Dengan memperhatikan tahapann process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat

boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri

disubmit [erorangan dalam bentuk resume note (tidak presentasi)

Nama : M.Afdhaluddin (192420012)
Kelas : AR1
Mata kuliah : IT Audit
Dosen : Dr. Widya Cholil S.Kom., M.I.T.

TUGAS

IT Audit components

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

Tahapan IT Audit

1. ***Information Gathering***

   Tahap ini, dimana seorang auditor yang mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien.seperti laporan audit sebelumnya, laporan buku besar.

2. ***Review prior audit issues***

Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. ***Risk assessment***

Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat , untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .

4. Develop IT audit

Setelah dilakukan rapat tersebut, auditor mulai menrealisasikan rencana audit , kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.

5. Execute IT audit Plan

Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Muhammad Fajar (192420037)
Kelas : MTI AR2

Tahapann process IT Audit

1. Information Gathering

Sebelum auditor menentukan sifat dan luas pengujian yang harus dilakukan, auditor harus memahami, mencari informasi dan bisnis audit (kebijakan, struktur organisasi, dan praktik yang dilakukan). Setelah itu, analisis risiko audit merupakan bagian yang sangat penting. Ini meliputi review atas pengendalian intern. Dalam tahap ini, auditor juga mengidentifikasi aplikasi yang penting dan berusaha untuk memahami pengendalian terhadap transaksi yang diproses oleh aplikasi tersebut. pada tahap ini pula auditor dapat memutuskan apakah audit dapat diteruskan atau mengundurkan diri dari penugasan audit.

2. Review Prior Audit Issues

Pada tahap ini auditnya berupaya mendapatkan informasi lebih mendalam untuk memahami pengendalian yang diterapkan dalam sistem komputer klien. Auditor harus dapat memperkirakan bahwa hasil audit pada akhirnya harus dapat dijadikan sebagai dasar untuk menilai apakah struktur pengendalian intern yang diterapkan dapat dipercaya atau tidak. Kuat atau tidaknya pengendalian tersebut akan menjadi dasar bagi auditor dalam menentukan langkah selanjutnya.

3. Risk Assessment

Pada tahap ini auditor diharapkan telah dapat memberikan penilaian apakah bukti yang diperoleh dapat atau tidak mendukung informasi yang diaudit. Hasil penilaian tersebut akan menjadi dasar bagi auditor untuk menyiapkan pendapatanya dalam laporan auditan. Auditor harus mengintegrasikan hasil proses dalam pendekatan audit yang diterapkan audit yang diterapkan. Audit meliputi struktur pengendalian intern yang diterapkan perusahaan, yang mencakup:

- Pengendalian umum,
- Pengendalian aplikasi, yang terdiri dari :

(a) pengendalian secara manual,

(b) pengendalian terhadap output sistem informasi, dan

Muhammad Fajar (192420037)
Kelas : MTI AR2

(c) pengendalian yang sudah diprogram.

Dalam melakukan audit tentu memiliki beberapa resiko seperti

- Risiko Inherent – Atau 'Inherent Risk' (IR) adalah risiko yang mungkin timbul akibat karakter bawaan dari suatu transaksi, bisa juga karena : kompleksitas transaksi dan klas transaksi, atau kompleksitas perhitungan, aset yg mudah tercuri/digelapkan, ketiadaan informasi yang sifatnya obyektif. Sudah menjadi pemahaman publik bahwa inherent risk adalah diluar jangkauan auditor dalam melakukan pencegahan. Bahkan, juga diluar kendali pihak auditee sendiri. Jadi dengan kata lain, auditor hanya bisa menemukan tetapi tidak bisa melakukan apa-apa.
- Risiko Pengendalian – Atau 'Control Risk' (CR) adalah risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, tak tahu karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain—thus tidak mampu mencegah potensi salahsaji bersifat material dan/atau penggelapan (fraud). Jadi CR tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee jika mereka mau.
- Risiko Deteksi – Atau 'Detection Risk' (DR), adalah risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud). Jadi DR ada dalam kendali auditor. Itu karena DR sepenuhnya ada pada kendali auditor, maka sudah pasti mereka harus berupaya untuk menekan risiko ini hingga ke tingkatakan yang paling minimal (tidak mungkin menghilangkan risiko ini sepenuhnya).

4. Develop IT Audit Plan

Tujuan perencanaan audit adalah untuk menentukan why, how, when dan by whom sebuah audit akan dilaksanakan. Aktivitas perencanaan audit meliputi :

- Penetapan ruang lingkup dan tujuan audit
- Pengorganisasian tim audit
- Pemahaman mengenai operasi bisnis klien
- Kaji ulang hasil audit sebelumnya (jika ada)
- Mengidentifikasikan faktor-faktor yang mempengaruhi resiko audit
- Penetapan resiko dalam lingkungan audit, misalkan bahwa inherent risk, control risk dan detection risk dalam sebuah on-line processing, networks, dan teknologi maju database lainnya akan lebih besar daripada sebuah sistem akuntansi manual.

5. Execute IT Audit Plan

Padatahapan ini menjalankan plan Audit yang sebelumnya dibuat. Terus menggunakan analitik Dalam audit untuk mendukung prosedur audit

• Meningkatkan kemampuan melalui penggunaan regresi dan analisis statistik

• Mengurangi prosedur pengujian yang tidak efektif melalui pengurangan kontrol yang akan diuji (dasbor pada efektivitas kontrol)

• HASIL: Hasil audit yang lebih efisien dan efektif

Muhammad Fajar (192420037)
Kelas : MTI AR2

6. Customer Satisfaction Evaluation

Pada tahap ini auditor diharapkan telah dapat memberikan penilaian apakah bukti yang diperoleh dapat atau tidak mendukung informasi yang diaudit. Akan adanya evaluasi ke customer dari apa yang di kerjakan dalam plan audit seperti Audit Service, Audit Staff, Conduct of Audit, Audit Reporting, Customer Service, Overall rating of internal Audit Authority Specific topics dan Text Question. Hasil penilaian tersebut akan menjadi dasar bagi auditor untuk menyiapkan pendapatanya dalam laporan auditan. Auditor harus mengintegrasikan hasil proses dalam pendekatan audit yang diterapkan audit yang diterapkan. Audit meliputi struktur pengendalian intern yang diterapkan perusahaan, yang mencakup :

(1) pengendalian umum,

(2) pengendalian aplikasi, yang terdiri dari :

(a) pengendalian secara manual,

(b) pengendalian terhadap output sistem informasi, dan (

c) pengendalian yang sudah diprogram.

Nama : Muhammad Hadrifiansyah
Kelas : AR1
Mata kuliah : IT Audit
Dosen : Dr. WidyaCholilS.Kom., M.I.T.

TUGAS

IT Audit components

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

Tahapan IT Audit

1. ***Information Gathering***

   Tahap ini, dimana seorang auditor yang mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien. seperti laporan audit sebelumnya, laporan buku besar.

2. ***Review prior audit issues***

Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. ***Risk assessment***

Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat ,untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , di karenakan organisasi tersebut dapat menerima atau tidak nyaresiko yang mungkin akan terjadi .

4. DevelopIT audit

Setelah dilakukan rapat tersebut, auditor mulai menrealisasikan rencana audit ,kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak .auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.

5. Execute IT audit Plan

Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkaitlainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan di lakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

TUGAS AUDIT IT

KOMPONEN DALAM PROSES AUDIT IT

Disusun Oleh : 1. Hendra Yada Putra (192420034)

2. Muhammad Ichsan (192420031)

Kelas : MTI 3B

Mata Kuliah : AUDIT IT

Dosen Pengajar : DR Widya Cholil S.KOM, MIT

UNIVERSITAS BINA DARMA

PALEMBANG

2020

PENDAHULULUAN

Audit IT merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan. sehingga menjadi Seorang auditor IT itu tidaklah mudah karena harus bertanggung jawab terhadap gagalnya pengembangan sistem informasi yang menyebabkan kerugian serta menuntut kedisiplinan kerja secara profesional.

Agar dapat memahami proses audit teknologi informasi, setidaknya harus memahami jenis/bagian secara umum dari teknologi informasi itu sendiri yang terdiri atas:

1. Systems and Applications

Pada bagian ini mewakili bagaimana sebuah data diproses melalui aplikasi perangkat lunak komputer yang dikelola melalui suatu sistem yang biasanya terdiri atas tingkatan hierarkis yang mengikuti aturan bisnis yang berlaku di organisasi yang menggunakannya. Sehingga proses auditnya sendiri akan meliputi verifikasi terhadap sistem dan aplikasinya apakah handal, efisien serta memiliki kontrol yang melekat untuk memastikan kebenaran, kehandalan, kecepatan maupun keamanan pada saat pengiriman, pemrosesan serta pengeluaran informasi di setiap tingkatan kegiatan sistem.

2. Information Processing Facilities

Merupakan komponen yang terkait dengan fasilitas-fasilitas yang digunakan untuk mengolah informasi di suatu organisasi. Biasanya ini terkait dengan perangkat keras seperti misalkan scanner, komputer server, formulir, dsb. Di komponen teknologi informasi ini dilakukan verifikasi untuk memastikan apakah fasilitas pemrosesan terkendalikan untuk memastikan kecepatan, ketepatan dan tingkat efisiensi dari aplikasi-aplikasi berada dalam kondisi normal serta di bawah kemungkinan adanya potensi kerusakan/gangguan.

3. Systems Development

Adalah bagian dari proses pembangunan maupun pengembangan dari sistem yang sudah ada dalam suatu organisasi sesuai tujuan-tujuan aktivitasnya. Proses audit pada komponen ini ditujukan untuk memverifikasi apakah setiap sistem yang sedang dalam proses pengembangan

sesuai dengan tujuan/pedoman/arahan/visi/misi dari organisasi penggunanya. Selain itu proses audit pada bagian ini juga ditujukan untuk memastikan apakah selama proses pengembangan sistem sesuai dengan standar-standar yang secara umum digunakan dalam pengembangan sistem.

4. Management of IT and Enterprise Architecture

Pengelolaan atas teknologi informasi serta arsitektur seluruh lingkup internal organisasi yang disesuaikan dengan struktur dan prosedur yang ditetapkan oleh manajemen adalah sangat penting. Pentingnya hal tersebut memerlukan proses audit yang dilaksanakan untuk memastikan apakah segenap lingkungan/komponen organisasi dalam pemrosesan informasinya dilakukan secara terkendali dan efisien.

5. Client/Server, Telecommunications, Intranets, and Extranets

Komputer, peralatan telekomunikasi, sistem jaringan komunikasi data elektronik (intranet/extranet) serta perangkat-perangkat keras pengolahan data elektronik lainnya adalah komponen dari sebuah teknologi informasi. Audit di bagian ini menjadi penting untuk melakukan verifikasi atas seperangkat pengendalian pada infrastruktur perangkat keras yang digunakan dalam pemrosesan serta komunikasi data secara elektronik dalam suatu sistem jaringan yang terintegrasi.

KOMPENAN APA SAJA DALAM PROSES AUDIT?

Dimana dalam melaksakan proses audit teknologi/sistem informasi meliputi tahapan-tahapan berikut :

1. Planning

Pada tahapan ini lakukan perencanaan menyeluruh atas hal-hal mendasar seperti:

- Fokus komponen yang akan diaudit
- Alat (framework) yang akan digunakan sebagai pedoman pelaksanaan audit
- Kebutuhan sumber daya yang diperlukan
- Hasil akhir yang diinginkan dari proses audit
- Jadual kegiatan
- Rencana Anggaran Biaya jika menggunakan jasa pihak lainnya

2. Studying and Evaluating Controls

Pada tahap ini setelah kita mempelajari bagaimana kondisi dari obyek audit kita. Biasanya secara mendasar fokus dari audit adalah kemampuan pengendalian/kontrol atas obyek tersebut. Kemudian dari hasil melakukan analisis tersebut disusun evaluasi atasnya.

3. Testing and Evaluating Controls

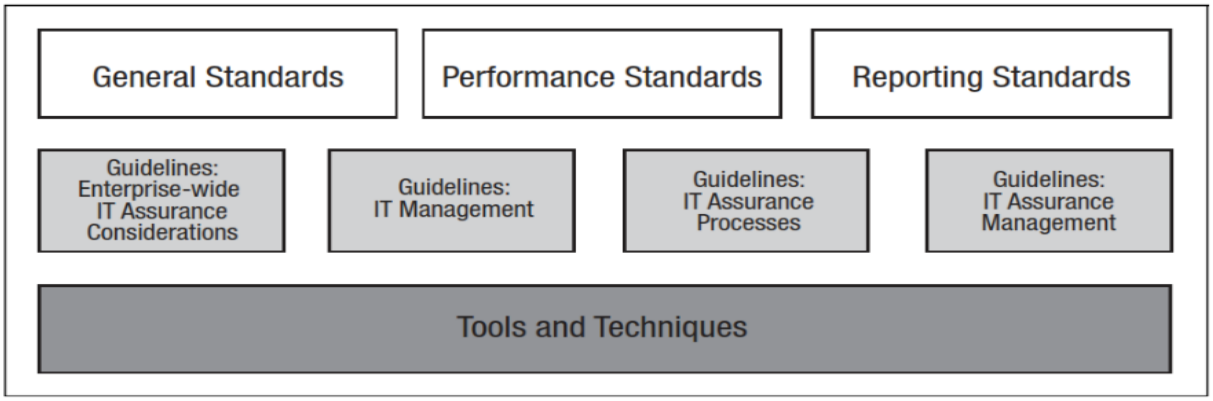
Setelah mempelajari dan mengevaluasi hasil analisisnya, tahap berikutnya adalah melakukan serangkaian pengujian atas obyek audit kita. Pengujian tersebut tentunya menggunakan standar-standar baku berdasarkan framework yang sudah ditetapkan sebelumnya untuk digunakan dalam proses audit. Sama halnya dengan tahapan sebelumnya, inti dari proses audit adalah melakukan telaah uji atas kemampuan pengendalian atas setiap aspek dari sumber daya teknologi informasi yang ada berdasarkan batasan-batasan yang sudah disepakati sebelumnya.

Standar yang digunakan dalam mengaudit sistem informasi adalah standar yang diterbitkan oleh ISACA yaitu ISACA IS Auditing Standard. Selain itu ISACA juga menerbitkan IS Auditing Guidance dan IS Auditing Procedure.

Perlu adanya penelitian berupa pengembangan kerangka kerja penyusunan program audit sistem informasi dengan menggunakan Information Technology Assurance Framework (ITAF) dari ISACA yang lebih menitikberatkan pada proses audit, didesain untuk profesional yang bergerak di bidang jasa audit atau assurance dan menggunakan istilah-istilah yang lebih familiar bagi peneliti.

Konsep ITAF

ISACA merupakan organisasi internasional yang bergerak dalam jasa IT Governance yang didirikan tahun 1969. ISACA merupakan sponsor utama konferensi internasional bidang IT Governance, penerbit System Control Journal, pengembang utama standar audit dan pengendalian sistem serta merupakan administrator CISA (Certified Information System Auditor). Pada tahun 2008 ISACA mengeluarkan produk berupa Information Technology Assurance Framework (ITAF), sebuah sumber pembelajaran bagi para profesional yang bergerak dalam jasa assurance. ITAF merupakan produk dari Information System Audit and Control Association(ISACA) yang menyediakan sebuah kerangka tunggal yang berisi standar, pedoman (Guidelines) dan teknik dalam melaksanakan audit dan assurance termasuk di dalamnya perencanaan, lingkup audit, pelaksanaan dan pelaporan audit dan jasa assurance TI.



Gambar 1 pembagian ruang likgkup kerja ITAF

ITAF terbagi menjadi tiga bagian seperti terlihat dalam gambar yaitu:

1) Standar dikelompokkan menjadi standar umum, standar kinerja dan standar pelaporan. Standar digambarkan di gambar 1 dengan warna putih, artinya standar tersebut harus

dilaksanakan(mandatory), bila ada penyimpangan atas standar harus diungkapkan penyebab dan konsekuensinya terhadap pelaksanaan audit. Standar didesain bersifat keharusan (mandatory) untuk setiap kasus penugasan. Setiap penyimpangan dari standar dalam penugasan audit atau assurance harus diungkapkan dalam laporan audit. Standar audit TI mengadopsi standar audit umum terdiri dari atandar umum, standar pelaksanaan dan standar pelaporan. Isi dan substansinya relatif sama dengan standar audit keuangan. 2)Pedoman dikelompokkan menjadi empat bagian dan digambarkan dengan warna abu-abu. Ini berarti pedoman tersebut tidak bersifat mandatory atau tidak bersifat keharusan, namun sangat direkomendasikan penggunaannya. Auditor harus mampu membuktikan adanya penyimpangan TI dengan metode pengumpulan bukti menurut pedoman ini. Meski tidak seluruh pedoman dapat diterapkan untuk seluruh situasi, namun pedoman tersebut tetap patut menjadi bahan pertimbangan auditor dalam melaksanakan audit. Pedoman audit berisi informasi dan petunjuk mengenai area audit. Sejalan dengan tiga kategori standar di atas, pedoman ini berfokus terhadap berbagai pendekatan audit, metode audit, alat dan teknik audit dan materi lain untuk membantu dalam perencanaan, pelaksanaan, penilaian dan pelaporan audit. Pedoman tersebut juga membantu menjernihkan hubungan antara kegiatan perusahaan dan kegiatan penugasan audit oleh auditor (ITAF's summary, 2009). Pedoman audit ini tidak bersifat keharusan, namun sangat direkomendasikan penggunaannya. Auditor harus mampu membuktikan adanya penyimpangan TI dengan metode pengumpulan bukti menurut pedoman ini. Meski tidak seluruh pedoman dapat diterapkan untuk seluruh situasi, namun pedoman tersebut tetap patut menjadi bahan pertimbangan auditor dalam melaksanakan audit

3) Alat dan Teknik Audit, menyediakan infromasi spesifik mengenai metode, alat dan template dan juga menyediakan petunjuk penerapan dalam aktivitas audit. Khusus untuk alat dan teknik audit SI ini, bentuk dari kerangka ITAF berasal dari dokumen lain publikasi ISACA baik berupa buku, jurnal, petunjuk teknis dan sebagainya. Alat dan teknik dari ITAF ini digambarkan abu-abu kehitaman artinya penggunaannya bersifat fleksibel, dapat digunakan atau tidak oleh auditor sesuai kondisi lapangan. Sedangkan alat dan teknik audit berisi informasi dan bahan pelengkap yang mendukung pedoman audit TI. Dalam beberapa kasus, teknik audit berisi prosedur alternatif yang dapat diterapkan dalam penugasan audit. Auditor hanya mengadopsi alat dan teknik tersebut bila sesuai dengan kondisi, relevan dengan tujuan

dan tidak memberikan informasi yang bias. Sampai dengan saat ini sudah terdapat 11 prosedur audit TI yang dipublikasikan ISACA. Prosedur-prosedur tersebut dipublikasikan secara terpisah dari ITAF, namun menjadi bagian dari kerangka ITAF yang dapat dipedomani dalam melaksanakan kegiatan audit.

Hasil dari pengujian tersebut kemudian dievaluasi untuk disusun dalam laporan hasil pemeriksaan.

4. Reporting

Seluruh tahapan yang telah dilakukan sebelumnya dalam proses audit teknologi informasi kemudian didokumentasikan dalam suatu laporan hasil pemeriksaan/audit.

5. Follow-up

Hasil dari laporan hasil pemeriksaan/audit kemudian ditindaklanjuti sebagai acuan para pemegang kebijakan di setiap tingkatan manajemen organisasi dalam menentukan arah pengembangan dari penerapan teknologi informasi di organisasi tersebut.

Risiko-risiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain :

- Biaya pengembangan sistem melampaui anggaran yang ditetapkan.
- Sistem tidak dapat diimplementasikan sesuai dengan jadwal yang ditetapkan.
- Sistem yang telah dibangun tidak memenuhi kebutuhan pengguna.
- Sistem yang dibangun tidak memberikan dampak effisiensi dan nilai ekonomis terhadap jalannya operasi institusi, baik pada masa sekarang maupun masa datang.
- Sistem yang berjalan tidak menaati perjanjian dengan pihak ketiga atau memenuhi aturan yang berlaku.

Nama : M.Nang Alhafiz
NIM : 192420008
Kelas : AR1
Mata kuliah : IT Audit
Dosen : Dr. Widya Cholil S.Kom., M.I.T.

TUGAS

IT Audit components

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

Tahapan IT Audit

1. ***Information Gathering***

   Tahap ini, dimana seorang auditor yang mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien.seperti laporan audit sebelumnya, laporan buku besar.

2. ***Review prior audit issues***

Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. ***Risk assessment***

Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat , untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .

4. Develop IT audit

Setelah dilakukan rapat tersebut, auditor mulai menrealisasikan rencana audit , kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.

5. Execute IT audit Plan

Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Nizar Firliansa
192420005

Komponen dalam IT Audit

1. **Pendefinisian tujuan perusahaan**
2. **Penentuan isu, tujuan dan perspektif bisnis antara penanggung jawab. bagian dengan bagian TI**
3. **Review terhadap pengorganisasian bagian TI yang meliputi perencanaan.**
4. **Assessment infrastruktur teknologi, assessment aplikasi bisnis**
5. **Temuan-temuan**
6. **Laporan rekomendasi.**

Tugas Auditor TI :

1. Memastikan sisi-sisi penerapan IT memiliki kontrol yang diperlukan.
2. Memastikan kontrol tersebut diterapkan dengan baik sesuai yang diharapkan.

Audit Internal

1. Dilakukan oleh atau atas nama perusahaan sendiri
2. Biasanya untuk management review atau tujuan internal perusahaan

fungsi audit internal :

- mengevaluasi efektivitas pengendalian yang dilakukan; mengkonfirmasikan kepatuhan terhadap kebijakan internal, proses, dan prosedur;
- memeriksa kesesuaian dengan tata kelola TI atau kontrol kerangka kerja dan standar;
- menganalisis kerentanan dan pengaturan konfigurasi untuk mendukung pemantauan terus menerus;
- mengidentifikasi kelemahan dan kekurangan sebagai bagian dari manajemen risiko awal atau berkelanjutan

Audit TI eksternal

1. Dilakukan oleh pihak yang memiliki kepentingan thd perusahaan
2. Dilakukan oleh pihak independen dari luar perusahaan. Misalnya untuk sertifikasi (ISO 9001, BS7799 dll).

Audit ekternal dilakukan oleh auditor dan entitas luar subjek organisasi untuk audit. Tergantung pada ukuran organisasi dan ruang lingkup dan kompleksitas audit TI, audit eksternal dapat dilakukan oleh auditor tunggal atau tim.

Audit Proses

- Perencanaan
- Pengujian
- Pelaporan
- Follow up

Perencanaan

1. Penilaian Risiko Tahunan
2. Rencana Audit Awal
3. Persetujuan Dewan Pengunjung
4. Pemberitahuan dan Permintaan Informasi
5. Pahami Risiko dan Kontrol Anda
6. Konferensi Pembukaan

Pengujian

1. Melakukan Pengujian Pengendalian. Pengujian pengendalian adalah pengumpulan bukti-bukti yang berfungsi secara efektif dan konsisten.
2. Mengevaluasi Pengujian Pengendalian yang diperoleh
3. Penilaian Akhir terhadap Risiko Pengendalian
4. Mengembangkan Program Audit Final

Pelaporan

1. Mencatat Laporan Audit.
2. Mencatat Kondisi-kondisi yang dapat dilaporkan

Pada tahap penyelesaian operasional audit laporan diberikan kepada manajemen dan komite audit perusahaan.Isi dari laporan ini bervariasi sesuai pada harapan manajemen.
contohnya : laporan mungkin terdiri dari pendapat yang mengacu pada fungsi pengelolaan informasi yang efektif dan efisien, dan saran-saran yang membangun.

Follow up

Internal auditor diwajibkan untuk melakukan follow up pada report audit findings dan memberikan rekomendasi untuk memastikan bahwa komite audit mengambil langkah yang tepat.

AUDIT PROCESS

MTI REG-B || AUDIT

DANOVRUD

> Daniel > Novita > Rudi

INTRODUCTION

Audit Internal membantu organisasi mencapai tujuan mereka Tujuan dengan mengevaluasi risiko bisnis dan kontrol dan jika sesuai, tawarkan rekomendasi kepada meningkatkan manajemen risiko dan tata kelola proses.

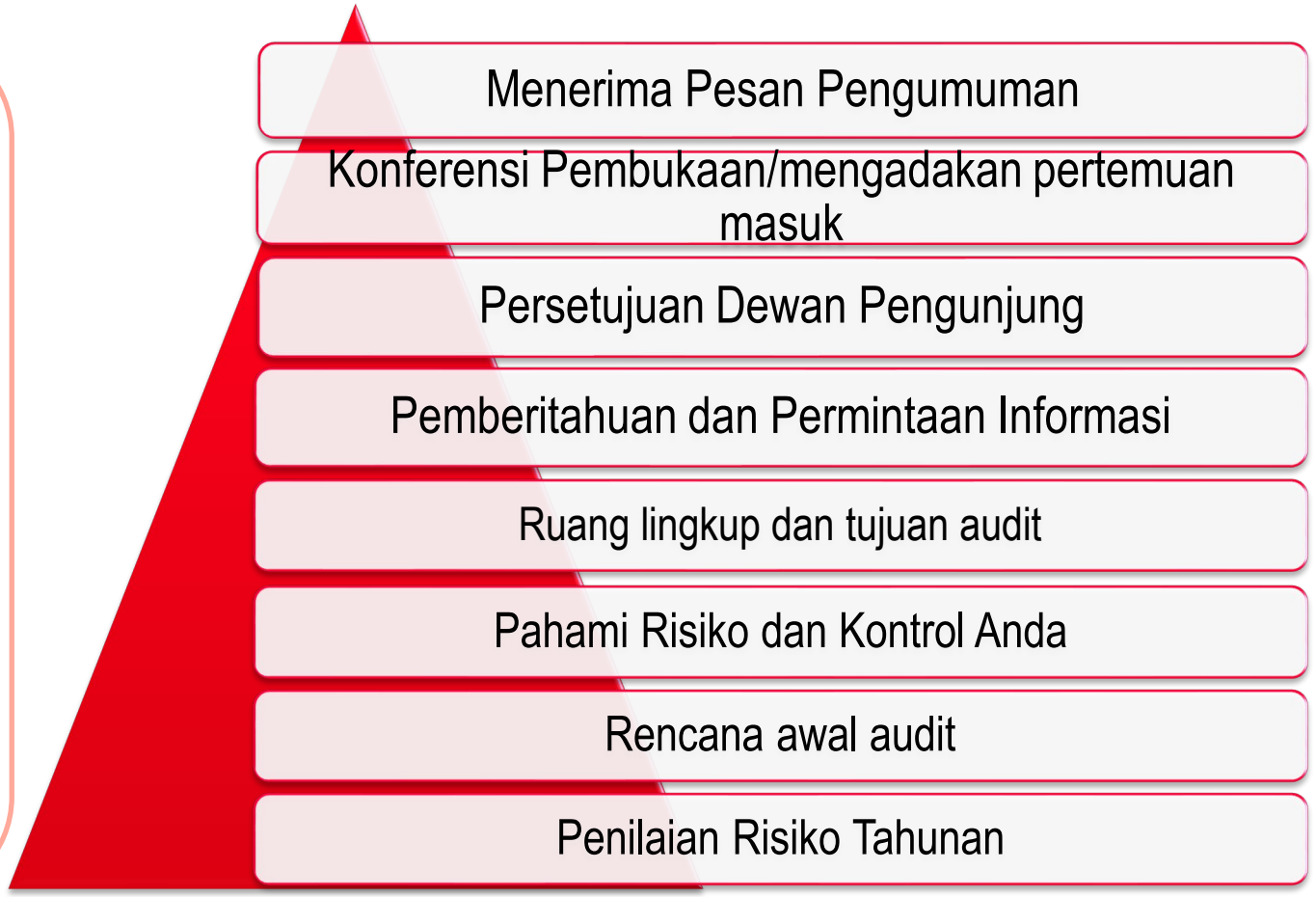
Proyek audit yang paling sukses adalah proyek di mana Anda, klien audit, dan Audit Internal memiliki hubungan kerja yang konstruktif.

AUDIT PROCESS

PLANNING

Planning adalah komunikasi. Selama tahap perencanaan, tim akan memberi tahu organisasi/pihak terkait tentang audit tersebut melalui surat pengumuman, pesan, dll.

Komponen dan Tugas



TESTING

Testing adala terjun kelapangan. Dalam fase ini auditor mengumpulkan informasi yang relevan tentang unit untuk memperoleh gambaran umum operasi dan pengendalian internal serta melakukan pengujian transaksi.

Komponen dan Tugas

- Melakukan walk-thru pengendalian umum dan melakukan manajemen risiko awal
- Bertanya atau interview pada staf dalam prosedure
- Manajemen Sumber Daya
- Melakukan audit uji pekerjaan
- Keamanan
- Pencadangan & Pemulihan
- Manajemen Sumber Daya
- SituS Web
- Scope atau ruang lingkup (resorce mng, data, security, stakholder)
- komunikasi selama kemajuan audit dan temuan potensial (Komunikasi berkesinambiungan)

REPORTING

Reporting adalah hasil auditing.
Audit haruslah observasi, pengamatan, bagaimana proses, peraturan, masalah, baru dilaporkan dalam laporan audit, kemudian membahas rekomendasi atau solusi setelah analisis (apa yang harus kita lakukan terhadap masalah, penyebabnya apa saja.

Komponen dan Tugas

- Melakukan Pertemuan penutup dengan management untuk membahas observasi dan rekomendasi
- Menerbitkan draf laporan kepada manajemen unit dan meminta tanggapan manajemen untuk menangani rekomendasi.
- Menerbitkan memorandum manajemen untuk mengkomunikasikan temuan yang kurang signifikan
- Terbitkan laporan akhir ke unit dan manajemen senior dengan respon manajemen disertakan
- Meminta manajemen untuk menyelesaikan evaluasi survei klien
- Mengembangkan Rencana, Jadwal, dan Prioritas

REPORTING

Komponen dan Tugas

Reporting adalah hasil auditing. Pada akhirnya laporan sent to pihak berwajib *management, ceo, board of visitor, dll.*

- Human Error (Adm, dll)
- Kesenjangan Prosedure
- Keamanan (Operating System, Security)
- Cyber Crime
- Surat pernyataan (
- Bukti Releven (Bukti memperkuat alasan)
- Metode (Framework, metode penyelesaian, dll)
- Solusi (Penawaran penanganan, penanggulanan,note)
- Keterbatasan (Keterbatasan audit, seperti alat, tools)
- Referensi (daftar rujukan)

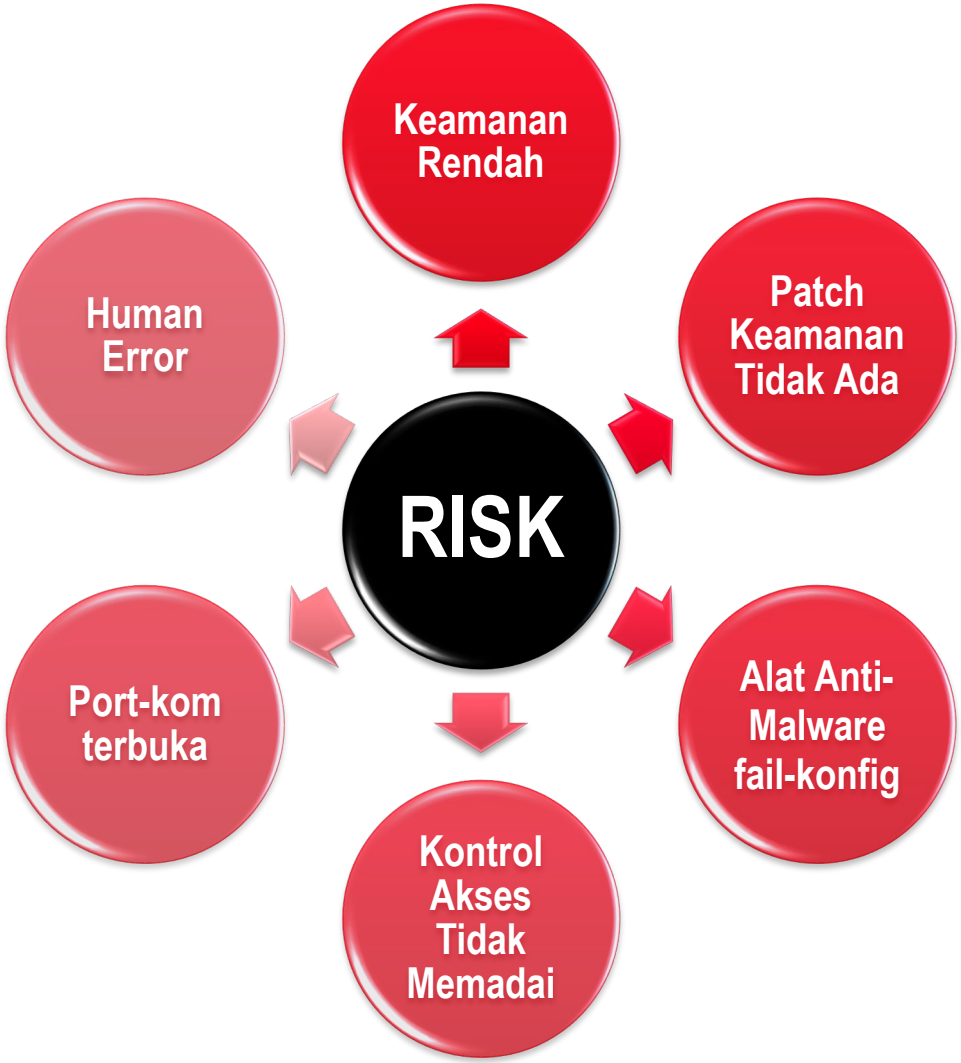
FOLLOW-UP

Follow-Up adalah memantau. Audit Internal akan melakukan review tindak lanjut.

Komponen dan Tugas

- Tim akan menghubungi unit untuk mendapatkan pembaruan tentang melaporkan kemajuan rekomendasi.
- Penyelidikan atau pengujian tambahan dapat dilakukan.
- Tindakan Tindak Lanjut Berdasarkan "Rencana Tindakan Manajemen"
- Kemajuan Dipantau
- Beberapa Pengujian Ulang Mungkin Diperlukan
- Dewan Pengunjung Diperbarui
- Progress
- Update report 1st (dengan diskusi, komunikasi dll)
- Audit is closed

GENERAL OBSERVATION

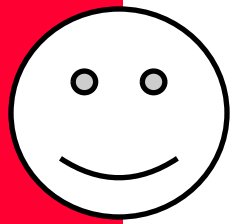


OTHER

Tujuan penulis adalah agar anda terus terlibat di setiap tahap audit process, sehingga Anda memahami apa yang kami lakukan dan mengapa.

TERIMA KASIH

PENUTUP



MTI REG-B || AUDIT

DANOVRUD

> Daniel > Novita > Rudi

Note;
Maaf buk kami membuat tenplate dengan power point disebabkan poin - poin kami deskripsikan kembali dalam note dan ada alasan tahapan - tahapan.

Nama : **Rachmat Akbar**
Nim : **192420036**
Kelas **: Mti A2**
Mata Kuliah : **IT AUDIT**

IT Audit

It audit adalah Penilaian / pengujian kontrol dalam sistem informasi atau infrastruktur teknologi informasi . IT Audit adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh.

Stakeholders yang terlibat dalam proses it audit adalah

– Internal IT Deparment
– External IT Consultant
– Board of Commision
– Management
– Internal IT Auditor
– Internal IT Audit Officer
– External IT Auditor

Komponen yang di IT audit

- System Audit
  Audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi strandar nasional atau internasional
- Compliance Audit
  Untuk menguji efektifitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain
- Product / Service Audit
  Untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

Pendekatan dalam proses IT audit

1. *Auditing Around Computer* (Audit Sekitar Komputer) yaitu dimana penggunaan komputer pada tahap proses diabaikan.
2. *Auditing Throught Computer* (Auditing Melalui Komputer) yaitu dimana pada tahap proses penggunaan komputer telah aktif.
3. *Auditing With Computer* (Auditing Dengan Komputer) yaitu dimana input, proses dan output telah menggunakan komputer.

Framework yang dapat digunakan pada kegiatan IT audit

1. COBIT® (Control Objectives for Information and related Technology)
2. COSO (Committee of Sponsoring Organisations of the Treadway Commission) Internal Control—Integrated Framework
3. ISO/IEC 17799:2005 Code of Practice for Information Security Management
4. FIPS PUB 200
5. ISO/IEC TR 13335
6. ISO/IEC 15408:2005/Common Criteria/ITSEC
7. PRINCE2
8. PMBOK
9. TickIT
10. CMMI
11. TOGAF 8.1
12. IT Baseline Protection Manual
13. NIST 800-14

Tahapan yang dilakukan pada IT audit

1. Information gathering
   Mengumpulkan informasi penting tentang bisnis, budaya, organisasi TI, dll.
2. Review Prior Audit Issues
   Melakukan tindak lanjut masalah yang ada pada audit sebelumnya berdasarkan tanggal penyelesaian yang telah ditetapkan sebelumnya
3. Risk Assessment
   Melakukan Identifikasi High Risk Area. Melakukan Validasi dan prioritaskan High Risk Area tersebut
4. Develop IT Audit Plan
   Mengusulkan Rencana Audit TI yang kemudian akan difinalisasi oleh tim manajemen klien
5. Execute IT Audit Plan
   Mengkoordinasikan dan melaksanakan proyek audit yang disetujui, melaporkan temuan, dan tindakan yang disarankan
6. Customer Satisfaction Evaluation
   Adalah merupakan feedback dari costumer tentang audit yang telah dilaksanakan

Nama : Ria Aprinda

NIM : 192420022

Kelas : MTI 21 Regular A R1

Tugas IT Audit Components

Tahapan Proses Audit

Dalam melaksanakan tugasnya, auditor yang akan melakukan proses audit di lingkungan PDE mempunyai 4 tahapan audit sebagai berikut :

1. Perencanaan Audit (Audit Planning) : Tujuan perencanaan audit adalah untuk menentukan why, how, when dan by whom sebuah audit akan dilaksanakan.

   Aktivitas perencanaan audit meliputi:

   - Penetapan ruang lingkup dan tujuan audit
   - Pengorganisasian tim audit
   - Pemahaman mengenai operasi bisnis klien
   - Kaji ulang hasil audit sebelumnya (jika ada)
   - Mengidentifikasikan faktor-faktor yang mempengaruhi resiko audit
   - Penetapan resiko dalam lingkungan audit, misalkan bahwa inherent risk, control risk dan detection risk dalam sebuah on-line processing, networks, dan teknologi maju database lainnya akan lebih besar daripada sebuah sistem akuntansi manual.

2. Penyiapan program audit (Prepare audit program) : yaitu antara lain adalah mengumpulkan bukti audit (Collection of Audit Evidence) yang meliputi :

   - Mengobservasi aktivitas operasional di lingkungan PDE.
   - Mengkaji ulang sistem dokumentasi PDE.
   - Mendiskusikan dan mengajukan pertanyaan-pertanyaan dengan petugas berwenang.
   - Pengujian keberadaan dan kondisi fisik aktiva.
   - Konfirmasi melalui pihak ketiga
   - Menilai kembali dan re-performance prosedur sistem PDE.

- Vouching ke dokumen sumber.
- Analytical review dan metodesampling.

3. Evaluasi bukti (Evaluation of Audit Evidence) : Auditor menggunakan bukti untuk memperoleh keyakinan yang memadai (reasonable assurance), jika inherent risk dan control risk sangat tinggi, maka harus mendapatkan reasonable assurance yang lebih besar.
   Aktivitas evaluasi bukti yang diperoleh meliputi :
   - Menilai (assess) kualitas pengendalian internal PDE.
   - Menilai reliabilitas informasi PDE.
   - Menilai kinerja operasional PDE.
   - Mempertimbangkan kembali kebutuhan adanya bukti tambahan.
   - Mempertimbangkan faktor resiko.
   - Mempertimbangkan tingkat materialitas.
   - Bagaimana perolehan bukti audit.
4. Mengkomunikasikan hasil audit : Auditor menyiapkan beberapa laporan temuan dan mungkin merekomendasikan beberapa usulan yang terkait dengan pemeriksaan dengan di dukung oleh bukti dan dalam kertas kerjanya. Setelah direkomendasikan juga harus dipantau apakah rekomendasinya itu ditindaklanjuti.

Komponen IT Auditing

Komponen *IT Auditing* berasal dari berbagai area:

1. *Auditing* tradisional, membantu menambah pengetahuan praktik kontrol internal dan keseluruhan filosofi mengenai kontrol.
2. *IS management*, membantu memberikan metodologi untuk mencapai kesuksesan perancangan dan pengembangan sistem.
3. Ilmu perilaku, membantu dalam menganalisis faktor penyebab kegagalan sistem informasi yang disebabkan oleh manusia.
4. Ilmu computer, berkontribusi menambah pengetahuan mengenai konsep kontrol, disiplin, teori dan model formal lainnya yang menjadi dasar perancangan *hardware* dan *software* sebagai dasar dalam menjaga validitas, reliabilitas dan integritas data.

AUDIT PROCESS

MTI REG-B || AUDIT

DANOVRUD

> Daniel > Novita > Rudi

INTRODUCTION

Audit Internal membantu organisasi mencapai tujuan mereka Tujuan dengan mengevaluasi risiko bisnis dan kontrol dan jika sesuai, tawarkan rekomendasi kepada meningkatkan manajemen risiko dan tata kelola proses.

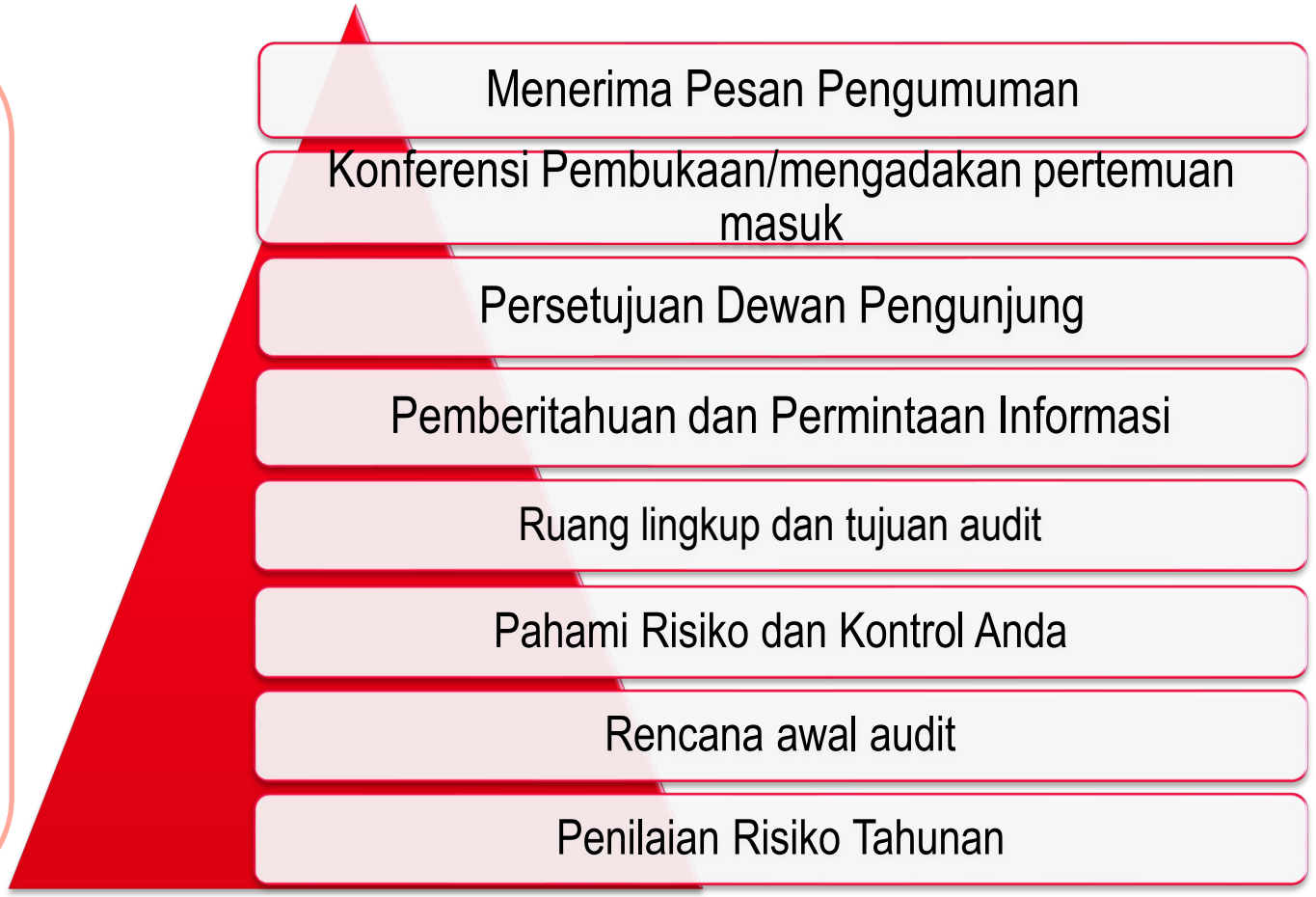
Proyek audit yang paling sukses adalah proyek di mana Anda, klien audit, dan Audit Internal memiliki hubungan kerja yang konstruktif.

AUDIT PROCESS

PLANNING

Planning adalah komunikasi. Selama tahap perencanaan, tim akan memberi tahu organisasi/pihak terkait tentang audit tersebut melalui surat pengumuman, pesan, dll.

Komponen dan Tugas



TESTING

Testing adala terjun kelapangan. Dalam fase ini auditor mengumpulkan informasi yang relevan tentang unit untuk memperoleh gambaran umum operasi dan pengendalian internal serta melakukan pengujian transaksi.

Komponen dan Tugas

- Melakukan walk-thru pengendalian umum dan melakukan manajemen risiko awal
- Bertanya atau interview pada staf dalam prosedure
- Manajemen Sumber Daya
- Melakukan audit uji pekerjaan
- Keamanan
- Pencadangan & Pemulihan
- Manajemen Sumber Daya
- SituS Web
- Scope atau ruang lingkup (resorce mng, data, security, stakholder)
- komunikasi selama kemajuan audit dan temuan potensial (Komunikasi berkesinambiungan)

REPORTING

Reporting adalah hasil auditing.
Audit haruslah observasi, pengamatan, bagaimana proses, peraturan, masalah, baru dilaporkan dalam laporan audit, kemudian membahas rekomendasi atau solusi setelah analisis (apa yang harus kita lakukan terhadap masalah, penyebabnya apa saja.

Komponen dan Tugas

- Melakukan Pertemuan penutup dengan management untuk membahas observasi dan rekomendasi
- Menerbitkan draf laporan kepada manajemen unit dan meminta tanggapan manajemen untuk menangani rekomendasi.
- Menerbitkan memorandum manajemen untuk mengkomunikasikan temuan yang kurang signifikan
- Terbitkan laporan akhir ke unit dan manajemen senior dengan respon manajemen disertakan
- Meminta manajemen untuk menyelesaikan evaluasi survei klien
- Mengembangkan Rencana, Jadwal, dan Prioritas

REPORTING

Komponen dan Tugas

Reporting adalah hasil auditing. Pada akhirnya laporan sent to pihak berwajib *management, ceo, board of visitor, dll.*

- Human Error (Adm, dll)
- Kesenjangan Prosedure
- Keamanan (Operating System, Security)
- Cyber Crime
- Surat pernyataan (
- Bukti Releven (Bukti memperkuat alasan)
- Metode (Framework, metode penyelesaian, dll)
- Solusi (Penawaran penanganan, penanggulanan,note)
- Keterbatasan (Keterbatasan audit, seperti alat, tools)
- Referensi (daftar rujukan)

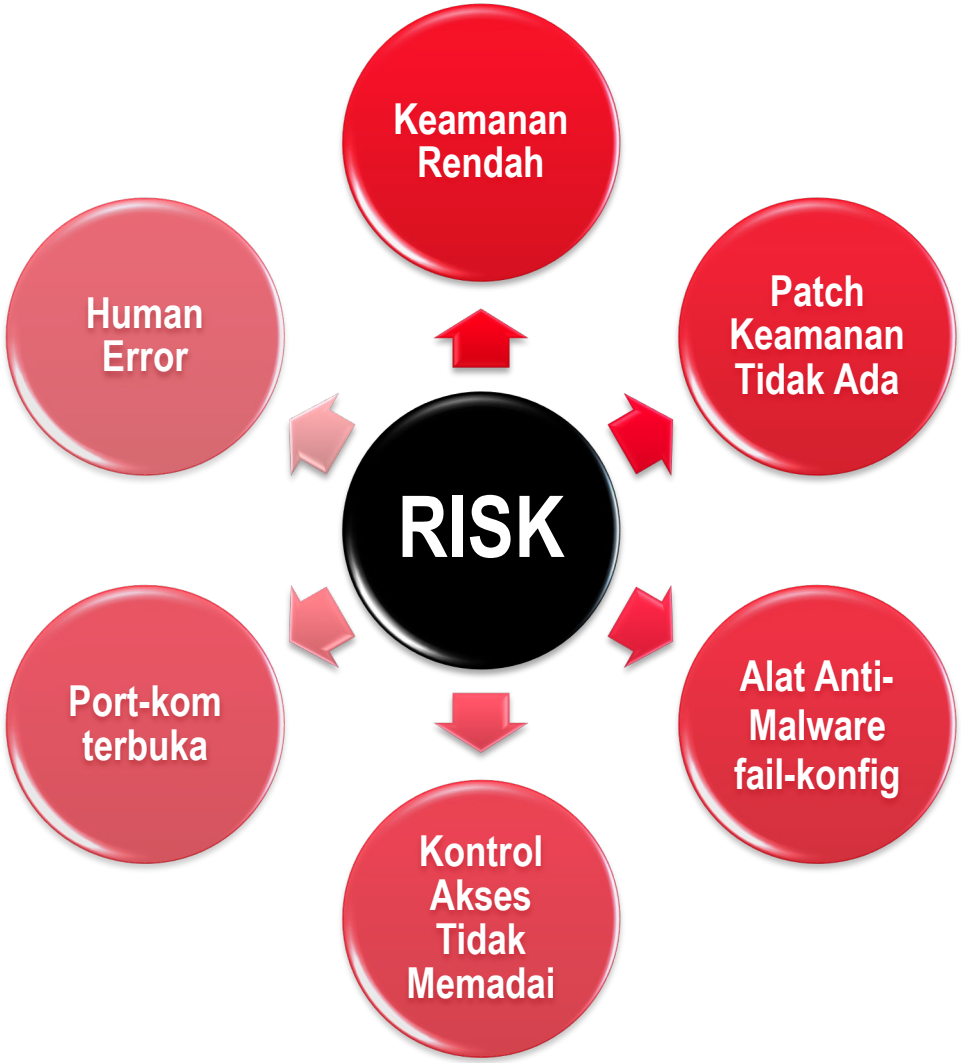
FOLLOW-UP

Follow-Up adalah memantau. Audit Internal akan melakukan review tindak lanjut.

Komponen dan Tugas

- Tim akan menghubungi unit untuk mendapatkan pembaruan tentang melaporkan kemajuan rekomendasi.
- Penyelidikan atau pengujian tambahan dapat dilakukan.
- Tindakan Tindak Lanjut Berdasarkan "Rencana Tindakan Manajemen"
- Kemajuan Dipantau
- Beberapa Pengujian Ulang Mungkin Diperlukan
- Dewan Pengunjung Diperbarui
- Progress
- Update report 1st (dengan diskusi, komunikasi dll)
- Audit is closed

GENERAL OBSERVATION

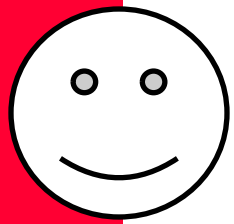


OTHER

Tujuan penulis adalah agar anda terus terlibat di setiap tahap audit process, sehingga Anda memahami apa yang kami lakukan dan mengapa.

TERIMA KASIH

PENUTUP



MTI REG-B || AUDIT

DANOVRUD

> Daniel > Novita > Rudi

Nama : Ryan Andrian

NIM : 192420006

Kelas : MTI A R1

Mata Kuliah : IT Audit

Identifikasi komponen yang terlibat pada Proses Audit TI

Proses Audit TI :

1. Pengumpulan informasi
2. Review isu pada audit sebelumnya
3. Penilaian Resiko
4. Perencanaan audit TI
5. Pelaksanaan audit TI
6. Evaluasi kepuasan pelanggan

Komponen yang terlibat :

1. Manajemen perusahaan
2. Teknologi sistem informasi
3. Keamanan sistem informasi
4. Kinerja sistem informasi
5. Proses bisnis yang berjalan pada sistem informasi
6. Infrastruktur TI
7. Seluruh pihak yang terkait dalam penggunaan teknologi informasi di perusahaan

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026

KOMPONEN AUDIT IT

Menetapkan ruang lingkup audit IT

Prasyarat utama untuk program audit organisasi adalah menentukan jenis audit apa yang diperlukan dan mengidentifikasi apa yang harus atau bisa diaudit. Potensi audit yg di kembangkan oleh inventaris disebut dengan Ruang Lingkup. manajemen aset, arsitektur perusahaan, kerangka tata kelola, atau pendekatan lain apa pun yang membantu mengidentifikasi elemen-elemen penyusun organisasi. Organisasi kemudian melakukan penilaian risiko pada setiap item yang termasuk dalam ruang lingkup audit untuk memberikan prioritas pada subyek audit, Dengan mempertimbangkan faktor-faktor untuk setiap item seperti, besarnya relatif risiko pentingnya bagi organisasi, atau potensi manfaat bagi organisasi dari melakukan audit. Prioritasi mencerminkan efisiensi sumber daya organisasi yang tersedia untuk mendukung audit, Aspek organisasi dapat di audit secara memadai Tata kelola formal dan manajemen resiko, kedua domain organisasi ini menekankan identifikasi dan penilaian asset sebagai dasar untuk menyusun kegiatan manajemen dan mengalokasikan sumber daya organisasi, sumber daya kontrol lainnya pada area organisasi yang terkait dengan sumber risiko terbesar.

Mengembangkan dan mempertahankan ruang lingkup audit

Audit di setiap organisasi biasanya mencerminkan cara organisasi itu sendiri terstruktur dan dikelola. Semesta audit dapat diatur atau dikategorikan berdasarkan hierarki unit bisnis, arsitektur perusahaan, model proses bisnis, kerangka kerja tata kelola, katalog layanan, atau dekomposisi fungsional lainnya yang paling sesuai dengan cara organisasi memandang operasi dan aset mereka. ada beberapa level kontrol atau tingkat entitas umum yang menyeluruh yang dapat diaudit. audit kontrol tingkat entitas sering kali memerlukan beberapa pendekatan audit karena biasanya mencakup berbagai jenis kontrol internal. Ruang lingkup audit ini penerapannya di semua tingkat organisasi juga berarti bahwa laporan audit tingkat entitas memiliki khalayak yang lebih luas daripada yang dihasilkan dalam jenis audit lainnya. Auditor yang melakukan audit pada level apa pun di bawah seluruh organisasi perlu memastikan bahwa ruang lingkup audit mereka mencakup level entitas dan kontrol bersama lainnya, serta yang diterapkan secara khusus untuk komponen yang diperiksa oleh audit.

Unsur-unsur organisasi yang biasanya dimasukkan dalam ruang lingkup meliputi:

- unit struktur organisasi seperti unit bisnis, divisi operasi, fasilitas, atau anak perusahaan
- struktur akuntansi seperti pusat biaya, lini bisnis, atau area proses
- sasaran, sasaran, dan hasil strategis, yang dievaluasi sebagian dengan mengaudit sumber daya yang dialokasikan untuk pencapaiannya;
- misi dan proses bisnis, layanan, dan fungsi operasional yang dijalankan oleh organisasi

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026

- aset termasuk aset TI organisasi memiliki, mengoperasikan, mengelola, atau mengendalikan;
- program, proyek, dan investasi di mana organisasi melakukan pendanaan atau sumber daya lainnya;
- kontrol internal dan eksternal yang dilaksanakan oleh organisasi atau atas namanya;
- fungsi atau program manajemen seperti tata kelola, manajemen risiko, jaminan kualitas, sertifikasi, dan kepatuhan serta audit internal.

Penggerak tata kelola, risiko, dan kepatuhan

organisasi menetapkan dan memelihara program di bidang ini, kebutuhan untuk menilai efektivitasnya dan mengukur pencapaian tujuan program mempengaruhi ruang lingkup dan frekuensi audit TI dan prosedur, standar, dan kriteria yang digunakan dalam audit TI internal.
Meskipun kerangka kerja dan tata kelola manajemen risiko jarang menentukan elemen yang cukup, untuk menyediakan inventaris subjek potensial audit, mereka menawarkan fondasi yang kuat, khususnya untuk komponen dan kontrol terkait-TI di dunia audit.
Program kepatuhan memiliki pengaruh, di mana kebutuhan untuk memenuhi tujuan atau persyaratan kepatuhan, adalah faktor utama dalam penentuan prioritas dan kriteria yang digunakan sebagai dasar untuk menunjukkan kepatuhan menetapkan ruang lingkup minimum untuk audit dilakukan untuk mendukung kepatuhan.
Misalnya, versi yang dipakai secara luas 4.1 dari tujuan pengendalian untuk informasi dan teknologi (COBIT) mencakup 34 proses dalam 4 domain tata kelola utama dan mendefinisikan lebih dari 200 tujuan pengendalian yang terkait dengan proses tersebut. COBIT 5 memperluas proses model referensi ke 37 proses di antara 5 domain, menggantikan tujuan kontrol dengan tata kelola dan praktek manajemen yang disarankan dan kriteria audit pada tujuh faktor, mirip dengan kategori ruang lingkup audit : prinsip, kebijakan, dan kerangka kerja, struktur organisasi; Kebudayaan, etika, dan perilaku. Informasi; Layanan, infrastruktur, dan aplikasi.
Enterprise risk management menggunakan ruang lingkup audit development dan IT untuk mengaudit ruang lingkup dengan memberikan identifikasi aset organisasi yang berisiko dan menetapkan jenis risiko-risiko yang berlaku pada komponen atau aspek operasional organisasi. Sementara risiko yang terkait dengan mata pelajaran audit yang berbeda membantu meningkatkan sumber daya yang seharusnya, mempertimbangkan semua jenis risiko yang ada dan dapat memengaruhi cakupan audit.

Strategi dan prioritas audit

Pada bab 3 sudah dijelaskan pentingnya strategi audit terhadap sebuah organisasi dan program audit internalnya. Strategi audit adalah sebuah kunci utama yang menentukan jenis, lingkup, dan frekuensi audit sebuah organisasi memimpin dan mendefinisikan kriteria yang digunakan oleh organisasi untuk memprioritaskan materi di alam semesta audit. Organisasi mengikuti prosedur dalam strategi audit untuk membentuk prioritas audit dan menggunakan determinasi untuk

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
pengalokasikan sumber-sumber audit internal. Rencana pada audit yang terkait untuk menguraikan sumber-sumber yang harus dialokasikan untuk dapat menjawab persyaratan wajib dan tujuan serta persyaratan audit tambahan apa pun. Banyak suatu organisasi menetapkan peringkat prioritas tinggi untuk mengaudit kegiatan yang mendukung kepatuhan hukum atau peraturan, semacam laporan kontrol internal yang diwajibkan dari perusahaan yang diperdagangkan pada bawah pasal 404 dari undang-undang Sarbanes-Oxley [5]. Kegagalan untuk mematuhi persyaratan wajib adalah salah satu dari beberapa jenis risiko organisasi yang dihadapi yang dapat mengakibatkan dampak negatif yang diukur secara langsung dalam istilah keuangan atau tidak langsung dari kerusakan reputasi, publisitas negatif, sanksi hukuman, atau hasil potensial lainnya.

Jenis kontrol

Jenis kontrol adalah sebuah elemen yang berbeda-beda yang ada pada audit, operasi bisnis, aset-asetnya, dan sumber-sumber pendukung yang membentuk kemampuan fungsional suatu organisasi, sementara kontrol pada kemampuan-kemampuan tersebut mencakup struktur manajemen, proses dan protokol, serta langkah-langkah teknis yang menyediakan efisiensi dan keefektifan operasional, kepatuhan, keandalan, dan jaminan operasional. Seperangkat kontrol individu (baik secara internal maupun eksternal) dijalankan oleh sebuah organisasi bertentangan dengan proses pemerintahan pengendalian internal, yang ada untuk membantu organisasi mencapai tujuan manajemen yang berkaitan dengan strategi, operasi, suatu kepatuhan manajemen yang sah atau peraturan, kualitas, keamanan, atau manajemen risiko. Kontrol terutama kontrol internal adalah fokus dari banyak jenis audit, baik dilakukan oleh auditor internal ataupun eksternal. Satu jenis kontrol atau lebih biasanya berlaku untuk semua benda dalam ruang lingkup organisasi. Organisasi dan auditor perlu memiliki pemahaman yang luas tentang berbagai jenis kontrol dan penerapan tujuan dan fungsinya untuk dapat merencanakan dan melaksanakan sebuah audit dengan benar dari kontrol sebuah organisasi dan untuk menyelaraskan jenis kontrol yang digunakan dengan cara kompetensi, keterampilan, dan pengalaman sebelumnya kepada para auditor.

Kontrol Kategorisasi

Kontrol Kategorisasi adalah Kontrol yang luas dan memilih kontrol tersebut dari susunan kontrol yang sama luas atau lebih luas yang disusun untuk implementasi. Seperti halnya item-item dalam ruang lingkup audit dapat diatur atau dikategorikan dalam banyak cara, banyak pendekatan kategorisasi kontrol yang berbeda-beda digunakan dalam kerangka kerja yang tersedia, metodologi, dan panduan. Skema pengukuran umum untuk kontrol termasuk yang didasarkan pada tujuan, sasaran, fungsi, sifat implementasi, dan tingkat penerapan dalam organisasi. Tabel 6.1 memberikan sebuah daftar pendekatan kategorisasi kontrol yang representatif dengan menggunakan basis kategorisasi yang berbeda.

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
Kategorisasi kontrol terutama dimaksudkan untuk memperkenalkan konsisten dengan cara kontrol dirujuk dan diterapkan dalam konteks yang berbeda-beda dan untuk tujuan berbeda. Seperti yang ditunjukkan oleh Tabel 6.1, tidak ada standar tunggal yang dapat diterima untuk mengkategorikan kontrol, sehingga organisasi dapat memilih atau mengadaptasi pendekatan yang ditentukan dalam susunan kerangka kerja atau metodologi eksternal, mengembangkan kategorisasi mereka sendiri, atau mengikuti standar yang ditetapkan dalam aturan hukum, peraturan, atau kebijakan sebuah organisasi. harus memuaskan. Peraturan keamanan yang diundangkan di bawah Undang-undang Portabilitas dan Akuntabilitas Asuransi Kesehatan tahun 1996 (dikenal secara kolektif sebagai Peraturan Keamanan HIPAA) misalnya, memisahkan persyaratan menjadi pengamanan administratif, teknis, dan fisik, sehingga organisasi yang dicakup oleh hukum mungkin menemukan bahwa menggunakan kategorisasi yang sama pendekatan untuk kontrol internal memfasilitasi kepatuhan.
Tabel 6.1

Basis	Kategorisasi Representatif
Tujuan kontrol	Pencegahan, detektif, korektif
Kontrol objektif	Operasi, pelaporan, kepatuhan Tata kelola, manajemen risiko, kepatuhan
Fungsi kontrol	Administratif, teknis, fisik Manajemen, operasional, teknis
Sifat implementasi	Terpusat, dibagikan, didesentralisasi
Tingkat penerapan	Organisasi, divisi, unit bisnis, fungsi Program, proyek, sistem, komponen

Kontrol Organisasi

Kontrol organisasi adalah control yang ditingkat entitas penting sebagai area fokus untuk audit internal dan eksternal karena mereka memberikan dasar untuk bagaimana organisasi mengelola fungsi yang didukung oleh sebuah kontrol. Kontrol pada level entitas juga disertakan dengan referensi ke dalam banyak jenis audit dilakukan di tingkat organisasi lainnya, sebagai unit bisnis, program dan proyek, dan aset teknologi semuanya yang memanfaatkan jenis-jenis kontrol tingkat entitas. Gambar 6.2 menunjukkan berbagai kategori utama dari entitas level dan jenis kontrol dalam setiap kategori Itu mungkin diterapkan dan akan tunduk pada audit dalam organisasi yang berbeda.

Audit dari kontrol tingkat entitas berbeda pada tingkat tertentu dari pemeriksaan yang difokuskan pada unsur-unsur yang sempit di dalam organisasi. Efektivitas kontrol tingkat entitas sebagian bergantung pada sejauh mana organisasi yang membentuk otoritas kontrol dan menerapkan setiap kontrol dengan cara yang meliputi seluruh organisasi. Dari perspektif ini, audit dari

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
kontrol tingkat entitas pada dasarnya memeriksa kemampuan manajemen dan tata kelola organisasi, termasuk struktur organisasi, penyelarasan bisnis dan tujuannya, keberadaan serta penggunaan kegiatan perencanaan strategis dan operasional. Unsur-unsur pada kontrol ini membantu memastikan bahwa control yang di tentukan organisasi kebijakan sebenarnya diimplementasikan dan digunakan untuk mendukung pencapaian tujuan kontrol organisasi. Tata kelola terkemuka dan kerangka manajemen risiko menekankan bahwa pentingnya menetapkan kontrol tingkat entitas dan tampaknya mengasumsikan bahwa hampir semua organisasi mengenali nilai dari menerapkan jenis-jenis pada kontrol ini [2,8,9]. Asumsi seperti itu sebagian berasal dari proporsi besar perusahaan atau organisasi yang saling tukar di industri atau lingkungan operasi yang diatur untuk membentuk sebuah audit yang diinginkan tentang tata kelola, manajemen risiko, kepatuhan, dan audit.

Mengaudit aset yang berbeda

Auditing aset yang berbeda adalah untuk melakukan pengecekan asset dan kontrol teknis yang terkait, baik sebagai focus utama dalam audit sentris atau dalam konteks seperti fungsi manajemen audit dan proses bisnis yang didukung oleh aset-asetnya.
Untuk melakukan pengecekan asset-aset para auditor yang bertugas perlu untuk memilih prosedur audit yang tepat, sesuai dengan jenis audit yang akan diadakan dan membutuhkan pemahaman cukup tentang konteks asset yang dipakai sebagai bukti yang relevan untuk mendukung temuan audit. Auditors memeriksa beberapa komponen-komponen dalam ruang lingkup sebuah audit tunggal yang memiliki kriteria dan prosedur audit dengan kebutuhan dengan pendekatan konsisten untuk mengumpulkan dan menganalisis sebuah informasi serta melaporkan temuan audit. Di sebagian besar aset TI, ada bidang-bidang umum atau prosedur audit yang dapat membantu menyediakan konsistensi ini, seperti yang dirangkum pada tabel 6.2. Secara kolektif, prosedur-prosedur ini menyoroti penggunaan terpadu dari dokumentasi, penyelidikan, pengamatan, dan uji coba langsung untuk menyediakan bukti yang diperlukan untuk mendukung temuan audit.

Fokus Audit TI	Audit Prosedur
Configuration	Memindai atau menganalisis konfigurasi aset dan membandingkan konfigurasi aktual dengan kebijakan, baseline, dan standar yang disetujui
Logging and monitoring	Konfirmasi logging diaktifkan pada tingkat detail yang sesuai dan output log dipantau dan ditinjau atau dianalisis secara teratur

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026

Access control	Tinjau kebijakan, prosedur, dan mekanisme untuk mengontrol akses ke subjek audit, termasuk pemberian dan pencabutan hak akses dan otentikasi dan otorisasi akses

Dekomposisi Komponen IT

Dekomposisi Komponen IT adalah komponen yang di gunakan untuk kinerja audit untuk lebih efisien dan membantu menentukan ruang lingkup yang lebih akurat untuk menyelesaikan proses audit. menentukan lingkup audit, seperangkat keterampilan dan kompetensi yang diperlukan oleh audit, dan tingkat sumber yang diperlukan untuk menyelesaikan proses audit. Sistem pengaudit ini mencerminkan jenis audit dan tujuannya dimaksudkan, komponen-komponennya akan diperiksa, dan prosedur, protokol, standar, atau auditor kriteria yang akan digunakan.
Tidak ada metode standar tunggal atau "terbaik" untuk mengevaluasi sistem lingkungan teknis. Salah satu caranya adalah menguraikan suatu sistem ke dalam bagian-bagian penyusunnya dan mengaudit setiap komponen secara individu, menerapkan protokol audit yang serupa di semua unsur utama, tetapi juga menggunakan prosedur atau daftar periksa yang spesifik dalam hal teknologi jika perlu
Kategori umum atau komponen yang mewakili bidang audit mencakup delapan unsur yang diperlihatkan pada Gambar 6.1. Beberapa contoh audit istimewa Pertimbangan juga berlaku pada jenis-jenis tertentu dari lingkungan operasi seperti komputasi awan atau penggunaan lainnya dari teknologi virtualisasi server, dan sistem atau akses aplikasi menggunakan peramban web, perangkat seluler, atau jenis aplikasi dan antarmuka klien lainnya. Bagian berikut menjelaskan secara singkat dan pertimbangan audit yang berlaku untuk berbagai komponen-komponennya.

Sistem dan aplikasi

Sistem dan aplikasi memiliki beragam karakteristik seperti arsitektur teknis, sistem operasi, bahasa pemrograman, titik-titik integrasi, dan fungsi yang diinginkan. Pilihan prosedur audit yang sesuai untuk sistem dan aplikasi tergantung pada arsitekturnya dan berbagai jenis komponen teknis yang digunakan untuk pemeriksaan setiap sistem atau subjek aplikasi. Auditor aplikasi sistem fokus pada kemampuan dan kontrol non-fungsional. Masalah fungsional mencakup memastikan bahwa apa yang organisasi lakukan untuk menjalankan fungsinya memenuhi persyaratan yang ditentukan. Aspek yang tidak fungsional mencakup kinerja, kegunaan, keandalan, dan keamanan, di mana para auditor sering menguji atau meninjau bukti yang memperlihatkan penerapan kontrol yang sesuai dengan penggunaan sistem atau penerapan yang diharapkan dan cara pengguna berinteraksi dengannya. Misalnya, audit aplikasi berbasis

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
web sering kali memeriksa penggunaan kendali terhadap kerentanan yang diketahui, kesalahan konfigurasi, dan pengungkapan informasi sensitif yang tidak sah.

Database

Istilah database umumnya berarti setiap kumpulan atau repositori informasi yang disimpan oleh suatu organisasi, tetapi dalam praktik paling sering menyiratkan jenis teknologi spesifik yang menyimpan dan menyediakan akses ke data dalam mendukung satu atau lebih aplikasi dan proses bisnis. Basis data mewakili sebuah jenis perangkat lunak aplikasi khusus, yang tunduk pada banyak prosedur audit dan kriteria pemeriksaan yang sama sebagai aplikasi dan sistem. Sifat dan kepekaan data yang disimpan dalam basis data organisasi mempengaruhi kriteria yang digunakan untuk mengaudit mereka, khususnya sehubungan dengan memeriksa kontrol keamanan atau privasi seperti enkripsi data, pengawasan akses, dan backup data serta pemulihan.

Sistem Operasi

Organisasi Modern sering menggunakan berbagai sistem operasi untuk mendukung berbagai kebutuhan sistem dan komputer, yang paling umum termasuk Microsoft Windows, berbagai versi Unix atau Linux, serta alternatif - dan platform-spesifik seperti z/OS untuk komputer mainframe IBM. Sistem operasi sangat dapat disesuaikan dan dapat diterapkan secara berbeda di seluruh organisasi atau dalam organisasi yang sama. Untuk meningkatkan ketahanan, administrasi, keamanan, dan dukungan, berbagai organisasi sering kali melakukan konfigurasi sistem operasi untuk server, komputer desktop dan laptop, dan perangkat seluler. Banyak pemasok sistem operasi menawarkan rekomendasi konfigurasi yang dimaksudkan untuk mengoptimalkan keamanan atau kesesuaian untuk penggunaan yang berbeda. Audits sistem operasi mengkonfirmasikan penggunaan dan konfigurasi yang sesuai dari sistem operasi pada platform komputasi yang berbeda yang diluncurkan dalam organisasi.

Perangkat Keras

Perangkat keras terdiri dari perangkat fisik yang digunakan untuk membangun jaringan, infrastruktur telekomunikasi, sistem komputer, pelanggan komputasi akhir, dan banyak komponen keamanan fisik. Dalam banyak penguraian arsitektur teknis, perangkat keras menghubungkan server, komputer desktop dan laptop, serta berbagai organisasi perangkat seluler yang digunakan serta router, switch, firewall, dan komponen-komponen lain yang digunakan dalam jaringan. Audit aset perangkat keras itu biasanya berfokus pada konfigurasi yang konsisten dan benar serta kepatuhan terhadap kebijakan dan standar internal. Dibandingkan dengan perangkat lunak, proporsi yang lebih besar dari suatu perangkat keras organisasi ini kemungkinan besar akan dibeli secara komersial, jadi auditor perangkat keras juga

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
mempertimbangkan vendor dan proses-proses internal yang digunakan untuk memperoleh perangkat keras.

Jaringan

Jaringan menyediakan konektivitas dan memungkinkan pertukaran komunikasi dan informasi untuk sebagian besar, jika bukan dari aset-aset organisasi IT. Jaringan meliputi aset-aset perangkat keras seperti router dan firewall yang memungkinkan aliran informasi antara komponen dan komunikasi dan kontrol keamanan yang melindungi kualitas layanan dalam komunikasi jaringan dan informasi rahasia, integritas, dan ketersediaan data melintasi infrastruktur jaringan. Audit jaringan memeriksa implementasi dan konfigurasi perangkat keras, layanan, dan protokol yang dijalankan pada jaringan tersebut, dan kontrol keamanan seperti firewall dan sistem deteksi jaringan. Audit ini juga mempertimbangkan sifat komunikasi di dalam jaringan sehingga auditor dapat memilih prosedur audit yang sesuai untuk menggunakan nirkabel, satelit, seluler dan teknologi jaringan lainnya. Prosedur audit khusus yang digunakan untuk memeriksa jaringan tergantung pada jenis perangkat keras, layanan, kontrol keamanan, dan infrastruktur telekomunikasi yang diterapkan oleh suatu organisasi dan pada skala jaringan dalam ukuran geografisnya serta jumlah dan berbagai sistem dan fasilitas yang terhubung dengannya. Sementara sebagian besar teknologi yang mendasarkannya sangat mirip terlepas dari skala jaringan, ada perbedaan praktis dalam mengaudit konvensional atau virtual jaringan area lokal yang digunakan dalam satu lokasi dengan jaringan luas area mencakup berbagai situs.

Tempat Penyimpanan

Meskipun organisasi menyimpan sejumlah besar data dalam basis data antarnegara, konten dan dokumen sistem manajemen, dan komponen-komponennya yang serupa, penggunaan teknologi penyimpanan yang mutakhir membuat tempat, jaringan, dan infrastruktur merupakan bagian yang unik dari program ini yang digunakan pada audit. Solusi penyimpanan menggunakan perangkat keras, perangkat lunak, protokol komunikasi, dan metode penyimpanan data serta akses, meskipun bidang penekanannya untuk audit penyimpanan tumpang tindih secara substansial dengan bidang-bidang yang ada pada basis data. Prosedur Audit dan kriteria penyimpanan bergantung pada jenis spesifik teknologi penyimpanan yang digunakan suatu organisasi dan sifat serta kepekaan data yang ditampung di lingkungan penyimpanan. Penyimpanan dapat diaudit secara terpisah atau dalam teknologi operasional yang lebih luas seperti ini biasanya ditetapkan sebagai komponen pendukung dari pusat data atau lingkungan operasi teknis lainnya, di mana sebuah infrastruktur penyimpanan tunggal dapat menerima data dari berbagai sistem.

Pusat Data

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
Sebagai fasilitas yang digunakan sistem, perangkat keras, infrastruktur jaringan, dan teknologi terkait, pusat data menyediakan fondasi yang penting bagi cara kerjanya. Selain berfungsi sebagai lokasi fisik bagi banyak komponen teknologi, pusat data juga menjadi titik pelaksanaan bagi banyak proses, prosedur, dan fungsinya yang mendukung proses tersebut. Audit fasilitas pusat data berfokus pada kontrol jenis khusus ini dan proses dukungan operasional, sumber, dan personil yang memastikan bahwa komponen yang berasal di pusat data beroperasi secara normal untuk mendukung proses dan fungsi bisnis yang bergantung padanya. Apakah dimiliki dan dikelola oleh suatu organisasi atau pihak ketiga, pusat data sering dianggap penyedia jasa dan oleh karena itu digunakan pada standar eksplisit yang ditetapkan untuk audit organisasi layanan.

Lingkungan tervirtualisasi

Teknologi virtualisasi menyediakan sebuah pendekatan teknis alternatif untuk menyediakan infrastruktur, platform dan sistem operasi, server, perangkat lunak, serta sistem dan aplikasi. Kebanyakan lingkungan komputasi yang berkualitas memiliki banyak kesamaan dengan pusat data konvensional, Pendekatan ini meningkatkan pemanfaatan kapasitas dan di dalamnya layanan model berbasis cloud seperti komputasi cloud, memungkinkan organisasi untuk menggunakan sumber daya teknologi ini lebih efisien dengan naik atau turun sebagai surat perintah kebutuhan bisnis. Audit lingkungan komputasi berkualitas menggunakan banyak prosedur dan kriteria yang sama yang digunakan untuk audit pusat data, dengan penekanan tambahan pada server penyedia, deprovisioning, manajemen, pemeliharaan berbagai server virtual yang berbagi komputasi, jaringan, dan sumber daya infrastruktur.
Penggunaan komputasi cloud dan penyedia layanan pihak ketiga menjadi cukup umum sehingga para audits mungkin menanggapi layanan demikian yang berbeda dengan komponen audit lainnya. Perbedaan yang ditekankan oleh para penyedia layanan cloud antara lain penyedia layanan termasuk akses jaringan, akses sumber daya, sumber daya pooling, kemampuan dan jasa yang fleksibel, dan penggunaan yang bermebel serta model pembayaran dan pembayaran yang terkait. Pertumbuhan yang diharapkan dalam komputasi cloud adalah salah satu faktor yang mendorong kerangka kerja kontrol yang spesifik di awan, Kerangka kerja yang tersedia termasuk matriks kontrol awan yang dikembangkan oleh aliansi keamanan cloud dan risiko Federal dan Program manajemen wewenang yang dikelola oleh administrasi layanan umum untuk digunakan oleh penyedia layanan awan yang melayani instansi pemerintah as.

Antarmuka

interface adalah titik integrasi atau koneksi antara dua komponen atau lebih, yang memungkinkan transmisi informasi antara sistem atau mengekspos layanan atau kemampuan fungsional dari satu sistem atau aplikasi pada orang lain. Auditor sering kali menekankan langkah-langkah keamanan yang diimplementasikan untuk melindungi informasi dalam perjalanan melintasi antarmuka dan untuk mengendalikan akses ke antarmuka yang terpapar oleh setiap sistem. Audit antarmuka mengandalkan pada kedua dokumentasi seperti spesifikasi

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
antarmuka formal dan tes yang menunjukkan fungsi yang benar dari tiap antarmuka, mempertimbangkan tujuan yang dimaksudkan, aliran informasi, mekanisme akses teknis, dan proses oketifikasi dan otorisasi tingkat mesin.

Kontrol atau proses prosedural audit

Ruang lingkup audit teknologi informasi sangat luas dan beragam seperti yang dimiliki oleh organisasi sendiri, yang meliputi berbagai macam teknologi, kemampuan teknis, dan kontrol serta kebijakan, proses, dan prosedur yang berkaitan dengan fungsi operasional dan tata kelola. Bergantung pada jenis dan lingkup audit yang direncanakan oleh suatu organisasi, auditor bisa saja memeriksa basis proses atau kontrol prosedural yang berkaitan dengan asetnya dan komponen IT yang mendukung mereka, atau secara terpisah dengan audit yang spesifik dalam proses. Penekanan relatif yang menempatkan suatu organisasi pada audit proses-proses itu dipengaruhi hingga batas tertentu oleh tata kelola, risiko, kepatuhan, dan kerangka manajemen yang dipilih untuk dijalankan. Banyak jenis audit eksternal termasuk yang dimaksudkan untuk memperoleh sertifikasi atau menunjukkan keterlibatan peraturan yang mengharuskan auditor untuk mempertimbangkan pengawasan administratif, teknis, dan fisik dalam lingkup audit yang sama. Organisasi biasanya memiliki lebih banyak kebijaksanaan untuk merencanakan, mendefinisikan ruang lingkup, dan melakukan audit internal dengan cara yang memisahkan audit proses dan kontrol prosedural dari audit aset, sistem, dan teknologi IT. Ada banyak alasan untuk mengejar pendekatan seperti itu, termasuk kemampuan untuk meningkatkan keterampilan dan kompetensi para auditor terhadap masalah audit yang mereka lakukan.

Operasi IT

Operasional IT audits berfokus pada proses dan prosedur yang dilaksanakan oleh suatu organisasi dan penyelarasan kegiatan-kegiatan tersebut dengan sumber sistem, infrastruktur, dan teknologi informasi lainnya. Untuk berhasil melakukan jenis audit ini, organisasi perlu mengembangkan inventarisasi dari proses dan kontrol prosedural yang digunakannyan (atau mengidentifikasi informasi ini dalam dokumentasi yang ada di dalam sistem audit di ruang lingkup audit) dan menyiapkan strategi audit serta rencana audit yang sesuai dengan rencana audit yang digunakan pada jenis audit lain. Proses pemeriksaan yang relevan mencakup mereka dalam bidang bisnis yang lebih spesifik maupun umum, termasuk :

- Perencanaan strategis dan taktis
- Manajemen Resiko
- Manajemen kualitas
- Pengelolaan keuangan
- Pengelolaan sumber daya manusia
- Akuisisi atau pengadaan

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026

- Pengelolaan rantai pasokan
- Program dan manajemen proyek
- Manajemen perubaham
- Manajemen pelayanan
- Dukungan pelanggan dan teknis
- Manajemen keamanan
- Manajemen fasilitas
- Manajemen vendor

Proses operasional dan kontrol prosedural juga digunakan pada prioritas sehingga sumber audit dapat dialokasikan dengan efektif. Prioritas dalam konteks ini mempertimbangkan kriteria seperti tingkat sumber daya yang terlibat, kompleksitas, hubungan ketergantungan dengan proses lain, dan kritik setiap proses terhadap organisasi secara keseluruhan atau pada fungsi misi atau bisnis yang didukung.

Program dan manajemen proyek

Program atau proyek sering digunakan secara bergantian, standar dan bimbingan untuk mengelola kegiatan-kegiatan yang berbeda, durasi, dan hasilnya, di mana program terdiri dari satu proyek atau lebih, memiliki jangka waktu yang kurang jelas, dan dimaksudkan untuk mencapai satu atau lebih hasil jangka panjang, proyek lebih terfokus secara sempit, usaha sementara dengan poin awal dan akhir yang jelas dimaksudkan untuk menghasilkan produk atau jasa tertentu. Program dan proyek dapat dikenakan pada audit operasional; Audit yang dikaitkan dengan sertifikasi, kepatuhan, atau jaminan kualitas; Audit yang spesifik berfokus pada teknologi, sistem, infrastruktur, atau proses yang mendukung program atau pelaksanaan proyek yang efektif. Para auditor melakukan audit jenis ini biasanya karena kriteria audit dasar setidaknya sebagian dari apa yang ditetapkan dalam metodologi atau standar siklus yang didefinisikan atau diterapkan oleh organisasi. Audit proyek dan Program, sebaliknya, berpusat pada proses, kontrol, dan artefak yang dihasilkan dalam pelaksanaan Program atau kegiatan proyek serta penyelarasan kegiatan tersebut dengan kebijakan, standar, dan persyaratan organisasi. Auditor yang memfokuskan pada audit jenis ini cenderung mengandalkan pemeriksaan bukti dokumenter, pengamatan langsung, dan wawancara dengan staf program atau proyek, karena metode pengujian kurang bisa diterapkan pada kegiatan manajemen. Beberapa pemeriksaan terhadap program dan kemampuan manajemen proyek sering kali disertakan dalam audit operasional atau kepatuhan, atau dalam audit sertifikasi menangani standar-standar untuk kualitas, manajemen pelayanan, atau proses kedewasaan.

Siklus kehidupan pengembangan system

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
Proyek-proyek ini dilakukan di banyak organisasi yang digunakan pada serangkaian proses dan kegiatan yang dikenal sebagai suatu sistem (atau perangkat lunak) siklus kehidupan pembangunan (SDLC). Saat proyek ini berjalan melalui fase berbeda dari SDG, tim proyek ini menjalankan berbagai kegiatan, menghasilkan keluaran yang berbeda, dan memenuhi persyaratan atau kriteria yang diperlukan untuk menyelesaikan satu fase dan beralih ke fase berikutnya. metodologi SDLC tidak mempunyai kesamaan untuk berbagai organisasi degan variasi luas sae siklus hidup dan durasi fase yang di harapkan standar SDLC, Dari prespektif holistik model SDLC memiliki kegiatan dan tujuan yang sama. Organisasi hanya menggunakan 4 fase atau 10 SDLC, pada dasarnya SDLC mencakup kegiatan yang berhubungan dengan inisiasi proyek, desain, operasi dan penghentian proyek. Organisasi hanya menerapkan satu SDLC standar. Audit proyek ini dapat dilaksanakan di setiap titik dalam kehidupan siklus atau potensi rentang siklus hidup beberapa fase siklus kehidupan untuk proyek besar atau kompleks atau mereka yang menggunakan metodologis-artinya auditor harus menyesuaikan kriteria pemeriksaan mereka untuk mencerminkan kegiatan, hasil, dan pencapaian yang berbeda dalam setiap fase. Bagian-bagian berikut mengikuti nama fase kehidupan sistem siklus kehidupan yang diperinci.

Konsep

Setiap proyek IT dimulai dengan ide, saran, persyaratan, atau kebutuhan organisasi lain yang diakui. Konsep proyek atau tahap inisiasi dimulai ketika suatu organisasi mengidentifikasi kebutuhan akan kemampuan baru atau yang ditingkatkan dan mulai menentukan bagaimana konsep dapat memenuhi kebutuhan itu. Selama fase konsep, organisasi dapat mengidentifikasi dan mengevaluasi beberapa alternatif, mempertimbangkan karakteristik teknis dan nonteknis seperti biaya, kompleksitas, strategi akuisisi, dan kelayakan. Audit proyek IT dalam fase konsep biasanya memeriksa proses manajemen proyek, standar, dan metodologi untuk memastikan mereka sesuai dengan kebijakan dan standar organisasi dan memverifikasi kelengkapan dan persetujuan (jika diperlukan) dokumentasi proyek yang diperlukan seperti rencana proyek proyek manajemen piagam, kasus bisnis, analisis alternatif, dan jadwal proyek. Fase konsep juga dapat menghasilkan spesifikasi persyaratan fungsional dan teknis, desain solusi tingkat tinggi, pemilihan kontrol awal, dan rancangan artefak proyek yang harus diselesaikan pada fase selanjutnya seperti rencana keamanan, rencana manajemen risiko, rencana darurat, atau jaminan kualitas. rencana. Organisasi mungkin memerlukan audit pada fase konsep sebagai prasyarat untuk menyetujui transisi proyek ke fase pengembangan.

Pengembangan

Fase pengembangan mencakup berbagai kegiatan yang dimaksudkan untuk memenuhi set lengkap persyaratan yang ditentukan untuk sistem, aplikasi perangkat lunak, atau solusi lainnya. Banyak metodologi SLDC membagi fase pengembangan tunggal yang didefinisikan dalam ISO /

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
IEC 15288 menjadi beberapa fase yang lebih kecil untuk analisis persyaratan dan desain selain pengembangan. Fase pengembangan meliputi spesifikasi persyaratan fungsional dan nonfungsional yang lengkap, dokumentasi desain terperinci yang membahas semua komponen dalam ruang lingkup proyek, rencana pengujian, dan pengiriman kode perangkat lunak, teknologi yang diperoleh, atau elemen solusi lain yang siap untuk diintegrasikan, pengujian, dan evaluasi kontrol. Selama pengembangan, tim proyek juga mengidentifikasi kebutuhan operasional yang diharapkan dalam hal infrastruktur, perangkat keras dan kapasitas jaringan, platform komputasi, dan operasi, pemeliharaan, dan kebutuhan dukungan. Audit proyek IT dalam fase pengembangan fokus pada keakuratan dan kelengkapan dokumentasi dan artefak utama, memastikan bahwa desain yang disetujui memenuhi semua persyaratan, termasuk kontrol internal yang memadai, dan mematuhi standar dan kriteria internal dan eksternal yang berlaku. Untuk melakukan proyek yang melibatkan pengembangan perangkat lunak khusus, ruang lingkup audit proyek IT dapat mencakup tinjauan atau proses kontrol kualitas perangkat lunak lainnya. Terlepas dari sumber atau jenis teknologi yang digunakan dalam proyek, pada akhir fase pengembangan, semua dokumentasi desain, antarmuka integrasi, dan spesifikasi teknis harus lengkap dan komponen sistem atau aplikasi perangkat lunak harus siap untuk evaluasi dan persetujuan sebelum penyebaran penuh.

Produksi

Istilah produksi seperti yang digunakan dalam ISO / IEC 15288 berhubungan dengan serangkaian kegiatan yang dimaksudkan untuk menguji solusi teknis atau mengkonfirmasi kemampuan organisasi untuk mengirimkan produk atau layanan yang dihasilkan dari proyek. Untuk proyek yang menggunakan sistem atau aplikasi perangkat lunak, ruang lingkup fase produksi terdiri dari unit kerja, integrasi, dan pengujian penerimaan untuk mengonfirmasi bahwa teknologi memenuhi persyaratan fungsional; memverifikasi implementasi dan konfigurasi kontrol internal yang tepat; dan menilai langkah-langkah perlindungan keamanan dan privasi yang diperlukan untuk menerima persetujuan untuk sistem atau perangkat lunak agar dapat beroperasi penuh. Audit proyek TI selama fase produksi memeriksa rencana pengujian dan prosedur untuk memastikan bahwa kegiatan pengujian cukup untuk menentukan kepuasan persyaratan. Karena produksi adalah fase terakhir sebelum sistem atau aplikasi perangkat lunak digunakan untuk digunakan, auditor juga memeriksa bahwa proyek telah menerima semua persetujuan yang diperlukan, berpotensi termasuk hasil uji fungsional, penerimaan pengguna, integrasi sistem, kesiapan lingkungan, penerimaan risiko, dan otorisasi untuk beroperasi.

Pemanfaatan

Dalam fase pemanfaatan, sistem atau layanan yang ingin disampaikan oleh proyek yang siap untuk di gunakan, di mana fokus proyek berpindah dari mempersiapkan penempatan untuk secara aktif mengoperasikan dan memelihara sistem dengan cara yang terus-menerus memenuhi

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
kebutuhan pengguna. Suatu sistem dalam tahap pemanfaatan biasanya digunakan pada audit operasional rutin untuk mengevaluasi efisiensi dan efektivitas sistem yang sedang berlangsung dan proses bisnis yang didukungnya. Organisasi juga dapat melakukan berbagai audit khusus IT yang membahas sistem secara keseluruhan atau komponen-komponennya. Sebaliknya, audit proyek IT dalam fase pemanfaatan fokus pada memverifikasi bahwa sistem ketika digunakan akan memberikan fungsionalitas yang dimaksud dan memenuhi persyaratan teknis dan standar yang berlaku, mengandalkan bukti yang didokumentasikan seperti hasil pengujian, penilaian kontrol, dan persetujuan dari personel yang berwenang. dalam organisasi. Audit proyek pada fase ini juga berusaha untuk memastikan bahwa sumber daya yang ditentukan dan disediakan untuk sistem operasional sudah benar dan memadai.

Bantuan

Untuk sistem operasional, dukungan terdiri atas pemantauan, administrasi teknis, pemecahan masalah dan penyelesaian masalah, dan kegiatan pemeliharaan rutin seperti backup, konfigurasi control, patch management, dan upgrade dan pelepasan manajemen untuk perangkat lunak atau komponen teknis lainnya. Bergantung pada kebijakan, prosedur, dan standar organisasi, dukungan dapat juga mencakup kegiatan manajemen keamanan informasi seperti analisis kerentanan, verifikasi otomatis atau manual terhadap pengaturan konfigurasi, serta informasi keamanan dan manajemen peristiwa. Fase dukungan dari proyek IT biasanya berjalan sejajar dengan pemanfaatan; Fase-fase serupa dengan dukungan dalam berbagai metodologi SDLC disebut pemeliharaan, dengan kombinasi pemanfaatan dan dukungan yang dikenal secara kolektif sebagai operasi dan pemeliharaan. Kemampuan dukungan teknis suatu organisasi memiliki dampak langsung pada efektivitas operasional sistemnya, jadi meskipun kegiatan fase dukungan-dukungan dapat diaudit dalam isolasi, cakupan audit pada fase pemanfaatan sering kali mencakup fungsi dukungan.

Pensiun

Proyek menurut definisi memiliki titik akhir yang terdefinisi dengan baik, biasanya bertepatan dengan keputusan organisasi untuk menonaktifkan atau mengganti sistem atau layanan. Fase pensiun dari siklus hidup proyek melibatkan kegiatan yang diperlukan untuk menghilangkan kemampuan operasional dan untuk memastikan disposisi peralatan, perangkat keras dan perangkat lunak, data, dan sumber daya lainnya yang sebelumnya dialokasikan untuk mengoperasikan dan mendukung system proyek baru. Prioritas utama untuk fase pensiun selaras langsung dengan bidang-bidang yang ditekankan untuk audit proyek-proyek IT yang mencapai fase akhir ini: membuang atau menggunakan kembali aset teknologi, melepaskan sumber daya yang berkomitmen pada sistem sehingga dapat diterapkan di tempat lain dalam organisasi yang baru dan membersihkan media penyimpanan yang tetap dan dapat dilepas untuk memastikan bahwa tidak ada data yang tersisa pada komponen yang dinonaktifkan. Auditor IT yang

Nama : Sapardi
Kelas : MTI 21 Reg B
NIM : 192420026
memeriksa proyek dalam fase pensiun mencari dokumentasi menyeluruh yang merinci disposisi sumber daya proyek dan aset IT dan untuk persetujuan resmi atas dokumentasi tersebut yang biasanya merupakan prasyaratan untuk secara resmi menutup proyek.

Nama : Sela Taramita
Kelas : AR1
Nim : 192420038
Mata kuliah : IT Audit
Dosen : Dr. Widya Cholil S.Kom., M.I.T.

TUGAS : IT Audit components

Soal :

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat. Boleh dikerjakan perkelompok, tetapi masing-masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

Jawaban :

Apa itu Audit Internal?

Audit internal bersifat independen, objektif jaminan dan aktivitas yang dapat dirancang untuk menambah nilai dan meningkatkan operasi organisasi.

Audit Internal membantu organisasi mencapai tujuan mereka dengan mengevaluasi risiko bisnis dan kontrol, memberikan rekomendasi untuk meningkatkan manajemen risiko dan tata kelola proses

Proses Audit terdiri dari 4 bagian yaitu :

1. Planning (Perencanaan)
2. Testing (Pengujian)
3. Reporting (Pelaporan)
4. Follow up (Pelaksanaan / Dilaksanakan)

Penjelasan :

1. Planning (Perencanaan) terdiri dari beberapa bagian :

• Penilaian Risiko Tahunan
• Rencana Audit Awal
• Persetujuan Dewan Pengunjung
• Pemberitahuan dan Permintaan Informasi
• Pahami Risiko dan Kontrol
• Konferensi Pembukaan

2. Testing (Pengujian)

• Keamanan
• Pencadangan & Pemulihan
• Pengelolaan sumber daya
• Situs web

• Security Testing

Servers, Printers, Routers, Workstations, dan laptop

• Pencadangan & Pemulihan

Anda Harus Memiliki Kontrol yang Efektif untuk Mencadangkan & Memulihkan

• Pengelolaan sumber daya

Hardware dan Software Komputer

3. Reporting (Pelaporan)

1. **Lakukan observasi**
2. **Rekomendasi :** Kami Mungkin Merekomendasikan Peluang Untuk Meningkatkan Kontrol Anda
3. **Management Action Plans :** Mengembangkan Rencana, Jadwal, dan Prioritas anda Untuk Menerapkan Solusi
4. **Laporan Akhir Dikirim ke Dewan Pengunjung**

4. Follow up (Pelaksanaan / Dilaksanakan) :

• Tindakan Tindak Lanjut Berdasarkan Anda "Rencana Tindakan Manajemen"
• Kemajuan Dipantau
• Beberapa Pengujian Ulang Mungkin Diperlukan
• Dewan Pengunjung Diperbarui
• Audit ditutup

Pada komponen audit itu sendiri terdiri dari 6 bagian yaitu :

1. Information Gathering

   Tahap untuk mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Dimana auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien seperti laporan audit sebelumnya dan laporan buku besar.

2. Review prior audit issues

   Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan.

3. Risk assessment

   Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat, untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan dan masalah lain yang perlu dibahas dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .

4. Develop IT audit

   Setelah dilakukan pertemuan, auditor mulai merealisasikan rencana audit, kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak. auditor juga memberikan kesempatan kepada klien untuk memberikan masukan kepada auditor.

5. Execute IT audit Plan

   Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis, teknis, material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan IT yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

   Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Standar Audit dan Jaminan Sistem Informasi : 1003 Kemandirian Profesional

Kelompok 3 :

1. Ryan Andrian (NIM. 192420006)
2. Istikomah (NIM. 192420003)
3. Suriani (NIM. 192420011)
4. Yuni Astuti (NIM. 192420004)
5. Nizar Firliansa (NIM. 192420005)

IT Audit MTI AR1
Universitas Bina Darma
Tahun 2020

1003 Standar Kemadirian Profesional

- Profesional dalam bidang audit dan jaminan Sistem Informasi harus independen dan obyektif baik dari sikap dan penilaian dalam segala hal yang berkaitan dengan kegiatan audit dan jaminan.

1003 Standar Kemadirian Profesional

- Profesional dalam bidang audit dan jaminan SI harus memiliki kriteria :

  1. melaksanakan audit dan jaminan SI secara bertahap dan menyeluruh sampai dengan kesimpulan
  2. senantiasa independen
  3. menyampaikan seluruh fakta kelemahan yang ditemukan kepada pihak internal yang terkait dan merahasiakannya dari pihak luar
  4. meninjau independensi secara reguler baik dengan manajeman perusahaan atau dengan komite audit
  5. menghindari peran non audit di manajemen perusahaan untuk menjaga independensi penilaian / audit

1003 Standar Kemadirian Profesional

- Persyaratan :
  1. Bebas dari intervensi manajemen perusahaan
  2. independen / tidak ada kecenderungan ke manajemen perusahaan yang dapat mempengaruhi audit
  3. independen dalam sikap
  4. independen dalam menarik kesimpulan audit
  5. bersifat obyektif

1003 Standar Kemadirian Profesional

- Berkaitan dengan panduan 2003 Kemandirian Profesional
- Berlaku efektif mulai 1 November 2013

2003 Panduan Kemadirian Profesional

- Tujuan

  menyediakan framework yang memungkinkan para profesional auditor untuk :

  1. mengatasi gangguan pada independensi penilaian
  2. mempertimbangkan alternatif pendekatan dalam proses audit ketika independensi penilaian terganggu
  3. mengurangi/menghilangkan dampak independensi audit dalam menjalankan peran non audit, fungsi dan layanan
  4. menentukan persyaratan tambahan jika melihat adanya kemungkinan gangguan independensi penilaian
  5. menjadikan panduan ini sebagai dasar untuk pengambilan keputusan secara profesional dan mencari panduan tambahan sebagai penguatan keputusan tersebut.

2003 Panduan Kemadirian Profesional

- Panduan ini terkait dengan :
  1. Standar 1002 Kemandirian Organisasi
  2. Standar 1003 Kemandirian Profesional
  3. Standar 1005 Kepedulian Profesional

2003 Panduan Kemadirian Profesional

- Kerangka Konseptual

  Profesional auditor harus mengidentifikasi segala kemungkinan gangguan yang mungkin akan dihadapi lengkap dengan panduan untuk menyelesaikan gangguan yang akan mengganggu independensi dan obyektivitas penilaian dalam audit. Dalam menjalankan panduan tersebut juga diperlukan konsultasi baik dengan rekan kerja, manajemen, pihak yang bertanggung jawab dengan tata kelola perusahaan.

2003 Panduan Kemadirian Profesional

- Ancaman dan Pengamanan

  Ancaman dalam independensi penilaian, antara lain :

  1. Kepentingan Pribadi
  2. Penilaian Pribadi
  3. Posisi Auditee
  4. Kedekatan dengan Auditee
  5. Intimidasi
  6. Penilaian yang tidak obyektif
  7. Auditor termasuk dalam jajaran manajemen perusahaan

2003 Panduan Kemadirian Profesional

- Mengelolah Ancaman

1. Untuk merdeka menggunakan kerangka konseptual ketika fakta dan keadaan di mana para profesional melakukan pekerjaan mereka
2. Dapat menciptakan ancaman baru atau meningkatkan signifikansi ancaman yang ada terhadap kemerdekaan
3. Baik secara individu maupun secara agregat karena ancaman dapat memiliki efek kumulatif pada kemandirian profesional
4. Baik secara kualitatif dan kuantitatif saat menentukan signifikansi suatu ancaman

2003 Panduan Kemadirian Profesional

- Mengelolah Ancaman (Lanjutan)

1. Tentukan apakah pengamanan yang sesuai tersedia dan dapat diterapkan untuk menghilangkan ancaman atau menguranginya ke tingkat yang dapat diterima
2. Gunakan pertimbangan profesional dalam membuat keputusan itu, dan harus mempertimbangkan apakah kemandirian pikiran dan kemandirian dalam penampilan dipertahankan
3. Carilah panduan dari pihak yang tepat

2003 Panduan Kemadirian Profesional

- **Non-audit Layanan atau Peran**

Di banyak perusahaan, manajemen, staf IS, dan audit internal diharapkan agar para profesional dapat terlibat dalam memberikan layanan atau peran non-audit seperti:

1. Mendefinisikan strategi SI
2. Mengevaluasi, memilih dan menerapkan teknologi
3. Mengevaluasi, Merancang, mengembangkan, dan mengimplementasikan
4. Menetapkan praktik, kebijakan, dan prosedur yang baik
5. Menerapkan keamanan TI dan kendali TI
6. Mengelola proyek TI.

2003 Panduan Kemadirian Profesional

- **Non-audit Layanan atau Peran Itu Tidak Merusak Kemerdekaan**

Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggap bukan merupakan tanggung jawab manajemen sehingga tidak akan mengganggu independensi. Lebih lanjut, memberikan nasihat dan rekomendasi untuk membantu manajemen dalam melaksanakan tanggung jawabnya tidak dianggap sebagai tanggung jawab manajemen.

2003 Panduan Kemadirian Profesional

- Fungsi-fungsi sehubungan dengan layanan atau peran non-audit :

1. Mengemban semua tanggung jawab manajemen
2. Mengawasi layanan dengan menunjuk seseorang atau lebih
3. Mengevaluasi kecukupan dan hasil layanan yang dilakukan
4. Menerima tanggung jawab atas hasil layanan

2003 Panduan Kemadirian Profesional

- Layanan atau Peran Non-Audit yang Merusak Independensi

Contoh kegiatan yang umumnya dianggap sebagai tanggung jawab manajemen meliputi:

1. Menetapkan kebijakan dan arahan strategis
2. Mengarahkan dan mengambil tanggung jawab atas tindakan karyawan
3. Otorisasi transaksi
4. Memutuskan rekomendasi mana dari fungsi audit, fungsi audit internal, organisasi, KAP atau pihak ketiga lainnya yang akan diterapkan
5. Mengambil tanggung jawab untuk merancang, menerapkan atau memelihara pengendalian internal
6. Menerima tanggung jawab atas pengelolaan proyek

2003 Panduan Kemadirian Profesional

- Relevansi Independensi Saat Memberikan Layanan atau Peran Non-Audit

  Faktor-faktor berikut juga dapat mempengaruhi keputusan:

1. Para profesional tidak boleh ditempatkan dalam situasi untuk mengaudit pekerjaan mereka sendiri atau memberikan layanan
2. Apakah tersedia sumber daya untuk menjalankan fungsi non-audit dan audit independen dan asurans secara terpisah
3. Manajemen SI dan pihak yang bertanggung jawab atas persepsi tata kelola tentang nilai atau pentingnya jasa
4. Tingkat risiko fungsi audit terkait dengan peran atau jasa non-audit
5. Pengaruh keputusan terhadap persyaratan auditor atau regulator eksternal, jika ada
6. Ketentuan piagam audit SI

2003 Panduan Kemadirian Profesional

- Diterimanya Layanan atau Peran Non-audit

Information Sistem (IS) harus menetapkan apakah profesional diizinkan untuk terlibat dalam melaksanakan audit atau peran non-audit dan sifat, waktu, dan luas layanan atau peran yang luas tersebut, untuk memastikan bahwa independensi tidak terganggu sehubungan dengan sistem yang di audit.

2003 Panduan Kemadirian Profesional

- Pelaporan

  Pertimbangan audit dalam pelaporan :

1. Nama dan senioritas profesional yang terlibat dalam audit SI
2. Analisis dan deskripsi ancaman terhadap independensi
3. Pengamanan diterapkan untuk menghilangkan atau memitigasi berbagai ancaman terhadap independensi dan objektivitas
4. Fakta bahwa potensi penurunan independensi tela diungkapkan kepada pihak yang bertanggung jawa

2003 Panduan Kemadirian Profesional

- **Kaitan dengan Standar dan Proses COBIT 5**

Profesional audit dan asurans SI harus independen dan objektif baik dalam sikap maupun penampilan dalam semua hal yang terkait dengan perikatan audit dan asurans.

Proses : mengevaluasi dan menilai kepatuhan dengan persyaratan eksternal.

Tujuan : Pastikan perusahaan mematuhi semua persyaratan eksternal yang berlaku.

2003 Panduan Kemadirian Profesional

- Bimbingan lainnya
  - Saat menerapkan standar dan pedoman, para profesional didorong untuk mencari pedoman lain bila dianggap perlu.
- Audit dan jaminan SI:

1. Kolega di dalam dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau grup media sosial profesional
2. Manajemen
3. Badan tata kelola dalam perusahaan, misalnya, komite audit.

IT AUDIT

Audit dalam arti Umum adalah pemeriksaaan dalam arti luas bermakna evaluasi terhadap suatu organisasi, sistem, proses atau produk. Audit dilaksanakan oleh pihak yang kompeten, objektif serta tidak memihak, disebut auditor.

Audit dalam bidang IT adalah berfungsi untuk mengevaluasi jaringan dan sistem informasi yang ada dalam suatu organisasi atau perusahaan. Banyak metode dalam teknologi informasi, hal ini memungkinkan adanya perbedaan.

IT Audit teknologi informasi secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi maupun jaringan dalam perusahaan itu, hal ini menentukan apakah aset jaringan dan sistem informasi dalam suatu organisasi atau perusahaan itu apakah telah bekerja secara efektif, dan integratif dalam mencapai target organisasi.

Tujuan Audit IT adalah menjalankan pengelolaan IT dengan efektif dan efisien, meningkatkan kepuasan pelanggan dalam pelayanan, peningkatan kinerja, meningkatkan nilai jual (competitive advanced) produk layanan, meningkatkan tingkat kepatuhan terhadap ketentuan / peraturan pemerintah dan bidang usaha, meningkatkan pengawasan (controling) terhadap pengelolaan IT.

Hasil IT Audit akan memberikan gambaran yang komprehensif tentang Manajemen Risiko dalam penyelenggaraan operasional IT dan dapat digunakan sebagai dasar keputusan strategis dalam suatu organisasi atau perusahaan.

The assignment of IT Audit
From Mrs. Widya Cholil, S.Kom., MIT.

Yudy Pranata (192420001), Jepri Yandi (192420044)
AR2
Magister Teknik Informatika
Universitas Bina Darma

Dengan memperhatikan tahapann process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat

boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri

disubmit [perorangan dalam bentuk resume note (tidak presentasi)!

Jawaban:

Terdapat beberapa komponen yang terlibat dalam proses IT Audit tersebut antara lain:

1. Auditor
2. Auditi
3. Organisasi
4. Tools
5. Methods

Terdapat beberapa tahapan dalam proses IT Audit antara lain:

1. Information Gathering
   Tahapan pertama ini adalah tahapan dimana auditor mengumpulkan dan memahami seluruh informasi yang terdapat dalam bisnis auditi (kebijakan, struktur, dsb);

2. Review Prior Audit Issues
   Pada tahapan ini, auditor akan menentukan isu, tujuan dan prespektif bisnis antara penanggung jawab bagian dengan bagian IT;

3. Risk Assessment
   Dengan adanya tahapan kedua yang dimana auditor menentukan isu, tujuan dan prespektif bisnisnya, dalam tahap ini auditor mengambil langkah untuk meperdalam informasi tentang pengendalian yang diterapkan serta memperkirakan hasil audit tersebut apakah dapat dijadikan dasar dalam penilaian. Kuat ataupun tidaknya penilaian terhadap pengendalian tersebut akan dijadikan dasar oleh auditor untuk menentukan Langkah selanjutnya;

4. Develop IT Audit Plan
   Setelah auditor menentukan resiko dari langkah tersebut, pada tahap ini auditor akan melakukan penilaian terhadap langkah yang diambil dan mengembangkan lagi agar tidak memiliki resiko yang terlalu besar seperti sebelum dilakukannya audit.

5. Execute IT Audit Plan
   Pada tahap ini, auditor melakukan pemeriksaan langsung terhadap pengembangan yang dilakukan sebelumnya dan pada akhirnya akan menghasilkan beberapa laporan temuan maupun usulan yang didukung dengan bukti pemeriksaan pada kertas kerja auditor.

6. Customer Satisfaction Evaluation
   Auditor menyiapkan laporan temuan yang dihasilkan sebelumnya dan juga menyiapkan usulan-usulan untuk menindak lanjuti temuan yang ada serta akan memantau proses tindak lanjut dari rekomendasi usulan yang telah diberikan oleh auditor.

Nama : Yuliza Aryani
NIM : 192420024
Kelas : AR1
Mata kuliah : IT Audit
Dosen : Dr. Widya Cholil S.Kom., M.I.T.

TUGAS

IT Audit components

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

Tahapan IT Audit

1. ***Information Gathering***

   Tahap ini, dimana seorang auditor yang mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien.seperti laporan audit sebelumnya, laporan buku besar.

2. ***Review prior audit issues***

Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. ***Risk assessment***

Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat , untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .

4. Develop IT audit

Setelah dilakukan rapat tersebut, auditor mulai menrealisasikan rencana audit , kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.

5. Execute IT audit Plan

Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Nama : Yuni Astuti
NIM : 192420004
Mata Kuliah : IT Audit
Dosen : Dr. Widya Cholil S.Kom., M.I.T.

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat, boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi)

Tahapan IT Audit

1. Information Gathering (Pengumpulan Informasi)
   Untuk Tahapan ini, yaitu mengumpulkan sebanyak-banyaknya informasi penting dan meminta dokumen apa saja yang dibutuhkan terkait dengan kebutuhan Audit atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien seperti laporan audit sebelumnya, dan laporan buku besar.

2. *Review Prior Audit Issues* (Meninjau Masalah Audit Sebelumnya)
   Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. *Risk assessment* (Tugas Beresiko)

   Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat, untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .

4. *Develop IT audit* (Mengembangkan IT Audit)

   Auditor mulai menrealisasikan rencana audit, kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.

5. *Execute IT audit Plan* (Menjalankan Rencana IT Audit)

   Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. *Customer satisfaction Evaluation* (Mengevaluasi Kepuasan Pelanggan)

   Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Nama : A.Firdaus
Nim : 192420043
Kelas : MTI R2

Nama : Istiqomah Febrianty
Nim : 192420042
Kelas : MTI R2

Tugas II (Berkelompok)

Komponen Yang ada Pada IT Audit

a. Pendahuluan

Penerapan TIK diperusahan seiring berjalannya waktu akan banyak mengalami perubahan, karena perkembangan teknologi informasi berkembang begitu cepat. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting, baik untuk perkembangan organisasi maupun membaca persaingan pasar dan selanjutnya dapat digunakan untuk mengambil langkah strategis dengan tujuan memenangkan persaingan. Sistem Informasi digunakan di segala bidang dalam perusahaan untuk melakukan pemprosesan data menjadi suatu informasi, dan ini merupakan sebuah kegiatan dalam organisasi yang bersifat repetitive, dan agar menghasilkan kualitas informasi yang bermutu, maka harus dilaksanakan secara sistematis dan otomatis. Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola sistem dilakukan dengan melakukan audit

b. Kebutuhan IT Audit

1. Data Integritas
   Integritas data adalah menjamin konsistensi data terhadap semua konstrain yang diberlakukan terhadap data tersebut, sehingga memberikan jaminan keabsahan data itu sendiri.

2. Keamanan Aset
   Mengidentifikasi aset-aset apa yang perlu dilindungi pada perusahaan

3. Penggunaan Sumber Daya Yang Efektif dan Efesiensi
   Pemanfaatan sumebr daya yang effektif untuk menekan dan memaksimalkan kebutuhan

4. Capaian Tujuan Perusahaan
   Merupakan sasaran dari tujuan pendiri perusahaan

c. Dasar Dalam Menaudit
   Ada beberapa komponen pengetahuan dalam IT Audit antara lain :
   1. Perilaku Informasi
   2. Sistem Informasi Manajemen
   3. Perilaku Organisasi
   4. Proses Audit (auditing)

d. Standar yang harus dimiliki IT Audit
   Ada beberapa komponen standar yang harus dimiliki oleh auditor antara lain :
   1. Sertifikasi Audit
   2. Prosedur Audit
   3. Framework Audit
   4. Tools Audit
   5. Projek Manajemen

e. Metode IT Audit
   Metode2 yang digunakan dalam IT Audit :
   1. Audit Through The Computer
      dalah Audit yang berbasis komputer dimana dalam pendekatan ini auditor melakukan pemeriksaan langsung terhadap program-program dan file-file komputer pada audit sistem informasi berbasis komputer
   2. Audit With Computer
      Adalah suatu pendekatan yang langsung berhubungan dengan perangkat yg berhubungan dengan komputer
   3. Audit Arround Computer
      adalah suatu pendekatan audit yang berkaitan dengan komputer, lebih tepatnya pendekatan audit disekitar komputer.

f. Salah satu point atau komponen IT Audit adalah IT Security

Apa yang harus dilakukan saat menaudit Security pada IT. Audit keamanan informasi adalah audit pada tingkat keamanan informasi dalam suatu organisasi. Dalam cakupan luas audit keamanan informasi, terdapat berbagai jenis audit, berbagai tujuan untuk audit yang berbeda, dll.

Umumnya, pengendalian yang diaudit dapat dikategorikan menjadi teknis , fisik, dan administratif . Mengaudit keamanan informasi mencakup topik mulai dari mengaudit keamanan fisik pusat data hingga mengaudit keamanan logis dari database dan menyoroti komponen utama yang harus dicari dan metode berbeda untuk mengaudit area ini.

Ketika berpusat pada aspek TI dari keamanan informasi, itu dapat dilihat sebagai bagian dari audit teknologi informasi . Hal ini kemudian sering disebut sebagai audit keamanan teknologi informasi atau audit keamanan komputer. Namun, keamanan informasi mencakup lebih dari sekedar TI.

1. Sistem yang diaudit
   Ada beberapa sistem antara lain :
   a. Kerentanan jaringan
   b. Enkripsi dan audit TI
   c. Audit keamanan logis
   d. Alat khusus yang digunakan dalam keamanan jaringan
   e. Audit Perilaku
   f. Keamanan Aplikasi
   g. Tugas

2. Komponen Proses Audit
   Proses – proses yang dilakukakan dalam IT Audit Security
   a. Perencanaan dan persiapan
   b. Tujuan dari Audit
   c. Melakukan Riview
   d. Laporan

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027

KOMPONEN AUDIT IT

Menetapkan ruang lingkup audit IT

Prasyarat utama untuk program audit organisasi adalah menentukan jenis audit apa yang diperlukan dan mengidentifikasi apa yang harus atau bisa diaudit. Potensi audit yg di kembangkan oleh inventaris disebut dengan Ruang Lingkup. manajemen aset, arsitektur perusahaan, kerangka tata kelola, atau pendekatan lain apa pun yang membantu mengidentifikasi elemen-elemen penyusun organisasi. Organisasi kemudian melakukan penilaian risiko pada setiap item yang termasuk dalam ruang lingkup audit untuk memberikan prioritas pada subyek audit, Dengan mempertimbangkan faktor-faktor untuk setiap item seperti, besarnya relatif risiko pentingnya bagi organisasi, atau potensi manfaat bagi organisasi dari melakukan audit. Prioritasi mencerminkan efisiensi sumber daya organisasi yang tersedia untuk mendukung audit, Aspek organisasi dapat di audit secara memadai Tata kelola formal dan manajemen resiko, kedua domain organisasi ini menekankan identifikasi dan penilaian asset sebagai dasar untuk menyusun kegiatan manajemen dan mengalokasikan sumber daya organisasi, sumber daya kontrol lainnya pada area organisasi yang terkait dengan sumber risiko terbesar.

Mengembangkan dan mempertahankan ruang lingkup audit

Audit di setiap organisasi biasanya mencerminkan cara organisasi itu sendiri terstruktur dan dikelola. Semesta audit dapat diatur atau dikategorikan berdasarkan hierarki unit bisnis, arsitektur perusahaan, model proses bisnis, kerangka kerja tata kelola, katalog layanan, atau dekomposisi fungsional lainnya yang paling sesuai dengan cara organisasi memandang operasi dan aset mereka. ada beberapa level kontrol atau tingkat entitas umum yang menyeluruh yang dapat diaudit. audit kontrol tingkat entitas sering kali memerlukan beberapa pendekatan audit karena biasanya mencakup berbagai jenis kontrol internal. Ruang lingkup audit ini penerapannya di semua tingkat organisasi juga berarti bahwa laporan audit tingkat entitas memiliki khalayak yang lebih luas daripada yang dihasilkan dalam jenis audit lainnya. Auditor yang melakukan audit pada level apa pun di bawah seluruh organisasi perlu memastikan bahwa ruang lingkup audit mereka mencakup level entitas dan kontrol bersama lainnya, serta yang diterapkan secara khusus untuk komponen yang diperiksa oleh audit.

Unsur-unsur organisasi yang biasanya dimasukkan dalam ruang lingkup meliputi:

- unit struktur organisasi seperti unit bisnis, divisi operasi, fasilitas, atau anak perusahaan
- struktur akuntansi seperti pusat biaya, lini bisnis, atau area proses
- sasaran, sasaran, dan hasil strategis, yang dievaluasi sebagian dengan mengaudit sumber daya yang dialokasikan untuk pencapaiannya;
- misi dan proses bisnis, layanan, dan fungsi operasional yang dijalankan oleh organisasi

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027

- aset termasuk aset TI organisasi memiliki, mengoperasikan, mengelola, atau mengendalikan;
- program, proyek, dan investasi di mana organisasi melakukan pendanaan atau sumber daya lainnya;
- kontrol internal dan eksternal yang dilaksanakan oleh organisasi atau atas namanya;
- fungsi atau program manajemen seperti tata kelola, manajemen risiko, jaminan kualitas, sertifikasi, dan kepatuhan serta audit internal.

Penggerak tata kelola, risiko, dan kepatuhan

organisasi menetapkan dan memelihara program di bidang ini, kebutuhan untuk menilai efektivitasnya dan mengukur pencapaian tujuan program mempengaruhi ruang lingkup dan frekuensi audit TI dan prosedur, standar, dan kriteria yang digunakan dalam audit TI internal.
Meskipun kerangka kerja dan tata kelola manajemen risiko jarang menentukan elemen yang cukup, untuk menyediakan inventaris subjek potensial audit, mereka menawarkan fondasi yang kuat, khususnya untuk komponen dan kontrol terkait-TI di dunia audit.
Program kepatuhan memiliki pengaruh, di mana kebutuhan untuk memenuhi tujuan atau persyaratan kepatuhan, adalah faktor utama dalam penentuan prioritas dan kriteria yang digunakan sebagai dasar untuk menunjukkan kepatuhan menetapkan ruang lingkup minimum untuk audit dilakukan untuk mendukung kepatuhan.
Misalnya, versi yang dipakai secara luas 4.1 dari tujuan pengendalian untuk informasi dan teknologi (COBIT) mencakup 34 proses dalam 4 domain tata kelola utama dan mendefinisikan lebih dari 200 tujuan pengendalian yang terkait dengan proses tersebut. COBIT 5 memperluas proses model referensi ke 37 proses di antara 5 domain, menggantikan tujuan kontrol dengan tata kelola dan praktek manajemen yang disarankan dan kriteria audit pada tujuh faktor, mirip dengan kategori ruang lingkup audit : prinsip, kebijakan, dan kerangka kerja, struktur organisasi; Kebudayaan, etika, dan perilaku. Informasi; Layanan, infrastruktur, dan aplikasi.
Enterprise risk management menggunakan ruang lingkup audit development dan IT untuk mengaudit ruang lingkup dengan memberikan identifikasi aset organisasi yang berisiko dan menetapkan jenis risiko-risiko yang berlaku pada komponen atau aspek operasional organisasi. Sementara risiko yang terkait dengan mata pelajaran audit yang berbeda membantu meningkatkan sumber daya yang seharusnya, mempertimbangkan semua jenis risiko yang ada dan dapat memengaruhi cakupan audit.

Strategi dan prioritas audit

Pada bab 3 sudah dijelaskan pentingnya strategi audit terhadap sebuah organisasi dan program audit internalnya. Strategi audit adalah sebuah kunci utama yang menentukan jenis, lingkup, dan frekuensi audit sebuah organisasi memimpin dan mendefinisikan kriteria yang digunakan oleh organisasi untuk memprioritaskan materi di alam semesta audit. Organisasi mengikuti prosedur dalam strategi audit untuk membentuk prioritas audit dan menggunakan determinasi untuk

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
pengalokasikan sumber-sumber audit internal. Rencana pada audit yang terkait untuk menguraikan sumber-sumber yang harus dialokasikan untuk dapat menjawab persyaratan wajib dan tujuan serta persyaratan audit tambahan apa pun. Banyak suatu organisasi menetapkan peringkat prioritas tinggi untuk mengaudit kegiatan yang mendukung kepatuhan hukum atau peraturan, semacam laporan kontrol internal yang diwajibkan dari perusahaan yang diperdagangkan pada bawah pasal 404 dari undang-undang Sarbanes-Oxley [5]. Kegagalan untuk mematuhi persyaratan wajib adalah salah satu dari beberapa jenis risiko organisasi yang dihadapi yang dapat mengakibatkan dampak negatif yang diukur secara langsung dalam istilah keuangan atau tidak langsung dari kerusakan reputasi, publisitas negatif, sanksi hukuman, atau hasil potensial lainnya.

Jenis kontrol

Jenis kontrol adalah sebuah elemen yang berbeda-beda yang ada pada audit, operasi bisnis, aset-asetnya, dan sumber-sumber pendukung yang membentuk kemampuan fungsional suatu organisasi, sementara kontrol pada kemampuan-kemampuan tersebut mencakup struktur manajemen, proses dan protokol, serta langkah-langkah teknis yang menyediakan efisiensi dan keefektifan operasional, kepatuhan, keandalan, dan jaminan operasional. Seperangkat kontrol individu (baik secara internal maupun eksternal) dijalankan oleh sebuah organisasi bertentangan dengan proses pemerintahan pengendalian internal, yang ada untuk membantu organisasi mencapai tujuan manajemen yang berkaitan dengan strategi, operasi, suatu kepatuhan manajemen yang sah atau peraturan, kualitas, keamanan, atau manajemen risiko. Kontrol terutama kontrol internal adalah fokus dari banyak jenis audit, baik dilakukan oleh auditor internal ataupun eksternal. Satu jenis kontrol atau lebih biasanya berlaku untuk semua benda dalam ruang lingkup organisasi. Organisasi dan auditor perlu memiliki pemahaman yang luas tentang berbagai jenis kontrol dan penerapan tujuan dan fungsinya untuk dapat merencanakan dan melaksanakan sebuah audit dengan benar dari kontrol sebuah organisasi dan untuk menyelaraskan jenis kontrol yang digunakan dengan cara kompetensi, keterampilan, dan pengalaman sebelumnya kepada para auditor.

Kontrol Kategorisasi

Kontrol Kategorisasi adalah Kontrol yang luas dan memilih kontrol tersebut dari susunan kontrol yang sama luas atau lebih luas yang disusun untuk implementasi. Seperti halnya item-item dalam ruang lingkup audit dapat diatur atau dikategorikan dalam banyak cara, banyak pendekatan kategorisasi kontrol yang berbeda-beda digunakan dalam kerangka kerja yang tersedia, metodologi, dan panduan. Skema pengukuran umum untuk kontrol termasuk yang didasarkan pada tujuan, sasaran, fungsi, sifat implementasi, dan tingkat penerapan dalam organisasi. Tabel 6.1 memberikan sebuah daftar pendekatan kategorisasi kontrol yang representatif dengan menggunakan basis kategorisasi yang berbeda.

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027

Kategorisasi kontrol terutama dimaksudkan untuk memperkenalkan konsisten dengan cara kontrol dirujuk dan diterapkan dalam konteks yang berbeda-beda dan untuk tujuan berbeda. Seperti yang ditunjukkan oleh Tabel 6.1, tidak ada standar tunggal yang dapat diterima untuk mengkategorikan kontrol, sehingga organisasi dapat memilih atau mengadaptasi pendekatan yang ditentukan dalam susunan kerangka kerja atau metodologi eksternal, mengembangkan kategorisasi mereka sendiri, atau mengikuti standar yang ditetapkan dalam aturan hukum, peraturan, atau kebijakan sebuah organisasi. harus memuaskan. Peraturan keamanan yang diundangkan di bawah Undang-undang Portabilitas dan Akuntabilitas Asuransi Kesehatan tahun 1996 (dikenal secara kolektif sebagai Peraturan Keamanan HIPAA) misalnya, memisahkan persyaratan menjadi pengamanan administratif, teknis, dan fisik, sehingga organisasi yang dicakup oleh hukum mungkin menemukan bahwa menggunakan kategorisasi yang sama pendekatan untuk kontrol internal memfasilitasi kepatuhan.

Tabel 6.1

Basis	Kategorisasi Representatif
Tujuan kontrol	Pencegahan, detektif, korektif
Kontrol objektif	Operasi, pelaporan, kepatuhan Tata kelola, manajemen risiko, kepatuhan
Fungsi kontrol	Administratif, teknis, fisik Manajemen, operasional, teknis
Sifat implementasi	Terpusat, dibagikan, didesentralisasi
Tingkat penerapan	Organisasi, divisi, unit bisnis, fungsi Program, proyek, sistem, komponen

Kontrol Organisasi

Kontrol organisasi adalah control yang ditingkat entitas penting sebagai area fokus untuk audit internal dan eksternal karena mereka memberikan dasar untuk bagaimana organisasi mengelola fungsi yang didukung oleh sebuah kontrol. Kontrol pada level entitas juga disertakan dengan referensi ke dalam banyak jenis audit dilakukan di tingkat organisasi lainnya, sebagai unit bisnis, program dan proyek, dan aset teknologi semuanya yang memanfaatkan jenis-jenis kontrol tingkat entitas. Gambar 6.2 menunjukkan berbagai kategori utama dari entitas level dan jenis kontrol dalam setiap kategori Itu mungkin diterapkan dan akan tunduk pada audit dalam organisasi yang berbeda.

Audit dari kontrol tingkat entitas berbeda pada tingkat tertentu dari pemeriksaan yang difokuskan pada unsur-unsur yang sempit di dalam organisasi. Efektivitas kontrol tingkat entitas sebagian bergantung pada sejauh mana organisasi yang membentuk otoritas kontrol dan menerapkan setiap kontrol dengan cara yang meliputi seluruh organisasi. Dari perspektif ini, audit dari

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
kontrol tingkat entitas pada dasarnya memeriksa kemampuan manajemen dan tata kelola organisasi, termasuk struktur organisasi, penyelarasan bisnis dan tujuannya, keberadaan serta penggunaan kegiatan perencanaan strategis dan operasional. Unsur-unsur pada kontrol ini membantu memastikan bahwa control yang di tentukan organisasi kebijakan sebenarnya diimplementasikan dan digunakan untuk mendukung pencapaian tujuan kontrol organisasi. Tata kelola terkemuka dan kerangka manajemen risiko menekankan bahwa pentingnya menetapkan kontrol tingkat entitas dan tampaknya mengasumsikan bahwa hampir semua organisasi mengenali nilai dari menerapkan jenis-jenis pada kontrol ini [2,8,9]. Asumsi seperti itu sebagian berasal dari proporsi besar perusahaan atau organisasi yang saling tukar di industri atau lingkungan operasi yang diatur untuk membentuk sebuah audit yang diinginkan tentang tata kelola, manajemen risiko, kepatuhan, dan audit.

Mengaudit aset yang berbeda

Auditing aset yang berbeda adalah untuk melakukan pengecekan asset dan kontrol teknis yang terkait, baik sebagai focus utama dalam audit sentris atau dalam konteks seperti fungsi manajemen audit dan proses bisnis yang didukung oleh aset-asetnya.
Untuk melakukan pengecekan asset-aset para auditor yang bertugas perlu untuk memilih prosedur audit yang tepat, sesuai dengan jenis audit yang akan diadakan dan membutuhkan pemahaman cukup tentang konteks asset yang dipakai sebagai bukti yang relevan untuk mendukung temuan audit. Auditors memeriksa beberapa komponen-komponen dalam ruang lingkup sebuah audit tunggal yang memiliki kriteria dan prosedur audit dengan kebutuhan dengan pendekatan konsisten untuk mengumpulkan dan menganalisis sebuah informasi serta melaporkan temuan audit. Di sebagian besar aset TI, ada bidang-bidang umum atau prosedur audit yang dapat membantu menyediakan konsistensi ini, seperti yang dirangkum pada tabel 6.2. Secara kolektif, prosedur-prosedur ini menyoroti penggunaan terpadu dari dokumentasi, penyelidikan, pengamatan, dan uji coba langsung untuk menyediakan bukti yang diperlukan untuk mendukung temuan audit.

Fokus Audit TI	Audit Prosedur
Configuration	Memindai atau menganalisis konfigurasi aset dan membandingkan konfigurasi aktual dengan kebijakan, baseline, dan standar yang disetujui
Logging and monitoring	Konfirmasi logging diaktifkan pada tingkat detail yang sesuai dan output log dipantau dan ditinjau atau dianalisis secara teratur

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027

Access control	Tinjau kebijakan, prosedur, dan mekanisme untuk mengontrol akses ke subjek audit, termasuk pemberian dan pencabutan hak akses dan otentikasi dan otorisasi akses

Dekomposisi Komponen IT

Dekomposisi Komponen IT adalah komponen yang di gunakan untuk kinerja audit untuk lebih efisien dan membantu menentukan ruang lingkup yang lebih akurat untuk menyelesaikan proses audit. menentukan lingkup audit, seperangkat keterampilan dan kompetensi yang diperlukan oleh audit, dan tingkat sumber yang diperlukan untuk menyelesaikan proses audit. Sistem pengaudit ini mencerminkan jenis audit dan tujuannya dimaksudkan, komponen-komponennya akan diperiksa, dan prosedur, protokol, standar, atau auditor kriteria yang akan digunakan.
Tidak ada metode standar tunggal atau "terbaik" untuk mengevaluasi sistem lingkungan teknis. Salah satu caranya adalah menguraikan suatu sistem ke dalam bagian-bagian penyusunnya dan mengaudit setiap komponen secara individu, menerapkan protokol audit yang serupa di semua unsur utama, tetapi juga menggunakan prosedur atau daftar periksa yang spesifik dalam hal teknologi jika perlu
Kategori umum atau komponen yang mewakili bidang audit mencakup delapan unsur yang diperlihatkan pada Gambar 6.1. Beberapa contoh audit istimewa Pertimbangan juga berlaku pada jenis-jenis tertentu dari lingkungan operasi seperti komputasi awan atau penggunaan lainnya dari teknologi virtualisasi server, dan sistem atau akses aplikasi menggunakan peramban web, perangkat seluler, atau jenis aplikasi dan antarmuka klien lainnya. Bagian berikut menjelaskan secara singkat dan pertimbangan audit yang berlaku untuk berbagai komponen-komponennya.

Sistem dan aplikasi

Sistem dan aplikasi memiliki beragam karakteristik seperti arsitektur teknis, sistem operasi, bahasa pemrograman, titik-titik integrasi, dan fungsi yang diinginkan. Pilihan prosedur audit yang sesuai untuk sistem dan aplikasi tergantung pada arsitekturnya dan berbagai jenis komponen teknis yang digunakan untuk pemeriksaan setiap sistem atau subjek aplikasi. Auditor aplikasi sistem fokus pada kemampuan dan kontrol non-fungsional. Masalah fungsional mencakup memastikan bahwa apa yang organisasi lakukan untuk menjalankan fungsinya memenuhi persyaratan yang ditentukan. Aspek yang tidak fungsional mencakup kinerja, kegunaan, keandalan, dan keamanan, di mana para auditor sering menguji atau meninjau bukti yang memperlihatkan penerapan kontrol yang sesuai dengan penggunaan sistem atau penerapan yang diharapkan dan cara pengguna berinteraksi dengannya. Misalnya, audit aplikasi berbasis

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
web sering kali memeriksa penggunaan kendali terhadap kerentanan yang diketahui, kesalahan konfigurasi, dan pengungkapan informasi sensitif yang tidak sah.

Database

Istilah database umumnya berarti setiap kumpulan atau repositori informasi yang disimpan oleh suatu organisasi, tetapi dalam praktik paling sering menyiratkan jenis teknologi spesifik yang menyimpan dan menyediakan akses ke data dalam mendukung satu atau lebih aplikasi dan proses bisnis. Basis data mewakili sebuah jenis perangkat lunak aplikasi khusus, yang tunduk pada banyak prosedur audit dan kriteria pemeriksaan yang sama sebagai aplikasi dan sistem. Sifat dan kepekaan data yang disimpan dalam basis data organisasi mempengaruhi kriteria yang digunakan untuk mengaudit mereka, khususnya sehubungan dengan memeriksa kontrol keamanan atau privasi seperti enkripsi data, pengawasan akses, dan backup data serta pemulihan.

Sistem Operasi

Organisasi Modern sering menggunakan berbagai sistem operasi untuk mendukung berbagai kebutuhan sistem dan komputer, yang paling umum termasuk Microsoft Windows, berbagai versi Unix atau Linux, serta alternatif - dan platform-spesifik seperti z/OS untuk komputer mainframe IBM. Sistem operasi sangat dapat disesuaikan dan dapat diterapkan secara berbeda di seluruh organisasi atau dalam organisasi yang sama. Untuk meningkatkan ketahanan, administrasi, keamanan, dan dukungan, berbagai organisasi sering kali melakukan konfigurasi sistem operasi untuk server, komputer desktop dan laptop, dan perangkat seluler. Banyak pemasok sistem operasi menawarkan rekomendasi konfigurasi yang dimaksudkan untuk mengoptimalkan keamanan atau kesesuaian untuk penggunaan yang berbeda. Audits sistem operasi mengkonfirmasikan penggunaan dan konfigurasi yang sesuai dari sistem operasi pada platform komputasi yang berbeda yang diluncurkan dalam organisasi.

Perangkat Keras

Perangkat keras terdiri dari perangkat fisik yang digunakan untuk membangun jaringan, infrastruktur telekomunikasi, sistem komputer, pelanggan komputasi akhir, dan banyak komponen keamanan fisik. Dalam banyak penguraian arsitektur teknis, perangkat keras menghubungkan server, komputer desktop dan laptop, serta berbagai organisasi perangkat seluler yang digunakan serta router, switch, firewall, dan komponen-komponen lain yang digunakan dalam jaringan. Audit aset perangkat keras itu biasanya berfokus pada konfigurasi yang konsisten dan benar serta kepatuhan terhadap kebijakan dan standar internal. Dibandingkan dengan perangkat lunak, proporsi yang lebih besar dari suatu perangkat keras organisasi ini kemungkinan besar akan dibeli secara komersial, jadi auditor perangkat keras juga

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
mempertimbangkan vendor dan proses-proses internal yang digunakan untuk memperoleh perangkat keras.

Jaringan

Jaringan menyediakan konektivitas dan memungkinkan pertukaran komunikasi dan informasi untuk sebagian besar, jika bukan dari aset-aset organisasi IT. Jaringan meliputi aset-aset perangkat keras seperti router dan firewall yang memungkinkan aliran informasi antara komponen dan komunikasi dan kontrol keamanan yang melindungi kualitas layanan dalam komunikasi jaringan dan informasi rahasia, integritas, dan ketersediaan data melintasi infrastruktur jaringan. Audit jaringan memeriksa implementasi dan konfigurasi perangkat keras, layanan, dan protokol yang dijalankan pada jaringan tersebut, dan kontrol keamanan seperti firewall dan sistem deteksi jaringan. Audit ini juga mempertimbangkan sifat komunikasi di dalam jaringan sehingga auditor dapat memilih prosedur audit yang sesuai untuk menggunakan nirkabel, satelit, seluler dan teknologi jaringan lainnya. Prosedur audit khusus yang digunakan untuk memeriksa jaringan tergantung pada jenis perangkat keras, layanan, kontrol keamanan, dan infrastruktur telekomunikasi yang diterapkan oleh suatu organisasi dan pada skala jaringan dalam ukuran geografisnya serta jumlah dan berbagai sistem dan fasilitas yang terhubung dengannya. Sementara sebagian besar teknologi yang mendasarkannya sangat mirip terlepas dari skala jaringan, ada perbedaan praktis dalam mengaudit konvensional atau virtual jaringan area lokal yang digunakan dalam satu lokasi dengan jaringan luas area mencakup berbagai situs.

Tempat Penyimpanan

Meskipun organisasi menyimpan sejumlah besar data dalam basis data antarnegara, konten dan dokumen sistem manajemen, dan komponen-komponennya yang serupa, penggunaan teknologi penyimpanan yang mutakhir membuat tempat, jaringan, dan infrastruktur merupakan bagian yang unik dari program ini yang digunakan pada audit. Solusi penyimpanan menggunakan perangkat keras, perangkat lunak, protokol komunikasi, dan metode penyimpanan data serta akses, meskipun bidang penekanannya untuk audit penyimpanan tumpang tindih secara substansial dengan bidang-bidang yang ada pada basis data. Prosedur Audit dan kriteria penyimpanan bergantung pada jenis spesifik teknologi penyimpanan yang digunakan suatu organisasi dan sifat serta kepekaan data yang ditampung di lingkungan penyimpanan. Penyimpanan dapat diaudit secara terpisah atau dalam teknologi operasional yang lebih luas seperti ini biasanya ditetapkan sebagai komponen pendukung dari pusat data atau lingkungan operasi teknis lainnya, di mana sebuah infrastruktur penyimpanan tunggal dapat menerima data dari berbagai sistem.

Pusat Data

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
Sebagai fasilitas yang digunakan sistem, perangkat keras, infrastruktur jaringan, dan teknologi terkait, pusat data menyediakan fondasi yang penting bagi cara kerjanya. Selain berfungsi sebagai lokasi fisik bagi banyak komponen teknologi, pusat data juga menjadi titik pelaksanaan bagi banyak proses, prosedur, dan fungsinya yang mendukung proses tersebut. Audit fasilitas pusat data berfokus pada kontrol jenis khusus ini dan proses dukungan operasional, sumber, dan personil yang memastikan bahwa komponen yang berasal di pusat data beroperasi secara normal untuk mendukung proses dan fungsi bisnis yang bergantung padanya. Apakah dimiliki dan dikelola oleh suatu organisasi atau pihak ketiga, pusat data sering dianggap penyedia jasa dan oleh karena itu digunakan pada standar eksplisit yang ditetapkan untuk audit organisasi layanan.

Lingkungan tervirtualisasi

Teknologi virtualisasi menyediakan sebuah pendekatan teknis alternatif untuk menyediakan infrastruktur, platform dan sistem operasi, server, perangkat lunak, serta sistem dan aplikasi. Kebanyakan lingkungan komputasi yang berkualitas memiliki banyak kesamaan dengan pusat data konvensional, Pendekatan ini meningkatkan pemanfaatan kapasitas dan di dalamnya layanan model berbasis cloud seperti komputasi cloud, memungkinkan organisasi untuk menggunakan sumber daya teknologi ini lebih efisien dengan naik atau turun sebagai surat perintah kebutuhan bisnis. Audit lingkungan komputasi berkualitas menggunakan banyak prosedur dan kriteria yang sama yang digunakan untuk audit pusat data, dengan penekanan tambahan pada server penyedia, deprovisioning, manajemen, pemeliharaan berbagai server virtual yang berbagi komputasi, jaringan, dan sumber daya infrastruktur.
Penggunaan komputasi cloud dan penyedia layanan pihak ketiga menjadi cukup umum sehingga para audits mungkin menanggapi layanan demikian yang berbeda dengan komponen audit lainnya. Perbedaan yang ditekankan oleh para penyedia layanan cloud antara lain penyedia layanan termasuk akses jaringan, akses sumber daya, sumber daya pooling, kemampuan dan jasa yang fleksibel, dan penggunaan yang bermebel serta model pembayaran dan pembayaran yang terkait. Pertumbuhan yang diharapkan dalam komputasi cloud adalah salah satu faktor yang mendorong kerangka kerja kontrol yang spesifik di awan, Kerangka kerja yang tersedia termasuk matriks kontrol awan yang dikembangkan oleh aliansi keamanan cloud dan risiko Federal dan Program manajemen wewenang yang dikelola oleh administrasi layanan umum untuk digunakan oleh penyedia layanan awan yang melayani instansi pemerintah as.

Antarmuka

interface adalah titik integrasi atau koneksi antara dua komponen atau lebih, yang memungkinkan transmisi informasi antara sistem atau mengekspos layanan atau kemampuan fungsional dari satu sistem atau aplikasi pada orang lain. Auditor sering kali menekankan langkah-langkah keamanan yang diimplementasikan untuk melindungi informasi dalam perjalanan melintasi antarmuka dan untuk mengendalikan akses ke antarmuka yang terpapar oleh setiap sistem. Audit antarmuka mengandalkan pada kedua dokumentasi seperti spesifikasi

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
antarmuka formal dan tes yang menunjukkan fungsi yang benar dari tiap antarmuka, mempertimbangkan tujuan yang dimaksudkan, aliran informasi, mekanisme akses teknis, dan proses oketifikasi dan otorisasi tingkat mesin.

Kontrol atau proses prosedural audit

Ruang lingkup audit teknologi informasi sangat luas dan beragam seperti yang dimiliki oleh organisasi sendiri, yang meliputi berbagai macam teknologi, kemampuan teknis, dan kontrol serta kebijakan, proses, dan prosedur yang berkaitan dengan fungsi operasional dan tata kelola. Bergantung pada jenis dan lingkup audit yang direncanakan oleh suatu organisasi, auditor bisa saja memeriksa basis proses atau kontrol prosedural yang berkaitan dengan asetnya dan komponen IT yang mendukung mereka, atau secara terpisah dengan audit yang spesifik dalam proses. Penekanan relatif yang menempatkan suatu organisasi pada audit proses-proses itu dipengaruhi hingga batas tertentu oleh tata kelola, risiko, kepatuhan, dan kerangka manajemen yang dipilih untuk dijalankan. Banyak jenis audit eksternal termasuk yang dimaksudkan untuk memperoleh sertifikasi atau menunjukkan keterlibatan peraturan yang mengharuskan auditor untuk mempertimbangkan pengawasan administratif, teknis, dan fisik dalam lingkup audit yang sama. Organisasi biasanya memiliki lebih banyak kebijaksanaan untuk merencanakan, mendefinisikan ruang lingkup, dan melakukan audit internal dengan cara yang memisahkan audit proses dan kontrol prosedural dari audit aset, sistem, dan teknologi IT. Ada banyak alasan untuk mengejar pendekatan seperti itu, termasuk kemampuan untuk meningkatkan keterampilan dan kompetensi para auditor terhadap masalah audit yang mereka lakukan.

Operasi IT

Operasional IT audits berfokus pada proses dan prosedur yang dilaksanakan oleh suatu organisasi dan penyelarasan kegiatan-kegiatan tersebut dengan sumber sistem, infrastruktur, dan teknologi informasi lainnya. Untuk berhasil melakukan jenis audit ini, organisasi perlu mengembangkan inventarisasi dari proses dan kontrol prosedural yang digunakannyan (atau mengidentifikasi informasi ini dalam dokumentasi yang ada di dalam sistem audit di ruang lingkup audit) dan menyiapkan strategi audit serta rencana audit yang sesuai dengan rencana audit yang digunakan pada jenis audit lain. Proses pemeriksaan yang relevan mencakup mereka dalam bidang bisnis yang lebih spesifik maupun umum, termasuk :

- Perencanaan strategis dan taktis
- Manajemen Resiko
- Manajemen kualitas
- Pengelolaan keuangan
- Pengelolaan sumber daya manusia
- Akuisisi atau pengadaan

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027

- Pengelolaan rantai pasokan
- Program dan manajemen proyek
- Manajemen perubaham
- Manajemen pelayanan
- Dukungan pelanggan dan teknis
- Manajemen keamanan
- Manajemen fasilitas
- Manajemen vendor

Proses operasional dan kontrol prosedural juga digunakan pada prioritas sehingga sumber audit dapat dialokasikan dengan efektif. Prioritas dalam konteks ini mempertimbangkan kriteria seperti tingkat sumber daya yang terlibat, kompleksitas, hubungan ketergantungan dengan proses lain, dan kritik setiap proses terhadap organisasi secara keseluruhan atau pada fungsi misi atau bisnis yang didukung.

Program dan manajemen proyek

Program atau proyek sering digunakan secara bergantian, standar dan bimbingan untuk mengelola kegiatan-kegiatan yang berbeda, durasi, dan hasilnya, di mana program terdiri dari satu proyek atau lebih, memiliki jangka waktu yang kurang jelas, dan dimaksudkan untuk mencapai satu atau lebih hasil jangka panjang, proyek lebih terfokus secara sempit, usaha sementara dengan poin awal dan akhir yang jelas dimaksudkan untuk menghasilkan produk atau jasa tertentu. Program dan proyek dapat dikenakan pada audit operasional; Audit yang dikaitkan dengan sertifikasi, kepatuhan, atau jaminan kualitas; Audit yang spesifik berfokus pada teknologi, sistem, infrastruktur, atau proses yang mendukung program atau pelaksanaan proyek yang efektif. Para auditor melakukan audit jenis ini biasanya karena kriteria audit dasar setidaknya sebagian dari apa yang ditetapkan dalam metodologi atau standar siklus yang didefinisikan atau diterapkan oleh organisasi. Audit proyek dan Program, sebaliknya, berpusat pada proses, kontrol, dan artefak yang dihasilkan dalam pelaksanaan Program atau kegiatan proyek serta penyelarasan kegiatan tersebut dengan kebijakan, standar, dan persyaratan organisasi. Auditor yang memfokuskan pada audit jenis ini cenderung mengandalkan pemeriksaan bukti dokumenter, pengamatan langsung, dan wawancara dengan staf program atau proyek, karena metode pengujian kurang bisa diterapkan pada kegiatan manajemen. Beberapa pemeriksaan terhadap program dan kemampuan manajemen proyek sering kali disertakan dalam audit operasional atau kepatuhan, atau dalam audit sertifikasi menangani standar-standar untuk kualitas, manajemen pelayanan, atau proses kedewasaan.

Siklus kehidupan pengembangan system

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
Proyek-proyek ini dilakukan di banyak organisasi yang digunakan pada serangkaian proses dan kegiatan yang dikenal sebagai suatu sistem (atau perangkat lunak) siklus kehidupan pembangunan (SDLC). Saat proyek ini berjalan melalui fase berbeda dari SDG, tim proyek ini menjalankan berbagai kegiatan, menghasilkan keluaran yang berbeda, dan memenuhi persyaratan atau kriteria yang diperlukan untuk menyelesaikan satu fase dan beralih ke fase berikutnya. metodologi SDLC tidak mempunyai kesamaan untuk berbagai organisasi degan variasi luas sae siklus hidup dan durasi fase yang di harapkan standar SDLC, Dari prespektif holistik model SDLC memiliki kegiatan dan tujuan yang sama. Organisasi hanya menggunakan 4 fase atau 10 SDLC, pada dasarnya SDLC mencakup kegiatan yang berhubungan dengan inisiasi proyek, desain, operasi dan penghentian proyek. Organisasi hanya menerapkan satu SDLC standar. Audit proyek ini dapat dilaksanakan di setiap titik dalam kehidupan siklus atau potensi rentang siklus hidup beberapa fase siklus kehidupan untuk proyek besar atau kompleks atau mereka yang menggunakan metodologis-artinya auditor harus menyesuaikan kriteria pemeriksaan mereka untuk mencerminkan kegiatan, hasil, dan pencapaian yang berbeda dalam setiap fase. Bagian-bagian berikut mengikuti nama fase kehidupan sistem siklus kehidupan yang diperinci.

Konsep

Setiap proyek IT dimulai dengan ide, saran, persyaratan, atau kebutuhan organisasi lain yang diakui. Konsep proyek atau tahap inisiasi dimulai ketika suatu organisasi mengidentifikasi kebutuhan akan kemampuan baru atau yang ditingkatkan dan mulai menentukan bagaimana konsep dapat memenuhi kebutuhan itu. Selama fase konsep, organisasi dapat mengidentifikasi dan mengevaluasi beberapa alternatif, mempertimbangkan karakteristik teknis dan nonteknis seperti biaya, kompleksitas, strategi akuisisi, dan kelayakan. Audit proyek IT dalam fase konsep biasanya memeriksa proses manajemen proyek, standar, dan metodologi untuk memastikan mereka sesuai dengan kebijakan dan standar organisasi dan memverifikasi kelengkapan dan persetujuan (jika diperlukan) dokumentasi proyek yang diperlukan seperti rencana proyek proyek manajemen piagam, kasus bisnis, analisis alternatif, dan jadwal proyek. Fase konsep juga dapat menghasilkan spesifikasi persyaratan fungsional dan teknis, desain solusi tingkat tinggi, pemilihan kontrol awal, dan rancangan artefak proyek yang harus diselesaikan pada fase selanjutnya seperti rencana keamanan, rencana manajemen risiko, rencana darurat, atau jaminan kualitas. rencana. Organisasi mungkin memerlukan audit pada fase konsep sebagai prasyarat untuk menyetujui transisi proyek ke fase pengembangan.

Pengembangan

Fase pengembangan mencakup berbagai kegiatan yang dimaksudkan untuk memenuhi set lengkap persyaratan yang ditentukan untuk sistem, aplikasi perangkat lunak, atau solusi lainnya. Banyak metodologi SLDC membagi fase pengembangan tunggal yang didefinisikan dalam ISO /

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
IEC 15288 menjadi beberapa fase yang lebih kecil untuk analisis persyaratan dan desain selain pengembangan. Fase pengembangan meliputi spesifikasi persyaratan fungsional dan nonfungsional yang lengkap, dokumentasi desain terperinci yang membahas semua komponen dalam ruang lingkup proyek, rencana pengujian, dan pengiriman kode perangkat lunak, teknologi yang diperoleh, atau elemen solusi lain yang siap untuk diintegrasikan, pengujian, dan evaluasi kontrol. Selama pengembangan, tim proyek juga mengidentifikasi kebutuhan operasional yang diharapkan dalam hal infrastruktur, perangkat keras dan kapasitas jaringan, platform komputasi, dan operasi, pemeliharaan, dan kebutuhan dukungan. Audit proyek IT dalam fase pengembangan fokus pada keakuratan dan kelengkapan dokumentasi dan artefak utama, memastikan bahwa desain yang disetujui memenuhi semua persyaratan, termasuk kontrol internal yang memadai, dan mematuhi standar dan kriteria internal dan eksternal yang berlaku. Untuk melakukan proyek yang melibatkan pengembangan perangkat lunak khusus, ruang lingkup audit proyek IT dapat mencakup tinjauan atau proses kontrol kualitas perangkat lunak lainnya. Terlepas dari sumber atau jenis teknologi yang digunakan dalam proyek, pada akhir fase pengembangan, semua dokumentasi desain, antarmuka integrasi, dan spesifikasi teknis harus lengkap dan komponen sistem atau aplikasi perangkat lunak harus siap untuk evaluasi dan persetujuan sebelum penyebaran penuh.

Produksi

Istilah produksi seperti yang digunakan dalam ISO / IEC 15288 berhubungan dengan serangkaian kegiatan yang dimaksudkan untuk menguji solusi teknis atau mengkonfirmasi kemampuan organisasi untuk mengirimkan produk atau layanan yang dihasilkan dari proyek. Untuk proyek yang menggunakan sistem atau aplikasi perangkat lunak, ruang lingkup fase produksi terdiri dari unit kerja, integrasi, dan pengujian penerimaan untuk mengonfirmasi bahwa teknologi memenuhi persyaratan fungsional; memverifikasi implementasi dan konfigurasi kontrol internal yang tepat; dan menilai langkah-langkah perlindungan keamanan dan privasi yang diperlukan untuk menerima persetujuan untuk sistem atau perangkat lunak agar dapat beroperasi penuh. Audit proyek TI selama fase produksi memeriksa rencana pengujian dan prosedur untuk memastikan bahwa kegiatan pengujian cukup untuk menentukan kepuasan persyaratan. Karena produksi adalah fase terakhir sebelum sistem atau aplikasi perangkat lunak digunakan untuk digunakan, auditor juga memeriksa bahwa proyek telah menerima semua persetujuan yang diperlukan, berpotensi termasuk hasil uji fungsional, penerimaan pengguna, integrasi sistem, kesiapan lingkungan, penerimaan risiko, dan otorisasi untuk beroperasi.

Pemanfaatan

Dalam fase pemanfaatan, sistem atau layanan yang ingin disampaikan oleh proyek yang siap untuk di gunakan, di mana fokus proyek berpindah dari mempersiapkan penempatan untuk secara aktif mengoperasikan dan memelihara sistem dengan cara yang terus-menerus memenuhi

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
kebutuhan pengguna. Suatu sistem dalam tahap pemanfaatan biasanya digunakan pada audit operasional rutin untuk mengevaluasi efisiensi dan efektivitas sistem yang sedang berlangsung dan proses bisnis yang didukungnya. Organisasi juga dapat melakukan berbagai audit khusus IT yang membahas sistem secara keseluruhan atau komponen-komponennya. Sebaliknya, audit proyek IT dalam fase pemanfaatan fokus pada memverifikasi bahwa sistem ketika digunakan akan memberikan fungsionalitas yang dimaksud dan memenuhi persyaratan teknis dan standar yang berlaku, mengandalkan bukti yang didokumentasikan seperti hasil pengujian, penilaian kontrol, dan persetujuan dari personel yang berwenang. dalam organisasi. Audit proyek pada fase ini juga berusaha untuk memastikan bahwa sumber daya yang ditentukan dan disediakan untuk sistem operasional sudah benar dan memadai.

Bantuan

Untuk sistem operasional, dukungan terdiri atas pemantauan, administrasi teknis, pemecahan masalah dan penyelesaian masalah, dan kegiatan pemeliharaan rutin seperti backup, konfigurasi control, patch management, dan upgrade dan pelepasan manajemen untuk perangkat lunak atau komponen teknis lainnya. Bergantung pada kebijakan, prosedur, dan standar organisasi, dukungan dapat juga mencakup kegiatan manajemen keamanan informasi seperti analisis kerentanan, verifikasi otomatis atau manual terhadap pengaturan konfigurasi, serta informasi keamanan dan manajemen peristiwa. Fase dukungan dari proyek IT biasanya berjalan sejajar dengan pemanfaatan; Fase-fase serupa dengan dukungan dalam berbagai metodologi SDLC disebut pemeliharaan, dengan kombinasi pemanfaatan dan dukungan yang dikenal secara kolektif sebagai operasi dan pemeliharaan. Kemampuan dukungan teknis suatu organisasi memiliki dampak langsung pada efektivitas operasional sistemnya, jadi meskipun kegiatan fase dukungan-dukungan dapat diaudit dalam isolasi, cakupan audit pada fase pemanfaatan sering kali mencakup fungsi dukungan.

Pensiun

Proyek menurut definisi memiliki titik akhir yang terdefinisi dengan baik, biasanya bertepatan dengan keputusan organisasi untuk menonaktifkan atau mengganti sistem atau layanan. Fase pensiun dari siklus hidup proyek melibatkan kegiatan yang diperlukan untuk menghilangkan kemampuan operasional dan untuk memastikan disposisi peralatan, perangkat keras dan perangkat lunak, data, dan sumber daya lainnya yang sebelumnya dialokasikan untuk mengoperasikan dan mendukung system proyek baru. Prioritas utama untuk fase pensiun selaras langsung dengan bidang-bidang yang ditekankan untuk audit proyek-proyek IT yang mencapai fase akhir ini: membuang atau menggunakan kembali aset teknologi, melepaskan sumber daya yang berkomitmen pada sistem sehingga dapat diterapkan di tempat lain dalam organisasi yang baru dan membersihkan media penyimpanan yang tetap dan dapat dilepas untuk memastikan bahwa tidak ada data yang tersisa pada komponen yang dinonaktifkan. Auditor IT yang

Nama : ade saputra
Kelas : MTI 21 Reg B
NIM : 192420027
memeriksa proyek dalam fase pensiun mencari dokumentasi menyeluruh yang merinci disposisi sumber daya proyek dan aset IT dan untuk persetujuan resmi atas dokumentasi tersebut yang biasanya merupakan prasyaratan untuk secara resmi menutup proyek.

Nama Mahasiswa : Andriansyah

NIM : 192420020

Mata Kuliah : IT Audit

Jawaban

Komponan yang terlibat adalah

1. Sertifikasi IT Audit
2. Prosedur IT Audit
3. IT Audit Frameworks
4. IT Audit Tools
5. Manajemen Project

Information Technology Audit

Dr. Widya Cholil S.Kom., M.I.T.

Nama Mahasiswa : Ardiansyah
NIM : 192420013
Kelas : AR1

TUGAS

IT Audit components, dalam proses / tahapan yang ada dalam IT Audit terdapat 6 bagian tahapan yang menjadi dasar dalam penerapannya, yakni:

Tahapan IT Audit

1. ***Information Gathering***
   Tahap ini, dimana seorang auditor yang mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien.seperti laporan audit sebelumnya, laporan buku besar.
2. ***Review prior audit issues***
   Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.
3. ***Risk assessment***
   Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat , untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .
4. ***Develop IT audit***
   Setelah dilakukan rapat tersebut, auditor mulai menrealisasikan rencana audit , kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.
5. **Execute IT audit Plan**
   Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien
6. **Customer satisfaction Evaluation**
   Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Bhagaskara / 192420028
IT Audit

Komponen-komponen IT Audit adalah sebagai berikut:

1. Pendefinisian tujuan perusahaan
Tujuan perusahaan menjadi salah satu aspek yang penting dalam teori perusahaan. Dalam hal ini, tujuan menciptakan suatu kerangka terstruktur terkait aktivitas perusahaan yang akan menjadi acuan bagi perusahaan untuk mencapai efisiensi serta menunjukkan kebijakan-kebijakan yang akan diambil dalam rangka mencapai output yang diharapkan. Disamping itu, tujuan perusahaan juga menjadi ukuran bagi perusahaan dalam menentukan tingkat keberhasilan dari aktivitasny. Oleh karena itu, tujuan perusahaan harus jelas sehingga mampu menyediakan acuan bagi *stakeholders* perusahaan dalam menjalankan fungsinya masing-masing maupun dalam menilai kinerja perusahaan. Maka dari itu dengan mengetahui tujuan perusahaan Audit TI akan lebih terarah sesuai dengan tujuan perusahaan.

2. Penentuan isu, tujuan dan perspektif bisnis antara penanggung jawab bagian dengan bagian TI
Salah satu tujuan dari Audit TI adalah mencari bukti isu-isu yang terdapat pada suatu perusahaan, oleh karena itu perlu dilakukan penentuan isu. Masalah isu ini merupakan hal yang harus diselesaikan agar perusahaan dapat berjalan sesuai dengan tujuan dan persepektif bisnis. Selanjutnya, temuan isu ini akan dibahas dan didiskusikan kepada penanggung jawab bagian dimana isu itu ditemukan dan bagian TI.

3. Review terhadap pengorganisasian bagian TI
Masalah yang terjadi dapat berasal dari pengorganisasian bagian TI yang salah. Beberapa hal yang direview dalam pengorganisasin bagian TI meliput perencanaan proyek, status dan prioritasnya, staffing levels, belanja TI, dan IT change process management.

4. Assessment infrastruktur teknologi dan Assessment aplikasi bisnis
Melakukan assessment terhadap infrastruktur yang digunakan pada suatu perusahaan agar mengetahui terdapat bagian yang kurang atau salah pada infrastruktur yang telah diterapkan. Infrastruktur teknologi sendiri dapat dilakukan di banyak bidang seperti komputer, jaringan, atau alat-alat pendukung teknologi yang digunakan. Selain terhadap infrastruktur, assessment juga dilakukan terhadap aplikasi bisnis yang digunakan dalam proses bisnis. Hal ini dilakukan untuk mengetahui keadaan data-data yang berjalan selama proses bisnis baik dalam segi keamanan ataupun kebenaran data.

5. Temuan-temuan
Temuan-temuan yang didapat pada saat proses audit dilakukan haruslah dikumpulkan dan dievaluasikan agar dapat ditemukan solusi terhadap masalah yang ada. Proses ini merupakan proses penting agar temuan-temuan yang ada dapat terselesaikan dan jalannya perusahaan dapat menjadi lebih baik.

6. Laporan rekomendasi
Laporan rekomendasi merupakan laporan yang dihasilkan berdasarkan temuan-temuan isu dan hasil evaluasi terhadap temuan-temuan yang ada. Laporan ini digunakan oleh perusahaan yang diaudit untuk memperbaiki masalah yang dihadapi sehingga jalannya proses bisnis dapat lebih baik dan juga dipercaya (tersertifikasi)

Terdapat dua komponen penting dalam audit yaitu:

1. Audit interm yang bertujuan menetapkan seberapa besar system pengendalian internal dapat diandalkan, dan biasanya membutuhkan uji kelayakan. Uji kelayakan tersebut adalah untuk mengkonfirmasi keberadaan, menilai efektivitas, dan memeriksa kesinambungan operasi kelayakan telah dinyatakan oleh internal control.
2. Audit laporan keuangan yang melibatkan uji substantive. Pengujian bersifat substantive adalah verifikasi langsung terhadap angka-angka laporan keuangan, menempatkan keandalan pengendalian internal sebagai hasil jaminan audit interim.

Tiga pendekatan auditing:

- Auditing Around Computer (Audit Sekitar Komputer) yaitu dimana penggunaan komputer pada tahap proses diabaikan.
- Auditing Throught Computer (Auditing Melalui Komputer) yaitu dimana pada tahap proses penggunaan komputer telah aktif.
- Auditing With Computer (Auditing Dengan Komputer) yaitu dimana input, proses dan output telah menggunakan komputer.

Nama : Hasirul Qodar
NIM : 192420014
Kelas : AR1
Mata kuliah : IT Audit
Dosen : Dr. Widya Cholil S.Kom., M.I.T.

TUGAS

IT Audit components

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

Tahapan IT Audit

1. ***Information Gathering***

   Tahap ini, dimana seorang auditor yang mengumpulkan informasi yang dibutuhkan dengan meminta dokumen – dokumen yang dibutuhkan terkait kebutuhan audit. Atau auditor tersebut membuat *checklist* dokumen apa saja yang dibutuhkan kepada klien.seperti laporan audit sebelumnya, laporan buku besar.

2. ***Review prior audit issues***

Auditor mulai memeriksa informasi yang terdapat pada dokumen yang telah diberikan dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. *Workshop* akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. ***Risk assessment***

Auditor melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat , untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas , dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi .

4. Develop IT audit

Setelah dilakukan rapat tersebut, auditor mulai menrealisasikan rencana audit , kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan *feedback* kepada auditor.

5. Execute IT audit Plan

Auditor menyiapkan laporan audit yang berisi rincian temuan –temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis,teknis,material dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

TUGAS AUDIT IT

KOMPONEN DALAM PROSES AUDIT IT

Disusun Oleh : 1. Hendra Yada Putra (192420034)

2. Muhammad Ichsan (192420031)

Kelas : MTI 3B

Mata Kuliah : AUDIT IT

Dosen Pengajar : DR Widya Cholil S.KOM, MIT

UNIVERSITAS BINA DARMA

PALEMBANG

2020

PENDAHULULUAN

Audit IT merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan. sehingga menjadi Seorang auditor IT itu tidaklah mudah karena harus bertanggung jawab terhadap gagalnya pengembangan sistem informasi yang menyebabkan kerugian serta menuntut kedisiplinan kerja secara profesional.

Agar dapat memahami proses audit teknologi informasi, setidaknya harus memahami jenis/bagian secara umum dari teknologi informasi itu sendiri yang terdiri atas:

1. Systems and Applications

Pada bagian ini mewakili bagaimana sebuah data diproses melalui aplikasi perangkat lunak komputer yang dikelola melalui suatu sistem yang biasanya terdiri atas tingkatan hierarkis yang mengikuti aturan bisnis yang berlaku di organisasi yang menggunakannya. Sehingga proses auditnya sendiri akan meliputi verifikasi terhadap sistem dan aplikasinya apakah handal, efisien serta memiliki kontrol yang melekat untuk memastikan kebenaran, kehandalan, kecepatan maupun keamanan pada saat pengiriman, pemrosesan serta pengeluaran informasi di setiap tingkatan kegiatan sistem.

2. Information Processing Facilities

Merupakan komponen yang terkait dengan fasilitas-fasilitas yang digunakan untuk mengolah informasi di suatu organisasi. Biasanya ini terkait dengan perangkat keras seperti misalkan scanner, komputer server, formulir, dsb. Di komponen teknologi informasi ini dilakukan verifikasi untuk memastikan apakah fasilitas pemrosesan terkendalikan untuk memastikan kecepatan, ketepatan dan tingkat efisiensi dari aplikasi-aplikasi berada dalam kondisi normal serta di bawah kemungkinan adanya potensi kerusakan/gangguan.

3. Systems Development

Adalah bagian dari proses pembangunan maupun pengembangan dari sistem yang sudah ada dalam suatu organisasi sesuai tujuan-tujuan aktivitasnya. Proses audit pada komponen ini ditujukan untuk memverifikasi apakah setiap sistem yang sedang dalam proses pengembangan

sesuai dengan tujuan/pedoman/arahan/visi/misi dari organisasi penggunanya. Selain itu proses audit pada bagian ini juga ditujukan untuk memastikan apakah selama proses pengembangan sistem sesuai dengan standar-standar yang secara umum digunakan dalam pengembangan sistem.

4. Management of IT and Enterprise Architecture

Pengelolaan atas teknologi informasi serta arsitektur seluruh lingkup internal organisasi yang disesuaikan dengan struktur dan prosedur yang ditetapkan oleh manajemen adalah sangat penting. Pentingnya hal tersebut memerlukan proses audit yang dilaksanakan untuk memastikan apakah segenap lingkungan/komponen organisasi dalam pemrosesan informasinya dilakukan secara terkendali dan efisien.

5. Client/Server, Telecommunications, Intranets, and Extranets

Komputer, peralatan telekomunikasi, sistem jaringan komunikasi data elektronik (intranet/extranet) serta perangkat-perangkat keras pengolahan data elektronik lainnya adalah komponen dari sebuah teknologi informasi. Audit di bagian ini menjadi penting untuk melakukan verifikasi atas seperangkat pengendalian pada infrastruktur perangkat keras yang digunakan dalam pemrosesan serta komunikasi data secara elektronik dalam suatu sistem jaringan yang terintegrasi.

KOMPENAN APA SAJA DALAM PROSES AUDIT?

Dimana dalam melaksakan proses audit teknologi/sistem informasi meliputi tahapan-tahapan berikut :

1. Planning

Pada tahapan ini lakukan perencanaan menyeluruh atas hal-hal mendasar seperti:

- Fokus komponen yang akan diaudit
- Alat (framework) yang akan digunakan sebagai pedoman pelaksanaan audit
- Kebutuhan sumber daya yang diperlukan
- Hasil akhir yang diinginkan dari proses audit
- Jadual kegiatan
- Rencana Anggaran Biaya jika menggunakan jasa pihak lainnya

2. Studying and Evaluating Controls

Pada tahap ini setelah kita mempelajari bagaimana kondisi dari obyek audit kita. Biasanya secara mendasar fokus dari audit adalah kemampuan pengendalian/kontrol atas obyek tersebut. Kemudian dari hasil melakukan analisis tersebut disusun evaluasi atasnya.

3. Testing and Evaluating Controls

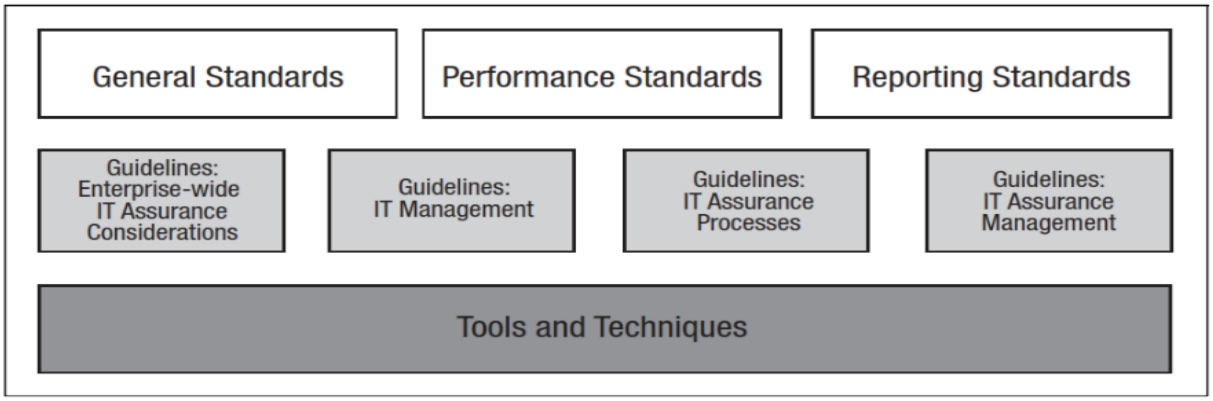
Setelah mempelajari dan mengevaluasi hasil analisisnya, tahap berikutnya adalah melakukan serangkaian pengujian atas obyek audit kita. Pengujian tersebut tentunya menggunakan standar-standar baku berdasarkan framework yang sudah ditetapkan sebelumnya untuk digunakan dalam proses audit. Sama halnya dengan tahapan sebelumnya, inti dari proses audit adalah melakukan telaah uji atas kemampuan pengendalian atas setiap aspek dari sumber daya teknologi informasi yang ada berdasarkan batasan-batasan yang sudah disepakati sebelumnya.

Standar yang digunakan dalam mengaudit sistem informasi adalah standar yang diterbitkan oleh ISACA yaitu ISACA IS Auditing Standard. Selain itu ISACA juga menerbitkan IS Auditing Guidance dan IS Auditing Procedure.

Perlu adanya penelitian berupa pengembangan kerangka kerja penyusunan program audit sistem informasi dengan menggunakan Information Technology Assurance Framework (ITAF) dari ISACA yang lebih menitikberatkan pada proses audit, didesain untuk profesional yang bergerak di bidang jasa audit atau assurance dan menggunakan istilah-istilah yang lebih familiar bagi peneliti.

Konsep ITAF

ISACA merupakan organisasi internasional yang bergerak dalam jasa IT Governance yang didirikan tahun 1969. ISACA merupakan sponsor utama konferensi internasional bidang IT Governance, penerbit System Control Journal, pengembang utama standar audit dan pengendalian sistem serta merupakan administrator CISA (Certified Information System Auditor). Pada tahun 2008 ISACA mengeluarkan produk berupa Information Technology Assurance Framework (ITAF), sebuah sumber pembelajaran bagi para profesional yang bergerak dalam jasa assurance. ITAF merupakan produk dari Information System Audit and Control Association(ISACA) yang menyediakan sebuah kerangka tunggal yang berisi standar, pedoman (Guidelines) dan teknik dalam melaksanakan audit dan assurance termasuk di dalamnya perencanaan, lingkup audit, pelaksanaan dan pelaporan audit dan jasa assurance TI.



Gambar 1 pembagian ruang likgkup kerja ITAF

ITAF terbagi menjadi tiga bagian seperti terlihat dalam gambar yaitu:

1) Standar dikelompokkan menjadi standar umum, standar kinerja dan standar pelaporan. Standar digambarkan di gambar 1 dengan warna putih, artinya standar tersebut harus

dilaksanakan(mandatory), bila ada penyimpangan atas standar harus diungkapkan penyebab dan konsekuensinya terhadap pelaksanaan audit. Standar didesain bersifat keharusan (mandatory) untuk setiap kasus penugasan. Setiap penyimpangan dari standar dalam penugasan audit atau assurance harus diungkapkan dalam laporan audit. Standar audit TI mengadopsi standar audit umum terdiri dari atandar umum, standar pelaksanaan dan standar pelaporan. Isi dan substansinya relatif sama dengan standar audit keuangan. 2)Pedoman dikelompokkan menjadi empat bagian dan digambarkan dengan warna abu-abu. Ini berarti pedoman tersebut tidak bersifat mandatory atau tidak bersifat keharusan, namun sangat direkomendasikan penggunaannya. Auditor harus mampu membuktikan adanya penyimpangan TI dengan metode pengumpulan bukti menurut pedoman ini. Meski tidak seluruh pedoman dapat diterapkan untuk seluruh situasi, namun pedoman tersebut tetap patut menjadi bahan pertimbangan auditor dalam melaksanakan audit. Pedoman audit berisi informasi dan petunjuk mengenai area audit. Sejalan dengan tiga kategori standar di atas, pedoman ini berfokus terhadap berbagai pendekatan audit, metode audit, alat dan teknik audit dan materi lain untuk membantu dalam perencanaan, pelaksanaan, penilaian dan pelaporan audit. Pedoman tersebut juga membantu menjernihkan hubungan antara kegiatan perusahaan dan kegiatan penugasan audit oleh auditor (ITAF's summary, 2009). Pedoman audit ini tidak bersifat keharusan, namun sangat direkomendasikan penggunaannya. Auditor harus mampu membuktikan adanya penyimpangan TI dengan metode pengumpulan bukti menurut pedoman ini. Meski tidak seluruh pedoman dapat diterapkan untuk seluruh situasi, namun pedoman tersebut tetap patut menjadi bahan pertimbangan auditor dalam melaksanakan audit

3) Alat dan Teknik Audit, menyediakan infromasi spesifik mengenai metode, alat dan template dan juga menyediakan petunjuk penerapan dalam aktivitas audit. Khusus untuk alat dan teknik audit SI ini, bentuk dari kerangka ITAF berasal dari dokumen lain publikasi ISACA baik berupa buku, jurnal, petunjuk teknis dan sebagainya. Alat dan teknik dari ITAF ini digambarkan abu-abu kehitaman artinya penggunaannya bersifat fleksibel, dapat digunakan atau tidak oleh auditor sesuai kondisi lapangan. Sedangkan alat dan teknik audit berisi informasi dan bahan pelengkap yang mendukung pedoman audit TI. Dalam beberapa kasus, teknik audit berisi prosedur alternatif yang dapat diterapkan dalam penugasan audit. Auditor hanya mengadopsi alat dan teknik tersebut bila sesuai dengan kondisi, relevan dengan tujuan

dan tidak memberikan informasi yang bias. Sampai dengan saat ini sudah terdapat 11 prosedur audit TI yang dipublikasikan ISACA. Prosedur-prosedur tersebut dipublikasikan secara terpisah dari ITAF, namun menjadi bagian dari kerangka ITAF yang dapat dipedomani dalam melaksanakan kegiatan audit.

Hasil dari pengujian tersebut kemudian dievaluasi untuk disusun dalam laporan hasil pemeriksaan.

4. Reporting

Seluruh tahapan yang telah dilakukan sebelumnya dalam proses audit teknologi informasi kemudian didokumentasikan dalam suatu laporan hasil pemeriksaan/audit.

5. Follow-up

Hasil dari laporan hasil pemeriksaan/audit kemudian ditindaklanjuti sebagai acuan para pemegang kebijakan di setiap tingkatan manajemen organisasi dalam menentukan arah pengembangan dari penerapan teknologi informasi di organisasi tersebut.

Risiko-risiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain :

- Biaya pengembangan sistem melampaui anggaran yang ditetapkan.
- Sistem tidak dapat diimplementasikan sesuai dengan jadwal yang ditetapkan.
- Sistem yang telah dibangun tidak memenuhi kebutuhan pengguna.
- Sistem yang dibangun tidak memberikan dampak effisiensi dan nilai ekonomis terhadap jalannya operasi institusi, baik pada masa sekarang maupun masa datang.
- Sistem yang berjalan tidak menaati perjanjian dengan pihak ketiga atau memenuhi aturan yang berlaku.

Dengan memperhatikan tahapann process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat
boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit [erorangan dalam bentuk resume note (tidak presentasi)

IT AUDIT

Information Technology audit (IT audit) adalah pemeriksaan akan pengendalian yang ada pada infrastruktur tekonologi informasi. Proses tersebut meliputi mendapatkan dan mengevaluasibukti-buktisisteminformasi, praktik, dan operasi perusahaan. Evaluasi yang dilakukan harus dapat memberikan keyakinan bahwa asset perusahaan terjaga, begitu pula integritas data, serta operasi perusahaan dapat berjalan secara efektif dan efisien untuk memenuhi tujuan perusahaan. IT audit dapat dilakukan secara gabungan antara audit atas laporan keuangan dan audit internal. Saat ini, IT audit juga dikenal dengan sebutan Electronic Data Processing audit (EDP audit). Secara garis besar, tujuan IT audit adalah:
1. Availability Yaitu ketersediaan informasi, apakah system informasi pada perusahaan dapat menjamin ketersediaan informasi dapat dengan mudah tersedia setiap saat.
2. Confidentiality Yaitu kerahasiaan informasi, apakah informasi yang dihasilkan oleh system informasi perusahaan hanya dapat diakses oleh pihak -pihak yang berhak dan memiliki otorisasi.
3. Integrity Yaitu apakah informasi yang tersedia akurat, handal, dan tepat waktu.
IT audit memliki focus pada pengidentifikasian resiko yang terkait pada asset informasi perusahaan dan menentukan pengendalian yang tepat untuk mengurangi (bukan menghilangkan sepenuhnya) resiko tersebut Sedangkan dalam bukunya, Mulen menjelaskan peran internal auditor dalam proses IT audit mencakup 4 bidang utama yaitu:
1. Membantu staf audit financial
2. Mengaudit bidang –bidang lingkungan pengolahan data
3.Mengaudit program -program system aplikasi computer
4.Mereview pengembangan system Karenafokus IT audit adalah pada penentuan resiko beserta pengendaliannya, tentu saja internal audit juga berperan dalam mengidentifikasi resiko-resiko yang ada beserta pengendalian yang relevan untuk meminimalisasikan resiko – resiko tersebut.

Enam komponen Audit TI :

1. Pendefinisian tujuan perusahaan;
2. Penentuan isu, tujuan dan perspektif bisnis antara penanggung jawab bagian dengan bagian TI;
3. review terhadap pengorganisasian bagian TI yang meliputi perencanaan proyek, status dan prioritasnya, staffing levels, belanja TI dan IT change process management;
4. assessment infrastruktur teknologi, assessment aplikasi bisnis;
5. temuan-temuan,
6. laporanrekomendasi.

Sedang subyek yang perlu diaudit mencakup :

1. Aspek keamanan, Masalah keamanan mencakup tidak hanya keamanan file servers dan penerapan metoda cadangan, melainkan juga penerapan standar tertentu, seperti C-ICT.
2. keandalan, Keandalan meliputi penerapan RAID V disk subsystems untuk server dengan critical applications dan prosedur penyimpanan data di file server, bukan di drive lokal C.
3. Kinerja Kinerja mencakup persoalan standarisasi PC, penggunaan LAN serta cadangan yang sesuai dengan beban kerja.
4. Manage ability

manage ability menyangkut penerapan standar tertentu dan pendokumentasian secara teratur dan berkesinambungan. Pengorganisasian bagian TI juga ditetapkan dalam audit assessment. Ini terbagi atas IT management, IT support dan IT staffing. Untuk pertamakalinya diperkenalkan visi jangka panjang mengenai IT management yang merujuk pada tujuan bisnis perusahaan. Ini didukung visi business support yang jelas dan orientasinya dipersiapkan untuk penerapan ERP (enterprise resource planning) sebagai infrastrukturnya. Selain itu, tanggung jawab dibebankan pada setiap karyawan pengguna, sedang manajemen TI lebih bertanggung jawab dalam mendukung dan memecahkan masalah yang muncul.

Audit itu harus dilakukan terhadap :

1. System informasi secara keseluruhan
2. perangkat TI yang digunakan
3. software, hardware, jaringan saja
4. aspek yang terliba tdan relevan dalam sistem informasi.

TUGAS INDIVIDU 1 IT AUDIT

Istiana Ruswita (192420032)
MTI AR1

Perintah :

Dengan memperhatikan tahapan process IT Audit, silahkan lihat slide yang saya share dengan link, identifikasi komponen apa saja yang terlibat boleh dikerjakan perkelompok, tetapi masing masing anggota harus ada point sendiri disubmit perorangan dalam bentuk resume note (tidak presentasi).

6 (enam) Tahapan IT Audit sebagai berikut :

1. Information Gathering

   Auditor mengumpulkan informasi yang dibutuhkan dengan meminta dokumen-dokumen yang dibutuhkan untuk proses audit. Auditor membuat checklist dokumen apa saja yang dibutuhkan untuk diinformasikan kepada klien. Misalnya : Dokumen audit sebelumnya.

2. Review prior audit issues

   Auditor memeriksa informasi dari dokumen yang diperoleh dan meninjau masalah audit yang ada sebelumnya dan merencanakan bagaimana proses audit akan dilakukan. Workshop akan dilakukan oleh tim audit dan auditor untuk mengidentifikasikan kemungkinan masalah yang akan muncul selama proses audit dilaksanakan.

3. Risk assessment

   Melakukan pertemuan dengan klien yaitu para manajemen senior dan staff dan pihak yang terkait dan terlibat , untuk membahas lingkup audit yang akan dilakukan, lama waktu pelaksanaan audit dan masalah lain yang perlu dibahas, dikarenakan organisasi tersebut dapat menerima atau tidak nya resiko yang mungkin akan terjadi.

4. Develop IT audit

   Setelah dilakukan rapat tersebut, auditor mulai merealisasikan rencana audit, kerja lapangan mulai dilaksanakan dengan berkomunikasi dengan anggota staf dan meninjau prosedur dan proses audit. Auditor akan menguji kelayakan dan kepatuhan dari staf

tersebut sudah memenuhi standar yang telah ditetapkan atau tidak . auditor juga memberikan kesempatan kepada klien untuk memberikan feedback kepada auditor.

5. Execute IT audit Plan

   Auditor menyiapkan laporan audit yang berisi rincian temuan-temuan masalah audit yang muncul selama proses audit dilaksanakan. Laporan tersebut lalu dirangkum baik berupa kesalahan matematis, teknis, material, dan non material, pembayaran yang tidak pada otoritasnya, standar keamanan it yang telah diterapkan dan laporan yang terkait lainya. Lalu memberikan solusi kepada klien tersebut apa saja yang akan dilakukan dan merekomendasikan kepada klien

6. Customer satisfaction Evaluation

   Tahap terakhir ini auditor meminta tanggapan dan persetujuan dari klien terkait masalah dan temuan dalam laporan audit dan menjelaskan secara terperinci rencana manajemen dalam mengatasi masalah dan temuan tersebut. Apabila terdapat masalah lain mereka akan langsung menyelesaikan dan mencari solusinya pada rapat penutupan.

Nama	: A.Firdaus	Nama	: Istiqomah Febrianty
Nim	: 192420043	Nim	: 192420042
Kelas	: MTI R2	Kelas	: MTI R2

Tugas II (Berkelompok)

Komponen Yang ada Pada IT Audit

a. Pendahuluan

Penerapan TIK diperusahan seiring berjalannya waktu akan banyak mengalami perubahan, karena perkembangan teknologi informasi berkembang begitu cepat. Dalam mendukung aktivitas sebuah organisasi, informasi menjadi bagian yang sangat penting, baik untuk perkembangan organisasi maupun membaca persaingan pasar dan selanjutnya dapat digunakan untuk mengambil langkah strategis dengan tujuan memenangkan persaingan. Sistem Informasi digunakan di segala bidang dalam perusahaan untuk melakukan pemprosesan data menjadi suatu informasi, dan ini merupakan sebuah kegiatan dalam organisasi yang bersifat repetitive, dan agar menghasilkan kualitas informasi yang bermutu, maka harus dilaksanakan secara sistematis dan otomatis. Dengan demikian, sangat diperlukan adanya pengelolaan yang baik dalam sistem yang mendukung proses pengolahan data tersebut. Dalam sebuah organisasi tata kelola sistem dilakukan dengan melakukan audit

b. Kebutuhan IT Audit

1. Data Integritas
   Integritas data adalah menjamin konsistensi data terhadap semua konstrain yang diberlakukan terhadap data tersebut, sehingga memberikan jaminan keabsahan data itu sendiri.
2. Keamanan Aset
   Mengidentifikasi aset-aset apa yang perlu dilindungi pada perusahaan
3. Penggunaan Sumber Daya Yang Efektif dan Efesiensi
   Pemanfaatan sumber daya yang effektif untuk menekan dan memaksimalkan kebutuhan
4. Capaian Tujuan Perusahaan
   Merupakan sasaran dari tujuan pendiri perusahaan

c. Dasar Dalam Mengaudit

Ada beberapa komponen pengetahuan dalam IT Audit antara lain :

1. Perilaku Informasi
2. Sistem Informasi Manajemen
3. Perilaku Organisasi
4. Proses Audit (auditing)

d. Standar yang harus dimiliki IT Audit
   Ada beberapa komponen standar yang harus dimiliki oleh auditor antara lain :
   1. Sertifikasi Audit
   2. Prosedur Audit
   3. Framework Audit
   4. Tools Audit
   5. Projek Manajemen

e. Metode IT Audit
   Metode2 yang digunakan dalam IT Audit :
   1. Audit Through The Computer
      dalah Audit yang berbasis komputer dimana dalam pendekatan ini auditor melakukan pemeriksaan langsung terhadap program-program dan file-file komputer pada audit sistem informasi berbasis komputer
   2. Audit With Computer
      Adalah suatu pendekatan yang langsung berhubungan dengan perangkat yg berhubungan dengan komputer
   3. Audit Arround Computer
      adalah suatu pendekatan audit yang berkaitan dengan komputer, lebih tepatnya pendekatan audit disekitar komputer.

f. Salah satu point atau komponen IT Audit adalah IT Risk Management

IT risk management (manajemen resiko teknologi informasi) adalah proses yang dilakukan oleh para manajer IT untuk menyeimbangkan kegiatan operasional dan pengeluaran *cost* dalam mencapai keuntungan dengan melindungi sistem IT dan data yang medukung misi organisasinya. Sangatlah penting untuk dilakukan evaluasi melalui sistem Internal Audit.

Fungsi Manajemen Risiko dan Internal Audit

Fungsi manajemen risiko bertugas untuk mengarahkan praktik *enterprise risk management* pada organisasi, terutama untuk menghadapi risiko-risiko utama yang dapat mengganggu pencapaian sasaran organisasi. Di sisi lain, fungsi internal audit bertugas untuk memonitor, memantau, dan menilai efektivitas pengendalian internal dan manajemen risiko.

Peran Internal Audit terkait Manajemen Risiko

Institute of Internal Auditors (IIA), menjelaskan kegiatan internal audit sebagai kegiatan independen yang mendukung pencapaian sasaran organisasi, dan aktivitas konsultasi yang dirancang untuk memberikan nilai tambah dan memperbaiki operasi organisasi. Aktivitas ini membantu organisasi untuk mencapai tujuannya dengan membawa pendekatan sistematik dan disiplin untuk mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses *governance*. Tugas inti auditor internal berkaitan dengan manajemen risiko adalah untuk memberikan kepastian bahwa kegiatan manajemen risiko telah berjalan dengan efektif dalam memberikan

jaminan yang wajar terhadap pencapaian sasaran organisasi. Dua cara penting untuk menjalankan tugasnya adalah dengan:

1. memastikan bahwa risiko utama dari bisnis telah ditangani dengan baik; dan
2. memastikan bahwa kegiatan manajemen risiko dan pengendalian internal telah berjalan dengan efektif.

Kolaborasi Fungsi Manajemen Risiko dan Internal Audit

Terdapat beberapa alasan yang mendasari paradigma bahwa fungsi manajemen risiko sebaiknya berkolaborasi dengan fungsi internal audit. Berdasarkan *case study* yang dilakukan oleh RIMS dan IIA, alasan-alasan tersebut adalah

- Untuk menghubungkan rencana audit dan penilaian risiko perusahaan, serta berbagi produk kerja lainnya. Hal ini dibutuhkan untuk meningkatkan koordinasi dalam usaha menjamin bahwa risiko-risiko utama dapat ditangani dengan efektif.
- Berbagi sumber daya-sumber daya tertentu untuk mendukung efisiensi. Sumber daya yang dimaksud termasuk sumber daya keuangan, manusia, dan waktu.
- Saling meningkatkan kompetensi, peran, dan tanggung jawab setiap fungsi. Menyediakan infrastruktur komunikasi yang konsisten.
- Menilai dan memantau risiko strategis. Dapat membentuk pemahaman yang lebih mendalam dan treatment yang fokus untuk mengatasi risiko strategis. Berdasarkan pengalamannya, *Irene Corbe (Whirlpool Corp.)* menyatakan bahwa pengadaan pertemuan dengan divisi manajemen risiko dapat meningkatkan pemahaman fungsi audit internal terhadap profil risiko perusahaan.

Kolaborasi antara fungsi manajemen risiko dan internal audit merupakan sebuah inisiasi yang dapat mendatangkan manfaat pada berbagai jenis perusahaan. manfaat-manfaat yang dapat diperoleh dari kolaborasi tersebut berupa:

1. Memastikan bahwa risiko-risiko kritikal telah diidentifikasi secara efektif;
2. Penggunaan sumber daya langka dengan efisien;
3. Komunikasi yang dalam dan konsisten, terutama pada level Board dan manajemen;
4. Pengertian yang lebih dalam dan penanganan yang terfokus pada risiko yang paling signifikan terhadap pencapaian tujuan organisasi.

Komunikasi secara terbuka dan konsisten merupakan metode utama yang dapat diterapkan dalam kolaborasi kedua fungsi ini. Komunikasi dapat membangun pendalaman pandangan terhadap risiko-risiko yang melekat pada organisasi dan meningkatkan kapabilitas tiap divisi untuk mengelola risiko-risiko tersebut. Namun kolaborasi tersebut harus memiliki batasan yang jelas mengenai tanggung jawab dan peran setiap fungsinya. Kolaborasi yang dilakukan juga harus disesuaikan dengan karakteristik dan tujuan perusahaan.

Tugas IT Audit Components
Oleh : 1. Jepri Yandi (192420044)
2. Yudi Pranata (192420001)

Audit Sistem Informasi adalah proses pengumpulan dan pengevaluasian bukti-bukti untuk membuktikan dan menentukan apakah sistem aplikasi komputerisasi yang digunakan telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, apakah aset organisasi sudah dilindungi dengan baik dan tidak disalah gunakan, apakah mampu menjaga integritas data, kehandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer.Komponen risiko audit, pada umumya terdiri atas tiga, yaitu:

1. Risiko bawaan (inherent risk)
2. Risiko pengendalian (control risk)
3. Risiko deteksi (detection risk)

Tujuan Audit Sistem Informasi menurut Ron Weber yaitu:

1) Meningkatkan keamanan aset-aset perusahaan.
2) Meningkatkan data dan menjaga integritasi data.
3) Meningkatkan efektifitas sistem
4) Meningkatkan efisiensi sistem
5) Ekonomis

Dua aspek utama tujuan audit sistem informasi yaitu:

1) Conformance (Kesesuaian)

   Yaitu audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian seperti kerahasiaan, Integritas, Ketersediaan, Kepatuhan.
2) Performance (Kinerja)
   Yaitu audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kenerja seperti Efektifitas, Efisiensi, Kehandalan.

Tujuan audit sistem informasi secara teknis yaitu:

1) Evaluasi atas kesesuaian antara rencana strategis dengan rencana tahunan organisasi,rencana tahunan dan rencana proyek.
2) Evaluasi atas kelayakan struktur organisasi yaitu termasuk pemisahan fungsi dan kelayakan pelimpahan wewennang dan otoritas.
3) Evaluasi atas pengelolahan personil yaitu termasuk perencanaan kebutuhan, rekrutmen dan seleksi, pelatihan dan pendidikan, promosi,mutasi, serta terminasi personil.
4) Evaluasi atas pengembangan yaitu termasuk analisis kebutuhan, perancangan, pengembangan, pengujian, implementasi, migrasi, pelatihan dan dokumentasi, serta manajemen perubahan.
5) Evaluasi atas kegiatan operasional yaitu termasuk pengelolaan keamanan dan kenerja pengelolaan pusat data, pengelolaan keamanan dan kenerja jaringan data, pengelolaan masalah dan insiden serta dukungan pengguna

Tugas IT Audit Components
Oleh : 1. Jepri Yandi (192420044)
2. Yudi Pranata (192420001)

6) Evaluasi atas kontinuitas layanan yaitu termasuk pengelolaan backup dan recovery, pengelolaan prosedure darurat, pengelolaan rencana pemulihan layanan, serta pengujian rencana kontijensi operasional.
7) Evaluasi atas kualitas pengendalian aplikasi yaitu termasuk pengendalian input, pengendalian proses dan pengendalian output.
8) Evaluasi atas kualitas data/informasi yaitu termasuk pengujian atas kelengkapan dan akurasi data yang dimasukkan, diproses, dan dihasilkan oleh sistem informasi.

Komponen risiko audit, pada umumya terdiri atas tiga, yaitu:

1. Risiko bawaan (inherent risk) Risiko bawaan adalah kerentanan suatu asersi terhadap salah saji material dengan asumsi tidak ada kebijakan dan prosedur struktur pengendalian intern yang terkait. Risiko bawaan selalu ada dan tidak pernah mencapai angka nol.
2. Risiko pengendalian (control risk) Risiko pengendalian adalah risiko bahwa suatu salah saji material, yang dapat terjadi dalam suatu asersi, tidak dapat dideteksi ataupun dicegah secara tepat pada waktunya oleh berbagai kebijakan dan prosedur struktur pengendalian intern perusahaan.
3. Risiko deteksi (detection risk) Risiko deteksi merupakan risiko bahwa auditor tidak dapat mendeteksi salah saji material yang terdapat dalam suatu asersi.

Nama : M danial sentosa
Nim : 192420040
MTI A R2

komponen Audit TI :
1. Pendefinisian tujuan perusahaan;
2. Penentuan isu, tujuan dan perspektif bisnis antara penanggung jawab bagian dengan bagian TI;
3. review terhadap pengorganisasian bagian TI yang meliputi perencanaan proyek, status dan prioritasnya, staffing levels, belanja TI dan IT change process management;
4. assessment infrastruktur teknologi, assessment aplikasi bisnis;
5. temuan-temuan,
6. laporanrekomendasi.

Unsur-unsur utama audit TI secara luas diklasifikasikan sebagai berikut

1. Physical and environmental review – Meliputi keamanan fisik, pasokan energi, AC, kontrol kelembaban dan faktor lingkungan lainnya.

2. System administration review – Meliputi ulasan keamanan sistem operasi, sistem manajemen database, semua prosedur administrasi sistem dan kepatuhan.

3. Application software review – Aplikasi bisnis dapat berupa penggajian, faktur, sistem pemrosesan order pelanggan berbasis web atau sistem perencanaan sumber daya perusahaan. Ulasan perangkat lunak aplikasi meliputi kontrol akses dan otorisasi, validasi, penanganan kesalahan dan eksepsi, alur proses bisnis dalam aplikasi perangkat lunak dan kontrol manual komplementer dan prosedur. Selain itu, review dari siklus hidup pengembangan sistem harus diselesaikan.

4. Network security review – Ulasan mengenai koneksi internal dan eksternal ke sistem, perimeter keamanan, ulasan firewall, daftar router akses kontrol, port scanning dan deteksi intrusi merupakan beberapa daerah khas cakupan.

5. Business continuity review – Meliputi keberadaan dan pemeliharaan toleransi kesalahan dan pemakaian hardware berlebihan, prosedur backup dan penyimpanan, dan dokumentasi dan pengujian pemulihan bencana/rencana kesinambungan bisnis.

6. Data integrity review – Tujuan dari hal ini adalah pengawasan data untuk memverifikasi kecukupan pengendalian dan dampak kelemahan. Pengujian substantif tersebut dapat dilakukan dengan menggunakan perangkat lunak audit umum (misalnya, komputer dengan bantuan teknik audit).

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045

KOMPONEN AUDIT IT

Menetapkan ruang lingkup audit IT

Prasyarat utama untuk program audit organisasi adalah menentukan jenis audit apa yang diperlukan dan mengidentifikasi apa yang harus atau bisa diaudit. Potensi audit yg di kembangkan oleh inventaris disebut dengan Ruang Lingkup. manajemen aset, arsitektur perusahaan, kerangka tata kelola, atau pendekatan lain apa pun yang membantu mengidentifikasi elemen-elemen penyusun organisasi. Organisasi kemudian melakukan penilaian risiko pada setiap item yang termasuk dalam ruang lingkup audit untuk memberikan prioritas pada subyek audit, Dengan mempertimbangkan faktor-faktor untuk setiap item seperti, besarnya relatif risiko pentingnya bagi organisasi, atau potensi manfaat bagi organisasi dari melakukan audit. Prioritasi mencerminkan efisiensi sumber daya organisasi yang tersedia untuk mendukung audit, Aspek organisasi dapat di audit secara memadai Tata kelola formal dan manajemen resiko, kedua domain organisasi ini menekankan identifikasi dan penilaian asset sebagai dasar untuk menyusun kegiatan manajemen dan mengalokasikan sumber daya organisasi, sumber daya kontrol lainnya pada area organisasi yang terkait dengan sumber risiko terbesar.

Mengembangkan dan mempertahankan ruang lingkup audit

Audit di setiap organisasi biasanya mencerminkan cara organisasi itu sendiri terstruktur dan dikelola. Semesta audit dapat diatur atau dikategorikan berdasarkan hierarki unit bisnis, arsitektur perusahaan, model proses bisnis, kerangka kerja tata kelola, katalog layanan, atau dekomposisi fungsional lainnya yang paling sesuai dengan cara organisasi memandang operasi dan aset mereka. ada beberapa level kontrol atau tingkat entitas umum yang menyeluruh yang dapat diaudit. audit kontrol tingkat entitas sering kali memerlukan beberapa pendekatan audit karena biasanya mencakup berbagai jenis kontrol internal. Ruang lingkup audit ini penerapannya di semua tingkat organisasi juga berarti bahwa laporan audit tingkat entitas memiliki khalayak yang lebih luas daripada yang dihasilkan dalam jenis audit lainnya. Auditor yang melakukan audit pada level apa pun di bawah seluruh organisasi perlu memastikan bahwa ruang lingkup audit mereka mencakup level entitas dan kontrol bersama lainnya, serta yang diterapkan secara khusus untuk komponen yang diperiksa oleh audit.

Unsur-unsur organisasi yang biasanya dimasukkan dalam ruang lingkup meliputi:

- unit struktur organisasi seperti unit bisnis, divisi operasi, fasilitas, atau anak perusahaan
- struktur akuntansi seperti pusat biaya, lini bisnis, atau area proses
- sasaran, sasaran, dan hasil strategis, yang dievaluasi sebagian dengan mengaudit sumber daya yang dialokasikan untuk pencapaiannya;
- misi dan proses bisnis, layanan, dan fungsi operasional yang dijalankan oleh organisasi

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045

- aset termasuk aset TI organisasi memiliki, mengoperasikan, mengelola, atau mengendalikan;
- program, proyek, dan investasi di mana organisasi melakukan pendanaan atau sumber daya lainnya;
- kontrol internal dan eksternal yang dilaksanakan oleh organisasi atau atas namanya;
- fungsi atau program manajemen seperti tata kelola, manajemen risiko, jaminan kualitas, sertifikasi, dan kepatuhan serta audit internal.

Penggerak tata kelola, risiko, dan kepatuhan

organisasi menetapkan dan memelihara program di bidang ini, kebutuhan untuk menilai efektivitasnya dan mengukur pencapaian tujuan program mempengaruhi ruang lingkup dan frekuensi audit TI dan prosedur, standar, dan kriteria yang digunakan dalam audit TI internal.
Meskipun kerangka kerja dan tata kelola manajemen risiko jarang menentukan elemen yang cukup, untuk menyediakan inventaris subjek potensial audit, mereka menawarkan fondasi yang kuat, khususnya untuk komponen dan kontrol terkait-TI di dunia audit.
Program kepatuhan memiliki pengaruh, di mana kebutuhan untuk memenuhi tujuan atau persyaratan kepatuhan, adalah faktor utama dalam penentuan prioritas dan kriteria yang digunakan sebagai dasar untuk menunjukkan kepatuhan menetapkan ruang lingkup minimum untuk audit dilakukan untuk mendukung kepatuhan.
Misalnya, versi yang dipakai secara luas 4.1 dari tujuan pengendalian untuk informasi dan teknologi (COBIT) mencakup 34 proses dalam 4 domain tata kelola utama dan mendefinisikan lebih dari 200 tujuan pengendalian yang terkait dengan proses tersebut. COBIT 5 memperluas proses model referensi ke 37 proses di antara 5 domain, menggantikan tujuan kontrol dengan tata kelola dan praktek manajemen yang disarankan dan kriteria audit pada tujuh faktor, mirip dengan kategori ruang lingkup audit : prinsip, kebijakan, dan kerangka kerja, struktur organisasi; Kebudayaan, etika, dan perilaku. Informasi; Layanan, infrastruktur, dan aplikasi.
Enterprise risk management menggunakan ruang lingkup audit development dan IT untuk mengaudit ruang lingkup dengan memberikan identifikasi aset organisasi yang berisiko dan menetapkan jenis risiko-risiko yang berlaku pada komponen atau aspek operasional organisasi. Sementara risiko yang terkait dengan mata pelajaran audit yang berbeda membantu meningkatkan sumber daya yang seharusnya, mempertimbangkan semua jenis risiko yang ada dan dapat memengaruhi cakupan audit.

Strategi dan prioritas audit

Pada bab 3 sudah dijelaskan pentingnya strategi audit terhadap sebuah organisasi dan program audit internalnya. Strategi audit adalah sebuah kunci utama yang menentukan jenis, lingkup, dan frekuensi audit sebuah organisasi memimpin dan mendefinisikan kriteria yang digunakan oleh organisasi untuk memprioritaskan materi di alam semesta audit. Organisasi mengikuti prosedur dalam strategi audit untuk membentuk prioritas audit dan menggunakan determinasi untuk

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
pengalokasikan sumber-sumber audit internal. Rencana pada audit yang terkait untuk menguraikan sumber-sumber yang harus dialokasikan untuk dapat menjawab persyaratan wajib dan tujuan serta persyaratan audit tambahan apa pun. Banyak suatu organisasi menetapkan peringkat prioritas tinggi untuk mengaudit kegiatan yang mendukung kepatuhan hukum atau peraturan, semacam laporan kontrol internal yang diwajibkan dari perusahaan yang diperdagangkan pada bawah pasal 404 dari undang-undang Sarbanes-Oxley [5]. Kegagalan untuk mematuhi persyaratan wajib adalah salah satu dari beberapa jenis risiko organisasi yang dihadapi yang dapat mengakibatkan dampak negatif yang diukur secara langsung dalam istilah keuangan atau tidak langsung dari kerusakan reputasi, publisitas negatif, sanksi hukuman, atau hasil potensial lainnya.

Jenis kontrol

Jenis kontrol adalah sebuah elemen yang berbeda-beda yang ada pada audit, operasi bisnis, aset-asetnya, dan sumber-sumber pendukung yang membentuk kemampuan fungsional suatu organisasi, sementara kontrol pada kemampuan-kemampuan tersebut mencakup struktur manajemen, proses dan protokol, serta langkah-langkah teknis yang menyediakan efisiensi dan keefektifan operasional, kepatuhan, keandalan, dan jaminan operasional. Seperangkat kontrol individu (baik secara internal maupun eksternal) dijalankan oleh sebuah organisasi bertentangan dengan proses pemerintahan pengendalian internal, yang ada untuk membantu organisasi mencapai tujuan manajemen yang berkaitan dengan strategi, operasi, suatu kepatuhan manajemen yang sah atau peraturan, kualitas, keamanan, atau manajemen risiko. Kontrol terutama kontrol internal adalah fokus dari banyak jenis audit, baik dilakukan oleh auditor internal ataupun eksternal. Satu jenis kontrol atau lebih biasanya berlaku untuk semua benda dalam ruang lingkup organisasi. Organisasi dan auditor perlu memiliki pemahaman yang luas tentang berbagai jenis kontrol dan penerapan tujuan dan fungsinya untuk dapat merencanakan dan melaksanakan sebuah audit dengan benar dari kontrol sebuah organisasi dan untuk menyelaraskan jenis kontrol yang digunakan dengan cara kompetensi, keterampilan, dan pengalaman sebelumnya kepada para auditor.

Kontrol Kategorisasi

Kontrol Kategorisasi adalah Kontrol yang luas dan memilih kontrol tersebut dari susunan kontrol yang sama luas atau lebih luas yang disusun untuk implementasi. Seperti halnya item-item dalam ruang lingkup audit dapat diatur atau dikategorikan dalam banyak cara, banyak pendekatan kategorisasi kontrol yang berbeda-beda digunakan dalam kerangka kerja yang tersedia, metodologi, dan panduan. Skema pengukuran umum untuk kontrol termasuk yang didasarkan pada tujuan, sasaran, fungsi, sifat implementasi, dan tingkat penerapan dalam organisasi. Tabel 6.1 memberikan sebuah daftar pendekatan kategorisasi kontrol yang representatif dengan menggunakan basis kategorisasi yang berbeda.

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
Kategorisasi kontrol terutama dimaksudkan untuk memperkenalkan konsisten dengan cara kontrol dirujuk dan diterapkan dalam konteks yang berbeda-beda dan untuk tujuan berbeda. Seperti yang ditunjukkan oleh Tabel 6.1, tidak ada standar tunggal yang dapat diterima untuk mengkategorikan kontrol, sehingga organisasi dapat memilih atau mengadaptasi pendekatan yang ditentukan dalam susunan kerangka kerja atau metodologi eksternal, mengembangkan kategorisasi mereka sendiri, atau mengikuti standar yang ditetapkan dalam aturan hukum, peraturan, atau kebijakan sebuah organisasi. harus memuaskan. Peraturan keamanan yang diundangkan di bawah Undang-undang Portabilitas dan Akuntabilitas Asuransi Kesehatan tahun 1996 (dikenal secara kolektif sebagai Peraturan Keamanan HIPAA) misalnya, memisahkan persyaratan menjadi pengamanan administratif, teknis, dan fisik, sehingga organisasi yang dicakup oleh hukum mungkin menemukan bahwa menggunakan kategorisasi yang sama pendekatan untuk kontrol internal memfasilitasi kepatuhan.
Tabel 6.1

Basis	Kategorisasi Representatif
Tujuan kontrol	Pencegahan, detektif, korektif
Kontrol objektif	Operasi, pelaporan, kepatuhan Tata kelola, manajemen risiko, kepatuhan
Fungsi kontrol	Administratif, teknis, fisik Manajemen, operasional, teknis
Sifat implementasi	Terpusat, dibagikan, didesentralisasi
Tingkat penerapan	Organisasi, divisi, unit bisnis, fungsi Program, proyek, sistem, komponen

Kontrol Organisasi

Kontrol organisasi adalah control yang ditingkat entitas penting sebagai area fokus untuk audit internal dan eksternal karena mereka memberikan dasar untuk bagaimana organisasi mengelola fungsi yang didukung oleh sebuah kontrol. Kontrol pada level entitas juga disertakan dengan referensi ke dalam banyak jenis audit dilakukan di tingkat organisasi lainnya, sebagai unit bisnis, program dan proyek, dan aset teknologi semuanya yang memanfaatkan jenis-jenis kontrol tingkat entitas. Gambar 6.2 menunjukkan berbagai kategori utama dari entitas level dan jenis kontrol dalam setiap kategori Itu mungkin diterapkan dan akan tunduk pada audit dalam organisasi yang berbeda.

Audit dari kontrol tingkat entitas berbeda pada tingkat tertentu dari pemeriksaan yang difokuskan pada unsur-unsur yang sempit di dalam organisasi. Efektivitas kontrol tingkat entitas sebagian bergantung pada sejauh mana organisasi yang membentuk otoritas kontrol dan menerapkan setiap kontrol dengan cara yang meliputi seluruh organisasi. Dari perspektif ini, audit dari

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
kontrol tingkat entitas pada dasarnya memeriksa kemampuan manajemen dan tata kelola organisasi, termasuk struktur organisasi, penyelarasan bisnis dan tujuannya, keberadaan serta penggunaan kegiatan perencanaan strategis dan operasional. Unsur-unsur pada kontrol ini membantu memastikan bahwa control yang di tentukan organisasi kebijakan sebenarnya diimplementasikan dan digunakan untuk mendukung pencapaian tujuan kontrol organisasi. Tata kelola terkemuka dan kerangka manajemen risiko menekankan bahwa pentingnya menetapkan kontrol tingkat entitas dan tampaknya mengasumsikan bahwa hampir semua organisasi mengenali nilai dari menerapkan jenis-jenis pada kontrol ini [2,8,9]. Asumsi seperti itu sebagian berasal dari proporsi besar perusahaan atau organisasi yang saling tukar di industri atau lingkungan operasi yang diatur untuk membentuk sebuah audit yang diinginkan tentang tata kelola, manajemen risiko, kepatuhan, dan audit.

Mengaudit aset yang berbeda

Auditing aset yang berbeda adalah untuk melakukan pengecekan asset dan kontrol teknis yang terkait, baik sebagai focus utama dalam audit sentris atau dalam konteks seperti fungsi manajemen audit dan proses bisnis yang didukung oleh aset-asetnya.
Untuk melakukan pengecekan asset-aset para auditor yang bertugas perlu untuk memilih prosedur audit yang tepat, sesuai dengan jenis audit yang akan diadakan dan membutuhkan pemahaman cukup tentang konteks asset yang dipakai sebagai bukti yang relevan untuk mendukung temuan audit. Auditors memeriksa beberapa komponen-komponen dalam ruang lingkup sebuah audit tunggal yang memiliki kriteria dan prosedur audit dengan kebutuhan dengan pendekatan konsisten untuk mengumpulkan dan menganalisis sebuah informasi serta melaporkan temuan audit. Di sebagian besar aset TI, ada bidang-bidang umum atau prosedur audit yang dapat membantu menyediakan konsistensi ini, seperti yang dirangkum pada tabel 6.2. Secara kolektif, prosedur-prosedur ini menyoroti penggunaan terpadu dari dokumentasi, penyelidikan, pengamatan, dan uji coba langsung untuk menyediakan bukti yang diperlukan untuk mendukung temuan audit.

Fokus Audit TI	Audit Prosedur
Configuration	Memindai atau menganalisis konfigurasi aset dan membandingkan konfigurasi aktual dengan kebijakan, baseline, dan standar yang disetujui
Logging and monitoring	Konfirmasi logging diaktifkan pada tingkat detail yang sesuai dan output log dipantau dan ditinjau atau dianalisis secara teratur

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045

Access control	Tinjau kebijakan, prosedur, dan mekanisme untuk mengontrol akses ke subjek audit, termasuk pemberian dan pencabutan hak akses dan otentikasi dan otorisasi akses

Dekomposisi Komponen IT

Dekomposisi Komponen IT adalah komponen yang di gunakan untuk kinerja audit untuk lebih efisien dan membantu menentukan ruang lingkup yang lebih akurat untuk menyelesaikan proses audit. menentukan lingkup audit, seperangkat keterampilan dan kompetensi yang diperlukan oleh audit, dan tingkat sumber yang diperlukan untuk menyelesaikan proses audit. Sistem pengaudit ini mencerminkan jenis audit dan tujuannya dimaksudkan, komponen-komponennya akan diperiksa, dan prosedur, protokol, standar, atau auditor kriteria yang akan digunakan.
Tidak ada metode standar tunggal atau "terbaik" untuk mengevaluasi sistem lingkungan teknis. Salah satu caranya adalah menguraikan suatu sistem ke dalam bagian-bagian penyusunnya dan mengaudit setiap komponen secara individu, menerapkan protokol audit yang serupa di semua unsur utama, tetapi juga menggunakan prosedur atau daftar periksa yang spesifik dalam hal teknologi jika perlu
Kategori umum atau komponen yang mewakili bidang audit mencakup delapan unsur yang diperlihatkan pada Gambar 6.1. Beberapa contoh audit istimewa Pertimbangan juga berlaku pada jenis-jenis tertentu dari lingkungan operasi seperti komputasi awan atau penggunaan lainnya dari teknologi virtualisasi server, dan sistem atau akses aplikasi menggunakan peramban web, perangkat seluler, atau jenis aplikasi dan antarmuka klien lainnya. Bagian berikut menjelaskan secara singkat dan pertimbangan audit yang berlaku untuk berbagai komponen-komponennya.

Sistem dan aplikasi

Sistem dan aplikasi memiliki beragam karakteristik seperti arsitektur teknis, sistem operasi, bahasa pemrograman, titik-titik integrasi, dan fungsi yang diinginkan. Pilihan prosedur audit yang sesuai untuk sistem dan aplikasi tergantung pada arsitekturnya dan berbagai jenis komponen teknis yang digunakan untuk pemeriksaan setiap sistem atau subjek aplikasi. Auditor aplikasi sistem fokus pada kemampuan dan kontrol non-fungsional. Masalah fungsional mencakup memastikan bahwa apa yang organisasi lakukan untuk menjalankan fungsinya memenuhi persyaratan yang ditentukan. Aspek yang tidak fungsional mencakup kinerja, kegunaan, keandalan, dan keamanan, di mana para auditor sering menguji atau meninjau bukti yang memperlihatkan penerapan kontrol yang sesuai dengan penggunaan sistem atau penerapan yang diharapkan dan cara pengguna berinteraksi dengannya. Misalnya, audit aplikasi berbasis

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
web sering kali memeriksa penggunaan kendali terhadap kerentanan yang diketahui, kesalahan konfigurasi, dan pengungkapan informasi sensitif yang tidak sah.

Database

Istilah database umumnya berarti setiap kumpulan atau repositori informasi yang disimpan oleh suatu organisasi, tetapi dalam praktik paling sering menyiratkan jenis teknologi spesifik yang menyimpan dan menyediakan akses ke data dalam mendukung satu atau lebih aplikasi dan proses bisnis. Basis data mewakili sebuah jenis perangkat lunak aplikasi khusus, yang tunduk pada banyak prosedur audit dan kriteria pemeriksaan yang sama sebagai aplikasi dan sistem. Sifat dan kepekaan data yang disimpan dalam basis data organisasi mempengaruhi kriteria yang digunakan untuk mengaudit mereka, khususnya sehubungan dengan memeriksa kontrol keamanan atau privasi seperti enkripsi data, pengawasan akses, dan backup data serta pemulihan.

Sistem Operasi

Organisasi Modern sering menggunakan berbagai sistem operasi untuk mendukung berbagai kebutuhan sistem dan komputer, yang paling umum termasuk Microsoft Windows, berbagai versi Unix atau Linux, serta alternatif - dan platform-spesifik seperti z/OS untuk komputer mainframe IBM. Sistem operasi sangat dapat disesuaikan dan dapat diterapkan secara berbeda di seluruh organisasi atau dalam organisasi yang sama. Untuk meningkatkan ketahanan, administrasi, keamanan, dan dukungan, berbagai organisasi sering kali melakukan konfigurasi sistem operasi untuk server, komputer desktop dan laptop, dan perangkat seluler. Banyak pemasok sistem operasi menawarkan rekomendasi konfigurasi yang dimaksudkan untuk mengoptimalkan keamanan atau kesesuaian untuk penggunaan yang berbeda. Audits sistem operasi mengkonfirmasikan penggunaan dan konfigurasi yang sesuai dari sistem operasi pada platform komputasi yang berbeda yang diluncurkan dalam organisasi.

Perangkat Keras

Perangkat keras terdiri dari perangkat fisik yang digunakan untuk membangun jaringan, infrastruktur telekomunikasi, sistem komputer, pelanggan komputasi akhir, dan banyak komponen keamanan fisik. Dalam banyak penguraian arsitektur teknis, perangkat keras menghubungkan server, komputer desktop dan laptop, serta berbagai organisasi perangkat seluler yang digunakan serta router, switch, firewall, dan komponen-komponen lain yang digunakan dalam jaringan. Audit aset perangkat keras itu biasanya berfokus pada konfigurasi yang konsisten dan benar serta kepatuhan terhadap kebijakan dan standar internal. Dibandingkan dengan perangkat lunak, proporsi yang lebih besar dari suatu perangkat keras organisasi ini kemungkinan besar akan dibeli secara komersial, jadi auditor perangkat keras juga

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
mempertimbangkan vendor dan proses-proses internal yang digunakan untuk memperoleh perangkat keras.

Jaringan

Jaringan menyediakan konektivitas dan memungkinkan pertukaran komunikasi dan informasi untuk sebagian besar, jika bukan dari aset-aset organisasi IT. Jaringan meliputi aset-aset perangkat keras seperti router dan firewall yang memungkinkan aliran informasi antara komponen dan komunikasi dan kontrol keamanan yang melindungi kualitas layanan dalam komunikasi jaringan dan informasi rahasia, integritas, dan ketersediaan data melintasi infrastruktur jaringan. Audit jaringan memeriksa implementasi dan konfigurasi perangkat keras, layanan, dan protokol yang dijalankan pada jaringan tersebut, dan kontrol keamanan seperti firewall dan sistem deteksi jaringan. Audit ini juga mempertimbangkan sifat komunikasi di dalam jaringan sehingga auditor dapat memilih prosedur audit yang sesuai untuk menggunakan nirkabel, satelit, seluler dan teknologi jaringan lainnya. Prosedur audit khusus yang digunakan untuk memeriksa jaringan tergantung pada jenis perangkat keras, layanan, kontrol keamanan, dan infrastruktur telekomunikasi yang diterapkan oleh suatu organisasi dan pada skala jaringan dalam ukuran geografisnya serta jumlah dan berbagai sistem dan fasilitas yang terhubung dengannya. Sementara sebagian besar teknologi yang mendasarkannya sangat mirip terlepas dari skala jaringan, ada perbedaan praktis dalam mengaudit konvensional atau virtual jaringan area lokal yang digunakan dalam satu lokasi dengan jaringan luas area mencakup berbagai situs.

Tempat Penyimpanan

Meskipun organisasi menyimpan sejumlah besar data dalam basis data antarnegara, konten dan dokumen sistem manajemen, dan komponen-komponennya yang serupa, penggunaan teknologi penyimpanan yang mutakhir membuat tempat, jaringan, dan infrastruktur merupakan bagian yang unik dari program ini yang digunakan pada audit. Solusi penyimpanan menggunakan perangkat keras, perangkat lunak, protokol komunikasi, dan metode penyimpanan data serta akses, meskipun bidang penekanannya untuk audit penyimpanan tumpang tindih secara substansial dengan bidang-bidang yang ada pada basis data. Prosedur Audit dan kriteria penyimpanan bergantung pada jenis spesifik teknologi penyimpanan yang digunakan suatu organisasi dan sifat serta kepekaan data yang ditampung di lingkungan penyimpanan. Penyimpanan dapat diaudit secara terpisah atau dalam teknologi operasional yang lebih luas seperti ini biasanya ditetapkan sebagai komponen pendukung dari pusat data atau lingkungan operasi teknis lainnya, di mana sebuah infrastruktur penyimpanan tunggal dapat menerima data dari berbagai sistem.

Pusat Data

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
Sebagai fasilitas yang digunakan sistem, perangkat keras, infrastruktur jaringan, dan teknologi terkait, pusat data menyediakan fondasi yang penting bagi cara kerjanya. Selain berfungsi sebagai lokasi fisik bagi banyak komponen teknologi, pusat data juga menjadi titik pelaksanaan bagi banyak proses, prosedur, dan fungsinya yang mendukung proses tersebut. Audit fasilitas pusat data berfokus pada kontrol jenis khusus ini dan proses dukungan operasional, sumber, dan personil yang memastikan bahwa komponen yang berasal di pusat data beroperasi secara normal untuk mendukung proses dan fungsi bisnis yang bergantung padanya. Apakah dimiliki dan dikelola oleh suatu organisasi atau pihak ketiga, pusat data sering dianggap penyedia jasa dan oleh karena itu digunakan pada standar eksplisit yang ditetapkan untuk audit organisasi layanan.

Lingkungan tervirtualisasi

Teknologi virtualisasi menyediakan sebuah pendekatan teknis alternatif untuk menyediakan infrastruktur, platform dan sistem operasi, server, perangkat lunak, serta sistem dan aplikasi. Kebanyakan lingkungan komputasi yang berkualitas memiliki banyak kesamaan dengan pusat data konvensional, Pendekatan ini meningkatkan pemanfaatan kapasitas dan di dalamnya layanan model berbasis cloud seperti komputasi cloud, memungkinkan organisasi untuk menggunakan sumber daya teknologi ini lebih efisien dengan naik atau turun sebagai surat perintah kebutuhan bisnis. Audit lingkungan komputasi berkualitas menggunakan banyak prosedur dan kriteria yang sama yang digunakan untuk audit pusat data, dengan penekanan tambahan pada server penyedia, deprovisioning, manajemen, pemeliharaan berbagai server virtual yang berbagi komputasi, jaringan, dan sumber daya infrastruktur.
Penggunaan komputasi cloud dan penyedia layanan pihak ketiga menjadi cukup umum sehingga para audits mungkin menanggapi layanan demikian yang berbeda dengan komponen audit lainnya. Perbedaan yang ditekankan oleh para penyedia layanan cloud antara lain penyedia layanan termasuk akses jaringan, akses sumber daya, sumber daya pooling, kemampuan dan jasa yang fleksibel, dan penggunaan yang bermebel serta model pembayaran dan pembayaran yang terkait. Pertumbuhan yang diharapkan dalam komputasi cloud adalah salah satu faktor yang mendorong kerangka kerja kontrol yang spesifik di awan, Kerangka kerja yang tersedia termasuk matriks kontrol awan yang dikembangkan oleh aliansi keamanan cloud dan risiko Federal dan Program manajemen wewenang yang dikelola oleh administrasi layanan umum untuk digunakan oleh penyedia layanan awan yang melayani instansi pemerintah as.

Antarmuka

interface adalah titik integrasi atau koneksi antara dua komponen atau lebih, yang memungkinkan transmisi informasi antara sistem atau mengekspos layanan atau kemampuan fungsional dari satu sistem atau aplikasi pada orang lain. Auditor sering kali menekankan langkah-langkah keamanan yang diimplementasikan untuk melindungi informasi dalam perjalanan melintasi antarmuka dan untuk mengendalikan akses ke antarmuka yang terpapar oleh setiap sistem. Audit antarmuka mengandalkan pada kedua dokumentasi seperti spesifikasi

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
antarmuka formal dan tes yang menunjukkan fungsi yang benar dari tiap antarmuka, mempertimbangkan tujuan yang dimaksudkan, aliran informasi, mekanisme akses teknis, dan proses oketifikasi dan otorisasi tingkat mesin.

Kontrol atau proses prosedural audit

Ruang lingkup audit teknologi informasi sangat luas dan beragam seperti yang dimiliki oleh organisasi sendiri, yang meliputi berbagai macam teknologi, kemampuan teknis, dan kontrol serta kebijakan, proses, dan prosedur yang berkaitan dengan fungsi operasional dan tata kelola. Bergantung pada jenis dan lingkup audit yang direncanakan oleh suatu organisasi, auditor bisa saja memeriksa basis proses atau kontrol prosedural yang berkaitan dengan asetnya dan komponen IT yang mendukung mereka, atau secara terpisah dengan audit yang spesifik dalam proses. Penekanan relatif yang menempatkan suatu organisasi pada audit proses-proses itu dipengaruhi hingga batas tertentu oleh tata kelola, risiko, kepatuhan, dan kerangka manajemen yang dipilih untuk dijalankan. Banyak jenis audit eksternal termasuk yang dimaksudkan untuk memperoleh sertifikasi atau menunjukkan keterlibatan peraturan yang mengharuskan auditor untuk mempertimbangkan pengawasan administratif, teknis, dan fisik dalam lingkup audit yang sama. Organisasi biasanya memiliki lebih banyak kebijaksanaan untuk merencanakan, mendefinisikan ruang lingkup, dan melakukan audit internal dengan cara yang memisahkan audit proses dan kontrol prosedural dari audit aset, sistem, dan teknologi IT. Ada banyak alasan untuk mengejar pendekatan seperti itu, termasuk kemampuan untuk meningkatkan keterampilan dan kompetensi para auditor terhadap masalah audit yang mereka lakukan.

Operasi IT

Operasional IT audits berfokus pada proses dan prosedur yang dilaksanakan oleh suatu organisasi dan penyelarasan kegiatan-kegiatan tersebut dengan sumber sistem, infrastruktur, dan teknologi informasi lainnya. Untuk berhasil melakukan jenis audit ini, organisasi perlu mengembangkan inventarisasi dari proses dan kontrol prosedural yang digunakannyan (atau mengidentifikasi informasi ini dalam dokumentasi yang ada di dalam sistem audit di ruang lingkup audit) dan menyiapkan strategi audit serta rencana audit yang sesuai dengan rencana audit yang digunakan pada jenis audit lain. Proses pemeriksaan yang relevan mencakup mereka dalam bidang bisnis yang lebih spesifik maupun umum, termasuk :

- Perencanaan strategis dan taktis
- Manajemen Resiko
- Manajemen kualitas
- Pengelolaan keuangan
- Pengelolaan sumber daya manusia
- Akuisisi atau pengadaan

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045

- Pengelolaan rantai pasokan
- Program dan manajemen proyek
- Manajemen perubaham
- Manajemen pelayanan
- Dukungan pelanggan dan teknis
- Manajemen keamanan
- Manajemen fasilitas
- Manajemen vendor

Proses operasional dan kontrol prosedural juga digunakan pada prioritas sehingga sumber audit dapat dialokasikan dengan efektif. Prioritas dalam konteks ini mempertimbangkan kriteria seperti tingkat sumber daya yang terlibat, kompleksitas, hubungan ketergantungan dengan proses lain, dan kritik setiap proses terhadap organisasi secara keseluruhan atau pada fungsi misi atau bisnis yang didukung.

Program dan manajemen proyek

Program atau proyek sering digunakan secara bergantian, standar dan bimbingan untuk mengelola kegiatan-kegiatan yang berbeda, durasi, dan hasilnya, di mana program terdiri dari satu proyek atau lebih, memiliki jangka waktu yang kurang jelas, dan dimaksudkan untuk mencapai satu atau lebih hasil jangka panjang, proyek lebih terfokus secara sempit, usaha sementara dengan poin awal dan akhir yang jelas dimaksudkan untuk menghasilkan produk atau jasa tertentu. Program dan proyek dapat dikenakan pada audit operasional; Audit yang dikaitkan dengan sertifikasi, kepatuhan, atau jaminan kualitas; Audit yang spesifik berfokus pada teknologi, sistem, infrastruktur, atau proses yang mendukung program atau pelaksanaan proyek yang efektif. Para auditor melakukan audit jenis ini biasanya karena kriteria audit dasar setidaknya sebagian dari apa yang ditetapkan dalam metodologi atau standar siklus yang didefinisikan atau diterapkan oleh organisasi. Audit proyek dan Program, sebaliknya, berpusat pada proses, kontrol, dan artefak yang dihasilkan dalam pelaksanaan Program atau kegiatan proyek serta penyelarasan kegiatan tersebut dengan kebijakan, standar, dan persyaratan organisasi. Auditor yang memfokuskan pada audit jenis ini cenderung mengandalkan pemeriksaan bukti dokumenter, pengamatan langsung, dan wawancara dengan staf program atau proyek, karena metode pengujian kurang bisa diterapkan pada kegiatan manajemen. Beberapa pemeriksaan terhadap program dan kemampuan manajemen proyek sering kali disertakan dalam audit operasional atau kepatuhan, atau dalam audit sertifikasi menangani standar-standar untuk kualitas, manajemen pelayanan, atau proses kedewasaan.

Siklus kehidupan pengembangan system

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
Proyek-proyek ini dilakukan di banyak organisasi yang digunakan pada serangkaian proses dan kegiatan yang dikenal sebagai suatu sistem (atau perangkat lunak) siklus kehidupan pembangunan (SDLC). Saat proyek ini berjalan melalui fase berbeda dari SDG, tim proyek ini menjalankan berbagai kegiatan, menghasilkan keluaran yang berbeda, dan memenuhi persyaratan atau kriteria yang diperlukan untuk menyelesaikan satu fase dan beralih ke fase berikutnya. metodologi SDLC tidak mempunyai kesamaan untuk berbagai organisasi degan variasi luas sae siklus hidup dan durasi fase yang di harapkan standar SDLC, Dari prespektif holistik model SDLC memiliki kegiatan dan tujuan yang sama. Organisasi hanya menggunakan 4 fase atau 10 SDLC, pada dasarnya SDLC mencakup kegiatan yang berhubungan dengan inisiasi proyek, desain, operasi dan penghentian proyek. Organisasi hanya menerapkan satu SDLC standar. Audit proyek ini dapat dilaksanakan di setiap titik dalam kehidupan siklus atau potensi rentang siklus hidup beberapa fase siklus kehidupan untuk proyek besar atau kompleks atau mereka yang menggunakan metodologis-artinya auditor harus menyesuaikan kriteria pemeriksaan mereka untuk mencerminkan kegiatan, hasil, dan pencapaian yang berbeda dalam setiap fase. Bagian-bagian berikut mengikuti nama fase kehidupan sistem siklus kehidupan yang diperinci.

Konsep

Setiap proyek IT dimulai dengan ide, saran, persyaratan, atau kebutuhan organisasi lain yang diakui. Konsep proyek atau tahap inisiasi dimulai ketika suatu organisasi mengidentifikasi kebutuhan akan kemampuan baru atau yang ditingkatkan dan mulai menentukan bagaimana konsep dapat memenuhi kebutuhan itu. Selama fase konsep, organisasi dapat mengidentifikasi dan mengevaluasi beberapa alternatif, mempertimbangkan karakteristik teknis dan nonteknis seperti biaya, kompleksitas, strategi akuisisi, dan kelayakan. Audit proyek IT dalam fase konsep biasanya memeriksa proses manajemen proyek, standar, dan metodologi untuk memastikan mereka sesuai dengan kebijakan dan standar organisasi dan memverifikasi kelengkapan dan persetujuan (jika diperlukan) dokumentasi proyek yang diperlukan seperti rencana proyek proyek manajemen piagam, kasus bisnis, analisis alternatif, dan jadwal proyek. Fase konsep juga dapat menghasilkan spesifikasi persyaratan fungsional dan teknis, desain solusi tingkat tinggi, pemilihan kontrol awal, dan rancangan artefak proyek yang harus diselesaikan pada fase selanjutnya seperti rencana keamanan, rencana manajemen risiko, rencana darurat, atau jaminan kualitas. rencana. Organisasi mungkin memerlukan audit pada fase konsep sebagai prasyarat untuk menyetujui transisi proyek ke fase pengembangan.

Pengembangan

Fase pengembangan mencakup berbagai kegiatan yang dimaksudkan untuk memenuhi set lengkap persyaratan yang ditentukan untuk sistem, aplikasi perangkat lunak, atau solusi lainnya. Banyak metodologi SLDC membagi fase pengembangan tunggal yang didefinisikan dalam ISO /

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
IEC 15288 menjadi beberapa fase yang lebih kecil untuk analisis persyaratan dan desain selain pengembangan. Fase pengembangan meliputi spesifikasi persyaratan fungsional dan nonfungsional yang lengkap, dokumentasi desain terperinci yang membahas semua komponen dalam ruang lingkup proyek, rencana pengujian, dan pengiriman kode perangkat lunak, teknologi yang diperoleh, atau elemen solusi lain yang siap untuk diintegrasikan, pengujian, dan evaluasi kontrol. Selama pengembangan, tim proyek juga mengidentifikasi kebutuhan operasional yang diharapkan dalam hal infrastruktur, perangkat keras dan kapasitas jaringan, platform komputasi, dan operasi, pemeliharaan, dan kebutuhan dukungan. Audit proyek IT dalam fase pengembangan fokus pada keakuratan dan kelengkapan dokumentasi dan artefak utama, memastikan bahwa desain yang disetujui memenuhi semua persyaratan, termasuk kontrol internal yang memadai, dan mematuhi standar dan kriteria internal dan eksternal yang berlaku. Untuk melakukan proyek yang melibatkan pengembangan perangkat lunak khusus, ruang lingkup audit proyek IT dapat mencakup tinjauan atau proses kontrol kualitas perangkat lunak lainnya. Terlepas dari sumber atau jenis teknologi yang digunakan dalam proyek, pada akhir fase pengembangan, semua dokumentasi desain, antarmuka integrasi, dan spesifikasi teknis harus lengkap dan komponen sistem atau aplikasi perangkat lunak harus siap untuk evaluasi dan persetujuan sebelum penyebaran penuh.

Produksi

Istilah produksi seperti yang digunakan dalam ISO / IEC 15288 berhubungan dengan serangkaian kegiatan yang dimaksudkan untuk menguji solusi teknis atau mengkonfirmasi kemampuan organisasi untuk mengirimkan produk atau layanan yang dihasilkan dari proyek. Untuk proyek yang menggunakan sistem atau aplikasi perangkat lunak, ruang lingkup fase produksi terdiri dari unit kerja, integrasi, dan pengujian penerimaan untuk mengonfirmasi bahwa teknologi memenuhi persyaratan fungsional; memverifikasi implementasi dan konfigurasi kontrol internal yang tepat; dan menilai langkah-langkah perlindungan keamanan dan privasi yang diperlukan untuk menerima persetujuan untuk sistem atau perangkat lunak agar dapat beroperasi penuh. Audit proyek TI selama fase produksi memeriksa rencana pengujian dan prosedur untuk memastikan bahwa kegiatan pengujian cukup untuk menentukan kepuasan persyaratan. Karena produksi adalah fase terakhir sebelum sistem atau aplikasi perangkat lunak digunakan untuk digunakan, auditor juga memeriksa bahwa proyek telah menerima semua persetujuan yang diperlukan, berpotensi termasuk hasil uji fungsional, penerimaan pengguna, integrasi sistem, kesiapan lingkungan, penerimaan risiko, dan otorisasi untuk beroperasi.

Pemanfaatan

Dalam fase pemanfaatan, sistem atau layanan yang ingin disampaikan oleh proyek yang siap untuk di gunakan, di mana fokus proyek berpindah dari mempersiapkan penempatan untuk secara aktif mengoperasikan dan memelihara sistem dengan cara yang terus-menerus memenuhi

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
kebutuhan pengguna. Suatu sistem dalam tahap pemanfaatan biasanya digunakan pada audit operasional rutin untuk mengevaluasi efisiensi dan efektivitas sistem yang sedang berlangsung dan proses bisnis yang didukungnya. Organisasi juga dapat melakukan berbagai audit khusus IT yang membahas sistem secara keseluruhan atau komponen-komponennya. Sebaliknya, audit proyek IT dalam fase pemanfaatan fokus pada memverifikasi bahwa sistem ketika digunakan akan memberikan fungsionalitas yang dimaksud dan memenuhi persyaratan teknis dan standar yang berlaku, mengandalkan bukti yang didokumentasikan seperti hasil pengujian, penilaian kontrol, dan persetujuan dari personel yang berwenang. dalam organisasi. Audit proyek pada fase ini juga berusaha untuk memastikan bahwa sumber daya yang ditentukan dan disediakan untuk sistem operasional sudah benar dan memadai.

Bantuan

Untuk sistem operasional, dukungan terdiri atas pemantauan, administrasi teknis, pemecahan masalah dan penyelesaian masalah, dan kegiatan pemeliharaan rutin seperti backup, konfigurasi control, patch management, dan upgrade dan pelepasan manajemen untuk perangkat lunak atau komponen teknis lainnya. Bergantung pada kebijakan, prosedur, dan standar organisasi, dukungan dapat juga mencakup kegiatan manajemen keamanan informasi seperti analisis kerentanan, verifikasi otomatis atau manual terhadap pengaturan konfigurasi, serta informasi keamanan dan manajemen peristiwa. Fase dukungan dari proyek IT biasanya berjalan sejajar dengan pemanfaatan; Fase-fase serupa dengan dukungan dalam berbagai metodologi SDLC disebut pemeliharaan, dengan kombinasi pemanfaatan dan dukungan yang dikenal secara kolektif sebagai operasi dan pemeliharaan. Kemampuan dukungan teknis suatu organisasi memiliki dampak langsung pada efektivitas operasional sistemnya, jadi meskipun kegiatan fase dukungan-dukungan dapat diaudit dalam isolasi, cakupan audit pada fase pemanfaatan sering kali mencakup fungsi dukungan.

Pensiun

Proyek menurut definisi memiliki titik akhir yang terdefinisi dengan baik, biasanya bertepatan dengan keputusan organisasi untuk menonaktifkan atau mengganti sistem atau layanan. Fase pensiun dari siklus hidup proyek melibatkan kegiatan yang diperlukan untuk menghilangkan kemampuan operasional dan untuk memastikan disposisi peralatan, perangkat keras dan perangkat lunak, data, dan sumber daya lainnya yang sebelumnya dialokasikan untuk mengoperasikan dan mendukung system proyek baru. Prioritas utama untuk fase pensiun selaras langsung dengan bidang-bidang yang ditekankan untuk audit proyek-proyek IT yang mencapai fase akhir ini: membuang atau menggunakan kembali aset teknologi, melepaskan sumber daya yang berkomitmen pada sistem sehingga dapat diterapkan di tempat lain dalam organisasi yang baru dan membersihkan media penyimpanan yang tetap dan dapat dilepas untuk memastikan bahwa tidak ada data yang tersisa pada komponen yang dinonaktifkan. Auditor IT yang

Nama : Muhammad Iqbal Rizky Tanjung
Kelas : MTI 21 Reg B
NIM : 192420045
memeriksa proyek dalam fase pensiun mencari dokumentasi menyeluruh yang merinci disposisi sumber daya proyek dan aset IT dan untuk persetujuan resmi atas dokumentasi tersebut yang biasanya merupakan prasyaratan untuk secara resmi menutup proyek.

Nama : Marhadi Wijaya
Dosen : Dr. Widya Cholil, S.Kom., M.IT.
NIM : 192420030
MK : IT AUDIT (MTIK319)

Identifikasi Komponen pada IT Audit Process

1. **Planning**

Tahap Planning (Perencanaan) merupakan tahap dimana akan ada pertemuan tim auditor dengan perusahaan untuk membahas kerangka acuan (framework) audit dan kebijakan yang akan diambil dalam mencapai output yang diinginkan. Framework Audit yang populer antara lain: COBIT, ISO, dan ITIL serta dapat digunakan sesuai dengan tujuan audit. Awalnya, tim Audit akan memberi notifikasi dan menentukan jadwal pertemuan dan waktu dilakukannya kegiatan audit. Surat audit ini kemudian akan mendapat persetujuan dari penangggung jawab perusahaan untuk dimulai secara sah.

Komponen yang akan direncanakan pada tahap ini adalah penentuan isu, tujuan dan perspektif bisnis antara penanggung jawab bagian IT. Penentuan isu merupakan daftar hal yang harus diselesaikan agar perusahaan dapat berjalan sesuai dengan tujuan dan persepektif bisnis. Penentuan tujuan akan menjadi tolak ukur perusahaan dalam menentukan tingkat keberhasilan dari proses bisnisnya. Selanjutnya, temuan isu dan tujuan dibahas dan didiskusikan kepada penanggung jawab bagian di bagian IT.

2. Testing

Tahap Testing (Pengujian) merupakan tahap dimana tim auditor mengumpulkan informasi yang relevan tentang unit-unit yang akan diaudit untuk mendapatkan gambaran umum proses bisnis IT yang dilakukan. Hasil dari pengumpulan informasi akan menjadi dasar pengendalian internal dalam pengecekan operasi yang berjalan, apakah sudah berjalan dengan benar dan sesuai dengan prosedur yang dijelaskan oleh klien. Kontrol internal yang dilakukan umumnya melihat faktor keakuratan dan kepatutan data informasi.

Selama tahap testing dilakukan, tim auditor akan mendiskusikan temuan-temuan penting dengan penganggung jawab bagian IT. Temuan-temuan tersubut dapat diambil baik dari metode *Audit Through the Computer* maupun *Audit Around the computer*. Temuan tersebut menjadi landasan penentuan langkah terbaik untuk menyelesaikan temuan tersebut. Setelah menyelesaikan tahap testing, tim auditor akan meringkas

temuan, kesimpulan, dan rekomendasi audit dan meninjaunya dengan penanggung jawab bagian IT.

3. **Reporting**

Tahap Reporting (Laporan) merupakan tahap dimana tim auditor bertemu dengan tim manajemen unit untuk membahas temuan, kesimpulan, dan rekomendasi. Tim auditor menyiapkan draf laporan, dengan mempertimbangkan setiap revisi yang dihasilkan dari rapat penutupan dan diskusi lainnya. Laporan tersebut terdiri dari beberapa bagian meliputi: daftar distribusi, ruang lingkup dan objek, penilaian keseluruhan, serta temuan dan rekomendasi.

Output dari tahap testing ini adalah tanggapan tertulis/ komentar dari draf laporan audit yang menunjukkan bagaimana dan kapan rekomendasi akan dilaksanakan. Proses Reporting akan ditutup dengan peggabungan naskah yang berisikan tanggapan dengan draf laporan, membuat laporan akhir. Laporan ini digunakan oleh perusahaan yang diaudit untuk memperbaiki masalah yang dihadapi sehingga jalannya proses bisnis dapat lebih baik dan juga dipercaya (tersertifikasi). Laporan akhir ini yang umumnya didistribusikan ke supervisor dan anggota manajemen yang bertanggung jawab pada bagiannya.

4. **Follow-Up**

Pada tahap ini, akan ada umpan balik kepada tim auditor berupa komentar tentang kinerja Audit Internal sebagai bagian dari program evaluasi diri tim auditor. Bentuk umpan balik dapat berupa survey evaluasi atau kuesioner. Umpan balik ini ditujukan sebagai landasan membuat perubahan dan pengembangan dalam prosedur kami sebagai hasil dari saran perusahaan. Tim audit akan melakukan review tindak lanjut untuk memverifikasi rekomendasi yang termasuk dalam laporan akhir telah dilaksanakan.