MANAJEMEN RESIKO TEKNOLOGI INFORMASI I UNTUK KEBERLANGSUNGAN LAYANAN PUBLIK MENGGUNAKAN *FRAMEWORK INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY* (ITIL VERSI 3)

Irfan Maliki
Jurusan Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia
Jl. Dipatiukur no 112-116 Bandung 40132
Telp. (022) 2533825
E-mail: irfanmaliki007@gmail.com

ABSTRAKS
Kemajuan teknologi informasi dan komunikasi (TIK) serta meluasnya perkembangan infrastruktur informasi global telah mengubah pola dan cara beraktivitas pada organisasi, institusi, industri, maupun pemerintahan. Fakta semakin meningkatnya ketergantungan organisasi kepada TI untuk mencapai tujuan strategi dan kebutuhan organisasi menjadi pendorong utama pentingnya TIK. Begitupula pemanfaatan TIK di pemerintahan, sebagai upaya mengefisiensikan dan mengefektifkan penggunaan TI agar dapat memberikan pelayanan kepada publik dengan baik. Keberlangsungan layanan pada pelayanan publik merupakan salah satu hal yang perlu ditata kelola agar penyelenggaran pelayanan dapat terselenggara dengan baik sehingga masyarakat dan pengguna dapat terlayani sesuai dengan kebutuhannya. Manajemen resiko TI perlu dilakukan untuk mengurangi dan menanggulangi resiko-resiko yang mungkin terjadi. Manajemen resiko TI dan merencanakan strategi-strategi dalam keberlangsungan layanan TI harus dilakukan secara sistematis dan latihan yang terus menerus untuk meningkatkan dan memperbaiki proses layanan TI. Kerangka kerja ITIL versi 3 digunakan sebagai panduan dalam rangka menyusun langkah-langkah operasional agar keberlangsungan layanan TI dapat berfungsi dengan baik.

Kata Kunci: Manajemen resiko TI, ITIL, Tata kelola, Keberlangsungan, Layanan TI

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi (TIK) serta meluasnya perkembangan infrastruktur informasi global telah mengubah pola dan cara beraktivitas pada organisasi, institusi, industri, maupun pemerintahan. Fakta semakin meningkatnya ketergantungan organisasi kepada TI untuk mencapai tujuan strategi dan kebutuhan organisasi menjadi pendorong utama pentingnya TIK. Ketergantungan tersebut menyebabkan tumbuhnya kebutuhan akan layanan TI berkualitas tinggi yang mengikuti kebutuhan organisasi dan *user* yang sesuai dengan perkembangannya. Layanan TI berkualitas tinggi berarti meningkatkan efisiensi dan efektivitas penggunaan TI untuk memenuhi kebutuhan organisasi. Begitupula pemanfaatan TIK di pemerintahan.

Penyelenggaraan pemerintahan dalam rangka pelayanan publik memerlukan tata kelola yang baik (Permenkominfo, 2007). Dengan menerapkan tata kelola yang baik akan menjamin transparansi, efisiensi, dan efektivitas penyelenggaraan pemerintahan. Di sisi lain, penggunaan TIK oleh institusi pemerintahan sudah dilakukan sejak beberapa dekade lalu, dengan intensitas yang semakin meningkat. Dalam upaya memastikan penggunaan TIK tersebut benar-benar mendukung tujuan penyelenggaraan pemerintahan, dengan memperhatikan efisiensi penggunaan sumber daya dan pengelolaan risiko terkait dengannya, maka diperlukan tata kelola TI (Permenkominfo, 2007).

Kegiatan pelayanan publik tidak dapat terhindar dari adanya gangguan/kerusakan yang disebabkan oleh alam maupun manusia misalnya terjadinya gempa bumi, bom, kebakaran, banjir, *power failure*, kesalahan teknis, kelalaian manusia, demo buruh, huru-hara dan sebagainya. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi yang digunakan, tetapi juga berdampak pada kegiatan operasional pelayanan publik. Bila tidak ditangani secara khusus, selain akan menghadapi risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan publik. Oleh sebab itu perlu dilakukan pengelolaan terhadap risiko-risiko sehingga dapat mereduksi resiko yang mungkin muncul.

Untuk meminimalisasi resiko tersebut, setiap instansi pemerintah daerah diharapkan dapat menyusun langkah-langkah terpadu untuk menjamin keberlangsungan layanan agar tetap dapat berfungsi dengan baik terutama dalam penggunaan layanan TI.

Information Technology Infrastructure Library (ITIL) sebagai suatu kerangka kerja manajemen layanan TI dapat digunakan sebagai panduan dalam menyusun langkah-langkah operasional tersebut. Dengan kerangka kerja ITIL diharapkan resiko-resiko yang mungkin terjadi dapat diminimalisasi serta dapat dilakukan mitigasi resiko dalam upaya menjaga keberlangsungan layanan TI.

2. MANAJEMEN RESIKO TI

Resiko merupakan fungsi kemungkinan (*likelihood*) sumber ancaman (*threat-source*) mengeksploitasi kerentanan (*vulnerability*) potensial, yang menghasilkan dampak (*impact*) kejadian yang merugikan organisasi (Spremic, 2008). Menurut Spremic (2008), resiko-resiko yang terjadi pada pemanfaatan TI dapat memberikan dampak negatif terhadap aset TI (data, *software*, hardware), layanan-layanan TI, bisnis proses, serta organisasi secara keseluruhan. oleh sebab itu resiko tersebut perlu dikelola dengan baik.

Manajemen resiko TI merupakan proses identifikasi resiko, penilaian resiko, dan pengambilan langkah-langkah untuk menurunkan resiko sampai level yang dapat diterima (Stoneburner, 2002).

Sedangkan menurut IT governance, IT Audit dan IT Security (dalam Spremic, 2008), manajemen resiko TI adalah proses untuk memahami dan memberikan respon terhadap faktor-faktor yang dapat menyebakan kegagalan dalam autentikasi, *non-repudiation*, kerahasiaan, integritas atau ketersediaan dari sistem informasi.

Manajemen resiko TI bukanlah hal yang mudah. Merupakan hal penting untuk menjaga keseimbangan dalam proses manajemen resiko. Meskipun secara umum metode manajemen resiko untuk organisasi memiliki persamaan, namun memiliki resiko yang berbeda-beda sehingga diperlukan manajemen resiko secara khusus. Terkait dengan pemerintah yang memberikan layanan publik, dampak dari resiko dapat diukur tidak hanya secara ekonomi, namun juga pengaruh sosial.

Sesuai dengan kebijakan yang tertuang didalam Permenkominfo no 41 tahun 2007, bahwa dalam rangka melakukan tata kelola TI oleh institusi pemerintahan perlu dilakukan manajemen resiko yang mencakup resiko proyek, resiko atas informasi, dan resiko atas keberlangsungan layanan (Permenkominfo, 2007).

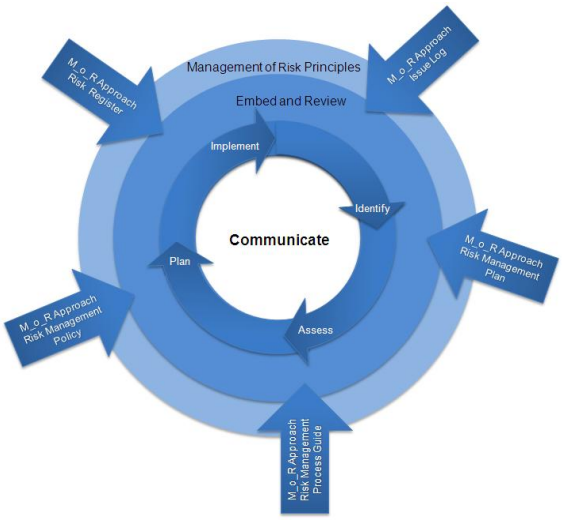
2.1 Perencanaan Manajemen Resiko TI

Menurut Spremic (2008) untuk keberhasilan dalam menjaga segala sesuatu yang dapat menyebabkan permasalahan, setiap organisasi harus membangun metode dan teknik untuk mengendalikan insiden-insiden yang terjadi pada TI dan untuk mengidentifikasi resiko yang mungkin terjadi. Terdapat tahapan-tahapan penting dalam perencanaan manajemen resiko TI:

1. Identifikasi dan klasifikasi resiko TI,
2. Penilaian resiko TI (*Business Impact Analysis*) dan menentukan prioritas,
3. Strategi penanggulangan resiko TI – identifikasi pengendalian TI,
4. Implementasi dan dokumentasi dari penanggulangan resiko (pengendalian TI),
5. Pendekatan portofolio resiko TI dan keselarasan dengan strategi bisnis,
6. Pengawasan berkala terhadap tingkat resiko TI dan audit.

2.2 Kerangka Kerja Manajemen Resiko TI

Management of Risk (M_o_R) merupakan metodologi standar yang dapat digunakan untuk manajemen resiko TI serta menilai resiko di organisasi (OGC, 2007). Pada gambar 1 merupakan kerangka kerja M_o_R.



Gambar 1. *Framework Management of Risk*

Berikut ini merupakan penjelasan dari gambar di atas:

Prinsip M_o_R – prinsip-prinsip tersebut merupakan esensi dalam pengembangan praktik manajemen resiko yang baik dan diturunkan dari prinsip-prinsip tatakelola perusahaan (*corporate governance*).

Pendekatan M_o_R – pendekatan organisasi untuk prinsip-prinsip tersebut dibutuhkan untuk mendefinisikan dan persetujuan dalam dokumen berikut:

a. Kebijakan manajemen resiko
b. Panduan proses
c. Perencanaan
d. Registrasi resiko
e. Permasalahan log

Proses M_o_R – berikut ini menjelaskan empat tahapan aktivitas dalam manajemen resiko:

a. Identifikasi – ancaman dan peluang dalam aktivitas yang dapat mempengaruhi kemampuan dalam mencapai tujuan

b. Menilai – pemahaman *net effect* dari identifikasi ancaman dan peluang aktivitas yang dilakukan.

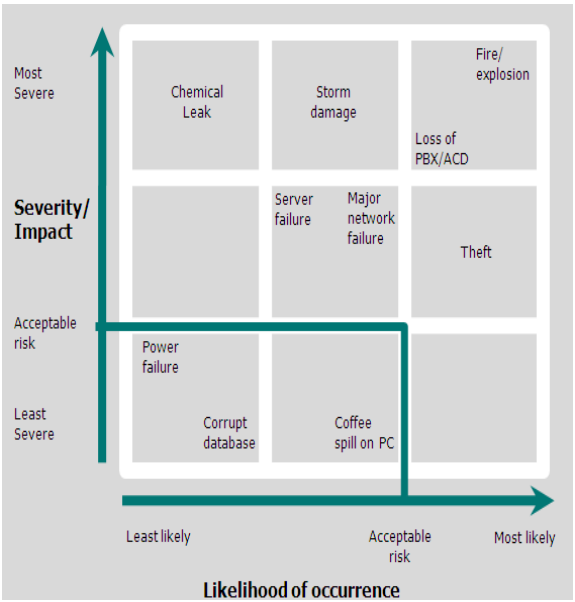
c. Merencanakan – mempersiapkan tanggapan manajemen secara spesifik yang dapat

mengurangi ancaman dan memaksimalkan peluang.

d. Implementasi – penerapan rencana manajemen resiko, mengawasi efektivitas dan mengambil langkah yang diperlukan dalam menanggulangi ekspektasi yang tidak sesuai.

***Embedding* dan *reviewing* M_o_R** – diperlukan *review* keberlanjutan dan peningkatan bahwa hal tersebut masih baik untuk digunakan

Komunikasi – diperlukan aktivitas komunikasi yang tepat dalam menjamin bahwa setiap orang tetap *up to date* dengan perubahan dalam ancaman, peluang dan seluruh aspek manajemen resiko.



Gambar 2. Profil Resiko Layanan TI

Tabel 1. Resiko dan Ancaman pada layanan TI

Resiko	**Ancaman**
Kerusakan internal sistem/jaringan TI PABX, ACD, dll.	Kebakaran, listrik padam, vandalisme, kebanjiran, tabrakan pesawat, cuaca buruk, angin topan, bencana alam, ancaman teroris, sabotase, kerusakan tidak sengaja, software kualitas rendah.
Kerusakan eksternal sistem/jaringan IT, seperti *server e-commerce*, sistem kriptografi, dll.	Semua yang diatas, permintaan yang berlebihan untuk layanan-layanan, Denial of service attack (DOS), kesalahan teknis.
Kehilangan data	Kesalahan tekniks, kesalahan manusia, virus, serangan, trojan, *malicious program*
Kehilangan layanan-layanan jaringan	Kerusakan atau kegagalan akses ke penyedia layanan jaringan, kerugian dari sistem/jaringan penyedia layanan TI, kerugian dari penyedia layanan data, kegagalan dari penyedia layanan
Ketidaktersediaan staf teknik dan pendukung	Aksi pemogokan, pelanggaran perjanjian kerja, pengunduran diri, sakit/cedera, kesulitan transportasi
Kegagalan dari penyedia layanan, contohnya *outsourcing* TI.	Kegagalan komersil, pelanggaran perjanjian, staf penyedia layanan yang tidak tersedia, kegagalan memenuhi SLA

Metode M_o_R membutuhkan evaluasi terhadap resiko dan pengembangan profil resiko, seperti pada gambar 2.

Pada gambar 2 tersebut menunjukan contoh profil resiko, berisi resiko-resiko yang diluar dari definisi resiko yang dapat terjadi. Pada tabel 1 menjelaskan rincian dari resiko-resiko dan ancaman-ancaman yang mungkin terjadi pada layanan TI.

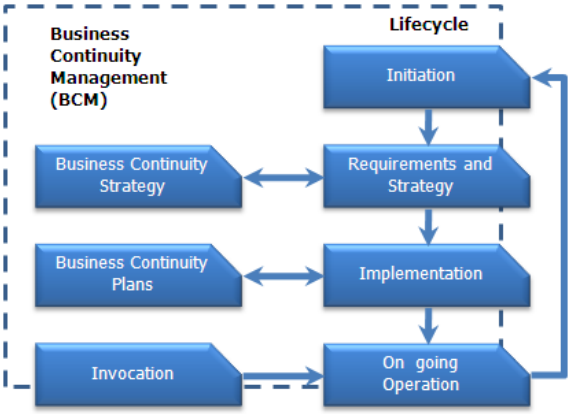
2.3 *Information Technology Service Continuity Management* (ITSCM)

ITSCM merupakan salah satu proses area dari *service design* ITIL versi 3. Tujuan dari ITSCM adalah untuk mendukung seluruh proses manajemen keberlangsungan bisnis dengan memastikan bahwa kebutuhan teknis TI dan fasilitas layanan (termasuk sistem komputer, jaringan, aplikasi, *data repositories*, telekomunikasi, lingkungan, dukungan teknis dan *service desk*) dapat kembali beroperasi dan sesuai dengan *timescale* bisnis.

Sasaran dari ITSCM diantaranya adalah untuk :

a. Memelihara rencana-rencana berkelanjutan layanan TI (*IT service continuity plans*) dan rencana-rencana pemulihan TI yang mendukung kelanjutan bisnis
b. Melengkapi *exercise business impact analysis* (BIA) secara teratur untuk menjamin seluruh rencana-rencana berkelanjutan dikelola agar selaras dengan dampak perubahan dan kebutuhan bisnis
c. Menyediakan panduan dan saran untuk seluruh area bisnis dan TI yang berkaitan dengan kelanjutan dan pemulihan
d. Memastikan mekanisme yang tepat untuk kelanjutan dan pemulihan agar sesuai dengan tujuan kelanjutan bisnis
e. Menilai dan dampak perubahan pada rencana-rencana kelanjutan layanan TI dan rencana-rencana pemulihan TI
f. Memastikan bahwa ketersediaan layanan diimplementasikan sesuai dengan anggaran yang ditetapkan

Pada gambar 3 merupakan siklus hidup dari ITSCM.



Gambar 3. Siklus hidup ITSCM
(Sumber : Service Design – ITIL ver 3)

Pada makalah ini hanya akan membahas tahapan awal dalam siklus ITSCM yaitu tahap inisiasi serta menentukan kebutuhan dengan melakukan penilaian dan analisis resiko serta merancang strategi-strategi untuk keberlangsungan layanan TI.

3. IMPLEMENTASI

3.1 Tahap Inisialisasi

Pada tahap ini dilakukan aktivitas-aktivitas sebagai berikut:

a. **Penentuan kebijakan** – hal ini harus dibangun dan dikomunikasikan sehingga semua orang yang ada di organisasi dapat terlibat. Dalam kebijakan ini ditentukan sasaran serta fokus dari manajemen. Peran dari pimpinan sangat menentukan keberhasilan dari kegiatan yang dilaksanakan.
b. **Lingkup** – pada tahap ini ditentukan lingkup serta tanggungjawab dari setiap staf yang ada diorganisasi. Kewenangan dan tanggungjawab dari setiap staf disesuaikan dengan kemampuan dan kapabilitas yang dimilikinya, agar mendukung terhadap setiap kegiatan yang akan dilaksanakan.
c. **Alokasi Sumberdaya** – keberlangsungan dari bisnis membutuhkan sumberdaya diantaranya uang dan sumberdaya manusia. Hal ini sangat penting untuk mendukung kelangsungan dari proses. Penentuan alokasi sumberdaya dengan tepat dapat mengefisiensikan kinerja yang dilakukan.
d. **Struktur pengendali dan Organisasi Proyek** – kegiatan yang dilakukan perlu diorganisir dan dikendalikan dengan baik, karena kegiatan yang bersifat kompleks sehingga perlu dilakukan langkah-langkah sistematis dan terkendali.
e. **Perencanaan dan Proyek yang berkualitas** – perencanaan yang baik dapat menjamin keberhasilan pencapaian kualitas kegiatan. Setiap kegiatan yang akan dilaksanakan perlu direncanakan dengan matang agar hasil yang diperoleh dapat dimaksimalkan serta meminimalisasi resiko-resiko yang terjadi.

3.2 Tahap Kebutuhan dan Strategi

3.2.1 Analisis Resiko

Pada tahap ini menilai level resiko dan membuat ranking resiko dengan mempertimbangkan faktor kecenderungan (*likelihood*) dan besarnya dampak resiko (*impact*). Pada proses penilaian ini memanfaatkan kerangka kerja *Management of Risk (M_o_R)*. Pendekatan analisa resiko dapat secara kualitatif atau kuantitatif. Level kecenderungan dan dampak dapat dikategorikan sesuai variasi yang ada, misalnya menjadi tinggi, sedang dan rendah.

Pada tabel 2 dapat dilihat hasil dari analisis resiko yang telah dilakukan.

3.2.2 Strategi Keberlangsungan Layanan TI

Setelah mengetahui resiko-resiko yang terjadi serta prioritas yang harus dilakukan dari hasil analisis resiko maka dapat dirancang strategi-strategi untuk keberlangsungan layanan TI. Pada tabel 3 dapat diperlihatkan strategi-strategi yang dapat dilakukan dalam rangka keberlangsungan layanan TI.

Tabel 2. Analisis Resiko Layanan TI

Sumber Resiko	Resiko	Kecenderungan (likelihood)	Dampak	Tingkat Resiko	Prioritas
Sumber resiko alami	Software, hardware, dan data dalam sistem TI dirusak atau tidak berfungsi karena bencana alam misal banjir, gempa, kebakaran, dan lain-lain	Rendah	Sangat tinggi	Tinggi	7
Sumber resiko manusia	Kesalahan operasional	Tinggi	Sedang	Tinggi	4
	Intended attack	Sedang	Tinggi	Tinggi	6
	Akses tidak terautorisasi	Sedang	Tinggi	Tinggi	6
	Infeksi virus komputer	Tinggi	Sangat tinggi	Sangat tinggi	2
Sumber resiko lingkungan	Kegagalan jaringan	Rendah	Tinggi	Sedang	8
	Kegagalan power	Sedang	Sangat tinggi	Tinggi	5
	polusi	Rendah	Sedang	Rendah	9
Spesifik sistem	Analisa historis log; data dari penyedia sistem mengenai insiden yang terjadi untuk pengguna lain	Tergantung pada pengguna			

Sumber Resiko	Resiko	Kecenderungan (likelihood)	Dampak	Tingkat Resiko	Prioritas
	dari sistem yang sama				
Resiko yang terkait dengan proses bisnis	Kesalahan memilih penyedia sistem	Rendah	Sangat tinggi	Tinggi	7
	Dukungan yang tidak cukup dari penyedia sistem	Tinggi	Sedang	Tinggi	4
	Backup yang tidak cukup	Tinggi	Tinggi	Tinggi	3
	Analisis dan record log yang tidak lengkap	Tinggi	Tinggi	Tinggi	3
	Tidak terlatih	Sedang	Tinggi	Tinggi	6
	Komunikasi antara departemen TI dan departemen lain	Sangat tinggi	Tinggi	Sangat tinggi	1

Tabel 3 Strategi Keberlangsungan Layanan TI

Sumber Resiko	Resiko	Strategi Keberlangsungan Layanan TI
Sumber resiko alami	Software, hardware, dan data dalam sistem TI dirusak atau tidak berfungsi karena bencana alam misal banjir, gempa, kebakaran, dan lain-lain	Membuat sistem backup Back up data secara berkala
Sumber resiko manusia	Kesalahan operasional	Pelatihan yang cukup, peningkatan tanggungjawab staf, pemahaman penggunaan sistem
	Intended attack	Pengecekan titik-titik yang bisa diserang, dan perbaiki. Menggunakan enkripsi data pada database atau data transfer
	Akses tidak terautorisasi	Gunakan metode pengecekan yang lebih aman, misal password dinamis, pengecekan pengguna, menghapus pengguna yang tidak berhak mengakses data
	Infeksi virus komputer	Sediakan antivirus dan lakukan update database antivirus. Lakukan restorasi dan backup data
Sumber resiko lingkungan	Kegagalan jaringan	Gunakan sistem jaringan duplikat, konfigurasi secara automatis
	Kegagalan power	Gunakan lebih dari satu power supply
	polusi	Lakukan backup sistem. Pengendalian sistem secara remote
Spesifik sistem	Analisa historis log; data dari penyedia sistem mengenai insiden yang terjadi untuk pengguna lain dari sistem yang sama	Pelajari dari pengguna lain untuk sistem yang sama. Analisa hasil pengujian sistem
Resiko yang terkait dengan proses bisnis	Kesalahan memilih penyedia sistem	Gunakan penyedia proses yang tepat, cari penyedia yang kompetitif
	Dukungan yang tidak cukup dari penyedia sistem	Buat SLA untuk seluruh sistem yang penting dan jaga kualitas layanan
	Backup yang tidak cukup	Backup regulasi secara berkala
	Analisis dan record log yang tidak lengkap	Buat regulasi log secara berkala dan laporkan.
	Tidak terlatih	Buat program pelatihan sistem untuk staf terkait
	Komunikasi antara departemen IT dan departemen lain	Buat hubungan yang baik antar departemen.

4. PENUTUP

Keberlangsungan layanan pada pelayanan publik merupakan salah satu hal yang perlu ditata kelola agar penyelenggaran pelayanan dapat terselenggara dengan baik sehingga masyarakat dan pengguna dapat terlayani sesuai dengan kebutuhannya. Manajemen resiko TI dan merencanakan strategi-strategi dalam keberlangsungan layanan TI harus dilakukan secara sistematis dan latihan yang terus menerus untuk meningkatkan dan memperbaiki proses layanan TI. Keberhasilan dari proses ini tentunya harus didukung oleh semua pihak agar tujuan yang diharapkan dapat terlaksana dengan baik.

PUSTAKA

Blokdijk, G., Engle, C., and Brester, J. (2008). *IT Risk Management Guide Risk Management Implementation Guide, Presentations, Blueprints, Templates; Complete Risk Management Toolkit Guide for Information Technology Processes and Systems*, The Art of Service.

Helgesson, and Li, Y. Y. (2009). Managing Risks on Critical IT Systems in Public Service Organizations. *International Conference on Computational Science and Engineering. IEEE*

Information Technology Service Management Forum (ITSMF). (2007). *An Inftroductory Overview of ITIL ® V3*, ITSMF ltd.

ITGI. (2009). *Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft*, IT Governance Institute

Office of Government Commerce (OGC). (2007). *ITIL version 3 Service Design*, Best Management Practice

Office of Government Commerce (OGC). (2007). *ITIL version 3 Continual Service Improvement*, Best Management Practice

Permenkominfo. (2007). *Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi*

Nasional, Departemen Komunikasi dan Informasi

Spremic, M., and Popovic, M., (2008). Emerging issues in IT Governance: Implementing the Corporate IT Risk Management Model, *WSEAS Transacions on Systems, issues 3 Volume 7*.

Stoneburner, G., Goguen, A., and Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology (NIST).

Widodo, J. (2001). *Good governance Telaah dari Dimensi Akuntabilitas dan Kontrol Birokrasi pada Era Desentralisasi dan Otonomi Daerah*. Insan Cendekia, Surabaya