1. Jelaskan tentang kategori pengendali internal?
2. Audit TI sering memberikan info yg membantu organisasi mengelola resiko, memastikan sumber daya terkait TI yg efisien, & mencapai tujuan TI & bisnis lainnya. Alasan yg digunakan unt membenarkan audit TI internal mungkin lebih bervariasi antar organisasi, jlskn apa saja yg dilakukan pada saat melakukan audit internal TI scr umum?
3. Apakah perbedaan audit internal dengan audit eksternal?
4. Apa yang dimaksud Sistem Manajemen Keamanan Informasi?
5. Jlskn ttg keamanan fisik, personal, opra, komunikasi, jaringan?
6. Dlm mlkukn audit proses pengadaan, RFP, mjdi bgian penting dalam proses audit, jelaskan tentang RFP tersebut?
7. Dlm mlksnakn audit SI unt aplikasi bisnis, ada bbrp teknologi yg relevan untuk diaudit diantaranya adalah EDI, jelaskan EDI tersebut?
8. Jelaskan 4 tahap proses audit!
9. Apa yang anda ketahui tentang isi dari dokumen rencana audit
10. Agar audit evidence menjadi data dukung yang baik, harus memenuhi kriteria/kualitas tertentu, jelaskan kriteria/kualitas tersebut!

Jawab

1. Kategori Pengendali Internal
   - Preventif: Mencegah hal yang tdk diinginkan
   - Detektif: Menemukan hal yang sedang terjadi
   - Korektif: Memperbaiki dan memulihkan kejadian yang telah terjadi
   - Dan dipisahkan dalam tujuan fungsi yang berbeda yaitu level administratif, teknis dan fisik
2. •mematuhi perubahan peraturan bahwa perusahaan memiliki audit internal
   •mengevaluasi efektivitas fungsi penerapan kontrol;
   •mengkonfirmasi kepatuhan terhadap kebijakan, proses, dan prosedur internal;
   •memeriksa kesesuaian dengan tata kelola atau standar tata kelola atau tata kelola TI;
   •menganalisis kerentanan dan pengaturan konfigurasi untuk mendukung pemantauan terus menerus
   •mengidentifikasi kelemahan dan kekurangan sebagai bagian dari risiko awal atau yang sedang berlangsung
   •mengukur kinerja terhadap tolok ukur mutu atau perjanjian tingkat layanan;
   •memverifikasi dan memvalidasi rekayasa sistem atau praktek manajemen proyek TI; dan
   •menilai sendiri organisasi terhadap standar atau kriteria yang akan digunakan di Indonesia sebagi antisipasi audit eksternal
3. - Untuk audit eksternal, baseline audit biasanya didefinisikan dalam peraturan atau persyaratan hukum atau peraturan yang berkaitan dengan tujuan dan sasaran audit eksternal.
   - Untuk audit internal, organisasi sering memiliki fleksibilitas untuk menentukan garis dasar mereka sendiri atau untuk mengadopsi standar, kerangka kerja, atau persyaratan yang ditentukan oleh organisasi.
4. Sistem manajemen kemamanan Infomrasi adalah kumpulan dari kebijakan dan prosedur ntuk mengatur data sensitif milik organisasi seccara sistematis (Rouse, 2011)
5. -Keamanan Fisik: Ini mencakup perlindungan fisik terhadap aset organisasi seperti bangunan, peralatan, dan infrastruktur fisik.
   -Keamanan Personal:Ini berkaitan dengan perlindungan terhadap karyawan, pengunjung, atau pihak lain yang memiliki akses ke lingkungan kerja organisasi.
   -Keamanan Operasional:Ini mencakup prosedur, kebijakan, dan praktik yang dirancang untuk melindungi sistem, data, dan operasi organisasi dari kerusakan, kehilangan, atau penyalahgunaan.
   -Keamanan Komunikasi:Ini berkaitan dengan perlindungan terhadap transmisi data dan informasi dari akses tidak sah atau modifikasi selama pengiriman.
   -Keamanan Jaringan:Ini mencakup perlindungan terhadap jaringan komputer dan sistem informasi dari serangan, peretasan, atau akses tidak sah.
6. RFP (Request For Proposal) adalah sebuah dokumen yang digunakan oleh organisasi atau perusahaan untuk mengundang vendor atau pihak ketiga lainnya untuk mengajukan proposal atau penawaran terkait dengan suatu proyek atau layanan tertentu. RFP umumnya digunakan dalam konteks pengadaan barang atau jasa, di mana organisasi membutuhkan solusi atau layanan tertentu yang tidak dapat dipenuhi secara internal dan perlu mencari penyedia eksternal. (Membuat RFP (Request for Proposal) untuk memilih vendor dan produk terbaik berdasarkan spesifikasi pada Tahap 2. •Melakukan bidding untuk memilih vendor dan produk ~ Konten utama RFP. Tentukan spesifikasi detail dari produk dan sistem yang diminta. Ini tidak hanya

mencakup spesifikasi fungsional tetapi juga non-fungsional spesifikasi seperti keandalan dan kinerja)

7. Transmisi data terstruktur antar organisasi melalui sarana elektronik. Ini digunakan untuk mentransfer dokumen elektronik atau data bisnis dari satu sistem komputer ke sistem komputer lain
8. -Perencanaan
   • Penetapan tujuan dan cakupan audit secara umum
   • Peningkatan pemahaman terhadap obyek audit
   • Penilaian risiko
   • Penentuan tujuan dan cakupan audit secara tepat
   • Penetapan kriteria audit
   • Pembuatan rencana audit TI yang detail (termasuk prosedur audit)

   -Pelaksanaan
   • Pemeriksaan desain (test of design)
   • Pemeriksaan efektifitas operasional
   • Evaluasi control (dan compliance testing jika ada)
   • Pengujian isi (substantive testing)
   • Verifikasi temuan

   -Pembuatan Laporan
   • Pembuatan draft laporan
   • Presentasi laporan audit termasuk temuan
   • Finalisasi laporan audit (termasuk rekomendasi,tanggapan audit, dan rencana aksi)

   -Pemeriksaan tindak lanjut
9. Dokumen rencana audit merinci tujuan, lingkup, metodologi, rencana kerja, pengukuran kinerja, prosedur pelaporan, kontrol kualitas, serta risiko dan tantangan yang akan dihadapi selama audit. Ini memberikan panduan yang jelas bagi auditor dalam menjalankan audit dengan efisien dan efektif, memastikan bahwa semua aspek relevan dari entitas yang diaudit ditangani dengan tepat dan terperinci.
10. -Sufficient (cukup): siapapun orangnya akan menghasilkan kesimpulan yang sama berdasarkan barang bukti yang sama.
    -Competent (layak): barang bukti didapatkan dari teknik pengumpulan data yang memadai/ jelas.
    -Relevant (sesuai): sesuai dengan objek audit dan dapat digunakan sebagai dasar temuan dan rekomendasi.
    -Useful (berguna): dapat digunakan organisasi untuk memperbaiki objek yang telah diaudit sehingga tujuan organisasi dapat tercapai.
    Cascarino (39:2007)