemungkinan dan dampak dari risiko, matriks kemungkinan dan dampak risiko, penetapan risk appetite dan risk tolerance dari stakeholder dan laporan.
2. Menetapkan ruang lingkup manajemen risiko yang meliputi internal, eksternal, proses manajemen risiko, dan mengembangkan kriteria risiko.

2. Identifikasi Risiko

Identifikasi risiko ini mengacu pada COBIT tahap pengumpulan data. Yang perlu dilakukan pada tahap ini adalah membuat risk scenario. Contoh tabelnya sebagai berikut:

NO	Jenis Risiko	Tipe Risiko			Sekenario Risiko	
		IT benefit / value Enablement Risk	IT programme and project delivery risk	IT operations and service delivery risk	**Sekenario Negatif**	**Sekenario Positif**

Tanggal Pengisian Form

Nama Anggota Penyusun :

Kepala Badan (Paraf Setuju)	Kepala Bidang Aset (Paraf Setuju)	Kepala Sub Bidang Analisa Kebutuhan Aset (Paraf Setuju)	Kepala Sub Bagian Data dan Teknologi Informasi dan unit kerja/divisi IT (Paraf Setuju)

COBIT membagi tipe risiko menjadi tiga, yaitu sebagai berikut:

a. IT benefit / value enablement risk, dimana risiko yang diidentifikasi masuk ke dalam tipe manfaat atau nilai risiko TI, yaitu apabila risiko terkait dengan (kehilangan) kesempatan untuk memanfaatkan TI dalam meningkatkan efisiensi atau efektivitas proses bisnis atau sebagai enabler untuk inisiatif proses bisnis baru. Contohnya adalah teknologi yang digunakan dalam inisiatif bisnis baru dan teknologi yang digunakan untuk mengefisiensikan proses operasional.

b. IT programme and project delivery risk, dimana risiko yang diidentifikasi masuk ke dalam tipe program dan kegiatan risiko TI, yaitu apabila risiko terkait dengan kontribusi TI untuk membuatkan atau meningkatkan solusi bisnis, biasanya dalam bentuk proyek dan program. Contohnya adalah kualitas proyek, relevansi proyek dan kelebihan waktu proyek dari yang ditentukan.

c. IT operations and service delivery risk, dimana risiko yang diidentifikasi masuk ke dalam tipe operasional dan layanan risiko TI, yaitu apabila risiko terkait dengan stabilitas operasional, ketersediaan, perlindungan dan pemulihan layanan TI, dimana risiko dapat membawa kerugian atau pengurangan nilai perusahaan. Contohnya adalah gangguan pada layanan TI, masalah keamanan dan isu-isu terkait.

Pada tabel diatas, IT benefit / value enablement risk, diisi dengan 'P' (Primer) apabila risiko terkait TI sebagai enabler untuk meningkatkan solusi binis, sedangkan jika tidak terkait maka diisi dengan 'S'.

IT programme and project delivery risk, diisi dengan 'P' (Primer) apabila risiko terkait dengan program dan penyusunan standar satuan harga TI, sedangkan jika tidak terkait maka diisi dengan 'S'.

IT operations and service delivery risk, diisi dengan 'P' (Primer) apabila risiko terkait dengan ketersediaan layanan, stabilitas operasional dan gangguan layanan, sedangkan jika tidak terkait maka diisi dengan 'S'.

Mengacu kepada standar COBIT 5 for Risks, terdapat dua puluh jenis (kategori) risiko TI untuk setiap risiko yang diidentifikasi, berikut merupakan pembagian dua puluh jenis risiko tersebut yang disajikan pada Tabel berikut :

Tabel Pembagian Jenis (Katagori) Risiko

NO	Kategori	Pengertian
1.	*Portfolio establishment and maintenance*	Pengadaan dan pemeliharaan portofolio
2.	*Programme/ projects life cycle management (programme/ project initiation, economics, delivery, quality and termination)*	Manajemen siklus hidup program atau penyusunan standar satuan harga (inisiasi program/penyusunan standar satuan harga, biaya, delivery, kualitas dan penutupan penyusunan standar satuan harga)
3.	*IT investment decision making*	Pengambilan keputusan investasi TI
4.	IT expertise and skills	Ketrampilan dan keahlian TI

5.	*Staff operations (human error and malicious intent)*	Staff operasional (kesalahan faktor manusia disengaja maupun tidak)
6.	*Information (data breach: damage, leakage and access)*	Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses)
7.	*Architectural (vision and design)*	Architectural (vision and design)
8.	*Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)*	Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan)
9.	*Software*	Perangkat lunak
10.	*Business ownership of IT*	Kepemilikan bisnis TI
11.	*Supplier selection/performanse, contractual compliance, termination of service and transfer*	Pemilihan kinerja pemasok, penyesuaian kontrak, pemberhentian layanan dan pengalihan
12.	*Regulatory compliance*	Pemenuhan regulasi
13.	*Geopolitical*	Geopolitik
14.	*Insfrastructure theft or destruction*	Pencurian infrastruktur atau pengrusakan
15.	*Malware*	Malware
16.	*Malware*	Serangan langsung pada sistem, perangkat lunak, ataupun data
17.	*Industrial action*	Situasi dalam dunia industri
18.	*Environmenta*	Lingkungan
19.	*Acts of Nature*	Bencana alam
20.	*Inovasi*	Inovasi

3. Analisis Risiko

Analisis kualitatif dibuat untuk memberikan gambaran umum tentang level risiko. Analisis kualitatif menggunakan bentuk kata atau skala deskriptif untuk menjelaskan seberapa besar potensi risiko yang diukur. Apakah termasuk level risiko rendah, sedang, atau tinggi.

Setelah itu dapat dilakukan analisis semi kuantitatif ataupun kuantitatif untuk lebih merinci level risiko yang ada.

Pada analisis semi kuantitatif, skala kualitatif yang telah disebutkan diatas diberi nilai yang menggambarkan besaran kemungkinan maupun dampak

risiko. Hasilnya berupa tingkat risiko yang merupakan perkalian dari keduanya. Pada analisis kuantitatif yang digunakan adalah nilai numerik. Probabilitas/frekuensi kejadian beserta dampaknya dituangkan dalam bentuk numerik untuk menentukan tingkatan risikonya.

Tabel Map Risk

Dampak / Kemungkinan	1 Sangat Kecil	2 Kecil	3 Biasa	4 Besar	5 Luar Biasa
5 Sering Terjadi	**5 Sedang**	**10 Sedang**	**15 Tinggi**	**20 Extrim**	**25 Extrim**
4 Sering	**4 Rendah**	**8 Sedang**	**12 Tinggi**	**16 Tinggi**	**20 Extrim**
3 Biasa	**3 Rendah**	**6 Sedang**	**9 Sedang**	**12 Tinggi**	**15 Tinggi**
2 Jarang	**2 Rendah**	**4 Rendah**	**6 Sedang**	**8 Sedang**	**10 Tinggi**
1 Sangat Jarang	**1 Rendah**	**2 Rendah**	**3 Rendah**	**4 Rendah**	**5 Sedang**

Di atas adalah tabel Risk Map untuk menentukan tingkat risiko berdasar kemungkinan yang dikalikan dengan dampak yang ditimbulkan.

Tabel Kriteria Risiko

Level Risiko	Kriteria	Uraian
Rendah	Dapat diterima dan dilakukan pemantauan	Dibutuhkan pengendalian normal
Sedang	Perlu pengendalian risiko	Dibutuhkan pengendalian yang baik
Tinggi	Perlu pengendalian yang ketat	Dibutuhkan pengendalian yang sangat baik (excellent)
Ekstrim	Tidak dapat diterima	Dibutuhkan pengendalian yang sangat baik (excellent)

Di atas adalah tabel kriteria risiko yang dipakai sebagai standar untuk merencanakan respon risiko yang akan dipilih.

4. Perencanaan Penanganan Risiko

Untuk menentukan respon terhadap risiko bisa digunakan metode estimasi/perkiraan secara subyektif. Metode ini disebut professional judgement (Control Self-Assessment Techniques/ CST). Pemilihan respon terhadap risiko berdasarkan alternatif yang tersedia (accept, mitigate, transfer, avoid) untuk risiko negatif, dan untuk risiko positif tersedia exploit, enhance, share, dan ignore.

NO	Uraian RIsiko	Kemuginan	Dampak	Kemungkinan X Dampak	Keriteria
(1)	(2)	(3)	(4)	(5)	(6)

Tanggal Penyusunan

Kepala Badan	Kepala Bidang Aset	Kepala Sub Bidang Analisa Kebutuhan Aset	Kepala Sub Bagian Data dan Teknologi Informasi dan unit kerja/divisi IT
(Paraf Setuju)	(Paraf Setuju)	(Paraf Setuju)	(Paraf Setuju)

Petunjuk pengisian berdasar kolom yang ada:

(1) Diisi nomor urut

(2) Diisi mengenai gambaran risiko yang ada

(3) Diisi kriteria risikonya

(4) Diisi dengan skala linkert (1 - 5) yang menunjukkan ukuran kemungkinan terjadinya risiko

(5) Diisi dengan skala linkert (1 - 5) yang menunjukkan ukuran dampak risiko

(6) Diisi dengan hasil perkalian kolom (4) dan (5) (7) Diisi respon risiko yang dipilih.

5. Pemantauan dan Pengendalian Risiko

Tabel Pemantauan Risiko

NO	Risiko	Respon/pengendalian	Tanggal Pengendalian	Status Pengendalian			Saran Perbaikan
				Baik	Cukup	Kurang	

Tangal Pengisian:

Kepala Badan (Paraf Setuju)	Kepala Bidang Aset (Paraf Setuju)	Kepala Sub Bidang Analisa Kebutuhan Aset (Paraf Setuju)	Kepala Sub Bagian Data dan Teknologi Informasi dan unit kerja/divisi IT (Paraf Setuju)

Di atas adalah tabel pengendalian risiko untuk memantau dan melihat status pengendalian dari risiko TI serta saran yang diusulkan sebagai perbaikan.

6. Komunikasi Dan Konsultasi

Untuk pengkomunikasian risiko adalah dengan menyampaikan laporan risk assessment serta mengkomunikasikan risiko proses dan kebijakan manajemen risiko kepada seluruh personel yang berkaitan.