Risk Assesment dalam Perancangan Business Continuity Plan
Studi Kasus : LPSE DIY

Mohamad Zainuri[1], Lukito Edi Nugroho[2], Widyawan[3]

Jurusan Teknik Elektro dan Teknologi Informasi,Fakultas Teknik UGM [1]
zainuri.cio14@mail.ugm.ac.id
Jurusan Teknik Elektro dan Teknologi Informasi,Fakultas Teknik UGM [2]
Jurusan Teknik Elektro dan Teknologi Informasi,Fakultas Teknik UGM[3]

Abstrak

Penggunaan Teknologi Informasi di pemerintahan semakin tinggi, untuk itu perlu adanya rencana untuk menjamin ketersediaan layanan untuk mengantisipasi terjadinya gangguan. Rencana tersebut biasa disebut dengan istlah Business Continuity Plan (BCP).Langkah utama dalam perancangan BCP adalah risk assessment. Risk assessment diperlukan untuk mengetahui, menganalisis dan mengevaluasi risiko yang berpotensi menimpa aktivitas organisasi sehingga akan didapatkan dampak risiko tersebut kepada aktivitas organisasi.Hasil dari analisis risiko ini digunakan sebagai pilihan untuk menentukan strategi business continuity organisasi.Data di kumpulkan dari interview kepada pengelola obyek penelitian dan mempelajari berbagai literature dan peraturan terkait obyek penelitian.Hasil dari penelitian ini menunjukkan bahwa risiko dari sisi teknologi mempunyai ancaman risiko yang paling besar.Untuk itu perlu adanya prioritas pada strategi business continuity untuk sisi teknologi informasi.

Kata Kunci: Business continuity, ISO 22301, ISO 31000, risk assessment, LPSE

1. Pendahuluan

Saat ini penggunaan Teknologi Informasi (TI) dalam proses pemerintahan semakin tinggi khususnya di lingkungan Pemerintah Daerah Daerah Istimewa Yogyakarta. Penggunaan Teknologi Informasi (TI) ini meliputi proses penyusunan Rencana Anggaran Pendapatan dan Belanja Daerah (RAPBD) dan Pelaksanaan transaksi keuangan (E-Budgeting), Monitoring APBD (E-Monev), maupun dalam aktivitas pengadaan barang dan jasa (E-Procurement). Aktivitas pengadaan barang dan jasa di pemerintahan merupakan salah satu hal yang krusial, dikarenakan hubungannya dengan penggunaan keuangan negara dan diakses oleh publik.Untuk itu ketersediaan layanan ini menjadi sangat diperlukan.Untuk menjaga keberlangsungan kegiatan maka dibutuhkan sebuah Rencana Keberlangsungan Kegiatan (*Business Continuity Plan /BCP).*

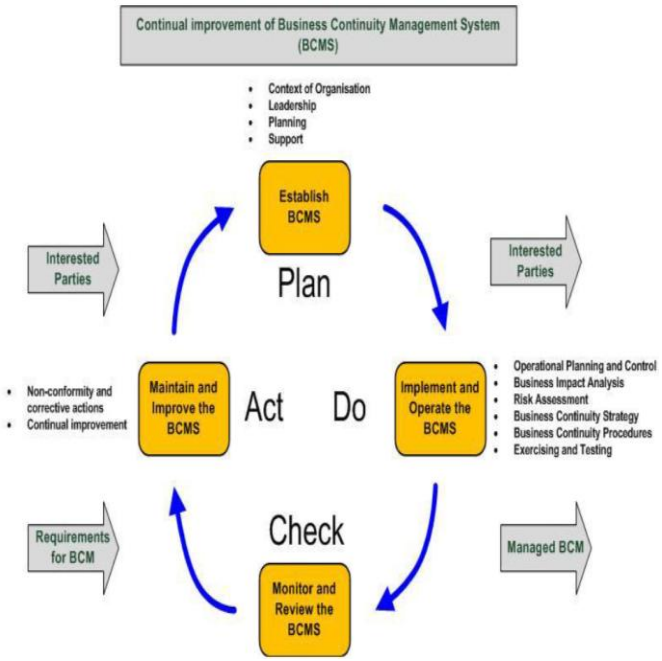
Definisi Business Continuity Plan atau Rencana kelangsungan usaha adalah Prosedur terdokumentasi yang memandu organisasi untuk merespon, memulihkan, melanjutkan, dan mengembalikan organisasi ke tingkat awal operasi setelah terjadi gangguan. Biasanya rencana tersebut mencakup sumber daya, layanan, dan kegiatan yang dibutuhkan untuk menjamin kelangsungan fungsi usaha yang vital. [SNI ISO 22301:2014]. Business Continuity mulai menjadi perhatian organisasi sejak awal tahun 2000-an yang dipicu oleh adanya ancaman Y2K dan kejadian penyerangan gedung *World Trade Center* pada 11 September 2001. Kejadian lain adalah berbagai bencana alam yang melanda dunia, diantaranya kejadian Tsunami Aceh yang melanda Aceh bahkan meluas sampai ke Thailand pada 26 Desember 2004. Kejadian selanjutnya adalah Gempa dan tsunami Jepang pada 11 Maret 2011 yang melumpuhkan sebagian besar aktivitas ekonomi Negara Jepang.Berbagai perusahaan besar di Jepang lumpuh kegiatan bisnisnya, salah satunya adalah Toyota.Namun Toyota bisa segera memulai kegiatan bisnisnya pada tanggal 17 Maret 2011 atau enam hari setelah kejadian gempa hebat tersebut.Ini menjadi bukti kematangan Toyota dalam mengantisipasi dampak bencana pada bisnisnya.

Pemerintah Indonesia juga telah menyadari akan pentingnya business continuity. Hal itu bisa dilihat dari terbitnya Peraturan Bank Indonesia Nomor: 10/6/PBI/2008 tentang Sistem Bank Indonesia *Real time Gross Settlement.* Pasal 8 pada peraturan tersebut mewajibkan penyelenggaran system RTGS-BI untuk menyusun mekanisme dan prosedur keberlangsungan penyelenggaraan system RTGS-BI *(Business Continuity Plan / BCP).*Selanjutnya peraturan yang lebih besar tentang BCP ini muncul dalam bentukPP No 82 Tahun 2011 tentang Penyelenggaraan Sistem dan Transaksi Elektronik pada pasal 17 ayat 1 yang menyebutkan bahwa Penyelenggara Sistem Elektronik untuk pelayanan publik wajib memiliki rencana keberlangsungan kegiatan

(business continuity plan) untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya. Di dalam PP No 82 Tahun 2012 Pasal 84 ayat 1 disebutkan bahwa pelanggaran terhadap pasal 17 ayat 1 akan dikenakan sanksi administratif. Pemerintah melalui Badan Standardisasi Nasional juga sudah mengadopsi standar business continuity Internasional yaitu ISO 22301:2012, Social Security – Business continuity management systems - Requirements menjadi Standar Nasional Indonesia dalam bentuk SNI ISO 22301:2014, Keamanan Masyarakat - Sistem Manajemen Kelangsungan Usaha – Persyaratan. Ada banyak standard dan *best practice* lain dari business continuity di antaranya COBIT, NIST SP 800-34, NFPA 1600:2010. Dari ke empatnya hanya Standard ISO 22301:2012 yang berlaku secara internasional dan dapat disertifikasi dalam bentuk lembaga.

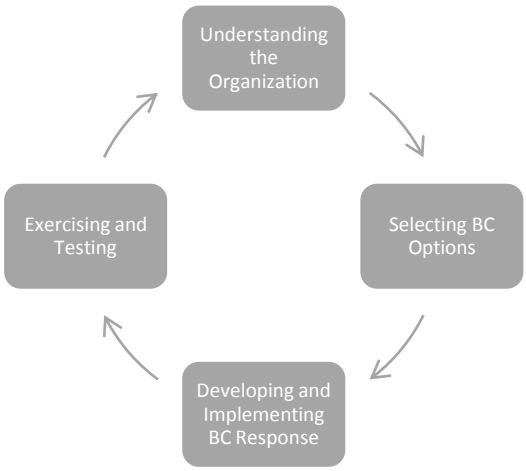
ISO 22301:2012 merupakan Standard Internasional untuk *business continuity*.Terdapat 10 klausa dan 1 pendahuluan dalam standard ini.Klausa 1 sampai dengan 3 berisi Ruang lingkup, acuan normatif, istilah dan definisi.Sedangkan klausa 4 sampai dengan 10, berisi elemen – elemen standar dalam business continuity management systems (bcms). Selain itu standard ini menerapkan model Plan-Do-Check-Act (PDCA) untuk merencanakan, menetapkan, melaksanakan, mengoperasikan, memantau, mengkaji-ulang, memelihara dan terus menerus meningkatkan efektivitas business continuity organisasi. Dengan penerapan model PDCA dalam standard ini menjamin suatu derajat konsistensi dengan standar system manajemen lainnya, seperti ISO 9001 tentang Quality Management Systems, ISO 14001 tentang Environmental management systems, ISO/IEC 27001 tentang Information Security Management Systems, ISO 20000-1, Information Technology – Service Management sehingga mendukung pelaksanaan dan pengoperasian yang konsisten dan terpadu dengan sistem manajemen terkait.

Hubungan antara klausa – klausa dalam ISO 22301:2012 dengan model PDCA dapat dilihat dalam Gambar 1:



Gambar 1. Siklus PDCA dalam ISO 22301

Salah satu hasil dalam system BCMS adalah Business Continuity Management Systems (BCMS) adalah BCP. BCP dapat dirancang dengan menggunakan kerangka kerja yang terdapat dalam ISO 22313, seperti dalam gambar 2 :



Gambar 2. Siklus BCP

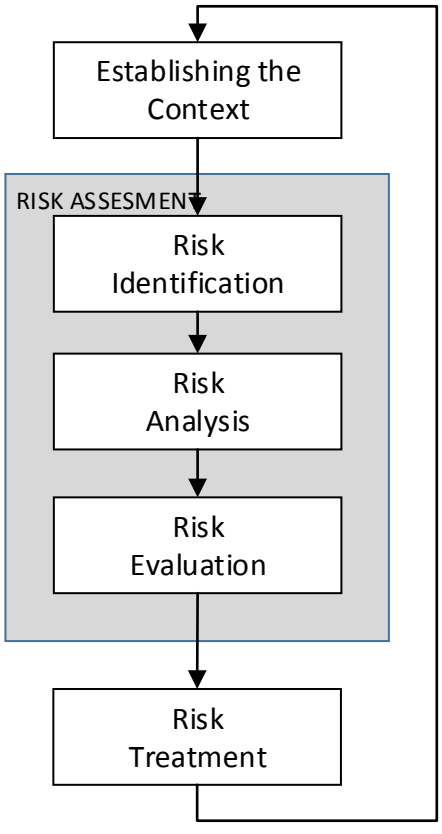
Fase pertama dalam siklus tersebut adalah understanding the organization. Dalam fase ini ada 2 aktivitas utama yaitu *risk assesment* dan *Business Impact Analysis(BIA)*. Maka Risk Assesment menjadi mutlak diperlukan untuk dilakukan dalam proses perancangan BCP.

Dalam ISO 22301:2012, Risk assessment didefinisikan sebagai keseluruhan proses identifikasi, analisis dan evaluasi risiko. *Risk*

*assessment*dalam business continuity harus dapat menjawab pertanyaan mendasar berikut ini :

- Risiko apa yang mungkin terjadi dan mengapa dapat terjadi ?
- Apa konsekuensi dari risiko tersebut ?
- Berapa kemungkinan risiko tersebut terjadi lagi di masa mendatang ?
- Hal apa yang dapat digunakan untuk melakukan mitigasi konsekuensi risiko dan atau mereduksi kemungkinan terjadinya risiko?

Dalam Business continuity risk assessment bertujuan untuk menilai, mengevaluasi dan mengidentifikasi risiko – risiko apa saja yang berpotensi mengganggu proses bisnis organisasi dan aktivitas – aktivitas terkait.
Pengertian risiko adalah Kemungkinan dari sebuah ancaman untuk mengeksploitasi kerawanan yang berpotensi memberikan kerugian pada asset.(Jones&Ashenden, 2005).
Salah satu Kerangka kerja yang dapat dijadikan acuan untuk melakukan risk assesmentsesuai dengan ISO 22301 adalah ISO 31000 yang ditampilkan seperti dalam gambar 3 :



:

Gambar 3. Risk Management ISO 31000

Fase pertama adalah Establishing the context.
Pada fase ini akan dihasilkan penentuan ruang lingkup dan tujuan dari diadakannya aktivitas risk assessment ini.

Fase kedua adalah Risk Assesment.
Risk assessment terdiri dari 3 tahapan, yaitu :

a. Risk identification

Merupakan proses untuk menemukan, menggambarkan risiko. Identifikasi ini meliputi sumber, waktu kejadian, penyebab dan potensi dampak dari suatu risiko.Identifikasi risiko dapat diperoleh dari data history (log), analisis teori, informasi maupun pendapat tenaga ahli dankeperluan pihak – pihak pemangku kepentingan.

b. Risk analysis

Proses untuk mengumpulkan risiko dan memberikan penilaian terhadap satu risiko. Analysis risiko ini menjadi dasar untuk evaluasi risiko dan penentuan penanganan risiko.Tahap ini terdapat 2 fase yaitu analisis dampak risiko dan penilaian risiko.Besarnya risiko dipandang sebagai hasil antara keseringan (likelihood) x consequence (dampak).

c. Risk evaluation

Proses untuk membandingkan hasil analisis risiko dengan kriteria risiko untuk menentukan apakah suatu risiko dan dampaknya dapat diterima atau ditoleransi.
Hasil penilaian risiko dari tahap risk analysis, digunakan untuk menentukan apakah risiko tersebut dapat diterima atau tidak.

Fase ketiga adalah Risk Treatment.
Risk treatment adalah proses penanganan risiko. Penanganan risiko dibagi menjadi 4 strategi :

a. Kurangi (Reduce)
b. Hindari (Avoid)
c. Terima (Accept)
d. Alihkan (Transfer)

LPSE merupakan Layanan Pengadaan Secara Elektronik yang dibentuk berdasarkan Perpres No 54 Tahun 2010. LPSE memiliki fungsi sesuai dengan Perka LKPP No 2 Tahun 2010 adalah sebagai berikut :

a. Penyusunan program kegiatan, ketatausahaan, evaluasi dan pelaporan pengadaan barang/jasa di lingkungan K/L/D/I.
b. Pengelolaan Sistem Pengadaan Secara Elektronik(SPSE) dan Infrastrukturnya
c. Pelaksanaan registrasi dan verifikasi pengguna SPSE.
d. Pelaksanaan pelayanan pelatihan dan dukungan teknis pengoperasian SPSE.

Sehingga dengan adanya risk assessment ini dapat menjadi dasar dalam penentuan strategi business continuity di LPSE DIY.

2.1 Metode

Metode yang digunakan dalam penelitian kali ini adalah metode kualitatif dengan dideskripsikan dan ditranslasikan dengan kuantitatif.

2.1 Metode Pengumpulan Data
Data didapatkan melalui interview dengan narasumber, yaitu para pemangku kepentingan di LPSE DIY.Selain itu juga dengan studi literature dan mempelajari berbagai peraturan pengelolaan LPSE DIY.

2.2 Metode Analisis Data.
Metode analisis data yang digunakan dalam penelitian kali ini adalah metode kuantitatif.Kriteria atau acuan yang digunakan dalam penelitian ini adalah standard ISO 31000 tentang risk management. Selain itu juga dsesuaikan penggunaannya dengan kriteria pada ISO 22301 sebagai standard business continuity dikarenakan penelitian tentang risk management ini adalah bagian dari penelitian yang lebih besar berupa perancangan business continuity plan dengan standard ISO 22301.
Metode analisis menggunakan matriks 4 x 4 dengan memandang level risiko sesuai dengan dampak (consequence) dan keseringan (likelihood) terjadinya risiko.

Risk = likelihood x consequence

Penilaian likelihood dengan skala sebagai berikut :

Level	Keseringan	Keterangan
1	Sangat Jarang	Terjadi kurang dari 1 kali dalam 1 tahun
2	Jarang	Terjadi antara 1-4 kali dalam setahun
3	Sering	Terjadi 5-8 kali dalam setahun
4	Sangat Sering	Terjadi lebih dari 8 kali dalam setahun

Tabel 1. Tingkat keseringan (Likelihood)

Penilaian Consequence dengan skala sebagai berikut :

Level	Dampak	Keterangan
1	Tidak Signifikan	Hanya bersifat local tidak berpengaruh pada layanan
2	Minor	Bersifat local dan berpengaruh pada kenyamanan layanan
3	Major	Berpengaruh pada keberlangsungan layanan
4	Kritis	Layanan terhenti

Tabel 2. Nilai Dampak (Consequence)

Hasil Risk analysis dikelompokkan menjadi 3 kategori yaitu risiko rendah, sedang dan tinggi.Hanya risiko rendah yang dapat diterima oleh LPSE DIY.

Keseringan \ Dampak	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Tabel 3. Tabel Analisis Risiko

Hasil dan Pembahasan

3.1 Establishing the Context

Tahapan ini dilakukan dengan melakukan interview dengan pengelola LPSE DIY untuk menentukan Ruang lingkup dan Tujuan dari risk assessment ini. Didapatkan hasil bahwa ruang lingkup dari penelitian ini adalah operasional dari LPSE DIY. Tujuan dariaktivitas risk asessment ini adalah untuk mendapatkan, mengevaluasi dan memberikan penanganan pada berbagai risiko tersebut. daftar risiko yang berpotensi terjadi dan mengganggu aktivitas utama dari LPSE DIY seperti yang disebutkan dalam fungsi LPSE di Perka No 2 Tahun 2010.
Sedangkan dari studi dokumentasi didapatkan juga asset yang dapat terdampak dari LPSE DIY, yang ditampilkan dalam tabel 1 .

No	Kategori Aset
1	Gedung Kantor
2	Perangkat TI (Server, PC, Network)
3	Client
4	Karyawan
5	Informasi
6	Reputasi

Tabel 4. Daftar Kategori Aset

3.2 Identifikasi Risiko

Pada tahapan ini di identifikasi risiko – risiko yang berpotensi menimpa LPSE DIY dan akan ditampilkan dalam bentuk tabel 1, dibawah ini:

No	Kategori Risiko	Daftar Risiko
1	Ancaman Alam / Lingkungan	• Gempa Bumi • Banjir • Angin • Kebakaran • Petir • Pandemik / Wabah Penyakit
2	Ancaman yang disebabkan	• Kebakaran • Pencurian

	manusia	• Vandalisme • Terorisme • Unjuk rasa • Kerusuhan
3	Ancaman terhadap Infrastruktur	• Kerusakan bangunan • Listrik/AC mati • Kerusakan fasilitas non-TI • Krisis BBM
4	Ancaman secara khusus untuk TI	• Cyber war • Malware, virus. • Kerusakan PC / Perangkat non server • Kerusakan Server

Tabel 5. Daftar Identifikasi Risiko

3.3 Analysis dan Evaluasi Resiko

Terdapat 2 tahapan dalam fase ini, yaitu analisis dampak risiko dan penilaian risiko.Tabel 3 menunjukkan analisis dampak risiko.

Ancaman	Kejadian	Aset terdampak	Konsekuensi
Alam / Lingkungan			
Gempa bumi	Gempa merusakkan bangunan / tempat tinggal	Gedung, Staf	Terhentinya layanan karena kerusakan fasilitas dan karyawan tidak dapat bekerja
Banjir	Banjir merendam jalan sehingga staf tidak dapat bekerja	Staf	Ketidakhadiran karyawan karena sulit transportasi
	Banjir merendam Datacenter dan listrik harus dimatikan	Peralatan TI	Terhentinya layanan
Angin	Kerusakan fasilitas bangunan	Peralatan kntor	Terhentinya layanan offline
Kebakaran	Arus pendek akibat kabel terkelupas	Gedung dan asset kantor	Terhentinya layanan.
Petir	Petir menyebabkan Perangkat TI mati	Perangkat TI	Terhentinya layanan
Wabah Penyakit / Pandemik	Terdapat penyebaran wabah penyakit di suatu daerah	Karyawan	Kehilangan Karyawan

Ancaman	Kejadian	Aset terdampak	Konsekuensi
Ulah Manusia			
Kebakaran	Pengunjung LPSE mematikan punting rokok	Gedung	Layanan offline terhenti
Pencurian	Pencurian terhadap asset LPSE	Aset LPSE, Informasi, Reputasi	Layanan terhenti
Vandalisme	Vandalisme terhadap gedung LPSE	Gedung, Reputasi	Reputasi LPSE turun
Terorisme	Kejadian pemboman terhadap gedung LPSE	Staf, Gedung	Layanan terhenti
Unjuk Rasa	Terjadi mogok kerja karyawan LPSE	Karyawan, Reputasi	Layanan terhenti, reputasi menurun
Kerusuhan	Terjadi kerusuhan di sekitar LPSE	Karyawan	Karyawan tidak dapat berangkat kerja, sehingga layanan terganggu

Ancaman	Kejadian	Aset terdampak	Konsekuensi
Infrastruktur non TI			
Kerusakan bangunan	Bangunan bocor, plafon rusak	Bangunan	Pelayanan kurang nyaman
Listrik / AC rusak	Mati / AC listrik di kantor layanan LPSE	Bangunan	Pelayanan offline terhenti
Kerusakan fasilitas non TI	Rusak / tidak tersedianya alat – alat kerja non TI	Aset kantor	Tidak berjalannya seluruh atau sebagian layanan offline
Krisis BBM	BBM tidak tersedia dipasaran	Karyawan,	Karyawan tidak bias berangkat / terlambat ke kantor

Ancaman	Kejadian	Aset terdampak	Konsekuensi
Ancaman Spesifik di TI			
Cyber Threat	Terjadi serangan cyber terhadap server SPSE	Perangkat TI, Informasi	Informasi rahasia dapat tersebar
	Kebocoran password	Reputasi	Rusaknya reputasi organisasi
Virus / malware	Menyebarnya virus di jaringan internal LPSE	Informasi	Kehilangan / Kerusakan data
Kerusakan Perangkat TI non Server	PC rusak, Printer rusak	Informasi	Kehilangan data / layanan terganggu
Kerusakan Server	Rusaknya server SPSE sehingga tidak dapat diakses informasinya	Informasi	Kehilangan Informasi

Tabel 6. Analisis dampak risiko

Kemudian diadakan penilaian terhadap berbagai risiko tersebut di atas. Risiko di dinilai dengan metode kualitatif dideskripsikan secara kuantitatif seperti metode di 2.2 dan dievaluasi dengan metode 2.2 dan dihasilkan sebagai berikut :

No	Nama Risiko	Likelihood	Consequence	Risk Score	Risk Category
Alam / Lingkungan					
1	Gempa bumi	1	4	4	Mid
2	Banjir	1	4	4	Mid
3	Angin	1	4	4	Mid
4	Kebakaran	1	4	4	Mid
5	Petir	2	4	8	High
6	Wabah Penyakit / Pandemik	1	4	4	Mid
Ulah Manusia					
7	Kebakaran	1	4	4	Mid
8	Pencurian	1	3	3	Low
9	Vandalisme	1	1	1	Low
10	Terorisme	1	4	4	Low
11	Unjuk Rasa	2	1	2	Low
12	Kerusuhan	1	2	2	Low
Infrastruktur non IT					
13	Kerusakan bangunan	1	2	2	Low
14	Listrik / AC rusak	1	3	3	Low
15	Kerusakan fasilitas non TI	2	1	2	Low
16	Krisis BBM	1	2	2	Low
Serangan TI					
17	Cyber Threat	3	3	9	High
18	Virus / malware	3	3	9	High
19	Kerusakan Perangkat TI non Server	3	2	6	High
20	Kerusakan Server	1	4	4	Mid

Tabel 7. Analisis dan Evaluasi Risiko

3.4 Penanganan Risiko (Risk Treatment)
Dari penilaian risiko di bab 3.3 dengan memperhatikan potensi dampak yang ditimbulkan, maka dapat diusulkan penanganan dari risiko yang ada, yaitu :

No	Nama Risiko	Penanganan Risiko
Alam / Lingkungan		
1	Gempa bumi	Disaster Recovery center untuk data center maupun ruang kerja pengelola LPSE
2	Banjir	
3	Angin	
4	Kebakaran	
5	Petir	
6	Wabah Penyakit / Pandemik	
Ulah Manusia		
7	Kebakaran	Kebijakan pelarangan rokok di lingkungan LPSE dan penguatan keamanan fisik dari Gedung operasional LPSE
8	Pencurian	
9	Vandalisme	
10	Terorisme	
11	Unjuk Rasa	
12	Kerusuhan	
Infrastruktur non IT		
13	Kerusakan bangunan	Maintenance secara teratur terutama untuk instalasi listrik dan AC
14	Listrik / AC rusak	
15	Kerusakan fasilitas non TI	
16	Krisis BBM	
Serangan TI		
17	Cyber Threat	Penerapan standar keamanan informasi
18	Virus / malware	
19	Kerusakan Perangkat TI non Server	
20	Kerusakan Server	Backup / DRC

Tabel 8. Usulan Penanganan Risiko

4. Kesimpulan

Dari aktivitas risk asessment tersebut tampak bahwa risiko ancaman di bidang teknologi informasi sangatlah tinggi dan mempunyai dampak yang besar. Untuk itu prioritas strategi business continuity akan diprioritaskan untuk sektor TI utamanya sesuai fungsi LPSE dalam pengelolaan infrastuktur SPSE (Sistem Pengadaan Secara Elektronik)

Penelitian ini hanya terbatas pada layanan LPSE di Pemda DIY, akan lebih baik kalau diperbanyak penelitian seperti yang dilakukan saat ini, untuk layanan – layanan lain yang ada di Pemda DIY.

Ucapan Terima Kasih

Terima Kasih kepada dosen pembimbing Pak Lukito dan Pak Widyawan, pengelola LPSE DIY, Tim LEMTEIUI dan semua pihak yang membantu dalam proses penelitian ini.

Daftar Pustaka

"INTERNATIONAL STANDARD ISO 22301 - Societal security — Business continuity management systems — Requirements," vol. 2012, 2012.

"INTERNATIONAL STANDARD ISO 31000 - Risk Management – principles and guidelines, 2009.

I. S. O. Tc, "Societal security — Business continuity management systems — Guidance," 2012.

LKPP RI, Perka LKPP No.2 Tahun 2010 tentang LPSE, Jakarta, 2010

Sekretariat Negara RI, PP No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Republik Indonesia, 2012.

P. P. Ardhiatno, "Perancangan business ...., Prabowo Priyo Ardhiatno, Fasilkom UI, 2013," 2013.

T. Drewitt, *A Manager ' s Guide to ISO22301*. IT Governance Publisher, 2014.