Model dan Simulasi Audit Teknologi Informasi Studi Kasus Penerapan TI di DJPK Kemenkeu

Suprayitno
Politeknik Keuangan Negara STAN
suprayitno@pknstan.ac.id

Abstrak

Tujuan *Penelitian ini bertujuan untuk melakukan simulasi pelaksanaan audit atas penerapan teknologi informasi.*
Desain/Metode *Adapun metode pada penelitian ini menggunakan simulasi audit dengan studi kasus atas penerapan TI suatu organisasi yaitu pada Dijten Perimbangan Keuangan, dengan data primer dan sekunder yang dikumpulkan melalui pengamatan, wawancara, konfirmasi, penelusuran dokumentasi organisasi.*
Temuan *Berdasarkan simulasi hasil audit TI pada DJPK, didapati bahwa secara umum sistem pengendalian internal organisasi cukup bagus dalam menyelaraskan TI organisasi sesuai dengan strategi bisnis organisasi. Namun demikian masih terdapat beberapa temuan yang perlu tindak lanjut manajemen organisasi seperti lemahnya kesadaran pengawasan atas penggunaan sumber daya TI organisasi, masih lemahnya SDM organisasi atas kesadaran pemanfaatan TI, dan kelemahan manajemen keamanan informasi organisasi.*
Implikasi *Hasil penelitian ini dapat dipergunakan untuk oleh para akademisi sebagai bahan kajian/perbandingan untuk mengembangkan metode dan teknik audit TI. Selain itu dapat juga dimanfaatkan oleh praktisi/auditor sebagai rujukan untuk melakukan audit atas penerapan TI pada organisasi.*
Originalitas *Simulasi pada penelitian ini menggunakan data dan fakta yang diperoleh dari sumber langsung objek penelitian.*
Tipe Penelitian *Simulasi dan Studi Kasus*

Kata Kunci *: Audit, Audit TI, Teknologi Informasi, TI, Sistem Pengendalian Internal, CAATs*

I. Pendahuluan

Perkembangan teknologi informasi (TI) dewasa ini bergerak ke seluruh sektor kehidupan. Mulai dari sektor kehidupan sehari-hari dimana manusia tinggal dan berinteraksi dengan masyarakat. Berbagai kebutuhan hidup manusia pun tidak lepas dari penetrasi kemajuan TI yang menembus batas-batas teritorial, negara, suku bangsa hingga mempengaruhi cara-cara manusia berinteraksi satu sama lain. Salah satu pendorong perkembangan TI adalah munculnya Internet, yang mempengaruhi pola komunikasi dan pertukaran informasi baik pada sektor formal maupun informal.

Berbagai kegiatan perekonomian yang meliputi industri dan perdagangan, jasa dan transportasi, pertanian, dan bahkan kegiatan pendidikan, olah-raga, hiburan mulai memanfaatkan perkembangan Internet, sebagai bagian dari operasional mereka sehari-hari. Tidak pula ketinggalan organisasi pemerintahan pun juga memanfaatkan teknologi berbasis jaringan tersebut pada organisasi dalam rangka memberikan layanan kepada masyarakat.

Bukan hal yang asing lagi, saat ini penggunaan TI telah menjadi bagian dari keunggulan kompetitif perusahaan. Mihalic dan Buhalis (2013) mengutip (Namasivayam, Enz, & Siguaw, 2000; Porter, 2001; Sirirak, Islam, Khang, 2011) menyimpulkan bahwa saat ini banyak peneliti mengklaim bahwa TI dan terutama Internet dapat menciptakan keunggulan daya saing dan meningkatkan kinerja.

Berkenaan dengan pemanfaatan TI pada organisasi, Turban dan Volonino (2011) mengungkapkan bahwa terdapat dua perhatian dan risiko terbesar bagi manajemen puncak perusahaan, yaitu kegagalan dalam menyelaraskan TI dan kebutuhan bisnis real, kegagalan menghantarkan suatu nilai bagi bisnis. Mengingat TI dapat berperan penting pada kinerja bisnis dan daya saing, kegagalan dalam mengelola TI secara efektif berdampak serius pada bisnis secara keseluruhan.Lebih lanjut Turban dan Volonino (2011) menguraikan bahwa organisasi mengembangkan perencanaan dan strategi TI yang mendukung tujuan dan strategi bisnis perusahaan, dengan empat aspek pokok rencana strategis TI yang meliputi:

a) Memperbaiki pemahaman manajemen atas peluang dan keterbatasan TI;
b) Melakukan penilaian kinerja saat ini;
c) Mengidentifikasi kapasitas dan kebutuhan sumber daya manusia;
d) Memperjelas tingkat investasi yang diperlukan.

Demikian pula sebagaimana dipaparkan Hong (2009) bahwa perencanaan strategis TI harus mencerminkan kebutuhan bisnis, sehingga menyelaraskan strategi TI dengan perencanaan bisnis merupakan hal yang penting dalam rangka membantu bisnis mencapai tujuannya melalui solusi-solusi berbasi TI.

Berkenaan dengan pencapaian tujuan-tujuan pemanfaatan TI dalam strategi bisnis organisasi, perlu kepastian pencapaian tujuan tersebut. Dalam rangka memberikan kepastian bahwa strategi TI berjalan selaras dengan bisnis organisasi, diperlukan audit dalam rangka menguji apakah praktik-praktik penggunaan TI dalam organisasi telah sesuai dengan standar, pedoman, atau dokumentasi proses bisnis yang telah dirancang organisasi.

Berkaitan dengan audit, Kim, Teo, Bhattacherjee, Nam (2015) mengutip (DeFond and Zhang, 2014) bahwa suatu audit akan bernilai atas kemampuannya menyajikan keyakinan yang memadai atas kredibilitas informasi, sehingga dapat memperbaiki alokasi sumber daya dan efisiensi yang ditetapkan. Sementara itu Dowling (dalam Tsai, Chen, Chang, dan Lee, 2017) menyatakan bahwa riset sebelumnya menunjukkan bahwa TI memainkan peran penting dalam memproses dan melakukan evaluasi informasi akuntansi. Tsai et al. mengemukakan bahwa keahlian auditor internal dan kapabilitas TI (misalnya software audit dan sistem ERP) biasanya dianggap menguntungkan atas pengendalian risiko, biaya pemeliharaan dan pekerjaan audit, sehingga pada akhirnya berdampak pada kinerja auditor internal.

Dengan demikian, kebutuhan untuk melaksanakan audit atas TI yang dimiliki organisasi merupakan hal yang tidak bisa diabaikan, mengingat keberhasilan pencapaian target dan sasaran organisasi dewasa ini juga tidak bisa dipisahkan dari pengelolaan TI yang memadai dan mencapai sasaran organisasi.

Pada penelitian ini bertujuan untuk melakukan simulasi audit TI dengan studi kasus penerapan TI di lingkungan Direktorat Jenderal Perimbangan Keuangan, Kemenkeu, dalam rangka mendapatkan gambaran umum penerapan TI beserta aspek-aspek terkait dengan sistem pengendalian internal organisasi.

II. KajianTeori

A. Konsep Audit TI

Arens dan Loebbecke (1991) mendefinisikan auditing sebagai sebuah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan oleh seorang yang kompeten dan independen dalam

rangka menentukan dan melaporkan kesesuian informasi yang dihasilkan dengan kriteria yang ditetapkan.

Sementarai itu definisi audit menurut ISACA (2013) adalah sebagai sebuah inspeksi formal dan verifikasi untuk melakukan pengujian apakah sebuah standar atau panduan diikuti, catatan-catatan akurat, atau target efisiensi dan keefektifan dipenuhi. Amnah (2014) mengutip (Hall and Singleton, 2007) bahwa audit secara umum adalah proses sistematis mengenai mendapatkan dan mengevaluasi secara objektif bukti-bukti yang berkaitan dengan penilaian berbagai kegiatan dan peristiwa untuk memastikan tingkat kesesuaian antara penilaian-penilaian tersebut dan membentuk kriteria serta menyampaikan hasilnya ke para pengguna yang berkepentingan.

Suatu audit strategis atas TI hendaknya dijalankan dengan arah tujuan utama untuk memastiakn bahwa sumber daya TI organisasi digunakan untuk mendukung tujuan-tujuan bisnis organisasi dan sumber daya TI organisasi tersebut hendaknya dipertimbangkan sebagai sebuah risiko bagi suatu organisasi jikalau kegagalannya berdampak pada pencapaian tujuan organisasi. Adapun langkah awal pada perencanaan dan pelaksanaan audit strategi TI adalah mendefinisikan dan mengevaluasi tujuan organisasi, strategi, model bisnis pokok dan peran TI dalam mendukung bisnis (Ackerman et al., 2009).

Ratanasongtham dan Ussahawanitchakit (2015) mengutip (KosmalaMacLullich, 2003), bahwa dalam suatu lingkungan kerja audit, perencanaan audit menjadi kegiatan utama yang dilakukan oleh auditor dalam rangka mencapai keefektifan laporan audit, mendapatkan kinerja audit dan meningkatkan keberhasilan audit. Perencanaan audit dirancang untuk memungkinkan auditor melaksanakan dan mengevaluasi risiko bisnis dan mengembangkan lingkup dan program audit tertentu untuk pengujian pada proses audit.

B. Audit dan Tujuan TI

Perkembangan TI yang telah memasuki ke hampir seluruh pola interaksi masyarakat, saat ini hampir seluruh sektor organisasi komersial maupun publik termasuk pemeritahan telah mengadopsi berbagai pemanfaatan TI pada kegiatan operasional proses bisnis organisasi. Kondisi tersebut mempengaruhi pula cara-cara auditor melakukan audit atas sumber daya TI perusahaan.

Sebagaimana juga dinyatakan oleh Mahzan dan Veerankutty (2011) bahwa perkembangan teknologi komputer yang semakin canggih, banyak organisasi pemerintahan yang semakin progresif bergantung pada sistem informasi berbasis komputer dalam rangka menjalankan operasional dan melakukan pemrosesan, pengelolaan, dan melaporkan informasi yang penting. Sehingga hal tersebut telah mengubah secara signifikan peningkatan organisasi dan prosedur akuntansi klien dan sistem pengendalian intern (SPI).

Rancangan audit hendaknya melibatkan struktur definitif yang memungkinkan melakukan penilaian terhadap hubungan fungsional TI dengan tujuan bisnis pokok organisasi. Selanjutnya perencanaan audit atas TI dibangun melalui empat tahapan, yaitu memahami bisnis, mendefinisikan lingkungan TI, melaksanakan penilaian risiko, dan memformalkan rencana audit (Ackerman et al., 2009).

Kebanyakan audit, termasuk audit TI dilaksanakan dengan pendekatan berbasis risiko, dimana risiko potensial diidentifikasi dan diprioritaskan, mekanisme pengendalian dinilai, dan pengendalian diuji. Adapun kegiatan dan prosedur yang dilaksanakan selama audit TI adalah mereview dokumentasi proses bisnis, mengevaluasi pengendalian yang melekat pada aplikasi seperti ERP, menguji interface sistem, review log audit pemrosesan transaksi, dsb (Merhout dan Havelka, 2008).

Berkenaan dengan proses audit, *the International Organisation of Supreme Audit Institutions* (INTOSAI) melalui publikasi standar audit internasional (ISSAI) nomor 100 tentang *Fundamental Principles of Public-Sector Auditing* membagi tiga proses audit utama, yaitu perencanaan audit, pelaksanaan audit, dan pelaporan serta tindak lanjut. Berkenaan dengan

perencanaan audit, INTOSAI menekankan prinsip bahwa auditor hendaknya mendapatkan pemahaman tentang sifat enttias/program yang akan diaudit, termasuk melaksanakan penilaian risiko atau analisis permasalahan. Identifikasi risiko-risiko dan pengaruhnya terhadap audit harus dipertimbangkan selama proses audit (INTOSAI, 2013).

Gheorghe (2010) berkenaan dengan identifikasi risiko tata kelola TIK, melalui hasil riset atas rancangan metode audit, mengusulkan 7 (tujuh) domain utama yang perlu dilakukan penilaian risiko, yaitu proses perencanaan strategis TI, manajemen organisasi TI, manajemen investasi TI dan proses pelayanannya, manajemen proyek TI, manajemen risiko TI, proses kinerja TI, dan ketaatan terhadap hukum. Melalui analisis dan penilaian ketujuh domain tersebut memberikan bekal bagi auditor TI opini tentang tingkat keselarasan antara strategi TI dan strategi bisnis dalam rangka melakukan mitigasi risiko TI dan manajemen sumber daya TI.

Berkaitan dengan lingkungan organisasi yang didukung dengan sistem informasi komputer, Ikatan Akuntan Indonesia juga menerbitkan Pernyataan Standar Audit (PSA) No.59 tentang Teknik Audit Berbantuan Komputer (TABK). Melalui PSA 59 tersebut diatur pedoman yang dapat dipergunakan oleh auditor untuk melakukan audit dengan bantuan komputer atau biasa dikenal dengan *Computer Assisted Audit Techniques* (CAATs) (Ikatan Akuntan Indonesia, 2001).

Adapun terkait penggunaan CAATs, Gorham and Lamont (1998) sebagaimana dikutip Mahzan dan Veerankutty (2011) menyatakan bahwa salah satu area pemrosesan audit yang sangat dinamis adalah penggunaan *Computer Assisted Auditing Tools and Techniques* (CAATTs). Hall dalam (Mahzan dan Veerankutty, 2011) menyatakan bahwa CAATTs merupakan piranti dan teknik yang digunakan untuk melakukan pengujian secara langsung logika internal aplikasi, termasuk secara tidak langsung untuk menyimpulkan tentang logika aplikasi.

Kacanski (2016) menguraikan hasil riset (Abdolmohammadi & Usoff, 2001; Banker, Chang, & Kao, 2002; Janvrin, Bierstaker, & Lowe, 2008, Elliot, Kielich, & Marwick, 1985) bahwa selama satu dekade terakhir, arus riset membincangkan mengenai peran dan pengaruh Teknologi Informasi dan Komunikasi (TIK) yang berimbas pada profesi audit dan auditor sebagai pengemban profesi. Pada sisi yang lain, banyak perusahaan audit yang mulai melirik TIK untuk meningkatkan efisiensi kerja dan kualitas laporan audit, yang dipergunakan sebagai piranti untuk menghasilkan keuntungan yang lebih besar dengan memperpendek durasi penugasan dan memberi layanan kepada lebih banyak klien pada suatu waktu.

Sebagaimana audit keuangan, tujuan audit atas TI adalah dalam rangka efisiensi dan keefektifan kinerja operasional, ketaatan terhadap regulasi dan perundang-undangan, kewaspadaan, dan implikasi pelaporan keuangan (Singleton, 2012). Sementara itu Popa (2011) berkenaan dengan audit, mengutip (SANS Institute, 2007) bahwa konsep audit lebih menekankan pada evaluasi atas pengendalian dan proses suatu organisasi, dimana evaluasi dilakukan atas standar atau proses yang terdokumentasi, sehingga hasilnya berupa penilaian yang independen atas evaluasi suatu sistem atau proses.

III. Metode Penelitian

Metode penelitian yang dipergunakan pada tulisan ini adalah menggunakan metode studi kasus. Adapun jenis data yang dipergunakan dalam penulisan berupa data primer yang dikumpulkan melalui pengamatan fisik, konfirmasi dan wawancara, beserta pengumpulan kuesioner yang dilakukan melalui dokumentasi kertas kerja audit (KKA).

Selain itu data sekunder dikumpulkan melalui pencarian literatur terkait teori yang relevan, data berkaitan dengan studi kasus yaitu fakta penerapan TIK pada Ditjen Perimbangan Keuangan. Beberapa dokumen sumber organisasi seperti struktur organisasi, proses bisnis, penerapan TIK dikumpulkan dengan teknik prosedur audit berbasis TIK, untuk selanjutnya dipergunakan sebagai bahan evaluasi dan analisis audit.

IV. Hasil dan Pembahasan

A. Standar dan Panduan Audit Teknologi Informasi dari ISACA

1) Pembuatan *Audit Charter/Engagement Letter*

Langkah pertama melakukan audit adalah membuat sebuah *audit charter* atau disebut juga *engagement letter* (untuk personal) yang merupakan sebuah surat penugasan untuk melaksanakan audit yang ditandatangani oleh pejabat dengan level yang sesuai. Dalam charter ini disebutkan secara jelas mengenai 4 (empat) aspek, yaitu:

a) Tujuan
Hal-hal yang diperhatikan dalam tujuan audit antara lain peran, sasaran, pernyataan misi, lingkup dan *objectives*.

b) Tanggungjawab
Tanggungjawab ini menyangkut prinsip-prinsip operasi, independensi auditor, hubungan dengan audit eksternal, persyaratan (*requirements*) dari *Auditee*, Faktor penentu kesuksesan (*Critical success factors*),Indikator Kinerja Utama (*Key performance indicators*), Manajemen Resiko dan ukuran kinerja lainnya.

c) Otoritas
Aspek yang dipertimbangkan dalam otoritas antara lain hak untuk mengakses informasi, personel, lokasi dan sistem yang berkaitan dengan audit, lingkup dan batasan, fungsi yang akan diaudit, harapan (expectations) Auditee, Struktur Organiasi termasuk Garis pelaporan dan Pemeringkatan staf audit.

d) Akuntabilitas
Dalam akuntabilitas aspek yang dipertimbangkan antara lain garis pelaporan kepada manajemen senior, penilaian kinerja penugasan, penilaian kinerja personal, hak auditee, review kualitas secara independen, penilaian ketaatan terhadap standar, *benchmarking* kinerja dan fungsi,Penilaian penyelesaian rencana audit, pembandingan anggaran dan biaya aktual, kesepakatan aksi misalnya sanksi kegagalan pemenuhan tanggungjawab

2) Perencanaan Audit

Tahap selanjutnya dibuat Perencanaan untuk Audit. Tapi sebelumnya ada aktivitas yang berhubungan dengan perencanaan audit yaitu aktivitas prosedur sehubungan dengan relasi dengan klien, evaluasi kepatuhan persyaratan etika dan memahami penugasan (*engagement*). Perencanaan audit meliputi strategi audit, memahami organisasi yang diaudit, menetapkan aspek materialitas dalam pelaksanaan audit nantinya, *risk assessment*, evaluasi pengendalian internal. Dalam pelaksanaannya rencana audit ini disupervisi dan dilakukan perubahan apabila diperlukan, serta didokumentasikan dengan baik.

3) Pelaksanaan Audit

Pengumpulan bukti dilaksanakan dengan metode sampling. Untuk penentuan besarnya sample yang dites, sebelum mulai mengumpulkan bukti pertama-tama terlebih dahulu dilakukan penilaian terhadap Pengendalian Internal. Apabila Pengendalian Internal dianggap tidak dapat diandalkan maka dilakukan tes yang luas terhadap sistem yang diaudit. Apabila pengendalian internal dinilai cukup baik maka dilakukan tes terhadap operasional pengendalian internal.

Apabila ternyata operasionalnya tidak baik maka pengendalian internal dianggap tidak dapat diandalkan dan dilakukan tes yang luas dengan ukuran sampel yang besar.Namun apabila operasional pengendalian internalnya baik maka tes yang dilakukan dapat dibatasi tidak terlalu luas dengan jumlah sampel yang lebih kecil.

Contoh pengendalian yang dinilai antara lain Implementasi software terpaket, Parameter sistem keamanan, rencana *disaster recovery*, validasi input data, adanya laporan eksepsi, dan pengelolaan akun pengguna. Penilaian dilakukan dengan observasi, wawancara,

review dokumentasi yang relevan dan menggunakan bantuan *tools computer*. Selanjutnya dilaksanakan pengumpulan bukti (*evidence*). Proses ini dapat dilaksanakan dengan menggunakan tehnik audit dengan berbantuan computer (TABK/(CAATs). Kegiatan yang dilakukan antara lain Tes atas detil transaksi dan saldo, prosedur review analisis,tes kepatuhan atas pengendalian sistem, tes kepatuhan pengendalian aplikasi sistem informasi dan *penetration testing.*

4) Pelaporan

Setelah proses pencarian bukti audit dijalankan, hasil dari audit dilaporkan kepada pihak yang berhak sesuai penugasan. Laporan ini menyatakan temuan audit, Kesimpulan, Rekomendasi dan batasan terkait audit yang dilaksankan.

5) Tindak Lanjut (*Follow Up*)

Dalam waktu yang ditentukan setelah penyampaian laporan audit dan rekomendasi, dilaksanakan evaluasi untuk melihat apakah rekomendasi yang diberikan telah dilaksanakan tepat waktu oleh pihak manajemen.

B. Kasus Audit TI di Direktorat Jenderal Perimbangan Keuangan

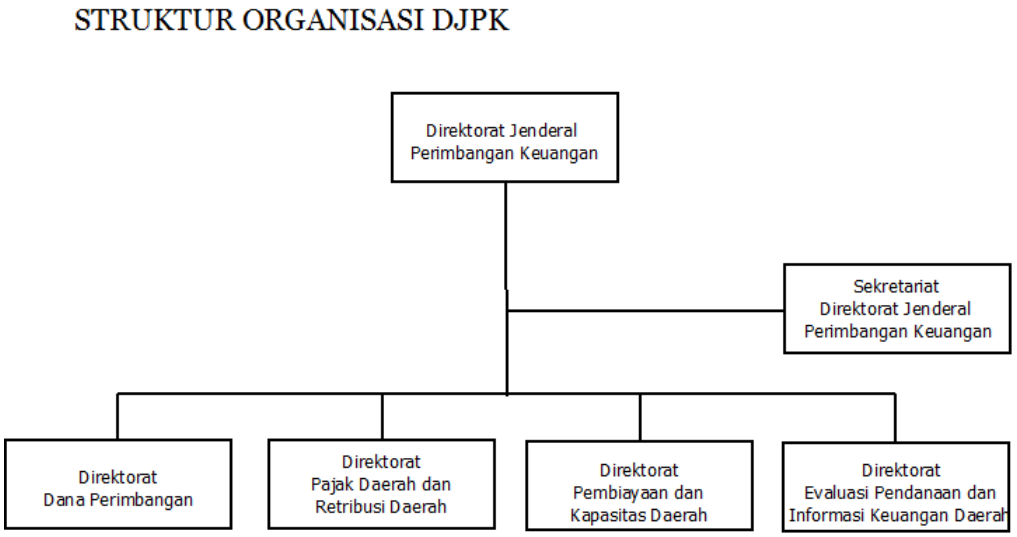
1) Gambaran Umum Instansi

Direktorat Jenderal Perimbangan Keuangan (DJPK) adalah Unit Kerja Eselon I di Kementerian Keuangan yang mempunyai tugas sebagaimana datur dalam Peraturan Menteri Keuangan Nomor 100/PMK.01/2008 Pasal 1166 dan 1167, yaitu merumuskan serta melaksanakan kebijakan dan standardisasi teknis di bidang perimbangan keuangan antara Pemerintah Pusat dan Daerah sesuai dengan kebijakan yang ditetapkan oleh Menteri Keuangan, dan berdasarkan peraturan perundang-undangan yang berlaku. Sedangkan fungsi DJPK adalah sebagai berikut:

a) penyiapan perumusan kebijakan di bidang perimbangan keuangan antara Pemerintah Pusat dan Daerah;
b) pelaksanaan kebijakan di bidang perimbangan keuangan antara Pemerintah Pusat dan Daerah;
c) penyusunan standar, norma, pedoman, kriteria, dan prosedur di bidang perimbangan keuangan antara Pemerintah Pusat dan Daerah;
d) pemberian bimbingan teknis dan evaluasi di bidang perimbangan keuangan antara Pemerintah Pusat dan Daerah; dan
e) pelaksanaan administrasi Direktorat Jenderal.

Dalam menjalankan tugas, DJPK melayani pelanggan utama yaitu pemerintah daerah provinsi, kabupaten dan kota di seluruh Indonesia. Dengan jumlah Pemda yang begitu besar (saat ini tidak kurang dari 542 daerah otonom yang terdiri dari 34 provinsi, 415 kabupaten dan 93 kota) dan tersebar dalam wilayah yang begitu luas, DJPK memerlukan strategi khusus dalam menjalankan tugas fungsinya dalam melayani dan memberikan informasi dan layanan dana perimbangan kepada pemda. Penggunaan Sistem Informasi yang berkualitas, efektif dan efisian akan sangat menentukan dalam pemberian layanan yang prima kepada daerah yang pada akhirnya akan dapat meningkatkan produktifitas pemerintah daerah dalam melaksanakan kegiatan pemerintahan dan pembangunan di daerahnya masing-masing.

DJPK terdiri dari 4 Direktorat, yaitu Direktorat Dana Perimbangan, Direktorat Pajak Daerah dan Retribusi Daerah, Direktorat Pembiayaan dan Kapasitas Daerah dan Direktorat Evaluasi Pendanaan dan Informasi Keuangan daerah. Keempat Direktorat ini menjalankan fungsi utama DJPK dan memberikan pelayanan yang sifatnya heterogen kepada Pemerintah Daerah.Kemudian ada Sekretariat yang menjalankan fungsi pendukung kegiatan Seluruh Direktorat Jenderal. Struktur organisasi digambarkan di gambar 1 berikut.



Gambar 1: Struktur Organisasi DJPK

Jika dilihat dari Uraian Jabatan yang dimiliki, tugas pokok dari masing-masing Direktorat dan Sekretariat tersebut adalah sebagai berikut:

1. Sekretariat Direktorat Jenderal Perimbangan Keuangan
   Tugas utamanya adalah memberikan pelayanan teknis dan administratif kepada semua unsur di lingkungan Direktorat Jenderal Perimbangan Keuangan.

2. Direktorat Dana Perimbangan
   Tugas utama Direktorat Dana Perimbangan adalah Menyiapkan perumusan kebijakan, koordinasi dan fasilitasi, perhitungan alokasi standarisasi, bimbingan teknis, pemantauan dan evaluasi di bidang belanja untuk daerah (Dana Perimbangan dan Dana Otonomi Khusus).

3. Direktorat Pajak Daerah dan Retribusi Daerah
   Tugas Utama Direktorat PDRD adalah Menyiapkan perumusan kebijakan, standardisasi, bimbingan teknis, pemantauan, analisis dan evaluasi di bidang pajak daerah dan retribusi daerah.

4. Direktorat Pembiayaan dan Kapasitas Daerah
   Tugas Utama Direktorat PKD adalah Menyiapkan perumusan kebijakan, standardisasi, bimbingan teknis, pemantauan, dan evaluasi di bidang pinjaman, hibah, dan kapasitas daerah. Direktorat Evaluasi Pendanaan dan Informasi Keuangan Daerah.

5. Direktorat Evaluasi Pendanaan dan Informasi Keuangan Daerah
   Tugas Utama Direktorat EPIKD adalah Menyiapkan perumusan kebijakan, standardisasi, bimbingan teknis, pemantauan,dan evaluasi pendanaan daerah serta penyelenggaraan informasi keuangan daerah.

Sebagaimana disebutkan sebelumnya *customer* utama DJPK adalah Pemerintah Daerah.Maka kebutuhan layanan informasi yang perlu disediakan adalah pelayanan informasi

kepada daerah.Dari tugas utama masing-masing direktorat diatas dapat kita simpulkan ada 3 aktivitas utama dari tiap Direktorat yang berhubungan dengan informasi.

Jika disimpulkan ada tiga kategori kegiatan utama unit-unit kerja di DJPK. Pertama yaitu merumuskan kebijakan, standarisasi, alokasi, dan bimbingan teknis.Untuk kegiatan ini kebutuhan layanan informasi kepada daerah adalah penyampaian informasi kepada pemda mengenai kebijakan dan standar yang telah dikeluarkan oleh DJPK dan pihak terkait sehingga pemda dapat memperolehnya dengan mudah untuk kemudian dapat dimengerti dan diimplementasikan dalam melaksanakan kegiatan mereka terkait penggunaan dana dari pemerintah pusat kepada daerah. Kemudian mengenai alokasi adalah tersedianya informasi yang jelas mengenai alokasi dana ini sehingga pemda tidak perlu berusaha mencari-cari informasinya dengan berbagai cara sampai dengan membayar kepada pihak-pihak tertentu. Dalam penyediaan informasi ini juga tentunya harus dijaga keamanan sistemnya agar informasi yang dihasilkan valid dan terjaga kerahasiaannya.

Kedua melaksanakan penyaluran dana kepada pemerintah daerah. Untuk kegiatan ini layanan informasi yang dibutuhkan adalah sampai dimana proses pencairan dana tersebut dan apabila ada masalah dalam pencairan yang memerlukan inisiatif dari pihak pemda mereka dapat mengetahuinya. Demikian pula ketika dana telah cair, pemda perlu mendapat informasinya agar dana dapat segera digunakan.

Ketiga melakukan Pemantauan dan evaluasi pendanaan/penyaluran dana kepada daerah serta penyelenggaraan informasi keuangan daerah. Kebutuhan layanan informasi untuk aktivitas ketiga adalah kebalikan dari yang lain yaitu agar pemda dapat menyampaikan informasi yang diperlukan oleh DJPK untuk melakukan evaluasi dan pelaporan dengan mudah, cepat dan terjaga keamanannya.

Kemudian pelanggan yang kedua yaitu pelanggan dari Sekretariat Direktorat Jenderal, yaitu seluruh Direktorat lain dan pegawai di seluruh DJPK. Kebutuhan layanan informasi yang dilayani oleh sekretariat ini sangat beragam, antara lain:

a) Adminstrasi Persuratan;
b) Pembayaran gaji dan pendapatan lain pegawai;
c) Pembayaran dana kegiatan operasonal instansi;
d) Layanan administrasi kepegawaian seperti cuti, absensi, berkas kepegawaian, pengurusan kenaikan pangkat, penilaian kinerja dan lain lain;
e) Layanan pengadaan barang dan jasa (*procurement*);
f) Pengelolaan data aset.

Layanan layanan diatas akan dapat diberikan secara optimal dengan pengunaan sistem dan teknologi informasi yang ada saat ini.

2) Identifikasi Sistem Informasi

DJPK cukup memahami pentingnya Teknologi informasi dalam upaya meningkatkan layanan kepada pelanggan. Cukup banyak biaya yang dikeluarkan untuk pengadaan barang dan kebutuhan perangkat TI. Selain itu DJPK juga mempunyai unit khusus yang bertugas untuk memberikan layanan teknis di bidang TI. Sampai saat ini sudah cukup banyak sistem yang telah dibangun untuk memberikan layanan, termask website resmi DJPK.

Secara teknis website ini dibuat oleh para programer DJPK mengunakan PHP dengan *framework code igniter*. Sedangkan server databasenya menggunakan aplikasi yang populer, gratis namun cukup *powerfull* dan *reliable* yaitu mysql database server. Untuk servernya mengunakan server *open source* yaitu centos. Website yang beralamat di http://www.djpk.kemenkeu.go.id ini memiliki fungsi utama sebagai media penyampaian informasi mengenai DJPK secara umum seperti profil, struktur organisasi, para pejabat, alamat kantor, kontak, dan informasi umum sebagaimana pada organisasi lainnya.

Selain itu juga berupa layanan untuk menerima informasi dari pemda berupa aplikasi *Web Based Reporting System* (WBRS) dan Komandan SIKD serta informasi hasil kompilasi dan evaluasi dari DJPK atas informasi dari Pemda tersebut.Kemudian ada forum pengaduan untuk menerima masukan dari pemda mengenai layanan DJPK secara umum.

Ada satu layanan yang tidak diakomodasi disini yaitu layanan informasi progres proses pencairan dana. Sampai saat ini layanan ini masih dilakukan melalui media lain selain website resmi DJPK ini. Salah satu unit telah menggunakan sistem berbasis selular (*SMS gateway*) yang memang lebih efektif untuk penyampaian informasi yang bersifat realtime seperti ini, dan relatif lebih aman dari kemungkinan penyalahgunaan atau pengacauan data oleh pihak yang tidak diinginkan.

Untuk memenuhi kebutuhan pihak internal saat ini juga telah ada beberapa aplikasi berbasis web yang telah dibuat terpisah-pisah sesuai kebutuhan unit penyedia layanan. Aplikasi yang tersedia antara lain

a) SIMPEG, yaitu aplikasi kepegawaian;
b) Intan, aplikasi administrasi persuratan;
c) Mondipa, aplikasi administrasi keuangan;
d) Aplikasi surat tugas dan perjalanan dinas;
e) Intranet berisi forum dan media informasi umum untuk pegawai DJPK;
f) SIKD, sistem informasi keuangan daerah;
g) Simtrada, sistem informasi transfer ke daerah;
h) Dsb.

3) Arsitektur Sistem Jaringan Informasi

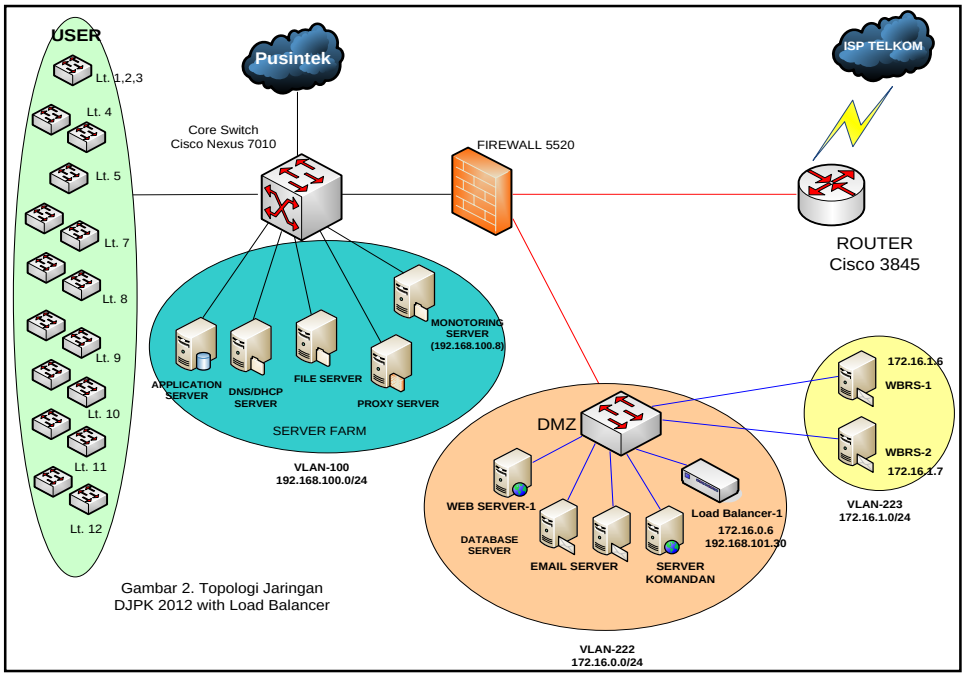
Untuk menyediakan layanan di atas diperlukan perangkat dan administrasi jaringan yang baik. Sistem berbasis web membutuhkan server untuk menyediakan data yang dapat diakses pengguna. Karena ada dua macam sistem yaitu untuk eksternal dan internal, maka diperlukan paling tidak dua server, satu untuk internal, dua untuk eksternal karena DJPK mengelola sendiri website resminya. Beberapa aplikasi memiliki server sendiri di luar web server, seperti email, WBRS dan SIKD.

Selain itu untuk keperluan pegawai mengakses informasi yang disediakan juga untuk berkomunikasi dan mencari informasi untuk mendukung pekerjaan perlu juga disediakan jaringan LAN DJPK yang juga tersambung ke internet.Jaringan ini dibentuk dengan mengunakan topologi Star.

Jaringan DJPK terhubung ke internet melalui dua jalur yaitu menggunakan ISP dan melalui jaringan yang disediakan oleh Sekretariat Kementerian Keuangan dalam hal ini Pusintek. Hardware dalam jaringan yang digunakan antara lain

- Router Cisco 3845.
- Core switch Cisco Nexus 7010.
- Beberapa server.
- Switch di setiap lantai berupa swith *wired* dan *wireless.*
- Kabel UTP dengan kecepatan minimal 1 Gbps.
- Komputer untuk setiap pegawai baik berupa desktop maupun laptop dengan Modul network berkeceptan minimal 1 Gbps (sekitar 450 unit).

Adapun arsitektur jaringan TI di lingkungan DJPK adalah seperti dalam gambar 2



Gambar 2. Topologi Jaringan
DJPK 2012 with Load Balancer

Gambar 2. Arsitektur Jaringan TIK di DJPK

4) Pengelolaan Jaringan

Jaringan DJPK konfigurasi awal dibuat oleh vendor jaringan.Kemudian untuk monitoring dan perawatan pihak DJPK yang mengelola, tetapi apabila ada permasalahan yang tidak dapat diselesaikan vendor tetap mempunyai tanggung jawab mengatasi permasalahan tersebut. Beberapa aturan yang dijalankan dalam pengelolaan antara lain:

a) Adanya firewall untuk akses ke internet selain untuk server-server yang memang untuk diakses dari internet yang berada di zona DMZ.
b) Server-server di DJPK menggunakan load balancer untuk menyeimbangkan kerja seluruh server sehingga semuanya bekerja secara optimal.
c) Akses internet dari jaringan mengunakan proxy untuk keamanan dan menjaga *Quality of Service* (QoS)
d) Untuk QoS dilakukan pembatasan akses internet ke beberapa situs tertentu selama jam kerja dan pembatasan besar file yang dapat di unduh. Untuk ini dijalankan sebuah manajemen *bandwidth*.

C. Simulasi Audit

Simulasi audit ini adalah berupa review atas pemanfaatan Teknologi Informasi di DJPK.

1) **Perencanaan**

Setelah mendapat pemahaman umum mengenai organisasi sebagaimana diatas, dilaksanakan pemahaman atas struktur pengendalian internal DJPK.

2) **Pemahaman atas Struktur Pengendalian Intern DJPK**

Berdasarkan *preliminary survey* atas pemahaman SPI organisasi, berikut ini adalah hasil penetapan risiko yang berkaitan dengan lingkup audit organisasi:

Penetapan risiko yang direncanakan dalam audit dengan formulasi PDR sebagai berikut:

√ PDR = AAR/IR*CR
√ AAR: 10%
√ IR : 100%
√ CR:40%
PDR = 10% / 100%*40%
PDR = **25%**

Keterangan:
- PDR : Planned Detected Risk (risiko deteksi yg direncanakan)
- AAR : Acceptable Audit Risk (risiko audit yg dapat diterima)
- IR : Inherent Risk (risiko melekat)
- CR : Control Risk (risiko pengendalian)

Secara umum organisasi DJPK mempunyai bentuk pengendalian intern yang cukup bagus, hal ini ditandai dengan adanya dokumentasi dan regulasi serta kebijakan yang mengatur proses bisnis organisasi secara mendalam, termasuk pengaturan pada lingkungan berbasis teknologi informasi (TI). Dengan risiko rencana deteksi audit yang direncanakan sebesar 25% tersebut selanjutnya diimplementasikan pada program audit, yang diterapkan pada lingkungan TI (lampiran 2)

3) **Pelaksanaan Audit**
Setelah melakukan pemahaman sistem pengendalian risiko organisasi, melakukan analisis risiko dan menetapkan rencana deteksi risiko (*planned detected risk*), langkah selanjutnya adalah menentukan lingkup pengujian bukti-bukti audit (*evidence*) yang dituangkan dalam rangkaian prosedur audit baik pada pengendalian umum (*general control*) maupun pengendalian aplikasi (*application control*) yang dituangkan dalam rencana program audit. Pada lampiran merupakan pengumpulan bukti audit dengan *checklist* yang dilakukan dengan tanya jawab, pengamatan fisik, observasi, konfirmasi baik pada internal organisasi maupun pihak eksternal.

4) **Hasil Temuan dan Laporan Audit**
Berdasarkan pemahaman terhadap bisnis organisasi, SPI yang diterapkan pada organisasi serta prosedur audit yang tergambar pada program audit, beberapa temuan yang penting yang bersifat positif dapat disimpulkan bahwa secara umum organisasi DJPK telah menerapkan bentuk sistem pengendalian umum yang sudah bagus sehingga pengendalian tersebut dapat secara andal mengamankan aset yang dimiliki oleh organisasi baik berupa infrastruktur TI organisasi, data pokok organisasi, program dan aplikasi termasuk berkas penting yang dimiliki organisasi.

Berbagai komponen pengendalian intern seperti lingkungan internal organisasi, identifikasi peristiwa, penilaian dan respon terhadap risiko, aktivitas pengendalian, monitoring, informasi dan komunikasi secara umum sudah diimplementasikan pada seluruh bagian organisasi sebagaimana nampak pula pada bentuk-bentuk pengendalian umum EDP/Sistem Informasi yang ada, termasuk juga pengendalian aplikasi, sehingga hal tersebut sudah dapat menjamin penggunaan sistem informasi secara efektif dan efisien untuk pencapaian tujuan organisasi DJPK.

Namun demikian, berdasarkan pengamatan fisik dan konfirmasi atas prosedur audit masih terdapat berberapa kelemahan struktur pengendalian intern pada bagian-bagian tertentu komponen SPI. Beberapa temuan yang bersifat negatif, walaupun secara keseluruhan

tidak berpengaruh secara material terhadap penggunaan SI organisasi dalam mencapai tujuan organisasi, namun apabila hal ini dibiarkan terus berlanjut, maka sedikit demi sedikit akan berdampak pada SPI organisasi. Dalam jangka panjang hal ini akan menggerus implementasi SPI organisasi DJPK.

Beberapa temuan audit yang perlu mendapatkan tindak lanjut untuk diperhatikan oleh manajemen organisasi antara lain sebaga berikut:

1) Masih terdapat lemahnya kesadaran pengawasan penggunaan perangkat EDP/SI organisasi terhadap staf oleh atasan organisasi. Walaupun pada lingkungan internal organisasi sudah disusun dan diterapkan regulasi dan kebijakan serta mekanisme tata kelola pemanfaatan TI, namun kurangnya pengawasan manajemen terhadap ditaatinya regulasi dan kebijakan tersebut oleh pegawai dapat berimplikasi pada penggunaan sumber daya (*resource*) yang tidak berkaitan langsung pada pencapaian tujuan organisasi secara efektif dan efisien. Penggunaan piranti TI organisasi untuk keperluan pribadi pegawai berarti adalah bentuk pemborosan sumber daya TI organisasi.
2) Sumber daya manusia masih kurang mendapatkan perhatian, terutama berkaitan dengan para pegawai baru belum mendapatkan semacam pelatihan yang cukup di bidang lingkungan berbasis TI. Seharusnya organisasi memberikan pelatihan yang cukup dan memadai terkait dengan regulasi, kebijakan dan mekanisme pemanfaatan TI organisasi kepada para pegawai baru sehingga muncul pemahaman awal mereka ketika berinteraksi dengan perangkat-perangkat TI. Dengan demikian dari awal sudah ada kesadaran yang tinggi pemanfaatan TI organisasi untuk mencapai tujuan organisasi secara efektif dan efisien.
3) Berkaitan dengan pengembangan sistem dan aplikasi organisasi masih terdapat kelemahan dari sisi keberadaan *framework* yang memudahkan pengembang untuk menyediakan layanan TI dengan mudah dan cepat. Selain itu implementasi sistem dan aplikasi yang baru masih kurang disosialisasikan kepada para pegawai secara intensif, setiap ada pengembangan aplikasi baru hanya disosialisasikan kepada sebagian pegawai yang menangani aplikasi tersebut itupun dalam rentang waktu yang singkat, disamping masih minimnya pelatihan bagi pegawai yang akan mengoperasikan aplikasi tersebut. Dengan demikian keberadaan manual aplikasi belum cukup untuk memberikan kemudahan implementasi aplikasi baru pada organisasi.
4) Berkaitan dengan manajemen security, terutama mengenai instalasi aplikasi dan pencegahan virus untuk melindungi data organisasi, walaupun sudah ada kebijakan dan prosedur pemanfaatan software anti-virus, namun berdasarkan pengamatan fisik ternyata masih terdapat beberapa instalasi program anti-virus yang bukan merupakan software yang resmi yang mendapat otorisasi untuk diinstall pada seluruh komputer para pegawai. Berdasarkan konfirmasi yang dilakukan, ternyata lemahnya pengawasan yang dilakukan oleh fungsi TI menjadi penyebab utama pengunaan software anti-virus yang tidak standar pada komputer beberapa pegawai. Apabila hal demikian tidak mendapatkan perhatian organisasi, maka sistem dan manajemen security organisasi tidak dapat mencapai tujuan yang diharapkan secara optimal.

V. Penutup

Berdasarkan hasil temuan selama pelaksananan audit TI pada organisasi DJPK, kami merekomendasikan bebarapa hal sebagai berikut:

1) DJPK hendaknya meningkatkan keandalan SPI organisasi sehingga lebih berkualitas, seperti peningkatkan kualitas manajemen dan gaya operasi dalam lingkungan internal organisasi, dengan demikian mampu mengarahkan pemanfaatan sumber daya TI organisasi untuk mencapai tujuan organisasi secara efektif dan efisien.

2) Pelatihan dan sosialisasi pemanfaatan TI pada seluruh pegawai perlu dilakukan secara intensif, termasuk bagi seluruh pegawai baru, sehingga memberikan kesadaran pemanfaatan TI yang selaras dengan tujuan organisasi.
3) Pengawasan/monitoring sebagai salah satu komponen penting SPI, perlu mendapatkan perhatian organisasi untuk ditingkatkan. Berbagai regulasi, kebijakan dan prosedur yang dituangkan pada SOP dan proses bisnis organisasi, serta berbagai kegiatan pengendalian baik pengendalian umum maupun pengendalian aplikasi perlu ditindaklanjuti dengan adanya pengawasan yang memadai sehingga dapat mengarahkan pengendalian tersebut secara efektif untuk mencegah dan memitigasi munculnya risiko yang kurang menguntungkan dan berpengaruh buruk pada pencapaian tujuan organisasi.

Daftar Pustaka

Ackerman, M., Beth R., Anecia W., Joseph W., Randy W. 2009. IT Strategic Audit Plan. *Journal of Technology Research.* Vol 1 pp 1-7.

Amnah. 2014. Audit Kehadiran Dosen Pada Pusat Layanan Perkuliahan Dan Pelaporan (PLPP) Di Ibi Darmajaya Menggunakan Frame Work Cobit 4.1. *Jurnal Informatika*. Vol 14 No 2 pp 182-190.

Avin A. Arens and James K. Loebbecke. 1991. Auditing. Prentice-Hall, Inc. New Jersey.

Gheorghe, M. 2010. Audit Methodology for IT Governance. Informatica Economica Vol. 14 No. 1 pp 32-42.

Hong, EK. 2009. Information Technology Strategic Planning. IT Pro. Published by IEEE Computer Society. pp 8-15.

Kacanski, S. 2016. ICT in Auditing: Impact of Audit Quality Norms on Interpersonal Interactions. European Financial and Accounting Journal. Vol 11 No 4 pp 39-64.

Kim, SL., Thompson SHT., Anol B., Kichan N. 2015. IS Auditor Characteristics, Audit Process Variables, and IS Audit Satisfaction: an Empirical Study in South Korea. Information Systems Frontiers. Springer. Published online 26 November 2015.

Mahzan, N., Farida V. 2011. IT auditing activities of public sector auditors in Malaysia. African Journal of Business Management. Vol 5 pp 1551-1563.

Merhout, JW., Douglas H. 2008. Information Technology Auditing: A Value-Added IT Governance Partners. Communication of the Association for Information System. Vol 23 pp 464-482

Mihalic, T., Buhalis, D. 2013. ICT as a New Competitive Advantage Factor – Case of Small Transitional Hotel Sector. Economic and Business Review. Vol 15 No 1 pp 33–56.

Popa, M. 2011. Methods and Techniques of Quality Management for ICT Audit Processes. Journal of Mobile, Embedded and Distributed Systems. Vol III No 3 pp 100-108.

Ratanasongtham, W., Phaprukbaramee U. 2015. Strategic Audit Planning and Audit Quality: an Empirical Research of CPAs in Thailand. The Business and Management Review. Vol 7 Number 1 pp 384-394.

Singleton., Tommie W., 2012. Auditing Applications, Part 1. ISACA Journal. Vol 3 pp 1-5.

Turban, E., Linda V. 2011. Information Technology for Management, Improving Strategic and Operational Performance. 8th edition. John Wiley & Sons, Inc. USA.

Tsai, WH., Hui CC., Jui CC., Hsiu LL. 2017. The Internal Audit Performance: The Effectiveness of ERM and IT Environments. Proceedings of the 50th Hawaii International Conference on System Sciences. pp 4898-4906.

Computer Audit Assisted Group. A Guide to Computer Assisted Audit Techniques. Department of Revenue, Massachusetts

ISACA. 2012. COBIT 5 Introduction. diakses dari laman http://www.isaca.org/cobit/pages/default.aspx pada 19 Juni 2014

ISACA. 2013 COBIT 5 A Business Framework for the Governance and Management of Enterprise IT. diakses dari laman http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx pada 19 Juni 2014

Republik Indonesia. 2008. Peraturan Pemerintah No. 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah

Republik Indonesia. 2008. Peraturan Menteri Keuangan Nomor 100/PMK.01/2008 tentang Organisasi Kementerian Keuangan

Ikatan Akuntan Indonesia. 2001. Pernyataan Standar Audit No. 59 tentang Teknik Audit Berbantuan Komputer. Standar Audit

INTOSAI, 2013. Fundamental Principles of Public-Sector Auditing. The International Standards of Supreme Audit Institutions. No.100. Copenhagen K. Denmark

Lampiran 1

STRUKTUR PENGENDALIAN INTERN DJPK

Lingkungan Internal Organisasi

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Dapatkan dan teliti landasan hukum organisasi	V				V	
2	Dapatkan dan periksa struktur organisasi	V				V	
3	Dapatkan dan periksa regulasi dan kebijakan organisasi di bidang TI		V			V	
4	Dapatkan dan periksa aturan organisasi mengenai komitmen terhadap komptensi organisasi	V				V	
5	Dapatkan dan periksa kode etik kepegawaian	V				V	
6	Dapatkan dan periksa catatan pelanggaran para pegawai		V			V	
7	Amati (lakukan observasi) perilaku pegawai secara acak terkait dg perilaku kerjanya sehari-hari		V				

Identifikasi Event

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Dapatkan dan periksa kegiatan organisasi yang berpotensi menimbulkan risiko	V				V	
2	Identifikasi apakah ada pengelompokkan kegiatan berdasarkan risiko	V				V	

Penilaian Risiko

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Dapatkan dan periksa apakah organisasi mengimplementasikan penilaian risiko terhadap kegiatan yang berpotensi menimbulkan risiko	V				V	

2	Apakah organisasi mengimplentasikan teknik dan strategi dalam penilaian risiko organisasi	V				V	

Respon terhadap Risiko

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Dapatkan dan periksa dokumen yang mengimplementasikan respon organisasi terhadap risiko yang dihadap		V			V	
2	Dapatkan dan periksa apakah organisasi menerapkan teknik analisis terhadap respon terhadap risiko		V			V	

Kegiatan Pengendalian

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Dapatkan dan periksa pemisahan fungsi organisasi	V				V	
2	Lakukan pengamatan (uji petik) terhadap kondisi tempat kerja pegawai, apakah ada cukup pemisahan yang jelas berdasarkan fungsi masing-masing organisasi		V			V	
3	Dapatkan prosedur umum organisasi (SOP), periksa dan lakukan uji petik SOP apakah SOP sudah menggambarkan prosedur untuk mengendalikan berbagai risiko yang ada	V				V	

Komunikasi dan Informasi

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Dapatkan cetak biru rancangan sistem informasi dan komunikasi yang dikembangkan organisasi	V				V	

2	Lakukan pengamatan dan konfirmasi apakah organisasi mengimplementasikan database tunggal untuk organisasi secara keseluruhan		**V**			**V**	
3	Lakukan tanya jawab kepada pegawai (uji petik) apakah pegawai memahami kebijakan dan regulasi pemanfaatan TI pada organisasi		**V**			**v**	

Monitoring

NO	URAIAN	Kondisi				KET	
		Bagus	Sedang	Kurang	Jelek	Ada	Tdk ada
1	Periksa apakah dilakukan pengawasan terhadap penggunaan TI yang dipergunakan untuk tujuan selain kepentingan organisasi		**V**			**V**	
2	Periksa dan konfirmasi apakah komponen pengendalian internal sudah cukup dimonitoring oleh organisasi		**V**			**V**	

Lampiran 2

REVIEW PEMANFAATAN TI DJPK

RINCIAN PROGRAM AUDIT :

NO	DESKRIPSI	YA	TDK	N/A
A	**ORGANISASI DAN ADMINISTRASI**			
-	**Tujuan Audit** Apakah organisasi pengolahan data menyediakan pembagian tugas yang memadai?			
-	**Prosedur Audit** Tinjauan bagan organisasi , dan bagan departemen pengolahan data dalam organisasi.			
1	Apakah ada departemen EDP/Sistem Informasi yang terpisah dalam oganisasi?	**V**		
2	Apakah ada steering komite dimana tugas dan tanggung jawab untuk mengelola MIS didefinisikan dengan jelas?		**V**	
3	Apakah organisasi mengembangkan strategi TI terkait dengan rencana jangka panjang dan menengah?	**V**		
4	Apakah Departemen EDP/SI independen dari departemen pengguna dan khususnya departemen akuntansi?		**V**	
5	Apakah ada uraian tugas yang tertulis untuk semua pekerjaan dan deskripsi pekerjaan ini dikomunikasikan kepada karyawan yang ditunjuk?	**V**		
6	Apakah personel EDP/SI dilarang memiliki tanggung jawab yang tidak kompatibel atau tugas dengan departemen pengguna atau sebaliknya?	**V**		
7	Apakah ada spesifikasi yang ditulis untuk semua pekerjaan di Departemen EDP/SI?	**V**		
8	Apakah fungsi berikut dalam Departemen EDP/sSI dilakukan oleh bagian yang terpisah:			
	▪ Desain system dan progam aplikasi ?	**V**		

NO	DESKRIPSI	YA	TDK	N/A
	▪ Operasi komputer?	V		
	▪ Administrasi database?	V		
	▪ Data entry dan kontrol?		V	
9	Apakah personil pengolahan data dilarang bertugas yang berkaitan dengan:			
	▪ Memulai transaksi?		V	
	▪ Recording transaksi?		V	
	▪ Merubah master file?	V		
	▪ Mengoreksi error?		V	
10	Apakah semua pengolahan dijadwalkan terlebih dahulu dan disahkan oleh personil yang berwenang?		V	
11	Apakah ada prosedur untuk mengevaluasi dan menetapkan siapa yang memiliki akses data ke dalam database?	V		
12	Apakah personil EDP cukup terlatih?	V		
13	Apakah sistem analis programmer dilarang akses ke ruangan komputer dan dibatasi dalam mengoperasikan komputer?		V	
14	Apakah operator dilarang melakukan perubahan pada program dan dari menciptakan atau mengubah data sebelum, selama, atau setelah pengolahan?	V		
15	Apakah aset dibatasi untuk personil di luar departemen EDP?			V
16	Apakah rencana pengolahan data strategis yang dikembangkan oleh perusahaan untuk pencapaian rencana bisnis jangka panjang?	V		
17	Apakah ada personil kunci dalam departemen TI yang ketidakhadirannya dapat meninggalkan sementara waktu di dalam organisasi?		V	
18	Apakah EDP Audit yang dilakukan oleh internal audit atau konsultan eksternal untuk memastikan kepatuhan terhadap kebijakan dan kontrol yang ditetapkan oleh manajemen?	V		
B	**PEMELIHARAAN PROGRAM DAN PENGEMBANGAN SISTEM**			

NO	DESKRIPSI	YA	TDK	N/A
-	**Tujuan Audit** Pengembangan dan perubahan pada program telah disyahkan, diuji, dan disetujui, sebelum ditempatkan dalam produksi			
	Program Audit Pemeliharaan - Prosedur			
-	Melihat secara detail struktur library program dan membuat catatan kontrol dimana hanya individu yang berwenang untuk mengakses setiap library.			
-	Memperhatikan prosedur yang digunakan untuk mengubah program.			
-	Memperoleh pemahaman dari setiap program library management yang digunakan.			
1	Apakah ditulis standar untuk pemeliharaan program?	**V**		
2	Apakah standar dipatuhi dan ditegakkan?	**V**		
3	Apakah standar selalui di review dan disetujui secara reguler?	**V**		
4	Apakah ada prosedur untuk memastikan bahwa semua program yang diperlukan untuk pemeliharaan disimpan terpisah dalam program test library?			**V**
5	Apakah programmer ditolak akses ke semua library selain test library?			**V**
6	Apakah perubahan program yang diprakarsai oleh permintaan tertulis dari departemen pengguna dan telah disetujui?	**V**		
7	Apakah perubahan diawali oleh departemen data processing telah di komunkasikan ke user dan disetujui oleh mereka?	**V**		
8	Apakah ada cukup kontrol untuk mentransfer dari produksi ke test library programmer?			**V**
9	Apakah semua sistem yang dikembangkan atau dirubah telah di tes ke sistem yang ada?	**V**		
10	Apakah uji coba telah dijalankan dan data tes telah di dokumentasikan?	**V**		
11	Apakah transfer dari developmen library ke production library telah mengikutsertakan independent programmer?		**V**	
12	Apakah prosedur menjamin dimana tidak ada lagi transfer yang memakan tempat tanpa merubah tes terlebih dahulu?			**V**

NO	DESKRIPSI	YA	TDK	N/A
13	Apakah laporan dari program transfer kedalam produksi di review setiap hari oleh senior official ?		V	
14	Seluruh program yang dirubah sebelumnya telah didokumentasikan?	V		
15	Apakah seluruh perubahan program sesegera mungkin untuk di back up?	V		
16	Apakah ada copy dari versi sebelumnya ?	V		
17	Apakah ada standar untuk perubahan yang darurat untuk membuat program aplikasi?			V
18	Apakah ada cukup kontrol dari program yang dikumpukan ulang?			V
19	Apakah seluruh amandemen di catat ke audit internal untuk dikomentari?	V		
20	Apakah sudah cukup kontrol, otorisasi, implementasi, dukungan dan dokumentasi dari perubahan sistem operasi?	V		
C	**PENGEMBANGAN SISTEM**			
1	Apakah ada formula standar untuk prosedur pengembangan sistem life cycle?	V		
2	Apakah cukup otorisasi dari bermacam macam tahapan pengembangan- studi feasibility, spesifikasi sistem, testing, parallel running, post implementation review, dan sebagainya?	V		
3	Apakah standar menyediakan framework untuk pengembangan dari aplikasi kontrol?		V	
4	Apakah standar di review secara rutin dan selalu di update?			V
5	Apakah dokumentasi sistem ada untuk:			
	▪ Programmer untuk memelihara dan memodifikasi program?	V		
	▪ Pengguna dalam mengoperasikan sistem?		V	
6	Apakah departemen audit internal dilibatkan dalam tahapan desain untuk menjamin adanya kontrol yang ada?	V		
7	Apakah sosialiasi dan pelatihan dilakukan secara intensif sebelum dilakukan impleentasi sistem dan aplikasi yang baru?.		V	

NO	DESKRIPSI	YA	TDK	N/A
8	Apakah user dan personil data prosesing cukup terlatih menggunakan aplikasi baru?		V	
9	Apakah penerapan sistem sebelumnya direncanakan dan penerapan dapat dilakukan secara bersamaan atau sendiri?		V	
10	Apakah ada cukup kontrol untuk mensetting data?	V		
11	Apakah setelah implementasi ada untuk dikaji ulang?		V	
12	Apakah user manuals disiapkan untuk seluruh pengembangan sistem yang baru dan meninjau kembali perubahan sesudahnyas?	V		
14	Apakah dilakukan fungsi *Quality Assurance* untuk memferifikasi, integritas, dan pengembangan aplikasi?	V		
D	**PEMBELIAN PERANGKAT LUNAK**			
1	Apakah cukup dokumentasi pemeliharaan untuk seluruh perangkat lunak yang dibeli?	V		
2	Apakah ada garansi vendor ?	V		
3	Apakah pembelian perangkat lunak termasuk dalam perencanaan?	V		
4	Apakah ada copy backup dari user/operations manual?	V		
E	**AKSES KE BERKAS DATA**			
-	**Audit Objective** Apakah akses berkas data dibatasi ?			
-	**Akses Data**			
1	Apakah ada kebijakan tertulis keamanan data secara formal? Pertimbangkan apakah kebijakan ini membahas tentang kepemilikan data, kerahasiaan informasi, dan penggunaan password .	V		
2	Apakah security policy dikomunikasikan ke setiap orang di dalam organisasi?	V		
3	Apakah akses secara fisik off-line data files dikontrol dalam:			

NO	DESKRIPSI	YA	TDK	N/A
	▪ Ruangan komputer?	V		
	▪ On-site library?		V	
	▪ Off-site library?		V	
4	Apakah organisasi memperkerjakan petugas perpustakaan penuh waktu yang independen terhadap operator dan programmer?		V	
5	Apakah aplikasi sensitif seperti daftar gaji dikelola pada mesin yang secara fisik pada area tertentu?		V	
6	Apakah teknik enkripsi dipergunakan untuk melindungi terhadap pengungkapan yang tidak diotorisasi atau modifikasi data sensitif yang tidak dideteksi?	V		
F	**PEMROSESAN KOMPUTER**			
1	Apakah ada sistem terjadwal untuk pelaksanaan program?		V	
2	Apakah pekerjaan yang tidak terjadwal telah mendapatkan persetujuan sebelum dijalankan?	V		
3	Apakah pemanfaatan program utilitas dikendalikan?			
4	Apakah pengujian program dibatasi pada salinan berkas langsung?	V		
5	Apakah akses komputer dibatasi hanya kepada personel yang berwenang?	V		
6	Apakah instruksi operasi secara cukup yang ada saat ini mencakup prosedur untuk diikuti pada operasi?	V		
7	Apabila demikian, apakah instruksi2 direview secara independen?	V		
G	**PENGENDALIAN AKSES**			
1	Apakah ada sintak password dg minimal 5 karakter, maksimal 8 karakter, termasuk dg karakter angka?	V		
2	Apakah ada prosedur penerbitan password bagi mereka yang lupa?	V		
4	Apakah kompabilitas akses sistem secara tepat berubah dengan perubahan status pegawai?		V	

NO	DESKRIPSI	YA	TDK	N/A
5	Apakah tanggungjawab pekerjaan individu dipertimbangkan ketika memberikan hak akses kepada individu?	V		
6	Apakah setiap pengguna diberikan akun dan password pengguna?	V		
7	Apakah ada prosedur yang dibuat untuk memastikan perubahan password setiap 30 hari?		V	
9	Apakah prosedur dan standar yang ada ditindaklanjuti terhadap pelanggaran keamanan?		V	
H	**PENGENDALIAN APLIKASI - INPUT**			
-	**Tujuan Audit** Apakah pengendalian telah memberikan kepastian memadai bahwa setiap tipe transaksi, input telah diotorisasi, lengkap, akurat sehingga kekeliruan dikoreksi dengan segera?			
1	Apakah seluruh transaksi secara tepat diotorisasi sebelum diproses melalui komputer?	V		
2	Apakah seluruh paket transaksi diotorisasi?		V	
3	Apakah pengendalian menjamin paket atau transaksi yang tidak diotorisasi dapat dicegah apabila telah dideteksi?	V		
4	Apakah input data yg penting diverifikasi terhadap berkas utama (*master file*)?	V		
5	Apakah pemanfaatan maksimum uji edit seperti uji digit, limit test, uji kelayakan?	V		
6	Apakah ada prosedur yang ditetapkan untuk menjamin bahwa transaksi atau paket tidak hilang, terjadi duplikasi atau berubah secara tidak tepat?	V		
7	Apakah seluruh kekeliruan dilaporkan untuk pengecekan dan koreksi?	V		
8	Apakah kekeliruan dikembalikan kepada departemen pengguna untuk koreksi?	V		
9	Apakah prosedur menjamin bahwa kekeliruan diproses ulang?	V		
10	Apakah log kekeliruan dikelola dan direview untuk mengidentifikasi kekeliruan yang berulang?		V	

NO	DESKRIPSI	YA	TDK	N/A
11	Apakah seseorang yang bertanggungjawab persiapan data dan entri data bersifat independen dari pengujian output?	V		
12	Apakah orang yang bertanggungjawab untuk entri data dicegah untuk melakukan perubahan berkas data utama (*master file*)?	V		
I	**OUTPUT DAN PEMROSESAN**			
-	**Audit Objective** Pengendalian memberikan kepastian memadai bahwa transaksi secara tepat diproses melalui komputer dan hasil transaksi lengkap, akurat sehingga item-item yang diperhitungkan telah diproses melalui komputer secara akurat:			
1	Ketika suatu hasil transaksi berasal dari input yang lain, apakah dijalankan penjumlahan, atau uji yang serupa dipergunakan untuk menjamin bahwa tidak ada data yang hilang atau yg korup?	V		
2	Apakah ada pengendalian yang cukup terhadap formulir yang mempunyai nilai moneter?	V		
3	Ketika ada kekeliruan dalam pemrosesan yang dideteksi, apakah ada prosedur formal untuk pelaporan dan investigasi?	V		
4	Apakah rekonsiliasi antara input, output dilaksanakan dan perbedaan diinvestigasi?	V		
J	**VIRUS**			
1	Apakah ada kebijakan formal tertulis *anti-virus*?	V		
2	Apakah kebijakan tersebut secara efektif dikomunikasian kepada setiap individu di organisasi?	V		
3	Apakah ada daftar penyedia software yang telah mendapatkan persetujuan?	V		
4	Apakah software yang hanya telah diotosasi saja yang diinstall pada mikrokomputer?		V	
5	Apakah ada semacam perpustakaan master untuk software yang demikian?	V		

NO	DESKRIPSI	YA	TDK	N/A
6	Apakah direktori file secara periodik dilakukan review untuk file-file yang mencurigakan?			
7	Apakah file-file sistem secara teratur dicek atas perubahan ukuran file?		V	
8	Apakah software antivirus diinstall pada mikrokomputer / laptop?			
9	Apakah software antivirus secara teratur diupdate untuk jenis definisi virus baru?	V		
10	Apakah file mencurigakan yang dikarantina dan dihaspus dari hard drive terminal dan drive jaringan secara teratur?		V	
11	Apakah disket/flashdiks diformat sebelum dipergunakan ulang?		V	
12	Apakah prosedur telah dikembangkan untuk membatasi atau mengatasi transfer data antara mesin?	V		
13	Apakah ada larangan bagi staf berbagi mesin (laptops/desktops)?		V	
14	Apakah seluruh staf diberitahui tentang prosedur pencegahan virus?	V		
15	Apakah download dari intenet dikendalikan dengan mengunci hard-drive dan mengarahkannya melalui drive network untuk mencegah virus (kalau ada) menyebar?		V	
K	**INTERNET**			
1	Apakah ada kebijakan yang tepat mengenai pemanfaatan internet oleh pegawai?	V		
2	Apakah kebijakan tersebut mengidentifikasikan perlindungan aset khusus oleh firewall dan tujuan perlinduangan tersebut?	V		
3	Apakah kebijakan tersebut mendukung penggunaan yg sah atas aliran data dan informasi?	V		
4	Apakah informasi yang melalui firewall dilakukan monitoring secara tepat?	V		
5	Apakah kebijakan secara tetpat dikomunikasikan kepada pengguna dan terdapat kesadaran yang dipertahankan?	V		
6	Apakah pimpinan unit organisasi melakukan pengawasan perilaku dan sikap kerja staf terhadap pemanfaatan internet		V	

NO	DESKRIPSI	YA	TDK	N/A
7	Apakah firewall dikonfigurasi berdasarkan kebijakan security?	V		
8	Apakah penyaringan URL dilakukan oleh Firewall?	V		
9	Apakah inspeksi anti-virus diterapkan?	V		
10	Apakah paket yg disaring karenakeberadaan kata-kata yang dilarang?, apabila demikian, tentukan bagaimana daftar kata-kata tersebut diadministrasikan dan dikelola.	V		
11	Apakah log akses secara reguler direview dan apakan ada tindakan tertentu yang diambil berdasarkan permintaan pengguna?	V		
L	**KEBERLANGSUNGAN OPERASI**			
	Perlindungan Fisik			
L.I	**Bahaya Kebakaran**			
1	Lakukan pengecekan keamanan terhadap kebakaran dengan berbagai macam cara berikut :			
	■ Bahan bangunan tahan api?	V		
	■ Apakah dinding dan penutup lantai tidak mudah terbakar?	V		
	■ Pemisahan dari area mudah terbakar	V		
	■ Media penyimpangan tahan api?	V		
2	Uji bentuk piranti deteksi api yang tepat:			
	■ Detektor panas / asap?	V		
	■ Detektor yg terletak di langit-langit dan bawah lantai?	V		
	■ Dihubungkan ke sistem alarm kebakaran?	V		
3	Lakukan pengujiaan dalam hal kasus gawat darurat kebakaran:			
	■ Apakah instruksi kebakaran secara jelas ditempelkan pada kantor	V		
	■ Apakah tomobol alarm kebakaran jelas terlihat	V		
	■ Prosedur tombol power-off ditempel	V		

NO	DESKRIPSI	YA	TDK	N/A
	▪ Rencana evakuasi, dengan pembebanan tanggungjawab dan peran	V		
4	Lakukan pengujian apakah ada pelatihan untuk menghindari bahaya kebakaran:			
	▪ Pelatihan dan simulasi teratur	V		
	▪ Inspeksi teratur/pengujian seluruh peralatan komputer	V		
5	Peralatan AC			
	Monitoring temperatur dan kelembaban dalam area TI sbb:			
	▪ Panas, perlindungan akses bagian perlindungan sensitif	V		
	▪ Back-up perlengkapan AC	V		
L.II	**Power Supply**			
	▪ Keandalan *power supply* lokal	V		
	▪ Pemisahan power supply yg terpisah untuk komputer	V		
	▪ Tersedia piranti UPS (*uninterrupted power supply*)	V		
	▪ Terdapat power supply alternatif (mis: generator) untuk sistem penerangan darurat.	V		
L.III	**Jaringan Komunikasi**			
	▪ Perlindungan fisik atas saluran komunikasi yg modern	V		
	▪ Lokasi perlengkapan komunikasiyang terpisah dari peralatan EDP	V		
L.IV	**Jalan Masuk (Area TI):**			
	▪ Tidak ada pintu masuk yg tidak diperlukan untuk sampai ke ruangan komputer		V	
	▪ Pintu yg tidak penting selalu tertutup dan terkunci bagi pihak luar		V	

NO	DESKRIPSI	YA	TDK	N/A
	(mis: pintu kebakaran)			
	▪ Ventilasi udara dan lokasi akses terhadap sinar matahari	V		
M	**PENGENDALIAN AKSES**			
1	Akses dibatasi terhadap pegawai tertentu	V		
2	Persetujuan akses diperlukan bagi seluruh pegawai	V		
3	Pintu masuk dikendalikan melalui :			
	▪ Diawasi oleh petugas		V	
	▪ Dikunci atau kombinasi elektronik	V		
4	Identifikasi positif bagi seluruh pegawia (kartu pegawai)	V		
5	Akses dikendalikan 24 jam termasuk akhir pekan (mekanisme pengendalian otomatis)		V	
M.I	**Pengendalian pengunjung/tamu**			
1	Ada identifikasi positif	V		
2	Tanda pengenal diberikan, dikendalikan dan dikembalikan	V		
3	Seluruh kunjungan diadministrasikan dalam buku tamu	V		
M.II	**Keamanan Umum**			
1	Sampah secara teratur dibersihkan dari area EDP Waste.	V		
2	Ada sistem alarm pintu.	V		
3	Monitoring televisi sirckuit tertutup (kamera CCTV)	V		
N	**KEBIJAKAN KEPEGAWAIAN**			
1	Pegawai yang baru direkrut diberikan pelatihan berdasarkan deskripsi pekerjaan	V		

NO	DESKRIPSI	YA	TDK	N/A
2	Pegawai diberikan kartu identitas pegawai.	V		
3	Evaluasi kinerja dan konseuling teratur	V		
4	Program pendidikan berkelanjutan	V		
5	Pelatihan dalam hal security, privasi dan prosedur recovery		V	
6	Pekerjaan kritis dirotasi secara periodeik (mis: operators, pengelolaan program).		V	
O	**PERLINDUNGAN**			
1	Apakah perlindungan diberikan secara cukup mencakup:			
	▪ Perlengkapan?	V		
	▪ Software dan dokumentasi ?	V		
	▪ Media penyimpanan?	V		
	▪ Biaya penggantian?	V		
	▪ Kehilangan data/aset)?	V		
	▪ Kerugian bisnis?	V		
2	Apakah pertimbangan yang cukup diberikan untuk menangani biaya tambahan pekerjaan dan kerugian?	V		
P	**PROSEDUR BACK-UP**			
P.I	**Perlengkapan Komputer dll**			
1	Terdapat pengelolaan pencegahan preventive	V		
2	Pengujian kompabilitas dilakukan secara teratur		V	
4	Ada waktu back-up komputer secara teratur	V		
P.II	**Pemasok eksternal (bencana/ temporer)**			

NO	DESKRIPSI	YA	TDK	N/A
-	(mis: pemasok peralatan, software)			
1	Apakah ada sumber alternatif persediaan/pengelolaan/layanan	V		
2	Dokumentasi yang aman dan memadai / back-up data dan program	V		
3	Apakah salinan back-up atas dokumentasi sistem disempan pada lokasi yang aman?	V		
P.III	**Media Simpan secara Terpisah:**			
1	lokasi terpisah yang aman	V		
2	Perlindungan fisik yang cukup	V		
4	Pemindahan berkas dilakukan dengna perlindungan fisik yang cukup	V		
5	Berkas back-up dilakukan pengujian secara periodeik	V		
P.IV	**Berkas Data**			
1	Terdapat prosedur retensi berkas yang secara teraur direview	V		
P.V	**Software**			
1	Salinan berikut ini dikelola pada media simpan terpisah : program aplikasi produksi			
	■ Program utama yang dikembangkan	V		
	■ Dokumentasi program dan sistem	V		
	■ Prosedur operasi	V		
	■ Software sistem dan operasi	V		
P.VI	**Operasi**			
1	Manual prosedur back-up	V		

NO	DESKRIPSI	YA	TDK	N/A
2	Prosedur untuk memulihkan berkas data dan prosedur software untuk instalasi back-up	V		
Q	**PERENCANAAN PEMULIHAN ATAS BENCANA (*DISASTER RECOVERY PLANS*)**			
1	Apakah organisasi mengembangkan rencana darurat yang komprehensif, didokumentasikan dan secara periodik diuji utnuk memastikan keberlangsungan layanan pemrosesan data?	V		
2	Apakah rencana darurat dipersiapkan untuk pemulihan dan pemrosesan aplikasi penting dalam hal terjadi musibah yang membahayakan organisasi?	V		
3	Apakah organisasi melakukan analisis pengaruh operasi bisnis dalam hal terjadi musibah (kebakaran, gempa bumi)?		V	
5	Apakah rencana tersebut dikomunikasikan kepada seluruh manajemen dan personil	V		
6	Apakah ada pembentukan tim pemulihan musibah untuk mendukung rencana pemulihan musibah?		V	
7	Apakah tanggung jawan secara individu pada tim tersebut didefinisikan dan dialokasikan waktu untuk melaksanakan tugas-tugasnya?		V	
8	Apakah organisasi mengembangkan dan mengimplementasikan prosedur pengelolaan rencana darurat yang cukup?		V	
9	Apakah rencana pemulihan secara teratur dilakukan pengujian?		V	