Pilih salah satu Standard yang ada pada dokumen ITAF (materi), dan jelaskan secara ringkas fungsi dari standard tersebut pada Audit TI dan jelaskan keterkaitannya dengan COBIT atau framework lain.

Standar (Pada File dibawah ini) yang digunakan adalah:

1007 ASSERTIONS (PENEGASAN)

Profesional IS audit dan assurance harus meninjau kembali pernyataan yang menjadi dasar subjek masalah akan dinilai untuk menentukan bahwa pernyataan tersebut dapat diaudit dan bahwa pernyataan itu cukup, valid dan relevan.

Profesional IS audit dan assurance harus:

- Mengevaluasi kriteria yang akan dinilai subjeknya untuk memastikan mereka mendukung asersi.
- Menentukan apakah asersi dapat diaudit dan didukung oleh informasi yang menguatkan.
- Menentukan apakah asersi didasarkan pada kriteria yang ditentukan secara tepat dan tunduk pada analisis objektif dan terukur.
- Di mana asersi telah dikembangkan oleh manajemen, pastikan bahwa, bila dibandingkan dengan standar lain dari pernyataan otoritatif bahwa pernyataan tersebut cukup sehubungan dengan apa yang pembaca yang berpengetahuan atau pengguna harapkan.
- Di mana pernyataan telah dikembangkan oleh pihak ketiga yang mengoperasikan kontrol atas nama perusahaan, memastikan bahwa asersi diverifikasi dan diterima oleh manajemen.
- Melaporkan secara langsung terhadap subjek (laporan langsung) atau terhadap pernyataan tentang subjek masalah (laporan tidak langsung).
- Bentuk kesimpulan tentang setiap asersi, berdasarkan pada agregat temuan terhadap kriteria bersama penilaian profesional.

Standards Statements

1003 Professional Independence

1003.1 profesional audit dan penjaminan IS harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang berkaitan dengan

perikatan audit dan penjaminan.

Profesional audit dan penjaminan IS harus:

- Melakukan audit SI atau keterlibatan jaminan dengan kerangka pikir yang adil dan tidak memihak dalam menyikapi masalah jaminan dan mencapai kesimpulan.
- Independen sebenarnya, tetapi juga tampak independen setiap saat.
- Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika independensi terganggu pada kenyataannya atau penampilan.
- Menilai independensi secara teratur dengan manajemen dan komite audit, jika ada.
- Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karenanya peran dapat merusak independensi masa depan.

Linkage to Guidelines Guideline 2003 Professional Independence

1.1.1 Tujuan dari pedoman ini adalah untuk menyediakan kerangka kerja yang memungkinkan audit dan jaminan IS profesional untuk:

- Menetapkan kapan kemerdekaan mungkin, atau mungkin tampak, terganggu
- Pertimbangkan pendekatan alternatif yang potensial untuk proses audit ketika independensi sedang, atau mungkin tampak menjadi, terganggu
- Mengurangi atau menghilangkan dampak pada independensi audit SI dan kinerja profesional penjaminan peran, fungsi dan layanan non-audit

- Menentukan persyaratan pengungkapan ketika independensi yang disyaratkan mungkin, atau mungkin tampak, terganggu

1.1.2 profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini ketika menentukan bagaimana menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

2.1.1 Banyak keadaan atau kombinasi keadaan yang berbeda mungkin relevan dalam menilai ancaman menuju kemerdekaan. Tidak mungkin mendefinisikan setiap situasi yang menciptakan ancaman bagi kemerdekaan dan tentukan tindakan yang sesuai. Oleh karena itu, pedoman ini menetapkan kerangka kerja konseptual yang membutuhkan profesional untuk mengidentifikasi, mengevaluasi, dan menangani ancaman terhadap independensi. Kerangka kerja konseptual

pendekatan membantu dalam mematuhi standar independensi, dan mengakomodasi banyak variasi dalam keadaan yang menciptakan ancaman bagi kemerdekaan.

2.1.2 Pendekatan kerangka kerja konseptual harus diterapkan oleh para profesional untuk:

- Identifikasi ancaman terhadap kemerdekaan.
- Mengevaluasi signifikansi ancaman yang diidentifikasi.
- Terapkan perlindungan, bila perlu, untuk menghilangkan ancaman atau menguranginya ke tingkat yang dapat diterima.

2.1.3 Ketika para profesional menentukan bahwa perlindungan yang sesuai tidak tersedia atau tidak dapat diterapkan menghilangkan ancaman atau mengurangi ancaman ke tingkat yang dapat diterima, profesional harus menghilangkan keadaan atau hubungan yang menciptakan ancaman, atau menolak atau menghentikan audit atau perikatan jaminan. Jika profesional tidak dapat menolak atau mengakhiri pertunangan, pengungkapan yang layak atas penurunan nilai terhadap independensi

harus dibuat untuk mereka yang bertanggung jawab atas tata kelola dan dalam laporan apa pun yang dihasilkan dari perikatan.

2.1.4 Profesional harus menggunakan penilaian profesional dalam menerapkan kerangka kerja konseptual ini.

2.1.5 Aspek penting ketika menerapkan kerangka kerja adalah konsultasi. Profesional audit dan penjaminan IS harus mencari bimbingan, bila dianggap perlu, dari:

- Kolega di dalam perusahaan
- Manajemen
- Mereka yang bertanggung jawab atas tata kelola
- Organisasi profesional yang relevan

2.1.6 Meskipun tidak ada persyaratan bagi para profesional untuk mandiri untuk melakukan layanan atau peran non-audit, objektivitas masih merupakan persyaratan profesional ketika melakukan hal tersebut. Profesional harus mempertimbangkan untuk mendaftar kerangka kerja konseptual ini untuk mengidentifikasi ancaman terhadap objektivitas, mengevaluasi signifikansi ancaman dan menerapkan perlindungan yang tepat saat melakukan layanan atau peran non-audit.

2.2.1 Ancaman dapat diciptakan oleh berbagai hubungan dan keadaan. Ketika suatu hubungan atau keadaan menciptakan ancaman, ancaman seperti itu dapat merusak, atau bisa dianggap merusak, profesional kemerdekaan. Keadaan atau hubungan dapat menciptakan lebih dari satu ancaman terhadap kemerdekaan. Ancaman jatuh menjadi satu atau lebih dari kategori berikut:

- Kepentingan pribadi — Ancaman bahwa kepentingan finansial atau lainnya akan memengaruhi penilaian profesional atau perilaku yang tidak tepat

- Tinjauan sendiri — Ancaman bahwa profesional tidak akan dengan tepat mengevaluasi hasil dari yang sebelumnya penilaian dibuat atau layanan dilakukan oleh mereka atau oleh orang lain dalam fungsi audit, di mana profesional akan mengandalkan saat membentuk penilaian sebagai bagian dari melakukan pertunangan saat ini
- Advokasi — Ancaman bahwa profesional akan mempromosikan posisi pihak yang diaudit ke titik profesional itu objektivitas terganggu
- Keakraban — Ancaman bahwa karena hubungan yang panjang atau dekat dengan pihak yang diaudit, para profesional juga akan demikian bersimpati pada kepentingan auditee atau akan terlalu menerima pekerjaan, pandangan atau argumen auditee
- Intimidasi — Ancaman bahwa para profesional akan terhalang untuk bertindak dengan integritas dan objektivitas karena tekanan aktual atau yang dirasakan, termasuk upaya untuk melakukan pengaruh yang tidak semestinya terhadap profesional
- Bias — Ancaman yang akan ditimbulkan oleh para profesional, sebagai akibat dari politik, ideologis, sosial, psikologis atau lainnya keyakinan, ambil posisi yang tidak objektif
- Partisipasi manajemen — Ancaman yang dihasilkan oleh para profesional yang berperan sebagai manajemen atau menjalankan fungsi manajemen atas nama entitas yang menjalani audit atau jaminan Keterikatan.

1.2 Linkage to

Standards

1.2.1 Standard 1002 Organisational Independence

1.2.2 Standard 1003 Professional Independence

1.2.3 Standard 1005 Due Professional Care

Linkage to Standards and COBIT 5 Processes

3.0 Introduction This section provides an overview of relevant:

3.1 Linkage to standards

3.2 Linkage to COBIT 5 processes

3.3 Other guidance

Tugas Audit Charter : Indri Endang Lestari & Sulistiyani

MTI19AR2

1. Standard 1001 - Audit Charter :

Audit Charter adalah sebuah dokumen formal yang menyatakan tujuan, wewenang, dan tanggung jawab unit audit intern pada suatu organisasi. Piagam Audit merupakan penegasan komitmen dari para pemangku kepentingan (*stakeholders*) terhadap arti pentingnya fungsi pengawasan di organisasinya. Adapun ketentuan dari piagram ini harus :

- Menetapkan posisi fungsi audit internal dalam perusahaan
- Memberikan Otorisasi akses ke catatan, personel dan properti fisik yang relevan dengan kinerja audit dan jaminan IS
- Tentukan ruang lingkup kegiatan fungsi audit

Adapun manfaat piagam audit adalah menjadi salah satu alat untuk mempertegas independensi. Penegasan itu nampak dari pengaturan posisi unit audit intern dalam struktur organisasi dan kepada siapa pimpinan unit tersebut bertanggung jawab secara fungsional. Penegasan tersebut sekaligus juga berguna untuk meningkatkan trust semua unsur organisasi terhadap fungsi audit intern.

adapun guideline yang digunakan dalam audit charter adalah **2001 Audit Charter**

2. Guideline 2001 – Audit Charter

a. Tujuan Guideline – 2001 Audit Charter :
   - Membantu professional audit dan penjaminan IS dalam menyiapkan piagam audit
   - Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

b. Guideline 2001 Audit charter selain digunakan untuk standard 1001 audit charter, juga bias digunakan untuk 1002 Organisational Independence, dan 1003 Professional Independence.

c. Contents of Audit Charter

Piagam audit harus dengan jelas membahas empat aspek, yaitu tujuan, tanggung jawab, wewenang dan akuntabilitas.

- **Tujuan** piagam audit dan fungsi audit harus berisi bagian-bagian berikut:
    - Maksud / tujuan piagam audit memberikan kerangka kerja fungsional dan organisasi di mana audit fungsi beroperasi.
    - Pernyataan misi dan tujuan fungsi audit membawa pendekatan terstruktur untuk mengevaluasi dan meningkatkan desain dan efektivitas operasional dari proses manajemen risiko, pengendalian internal sistem dan struktur tata kelola sistem informasi.
    - Lingkup fungsi audit adalah untuk seluruh perusahaan atau organisasi tertentu dalam perusahaan.
    - Tata kelola merinci badan otorisasi untuk piagam audit dan fungsi audit.
- **Tanggung jawab** fungsi audit harus berisi bagian-bagian berikut:
    - Prinsip operasi memberikan penghitungan yang lebih rinci dan kuantitatif dari berbagai tujuan fungsi audit.
    - Independensi merinci pelaksanaan persyaratan independensi untuk fungsi audit dan profesional, sebagaimana dijelaskan dalam Standar 1002 Organisational Independence, dan 1003 Professional Independence.
    - Hubungan dengan audit eksternal untuk merinci hubungan fungsi audit dengan auditor eksternal, adapun pertemuannya untuk mengoordinasikan upaya kerja untuk meminimalkan upaya duplikasi, Menyediakan akses ke kertas kerja, dokumentasi, dan bukti professional, dan Mempertimbangkan pekerjaan yang direncanakan oleh auditor eksternal ketika menyusun rencana audit untuk periode mendatang
    - Harapan audit merinci layanan dan hasil yang dapat diaudit dari fungsi audit dan professional, meliputi deskripsi masalah yang teridentifikasi, konsekuensi dan kemungkinan resolusi yang berkaitan dengan bidang tanggung jawab pihak yang diaudit
    - Kemungkinan untuk memasukkan respons manajemen dan tindakan korektif yang diambil atas temuan dalam audit, termasuk referensi untuk perjanjian tingkat layanan terkait (SLA) untuk barang-barang seperti

pengiriman laporan, tanggapan terhadap keluhan yang diaudit, kualitas layanan, tinjauan kinerja, proses pelaporan dan persetujuan temuan.

  - Persyaratan audit merinci tanggung jawab audit.
  - Komunikasi dengan auditee merinci frekuensi dan saluran komunikasi yang melaluinya audit fungsi akan berkomunikasi dengan pihak yang diaudit.

- **Otoritas** fungsi audit harus berisi bagian-bagian berikut:
  - Hak akses ke informasi yang relevan, sistem, personel dan lokasi oleh para profesional ketika melakukan perikatan audit. Fungsi audit, diwakili oleh para professional.
  - Keterbatasan kewenangan fungsi audit dan profesional, jika ada
  - Proses yang akan diaudit, di mana fungsi audit berwenang untuk mengaudit.
- **Akuntabilitas** fungsi audit harus berisi bagian-bagian berikut:
  - Struktur organisasi, termasuk jalur pelaporan ke dewan dan manajemen senior, dari fungsi audit, mis., fungsi audit harus memiliki akses terbuka dan tidak terbatas ke dewan dan anggotanya.
  - Pelaporan yang merinci format, konten, dan penerima komunikasi pada hasil setiap perikatan audit, mis., laporan audit tertulis akan dikeluarkan oleh fungsi audit setelah setiap audit keterlibatan dan didistribusikan kepada pemangku kepentingan yang tepat.
  - kinerja fungsi audit dibandingkan dengan rencana audit dan anggaran,
  - Kepatuhan terhadap standar yang merinci standar yang akan digunakan fungsi audit dan professional. mematuhi, mis., fungsi audit dan profesional akan mematuhi dan bertindak sesuai dengan semua Audit ISACA IS dan Standar dan Pedoman Jaminan.
  - Proses penjaminan kualitas
  - Aturan kepegawaian untuk perikatan audit
  - Komitmen pendidikan berkelanjutan dari fungsi audit terhadap para professional

- Tindakan yang disetujui mengenai fungsi fungsi audit dan perilaku profesional, mis., Hukuman saat salah satu pihak gagal melaksanakan tanggung jawabnya

- Aspek lain yang harus dipertimbangkan untuk ditambahkan dalam piagam audit adalah:
  - Meninjau dan mengubah piagam, yang merupakan tanggung jawab fungsi audit. Seharusnya secara berkala menilai apakah tujuan, tanggung jawab, wewenang dan akuntabilitas, sebagaimana didefinisikan dalam piagam audit, terus menjadi memadai dan mengomunikasikan hasil penilaian kepada komite audit.
  - Memperoleh persetujuan amandemen terhadap piagam audit dari pihak yang bertanggung jawab atas tata kelola.
  - Termasuk dokumen terkait seperti referensi standar terkait, pedoman, kebijakan, kerangka kerja, manual, dll.

3. Linkage to COBIT 5 Processes

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam COBIT 5

Proses Cobit 5 : MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.

Tujuannya : Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem internal mengendalikan dan, dengan demikian, memberikan kepercayaan dalam operasi, kepercayaan pada pencapaian perusahaan tujuan dan pemahaman yang memadai tentang risiko residual.

4 Contoh Piagam Audit Charter

PIAGAM AUDIT INTERNAL
(INTERNAL AUDIT CHARTER)
PT SINAR MAS AGRO RESOURCES & TECHNOLOGY Tbk.

smart
agribusiness and food

BAB I
DASAR DAN TUJUAN PEMBENTUKAN

1.1. PT Sinar Mas Agro Resources & Technology Tbk (selanjutnya disebut "PT SMART Tbk" atau "Perseroan"), sebagai perusahaan publik harus mematuhi peraturan perundangan di bidang pasar modal.

1.2 PT SMART Tbk wajib memiliki Unit Audit Internal ("AI") yaitu unit kerja yang menjalankan fungsi Audit Internal. Audit Internal adalah suatu kegiatan pemberian keyakinan dan konsultasi yang bersifat independen dan objektif, dengan tujuan untuk meningkatkan nilai dan memperbaiki operasional Perseroan dan anak perusahaannya, melalui pendekatan yang sistematis, dengan cara mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses tata kelola perusahaan.

1.3 Sehubungan dengan itu, AI wajib menyusun Piagam Audit Internal (selanjutnya disebut "Piagam"). Piagam ini disusun agar AI dapat melaksanakan tugas dan tanggung jawabnya secara efisien, transparan, kompeten, independen, dan dapat dipertanggungjawabkan sehingga dapat diterima oleh semua pihak yang berkepentingan. Piagam ini ditetapkan oleh Direksi setelah mendapat persetujuan Dewan Komisaris.

1.4 Dasar hukum Piagam ini adalah:

1.4.1 Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal;

1.4.2 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan; dan

1.4.3 Peraturan Otoritas Jasa Keuangan Nomor 56/POJK.04/2015 tentang Pembentukan dan Pedoman Penyusunan Piagam Unit Audit Internal.

BAB II
STRUKTUR, KEDUDUKAN DAN SYARAT KEANGGOTAAN

2.1 Struktur dan Kedudukan

2.1.1 AI dipimpin oleh seorang Kepala AI.

2.1.2 Kepala AI diangkat dan diberhentikan oleh Direktur Utama atas persetujuan Dewan Komisaris.

2.1.3 Direktur Utama dapat memberhentikan Kepala AI, setelah mendapat persetujuan Dewan Komisaris, jika tidak memenuhi persyaratan sebagai auditor internal sebagaimana diatur dalam piagam ini dan/atau gagal atau dianggap tidak cakap dalam menjalankan tugas terkait.

2.1.4 Kepala AI bertanggung jawab kepada Direktur Utama dan secara fungsional kepada Dewan Komisaris atau melalui Komite Audit.

2.1.5 Auditor internal atau anggota dalam AI bertanggung jawab secara langsung kepada Kepala AI.

2.1.6 Dalam melaksanakan tugasnya, manajemen dan Dewan Komisaris memberikan dukungan sepenuhnya kepada AI agar dapat bekerja dengan bebas dan obyektif tanpa campur tangan pihak manapun.

2.2 Syarat Keanggotaan

Auditor internal dalam AI wajib memenuhi persyaratan sebagai berikut:

2.2.1 memiliki integritas dan perilaku yang profesional, independen, jujur dan objektif;

2.2.2 berkompeten di bidangnya, baik mengenai teknis audit, disiplin ilmu lain yang relevan, peraturan perundang-undangan di bidang pasar modal dan peraturan perundang-undangan terkait lainnya, prinsip tata kelola perusahaan yang baik, maupun manajemen risiko;

2.2.3 memiliki kecakapan untuk berinteraksi dan berkomunikasi baik secara lisan maupun tertulis secara efektif;

2.2.4 mematuhi standar profesi yang dikeluarkan oleh asosiasi Audit Internal;

2.2.5 mematuhi Kode Etik AI;

2.2.6 menjaga kerahasiaan informasi dan/atau data Perseroan dan anak perusahaan terkait dengan pelaksanaan tugas dan tanggung jawab AI kecuali diwajibkan berdasarkan peraturan perundang-undangan atau penetapan atau putusan pengadilan; dan

2.2.7 bersedia meningkatkan pengetahuan, keahlian dan kemampuan profesionalismenya secara terus menerus.

BAB III
TUGAS, TANGGUNG JAWAB DAN WEWENANG

3.1 Tugas dan Tanggung Jawab

3.1.1 Menyiapkan dan melaksanakan rencana dan anggaran aktivitas audit internal tahunan berdasarkan prioritas risiko sesuai dengan tujuan Perseroan.

3.1.2 Menguji dan mengevaluasi pelaksanaan pengendalian internal dan sistem manajemen risiko sesuai dengan kebijakan Perseroan.

3.1.3 Melakukan pemeriksaan dan penilaian atas efisiensi dan efektivitas di seluruh bidang kegiatan Perseroan dan anak perusahaan.

3.1.4 Memberikan saran perbaikan dan informasi yang obyektif tentang kegiatan yang diperiksa pada semua tingkatan manajemen.

3.1.5 Membuat laporan hasil audit dan menyampaikan laporan tersebut kepada Manajemen terkait, Direktur Utama dan Dewan Komisaris atau Komite Audit.

3.1.6 Memantau, menganalisis dan melaporkan pelaksanaan tindak lanjut perbaikan yang telah disarankan.

3.1.7 Menyusun program untuk mengevaluasi mutu kegiatan audit yang dilakukannya.

3.1.8 Melakukan pemeriksaan khusus apabila diperlukan.

3.2. Wewenang

3.2.1 Mengakses seluruh informasi yang relevan tentang Perseroan dan anak perusahaan terkait dengan tugas dan fungsinya.

3.2.2 Berkomunikasi langsung dan/atau mengadakan rapat secara berkala maupun insidentil dengan Direksi, Dewan Komisaris, dan/atau Komite Audit serta anggota dari Direksi, Dewan Komisaris, dan/atau Komite Audit.

3.2.3 Melakukan koordinasi kegiatannya dengan kegiatan auditor eksternal.

BAB IV
KODE ETIK

4.1 Prinsip-prinsip

Dalam melaksanakan tugas dan tanggung jawabnya, auditor internal harus menerapkan dan menegakkan prinsip-prinsip berikut ini:

4.1.1 **Integritas**

Integritas yang dimiliki auditor internal membentuk kepercayaan, dan berdasarkan kepercayaan inilah maka pertimbangan mereka dapat diandalkan.

4.1.2 **Obyektivitas**

Auditor internal memperlihatkan tingkat obyektifitas tertinggi dalam mengumpulkan, mengevaluasi dan mengkomunikasikan informasi tentang aktivitas atau proses yang diperiksa. Auditor internal membuat penilaian yang seimbang atas segala kondisi yang terkait dan tidak dipengaruhi oleh kepentingan pribadi atau pihak lain dalam memberikan pertimbangan.

4.1.3 **Kerahasiaan**

Auditor internal menghormati nilai dan kepemilikan dari informasi yang diterimanya dan tidak mengungkapkan informasi tersebut tanpa kewenangan yang sah, kecuali diharuskan oleh hukum atau profesi.

4.1.4 **Kompetensi**

Auditor internal menggunakan pengetahuan, keterampilan dan pengalaman yang diperlukan dalam melakukan tugas/jasa audit internal.

4.2. Aturan pelaksanaan

4.2.1 **Integritas**

- Melakukan pekerjaannya dengan jujur, tekun dan penuh tanggung jawab.
- Mematuhi hukum/peraturan/kebijakan yang berlaku dan membuat pengungkapan sesuai dengan hukum/peraturan/kebijakan serta aturan profesi yang berlaku tersebut.
- Tidak secara sengaja terlibat dalam kegiatan terlarang atau melakukan tindakan yang mencemarkan nama baik profesi maupun Perseroan.
- Menghormati dan memberikan kontribusi pada tujuan Perseroan yang sah dan etis.

4.2.2 **Obyektivitas**

- Tidak ikut serta dalam segala kegiatan atau hubungan yang dapat mengganggu dalam memberikan penilaian yang tidak memihak. Keikutsertaan tersebut mencakup keikutsertaan dalam kegiatan atau hubungan yang bertentangan dengan kepentingan Perseroan.
- Tidak menerima apapun yang dapat membahayakan pertimbangan profesionalnya.
- Mengungkapkan seluruh fakta material yang diketahuinya, yang apabila tidak diungkapkan dapat menimbulkan distorsi atas pelaporan kegiatan yang diperiksa.

4.2.3 **Kerahasiaan**

- Berhati-hati dalam menggunakan dan menjaga informasi yang diperoleh selama menjalankan tugasnya.
- Tidak menggunakan informasi untuk keuntungan pribadi, atau dengan cara apapun yang bertentangan dengan hukum atau merusak tujuan Perseroan yang sah dan etis.

4.2.4 **Kompetensi**

- Hanya terlibat dalam pemberian jasa dimana mereka memiliki pengetahuan, keterampilan dan pengalaman yang dibutuhkan.
- Melaksanakan jasa audit internal yang sesuai dengan standar profesional untuk audit internal.
- Senantiasa meningkatkan keahlian, keefektifan dan kualitas jasanya secara berkelanjutan.

BAB V
PERTANGGUNGJAWABAN

AI akan menyiapkan dan menerbitkan laporan hasil audit secara tertulis setelah penugasan audit selesai, dan laporan hasil audit tersebut akan didistribusikan sebagaimana mestinya. Laporan audit internal juga akan disampaikan kepada Dewan Komisaris atau melalui Komite Audit.

Laporan hasil audit tersebut memuat respon manajemen dan tindakan/rencana tindakan perbaikan yang akan dilakukan manajemen terkait dengan temuan-temuan audit dan rekomendasinya. Respon manajemen harus memuat jadwal penyelesaian tindakan perbaikan oleh manajemen dan penjelasan jika suatu tindakan perbaikan tidak dapat dilakukan.

BAB VI
KEMANDIRIAN FUNGSIONAL

Auditor internal tidak memiliki tanggung jawab atau wewenang operasional atas apa yang mereka audit. Sesuai dengan hal tersebut, auditor internal juga tidak mengimplementasikan pengendalian internal, membuat prosedur, merancang sistem, membukukan transaksi atau terlibat dalam kegiatan-kegiatan lainnya yang dapat mempengaruhi penilaian mereka.

Piagam AI PT SMART Tbk ini mulai berlaku sejak tanggal ditetapkan dan selanjutnya Piagam AI dan Kode Etik AI yang ditetapkan tanggal 30 April 2009 dicabut dan dinyatakan tidak berlaku.

Disetujui oleh Dewan Komisaris melalui Rapat Dewan Komisaris tanggal 22 Desember 2016 dan selanjutnya ditetapkan oleh Direksi tanggal : 23 Desember 2016

tugas sulistiyani

ASSERTION (PENEGASAN)

BAGIAN 1007

PENGERTIAN ASSERTION (PENEGASAN)

- IS profesional audit dan penjaminan harus meninjau kembali pernyataan yang menjadi dasar subjek masalah akan dinilai untuk menentukan bahwa pernyataan tersebut dapat diaudit dan bahwa pernyataan itu cukup, valid dan relevan.
- IS profesional audit dan jaminan harus menilai, meninjau dan mengevaluasi pekerjaan orang lain ahli sebagai bagian dari perjanjian, dan mendokumentasikan kesimpulan tentang tingkat penggunaan dan mengandalkan pekerjaan mereka.

ASPEK KUNCI ASSERTION (PENEGASAN)

- Mengevaluasi kriteria yang akan dinilai subjeknya untuk memastikan mereka mendukung asersi.
- Menentukan apakah asersi dapat diaudit dan didukung oleh informasi yang menguatkan.
- Menentukan apakah asersi didasarkan pada kriteria yang ditentukan secara tepat dan tunduk pada analisis objektif dan terukur.
- Di mana asersi telah dikembangkan oleh manajemen, pastikan bahwa, bila dibandingkan dengan standar lain dari pernyataan otoritatif bahwa pernyataan tersebut cukup sehubungan dengan apa yang pembaca yang berpengetahuan atau pengguna harapkan.
- Di mana pernyataan telah dikembangkan oleh pihak ketiga yang mengoperasikan kontrol atas nama perusahaan, memastikan bahwa asersi diverifikasi dan diterima oleh manajemen.
- Melaporkan secara langsung terhadap subjek (laporan langsung) atau terhadap pernyataan tentang subjek masalah (laporan tidak langsung).
- Bentuk kesimpulan tentang setiap asersi, berdasarkan pada agregat temuan terhadap kriteria bersama penilaian profesional.

KETENTUAN ASSERTION (PENEGASAN)

- Deklarasi formal atau set deklarasi apa pun yang dibuat oleh manajemen.
- Penegasan biasanya harus secara tertulis dan biasanya berisi daftar spesifik atribut tentang materi pelajaran tertentu atau tentang proses yang melibatkan materi pelajaran.

KRITERIA ASSERTION (PENEGASAN)

IS profesional audit dan penjaminan harus memilih kriteria, di mana materi pelajaran akan dinilai, yang objektif, lengkap, relevan, dapat diukur, dimengerti, diakui secara luas, berwibawa dan dipahami oleh, atau tersedia untuk, semua pembaca dan pengguna laporan.

Materialitas ASSERTION (PENEGASAN)

- Tidak adanya kontrol atau kontrol tidak efektif
- Signifikansi dari defisiensi kontrol
- Kemungkinan kelemahan ini mengakibatkan defisiensi signifikan atau kelemahan material

PEDOMAN ASSERTION (PENEGASAN)

1. Tujuan pedoman dan keterkaitan dengan standar

- Tujuan dari pedoman ini adalah untuk merinci berbagai asersi, panduan IS audit dan profesional penjaminan dalam memastikan bahwa kriteria, yang menjadi dasar penilaian masalah, mendukung pernyataan, dan memberikan panduan untuk merumuskan kesimpulan dan menyusun laporan tentang asersi.
- Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

2. Konten pedoman

3. Keterkaitan dengan standar dan proses COBIT 5

4. Terminologi

5. Tanggal efektif

Standar Pelaporan ASSERTION (PENEGASAN)

- Identifikasi perusahaan, penerima yang dituju dan segala batasan pada konten dan sirkulasi
- Cakupan, tujuan keterlibatan, periode cakupan dan sifat, waktu, dan luasnya pekerjaan yang dilakukan
- Temuan, kesimpulan dan rekomendasi
- Setiap kualifikasi atau batasan dalam ruang lingkup yang dimiliki oleh audit SI dan profesional penjaminan sehubungan dengan pertunangan
- Tanda tangan, tanggal dan distribusi sesuai dengan ketentuan piagam audit atau surat pertunangan

Ketika menerapkan standar dan pedoman, para profesional didorong untuk mencari panduan lain ketika dipertimbangkan perlu. Ini bisa dari audit IS dan jaminan:

- Kolega dari dalam organisasi dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam organisasi, misalnya, komite audit
- Panduan lain (misalnya, buku, makalah, pedoman lainnya)

KETERKAITAN DENGAN PROSES COBIT 5

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam COBIT 5: Proses yang Memampukan.

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pemerintahan pengaturan kerangka kerja dan pemeliharaan.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan keputusan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

TERMININOLOGI ASSERTION (PENEGASAN)

ISTILAH	Definisi
Tuntutan	Deklarasi formal atau set deklarasi apa pun yang dibuat oleh manajemen
Kriteria	Standar dan tolok ukur yang digunakan untuk mengukur dan menyajikan materi pelajaran dan dimana auditor SI mengevaluasi materi pelajaran. Kriteria harus: • Objektif — Bebas dari bias • Lengkap — Sertakan semua faktor yang relevan untuk mencapai kesimpulan • Relevan — Berkaitan dengan pokok pembicaraan • Terukur — Menyediakan pengukuran yang konsisten • Dapat dimengerti Dalam pengikatan pengesahan, tolok ukur terhadap mana pernyataan tertulis manajemen pada materi pelajaran dapat dievaluasi. Praktisi membentuk kesimpulan tentang materi pelajaran dengan mengacu pada kriteria yang sesuai. Penilaian profesional Penerapan pengetahuan dan pengalaman yang relevan dalam membuat keputusan berdasarkan informasi tentang program tindakan yang sesuai dalam keadaan audit IS dan keterlibatan jaminan
Subjek	Informasi spesifik tunduk pada laporan auditor SI dan prosedur terkait, yang dapat mencakup hal-hal seperti desain atau operasi kontrol internal dan kepatuhan praktik atau standar privasi atau hukum dan peraturan tertentu (bidang kegiatan)

Organisasi ITAF IS audit dan jaminan standar dibagi menjadi tiga kategori:

1. Standar Umum (1000 series) -Apakah prinsip-prinsip di mana profesi jaminan IS beroperasi. Mereka berlaku untuk pelaksanaan semua tugas, dan berurusan dengan audit IS dan jaminan profesional etika, independensi, objektivitas dan hati-hati serta pengetahuan, kompetensi dan keterampilan.
2. Standar kinerja (1200 series) -Deal dengan pelaksanaan tugas, seperti perencanaan dan pengawasan, scoping, risiko dan materialitas, mobilisasi sumber daya, pengawasan dan tugas manajemen, audit dan bukti jaminan, dan berolahraga profesional penghakiman dan perawatan karena
3. Standar Pelaporan (1400 series) -Address jenis laporan, berarti komunikasi dan informasi yang dikomunikasikan ITAF IS pedoman audit dan jaminan menyediakan audit IS dan jaminan profesional dengan informasi dan arah tentang audit IS atau daerah jaminan. Sejalan dengan tiga kategori standar yang diuraikan di atas, pedoman fokus pada berbagai pemeriksaan pendekatan, metodologi dan materi yang terkait untuk membantu dalam perencanaan, pelaksanaan, menilai, menguji dan melaporkan IS proses, kontrol dan terkait IS audit atau jaminan inisiatif. Pedoman juga membantu memperjelas hubungan antara kegiatan perusahaan dan inisiatif, dan orang-orang yang dilakukan oleh IT.

keterkaitannya dengan COBIT atau framework lain.

COBIT adalah merupakan kerangka panduan tata kelola TI dan atau bisa juga disebut sebagai toolset pendukung yang bisa digunakan untuk menjembatani gap antara kebutuhan dan bagaimana teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi. COBIT memungkinkan pengembangan kebijakan yang jelas dan sangat baik digunakan untuk IT kontrol seluruh organisasi, membantu meningkatkan kualitas dan nilai serta menyederhanakan pelaksanaan alur proses sebuah organisasi dari sisi penerapan IT.

COBIT dikenal luas sebagai standard defacto untuk kerangka kerja tata kelola TI (IT Governance) dan yang terkait dengannya. Di sisi lain standard/framework ini terus berevolusi sejak pertama kali diluncurkan di 1996 hingga rilis terakhir yaitu COBIT 5 yang diluncurkan pada Juni 2012 yang lalu. Pada setiap rilisnya, kerangka kerja ini melakukan pergeseran-pergeseran beberapa paradigma.

COBIT berorientasi proses, dimana secara praktis COBIT dijadikan suatu standar panduan untuk membantu mengelola suatu organisasi mencapai tujuannya dengan memanfaatkan TI. COBIT memberikan panduan kerangka kerja yang bisa mengendalikan semua kegiatan organisasi secara detail dan jelas sehingga dapat membantu memudahkan pengambilan keputusan di level top dalam organisasi.

COBIT 5 memiliki Prinsip dan Enabler yang bersifat umum dan bermanfaat untuk semua ukuran perusahaan, baik komersial maupun non-profit ataupun sektor publik. 5 Prinsip tersebut adalah Meeting stakeholder needs, Covering enterprise end-to-end, Applying a single intergrated framework, Enabling a holistic approach dan Separating governance from management, berikut penjelasanya:

1. Meeting stakeholder needs, berguna untuk pendefinisan prioritas untuk implementasi, perbaikan, dan jaminan. Kebutuhan stakeholder diterjemahkan ke dalam Goals Cascade menjadi tujuan yang lebih spesifik, dapat ditindaklajuti dan disesuaikan, dalam konteks : Tujuan perusahaan (Enterprise Goal), Tujuan yang terkait IT (IT-related Goal), Tujuan yang akan dicapai enabler (Enabler Goal). Selain itu sistem tata kelola harus mempertimbangkan seluruh stakeholder ketika membuat keputusan mengenai penilaian manfaat, resource dan risiko.
2. Covering enterprise end-to-end, bermanfaat untuk mengintegrasikan tata kelola TI perusahaan kedalam tata kelola perusahaan. Sistem tata kelola TI yang diusung COBIT 5 dapat menyatu dengan sistem tata kelola perusahaan dengan mulus. Prinsip kedua ini juga meliputi semua fungsi dan proses yang dibutuhkan untuk mengatur dan mengelola TI perusahaan dimanapun informasi diproses. Dalam lingkup perusahaan, COBIT 5 menangani semua layanan TI internal maupun eksternal, dan juga proses bisnis internal dan eksternal.
3. Applying a single intergrated framework, sebagai penyelarasan diri dengan standar dan framework relevan lain,

sehingga perusahaan mampu menggunakan COBIT 5 sebagai framework tata kelola umum dan integrator. Selain itu prinsip ini menyatukan semua pengetahuan yang sebelumnya tersebar dalam berbagai framework ISACA (COBIT, VAL IT, Risk IT, BMIS, ITAF, dll).

4. Enabling a holistic approach, yakni COBIT 5 memandang bahwa setiap enabler saling memperngaruhi satu sama lain dan menentukan apakah penerapan COBIT 5 akan berhasil. Enabler didorong oleh Jenabaran tujuan.
5. Separating governance from management, COBIT membuat perbedaan yang cukup jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup brbagai kegiatan yang berbeda, memerlukan struktur organisasi yang berbeda, dan melayani untuk tujuan yang berbeda pula.

TUGAS ITAF TASK 3

Nama : Uci Suriani

Kelas : MTi Reguler A

NIK : 182420072

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PASCASARJANA UNIVERSITAS BINA DARMA

PALEMBANG

201

IS AUDIT AND ASSURANCE STANDARDS CONTOH KASUS : AUDIT CHARTER

Standar Audit dan Jaminan IS berfungsi untuk :

- Landasan kontribusi profesionalnya bagi komunitas audit dan jaminan
- Terdiri dari level pertama panduan ITAF
- Memberikan informasi yang diperlukan untuk memenuhi kebutuhan kepatuhan
- Memberikan panduan penting untuk meningkatkan efektivitas dan efisiensi
- Menawarkan pendekatan berbasis risiko yang selaras dengan metodologi ISACA
- Berlaku untuk individu yang memberikan jaminan atas beberapa komponen sistem IS, aplikasi, dan infrastruktur
- Semoga juga memberikan manfaat kepada khalayak yang lebih luas, termasuk pengguna audit IS dan laporan jaminan
- Standar ISACA menyediakan informasi yang diperlukan untuk memenuhi kebutuhan kepatuhan profesional audit dan penjaminan IS, serta memberikan panduan penting untuk meningkatkan efektivitas dan efisiensi. Pengetahuan dan kepatuhan terhadap standar ISACA memungkinkan profesional audit dan penjaminan IS untuk mendekati tantangan mereka dengan pendekatan berbasis risiko yang selaras dengan metodologi ISACA.

AUDIT CHARTER

Piagam **Audit** Internal (Internal **Audit Charter**) adalah pedoman bagi **Auditor**/Internal Controller agar dapat melaksanakan tugasnya secara profesional, memperoleh hasil **Audit** yang sesuai dengan standar mutu, dan dapat diterima oleh berbagai pihak baik internal maupun external. Audit charter bisa juga diartikan sebagai Dokumen yang disetujui oleh pihak yang bertanggung jawab atas tata kelola yang mendefinisikan tujuan, wewenang dan tanggung jawab kegiatan audit internal.

Audit charter tersebut berfungsi untuk :

- Menetapkan posisi fungsi audit internal dalam perusahaan
- Otorisasi akses ke catatan, personel, dan properti fisik yang relevan dengan kinerja audit SI dan keterlibatan jaminan
- Tentukan ruang lingkup kegiatan fungsi audit

Audit Charter Hubungan dengan frame work lain dalam cobit :

Sebagai mandat dokumen formal bagi audit IT yang menyatakan tujuan, wewenang, dan tanggung jawab audit intern untuk mengontrol frame work lainnya yang dirancang untuk mencapai serangkaian tujuan spesifik terkait.

IT AUDIT

1202 Risk Assessment in Planning

Kelompok 4 (Empat)

1. Yuniarti Denita Sari
2. Raju Septa Wijaya
3. Hendri

Dosen Pengampuh : Dr. Widya Cholil, S.Kom., M.IT.

Kelas : MTI 19 Reguler **B**

Magister Teknik Informatika
PASCASARJANA
Universitas Bina Darma Palembang

2019

1202. Risk Assessment in Planning

1202.1 Fungsi audit dan penjaminan IS harus menggunakan pendekatan penilaian risiko yang sesuai dan metodologi pendukung untuk dikembangkan rencana audit SI keseluruhan dan menentukan prioritas untuk alokasi sumber daya audit SI yang efektif.

1202.2 IS audit dan jaminan profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area yang dikaji, ketika merencanakan keterlibatan individu.

1202.3 Profesional audit dan penjaminan IS harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.

Key Aspects (Aspek Kunci)

Saat merencanakan kegiatan yang sedang berlangsung, fungsi audit dan jaminan SI harus:

- Melakukan dan mendokumentasikan, setidaknya setiap tahun, penilaian risiko untuk memfasilitasi pengembangan rencana audit SI.
- Sertakan, sebagai bagian dari penilaian risiko, rencana dan sasaran strategis organisasi dan perusahaan kerangka kerja dan inisiatif manajemen risiko.
- Untuk setiap audit SI dan perikatan jaminan, menghitung dan membenarkan jumlah sumber daya audit SI yang diperlukan untuk memenuhi persyaratan keterlibatan.
- Gunakan penilaian risiko dalam pemilihan area dan item yang menjadi minat audit dan keputusan untuk merancang dan melakukan audit IS dan keterlibatan jaminan tertentu.
- Mencari persetujuan penilaian risiko dari pemangku kepentingan audit dan pihak terkait lainnya.
- Prioritaskan dan jadwalkan pekerjaan audit dan penjaminan IS berdasarkan penilaian risiko.
- Berdasarkan penilaian risiko, kembangkan sebuah rencana yang:
    - Bertindak sebagai kerangka kerja untuk aktivitas audit dan penjaminan IS
    - Mempertimbangkan persyaratan dan kegiatan audit dan jaminan non-IS
    - Diperbarui setidaknya setiap tahun dan disetujui oleh pihak yang bertanggung jawab atas tata kelola
    - Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

Saat merencanakan keterlibatan individu, profesional audit dan penjaminan IS harus:

- Identifikasi dan nilai risiko yang relevan dengan area yang dikaji.

- Melakukan penilaian awal terhadap risiko yang relevan dengan area yang dikaji untuk setiap keterlibatan. Tujuan untuk setiap keterlibatan spesifik harus mencerminkan hasil penilaian risiko awal.
- Dalam mempertimbangkan bidang-bidang risiko dan merencanakan perikatan khusus, pertimbangkan audit, tinjauan, dan temuan sebelumnya, termasuk setiap kegiatan perbaikan. Juga pertimbangkan proses penilaian risiko menyeluruh dewan.
- Berusaha untuk mengurangi risiko audit ke tingkat yang dapat diterima, dan memenuhi tujuan audit dengan tepat penilaian materi IS dan kontrol terkait, saat merencanakan dan melakukan audit IS.
- Saat merencanakan prosedur audit IS spesifik, kenali bahwa semakin rendah ambang materialitas, semakin banyak tepatkan harapan audit dan semakin besar risiko audit.
- Untuk mengurangi risiko materialitas yang lebih tinggi, ganti rugi dengan memperpanjang uji kontrol (kurangi risiko kontrol) dan / atau memperluas prosedur pengujian substantif (mengurangi risiko deteksi) untuk mendapatkan jaminan tambahan.

Terms (ISTILAH)	**Definition(DEFINISI)**
Audit risk (Risiko audit)	Risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah: • Kontrol risiko • Risiko deteksi • Risiko yang melekat
Audit subject matter risk (Risiko materi pelajaran audit)	Risiko relevan dengan area yang sedang ditinjau: • Risiko bisnis (kemampuan pelanggan untuk membayar, kelayakan kredit, faktor pasar, dll.) • Risiko kontrak (kewajiban, harga, jenis, penalti, dll.) • Risiko negara (politik, lingkungan, keamanan, dll.) • Risiko proyek (sumber daya, keahlian, metodologi, stabilitas produk, dll.) • Risiko teknologi (solusi, arsitektur, perangkat keras, dan infrastruktur perangkat lunak jaringan, saluran pengiriman, dll.)
Control risk	Risiko bahwa ada kesalahan materi yang tidak akan dicegah atau

(Kendalikan risiko)	terdeteksi pada dasar tepat waktu oleh sistem pengendalian internal.
Detection risk (Risiko deteksi)	Risiko bahwa IS akan mengaudit atau prosedur substantif profesional jaminan akan tidak mendeteksi kesalahan yang bisa bersifat material, secara individu atau dalam kombinasi dengan lainnya kesalahan.
Inherent risk (Risiko yang melekat)	Tingkat risiko atau paparan tanpa memperhitungkan tindakan yang dilakukan manajemen telah mengambil atau mungkin mengambil (mis., menerapkan kontrol).
Materiality (Materialitas)	Konsep audit mengenai pentingnya item informasi yang berkaitan dengan dampak atau pengaruhnya terhadap fungsi entitas yang diaudit. Ekspresi dari signifikansi relatif atau pentingnya suatu hal tertentu dalam konteks perusahaan secara keseluruhan.
Risk assessment (Tugas beresiko)	Suatu proses yang digunakan untuk mengidentifikasi dan mengevaluasi risiko dan potensi dampaknya. Penilaian risiko digunakan untuk mengidentifikasi item-item atau area yang menyajikan risiko tertinggi, kerentanan atau paparan terhadap perusahaan untuk dimasukkan dalam IS rencana audit tahunan. Penilaian risiko juga digunakan untuk mengelola pengiriman proyek dan proyek risiko manfaat.
Substantive testing (Pengujian substantif)	Memperoleh bukti audit tentang kelengkapan, keakuratan, atau keberadaan kegiatan atau transaksi selama periode audit

Linkage to Guidelines **(Tautan ke Pedoman)**

Tipe	Judul
Guideline(Pedoman)	2202 Penilaian Risiko dalam Perencanaan

2202 Penilaian Risiko dan Perencanaan Audit

Pedoman disajikan dalam bagian berikut:

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman

3. Keterkaitan dengan standar dan proses COBIT 5

4. Terminologi

5. Tanggal efektif

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan

Bagian ini mengklarifikasi:

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tingkat pekerjaan audit yang diperlukan untuk memenuhi tujuan audit adalah keputusan subyektif yang dibuat oleh audit IS dan profesional penjaminan. Tujuan pedoman ini adalah untuk mengurangi risiko mencapai kesalahan kesimpulan berdasarkan temuan audit dan untuk mengurangi adanya kesalahan dalam area yang diaudit.

1.1.2 Pedoman ini memberikan panduan dalam menerapkan pendekatan penilaian risiko untuk mengembangkan:

• IS rencana audit yang mencakup semua perikatan audit tahunan

• Rencana proyek perikatan audit yang berfokus pada satu perikatan audit tertentu

1.1.3 Pedoman ini memberikan perincian tentang berbagai jenis risiko audit dan jaminan IS pertemuan profesional.

1.1.4 Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

1.2 Tautan ke

Standar

1.2.1 Perencanaan Keterlibatan Standar 1201

1.2.2 Standar 1202 Penilaian Risiko dalam Perencanaan

1.2.3 Standar 1203 Kinerja dan Pengawasan

1.2.4 Material 1204 Standar

1.2.5 Standar 1207 Penyimpangan dan Tindakan Ilegal

1.3 Penggunaan Jangka

1.3.1 Selanjutnya:

- 'Fungsi audit dan penjaminan IS' disebut sebagai 'fungsi audit'
- 'Profesional audit dan penjaminan' disebut sebagai 'profesional'

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang audit dan jaminan utama berikut topik keterlibatan:

2.1 Penilaian risiko dari rencana audit SI

2.2 Metodologi penilaian risiko

2.3 Penilaian risiko perikatan audit perorangan

2.4 Risiko audit

2.5 Risiko yang melekat

2.6 Mengontrol risiko

2.7 Risiko deteksi

2.1 Risiko Penilaian atas IS Rencana Audit

2.1.1 Ketika mengembangkan rencana audit SI secara keseluruhan, pendekatan penilaian risiko yang sesuai harus diikuti. Sebuah resiko penilaian harus dilakukan dan didokumentasikan setidaknya setiap tahun untuk memfasilitasi proses pengembangan dari rencana audit IS. Ini harus mempertimbangkan rencana dan sasaran strategis organisasi dan kerangka kerja dan inisiatif manajemen risiko perusahaan.

2.1.2 Untuk menilai dengan benar dan lengkap risiko yang terkait dengan cakupan lengkap area audit IS, profesional harus mempertimbangkan elemen-elemen berikut ketika mengembangkan rencana audit SI:

- Cakupan penuh semua area dalam lingkup semesta audit IS, yang mewakili kisaran semua kemungkinan kegiatan audit
- Keandalan dan kesesuaian penilaian risiko yang disediakan oleh manajemen
- Proses diikuti oleh manajemen untuk mengawasi, memeriksa, dan melaporkan risiko atau masalah yang mungkin terjadi

- Menutup risiko dalam kegiatan terkait yang relevan dengan kegiatan yang sedang ditinjau

2.1.3 Pendekatan penilaian risiko yang diterapkan harus membantu proses penentuan prioritas dan penjadwalan IS audit dan assurance berfungsi. Ini harus mendukung pemilihan bidang dan item kepentingan audit dan proses pengambilan keputusan untuk merancang dan melakukan perikatan audit IS tertentu.

2.1.4 Profesional harus memastikan bahwa pendekatan penilaian risiko yang diterapkan disetujui oleh mereka yang dituduh pemerintahan dan didistribusikan ke berbagai pemangku kepentingan pelibatan

2.1.5 Profesional harus menggunakan penilaian risiko untuk mengukur dan membenarkan jumlah sumber daya audit SI yang dibutuhkan untuk menyelesaikan rencana audit IS dan persyaratan untuk keterlibatan khusus

2.1.6 Berdasarkan penilaian risiko, para profesional harus mengembangkan rencana audit IS yang bertindak sebagai kerangka kerja untuk kegiatan audit dan penjaminan IS. Itu harus:

- Mempertimbangkan audit dan persyaratan serta kegiatan non-SI audit
- Diperbarui setidaknya setiap tahun
- Disetujui oleh mereka yang bertanggung jawab atas tata kelola
- Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

2.2 Risiko Penilaian Metodologi

2.2.1 Profesional harus mempertimbangkan metodologi penilaian risiko yang tepat untuk memastikan lengkap dan cakupan yang akurat dari perikatan audit dalam rencana audit SI.

2.2.2 Profesional harus setidaknya menyertakan analisis, dalam metodologi, risiko yang terkait dengan perusahaan untuk ketersediaan sistem, integritas data, dan kerahasiaan informasi bisnis.

2.2.3 Banyak metodologi penilaian risiko tersedia untuk mendukung proses penilaian risiko. Ini mulai dari klasifikasi sederhana tinggi, sedang dan rendah, berdasarkan penilaian profesional, hingga lebih banyak lagi perhitungan kuantitatif dan ilmiah memberikan peringkat risiko numerik, dan lainnya yang merupakan kombinasi di antara dua. Profesional harus mempertimbangkan tingkat kompleksitas dan detail yang sesuai untuk perusahaan atau subjek yang diaudit. Panduan khusus tentang melakukan penilaian risiko dapat ditemukan di ISACA publikasi *COBIT 5 untuk Risiko* .

2.2.4 Semua metodologi penilaian risiko bergantung pada penilaian subyektif di beberapa titik dalam proses (misalnya, untuk menugaskan bobot ke berbagai parameter). Profesional harus mengidentifikasi keputusan subjektif yang diperlukan untuk menggunakan metodologi tertentu dan mempertimbangkan apakah penilaian ini dapat dibuat dan divalidasi menjadi tingkat akurasi yang sesuai.

2.2.5 Dalam memutuskan metodologi penilaian risiko mana yang paling tepat, para profesional harus mempertimbangkannya hal-hal sebagai:

- Jenis informasi yang harus dikumpulkan (beberapa sistem menggunakan efek finansial sebagai satu-satunya ukuran ini tidak selalu sesuai untuk perikatan audit IS)
- Biaya perangkat lunak atau lisensi lain yang diperlukan untuk menggunakan metodologi ini
- Sejauh mana informasi yang diperlukan sudah tersedia
- Jumlah informasi tambahan yang harus dikumpulkan sebelum hasil yang andal dapat diperoleh, dan biaya pengumpulan informasi ini (termasuk waktu yang diperlukan untuk diinvestasikan dalam latihan pengumpulan)
- Pendapat dari pengguna lain dari metodologi, dan pandangan mereka tentang seberapa baik telah membantu mereka dalam meningkatkan efisiensi dan / atau efektivitas audit mereka
- Kesediaan mereka yang bertanggung jawab atas tata kelola area audit IS untuk menerima metodologi sebagai sarana untuk menentukan jenis dan tingkat pekerjaan audit yang dilakukan

2.2.6 Tidak ada metodologi penilaian risiko tunggal yang diharapkan sesuai dalam semua situasi. Kondisi mempengaruhi audit dapat berubah seiring waktu. Secara berkala, profesional harus mengevaluasi kembali kesesuaian metodologi penilaian risiko yang dipilih.

2.2.7 Para profesional harus menggunakan teknik penilaian risiko yang dipilih dalam mengembangkan rencana audit SI keseluruhan dan dalam perencanaan pengikatan audit khusus. Penilaian risiko, dalam kombinasi dengan teknik audit lainnya, harus dipertimbangkan dalam membuat keputusan perencanaan seperti:

- Area atau fungsi bisnis yang akan diaudit
- Jumlah waktu dan sumber daya yang akan dialokasikan untuk audit

• Sifat, luas dan waktu prosedur audit

2.2.8 Metodologi penilaian risiko yang diadopsi harus menghasilkan yang konsisten, valid, dapat dibandingkan, dan dapat diulang hasil. Penilaian risiko yang keluar dari metodologi harus konsisten (selama periode), valid, sebanding (dengan penilaian awal / nanti menggunakan metodologi penilaian yang sama) dan berulang (diberikan seperangkat fakta yang serupa, menggunakan metodologi penilaian yang sama akan menghasilkan hasil yang serupa).

2.3 Risiko Penilaian terhadap Audit Hubungan Perorangan

2.3.1 Ketika merencanakan keterlibatan individu, profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area tersebut sedang ditinjau. Hasil penilaian risiko ini harus tercermin dalam tujuan perikatan audit. Selama penilaian risiko, para profesional harus mempertimbangkan:

• Hasil dari perikatan audit sebelumnya, ulasan dan temuan, termasuk kegiatan perbaikan

• Proses penilaian risiko menyeluruh perusahaan

• Kemungkinan terjadinya risiko tertentu

• Dampak risiko tertentu (dalam ukuran nilai moneter atau lainnya) jika itu terjadi

2.3.2 Profesional harus memastikan pemahaman penuh tentang kegiatan dalam ruang lingkup sebelum menilai risiko. Mereka harus meminta komentar dan saran dari pemangku kepentingan dan pihak terkait lainnya. Ini diperlukan untuk menentukan dengan benar dan memeriksa dampak dari risiko yang mungkin terjadi dalam perikatan audit.

2.3.3 Tujuan dari penilaian risiko adalah pengurangan risiko audit ke tingkat yang dapat diterima, dan mengidentifikasi bagian-bagian dari suatu kegiatan yang harus menerima lebih banyak fokus audit. Ini perlu dilakukan oleh seorang penilaian yang tepat dari masalah IS dan kontrol terkait, sambil merencanakan dan melakukan IS audit.

2.3.4 Ketika merencanakan audit IS dan prosedur jaminan tertentu, profesional harus mengenali fakta itu semakin rendah ambang materialitas, semakin tepat ekspektasi audit dan semakin besar risiko audit.

2.3.5 Ketika merencanakan audit IS dan prosedur jaminan tertentu, profesional harus mempertimbangkan kemungkinan illegal tindakan yang dapat memerlukan modifikasi sifat, waktu, atau luas prosedur yang ada. Untuk lebih informasi mengacu pada Standar 1207 Penyimpangan dan Tindakan Ilegal dan Pedoman 2207.

2.3.6 Untuk mendapatkan jaminan tambahan dalam kasus di mana ada risiko audit tinggi atau ambang batas materialitas yang lebih rendah, profesional harus memberikan kompensasi dengan memperluas ruang lingkup atau sifat tes audit IS atau meningkatkan atau memperluas pengujian substantif.

2.4 Risiko Audit

2.4.1 Risiko audit mengacu pada risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah:

- Kontrol risiko
- Risiko deteksi
- Risiko yang melekat

2.4.2 Profesional harus mempertimbangkan masing-masing komponen risiko untuk menentukan tingkat risiko secara keseluruhan. Ini termasuk risiko materi, yang mencakup risiko bawaan dan risiko kontrol; bersama dengan risiko deteksi itu kemudian disebut sebagai risiko audit. Penjelasan lebih lanjut tentang berbagai komponen risiko audit dapat ditemukan di bagian 2.5 hingga 2.7.

2.5 Risiko Inheren

2.5.1 Risiko yang melekat adalah kerentanan area audit untuk melakukan kesalahan yang dapat bersifat material, secara individu atau dalam kombinasi dengan kesalahan lain, dengan asumsi bahwa tidak ada kontrol internal terkait. Sebagai contoh, risiko inheren yang terkait dengan sistem operasi tanpa kontrol yang sesuai biasanya tinggi, karena perubahan, atau bahkan pengungkapan, data atau program melalui kelemahan keamanan sistem operasi dapat mengakibatkan informasi manajemen yang salah atau kerugian kompetitif. Sebaliknya, risiko yang melekat terkait dengan keamanan untuk PC yang berdiri sendiri tanpa kontrol, ketika analisis yang tepat menunjukkan itu tidak digunakan untuk keperluan bisnis yang kritis, biasanya rendah.

2.5.2 Risiko yang melekat untuk sebagian besar area audit IS adalah tinggi karena potensi dampak kesalahan biasanya mencakup beberapa area sistem bisnis dan banyak pengguna.

2.6 Mengontrol Risiko

2.6.1 Risiko pengendalian adalah risiko kesalahan yang dapat terjadi di area audit dan dapat bersifat material, secara individu atau dalam kombinasi dengan kesalahan lain, tidak akan dicegah atau dideteksi dan diperbaiki tepat waktu oleh sistem kontrol internal. Misalnya, risiko kontrol yang terkait dengan tinjauan manual terhadap log komputer dapat menjadi tinggi karena volume informasi yang dicatat. Risiko kontrol terkait dengan data yang terkomputerisasi prosedur validasi biasanya rendah karena proses diterapkan secara konsisten.

2.6.2 Profesional harus menilai risiko kontrol setinggi kecuali kontrol internal yang relevan adalah:

- Diidentifikasi
- Dievaluasi sebagai efektif
- Diuji dan terbukti beroperasi dengan tepat

2.6.3 Para profesional harus mempertimbangkan kontrol IS yang meresap dan terperinci:

- Kontrol IS yang meresap dianggap sebagai bagian dari kontrol umum; mereka adalah kontrol-kontrol umum itu fokus pada manajemen dan pemantauan lingkungan IS. Karena itu mereka mempengaruhi semua yang terkait IS kegiatan. Efek dari kontrol IS yang meresap pada pekerjaan profesional tidak terbatas pada keandalan kontrol aplikasi dalam sistem proses bisnis. Mereka juga mempengaruhi keandalan IS rinci mengendalikan, misalnya, pengembangan program aplikasi, implementasi sistem, administrasi keamanan dan prosedur pencadangan. Lemahnya kontrol IS yang tersebar, dan dengan demikian manajemen dan pemantauan yang lemah Lingkungan IS, harus memberi tahu para profesional tentang kemungkinan risiko tinggi yang dirancang oleh control beroperasi pada level terperinci mungkin tidak efektif.

- Kontrol IS terperinci terdiri dari kontrol aplikasi ditambah kontrol umum yang tidak termasuk dalam kontrol IS meresap. Mengikuti kerangka COBIT, mereka adalah kontrol atas akuisisi, implementasi, pengiriman dan dukungan sistem dan layanan IS.

2.6.4 Risiko yang harus dipertimbangkan oleh para profesional adalah keterbatasan dan kekurangan dalam IS rinci yang mengontrolnya diinduksi oleh ketidakcukupan kontrol IS meresap.

2.7 Risiko Deteksi

2.7.1 Risiko deteksi adalah risiko bahwa prosedur substantif profesional tidak akan mendeteksi kesalahan yang mungkin terjadi materi, secara individu atau dalam kombinasi dengan kesalahan lain. Misalnya, risiko deteksi terkait dengan mengidentifikasi pelanggaran keamanan dalam sistem aplikasi biasanya tinggi karena log untuk seluruh periode audit tidak tersedia pada saat audit. Risiko deteksi terkait dengan mengidentifikasi kekurangan rencana pemulihan bencana biasanya rendah, karena keberadaannya mudah diverifikasi.

2.7.2 Dalam menentukan tingkat pengujian substantif yang diperlukan, para profesional harus mempertimbangkan:

• Penilaian risiko yang melekat

• Kesimpulan dicapai pada risiko kontrol setelah pengujian kepatuhan

2.7.3 Semakin tinggi penilaian risiko bawaan dan risiko kontrol, semakin banyak bukti audit yang harus dimiliki oleh para professional biasanya diperoleh dari kinerja prosedur audit substantif.

3. Keterkaitan dengan Standar dan Proses COBIT 5

3.0 Pendahuluan

Bagian ini memberikan ikhtisar yang relevan:

3.1 Keterkaitan dengan standar

3.2 Keterkaitan dengan proses COBIT 5

3.3 Pedoman lain

3.1 Tautan ke

Standar

Tabel ini memberikan gambaran umum tentang:

• Standar ISACA paling relevan yang secara langsung didukung oleh pedoman ini

• Pernyataan standar yang paling relevan dengan pedoman ini

Catatan: Hanya pernyataan standar yang relevan dengan pedoman ini yang terdaftar.

Judul Standar	Pernyataan Standar yang Relevan
1201 Keterlibatan Perencanaan	Profesional audit dan penjaminan IS harus merencanakan setiap audit dan perikatan jaminan IS untuk mengatasi: • Tujuan, cakupan, garis waktu, dan hasil • Kepatuhan terhadap hukum yang berlaku dan standar audit profesional • Penggunaan pendekatan berbasis risiko, jika perlu • Masalah khusus keterlibatan • Persyaratan dokumentasi dan pelaporan
1202 Penilaian Risiko dalam Perencanaan	Fungsi audit dan penjaminan IS harus menggunakan pendekatan penilaian risiko yang tepat dan mendukung metodologi untuk mengembangkan rencana audit SI keseluruhan dan menentukan prioritas untuk alokasi efektif sumber daya audit IS. IS audit dan jaminan profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area tersebut sedang ditinjau, saat merencanakan keterlibatan individu. Profesional audit dan penjaminan IS harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.
1203 Kinerja dan	IS profesional audit dan jaminan akan melakukan pekerjaan sesuai

Pengawasan	dengan rencana audit SI yang disetujui untuk mencakup risiko yang teridentifikasi dan dalam jadwal yang disepakati.
1204 Materialitas	Profesional audit dan penjaminan IS harus mempertimbangkan potensi kelemahan atau ketidakhadiran mengontrol sementara merencanakan suatu pertunangan, dan apakah kelemahan atau ketidakhadiran tersebut kontrol dapat menyebabkan defisiensi signifikan atau kelemahan material. Profesional audit dan penjaminan IS harus mempertimbangkan materialitas dan hubungannya dengan audit risiko sambil menentukan sifat, waktu dan tingkat prosedur audit. Profesional audit dan penjaminan IS harus mempertimbangkan efek kumulatif minor mengendalikan kekurangan atau kelemahan dan apakah tidak adanya kendali diterjemahkan menjadi defisiensi signifikan atau kelemahan material. IS profesional audit dan jaminan harus mengungkapkan hal berikut dalam laporan: • Tidak adanya kontrol atau kontrol tidak efektif • Signifikansi dari defisiensi control • Kemungkinan kelemahan ini mengakibatkan defisiensi signifikan atau kelemahan material
1207 Penyimpangan dan Tindakan Ilegal	IS profesional audit dan penjaminan akan mempertimbangkan risiko penyimpangan dan tindakan ilegal selama pertunangan.

3.2 Tautan ke

COBIT 5

Proses

Tabel ini memberikan ikhtisar yang paling relevan:

• proses COBIT 5

• Tujuan proses COBIT 5

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam *COBIT 5: Proses yang Memampukan.*

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pemerintahan pengaturan kerangka kerja dan pemeliharaan.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan keputusan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
EDM03 Pastikan risiko optimasi.	Pastikan bahwa risiko perusahaan yang terkait dengan TI tidak melebihi selera risiko dan toleransi risiko, dampak risiko IT terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi untuk kegagalan kepatuhan diminimalkan.
APO12 Kelola risiko.	Mengintegrasikan manajemen risiko perusahaan terkait TI dengan ERM secara keseluruhan, dan menyeimbangkannya biaya dan manfaat mengelola risiko perusahaan terkait TI.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.
MEA03 Monitor, mengevaluasi dan menilai kepatuhan dengan persyaratan eksternal.	Pastikan perusahaan mematuhi semua persyaratan eksternal yang berlaku.

3.3 Panduan Lain

Ketika menerapkan standar dan pedoman, para profesional didorong untuk mencari panduan lain, ketika dipertimbangkan perlu. Ini bisa dari audit IS dan jaminan:

- Kolega dari dalam organisasi dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau
- kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam organisasi, misalnya, komite audit
- Panduan lain (misalnya, buku, makalah, pedoman lainnya)

4. Terminologi

Istilah	Definisi
Piagam audit	Dokumen yang disetujui oleh pihak yang bertanggung jawab atas tata kelola yang mendefinisikan tujuan, wewenang dan tanggung jawab audit IS internal dan kegiatan penjaminan Piagam tersebut harus: • Menetapkan posisi audit IS dan fungsi jaminan internal di dalam perusahaan • Mengesahkan akses ke catatan, personel, dan properti fisik yang relevan dengan kinerja audit SI dan keterlibatan jaminan • Menentukan ruang lingkup kegiatan audit IS dan fungsi jaminan
Risiko audit	Risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah: • Kontrol risiko • Risiko deteksi • Risiko yang melekat
Kendalikan risiko	Risiko bahwa ada kesalahan materi yang tidak dapat dicegah atau terdeteksi pada waktu yang tepat dasar oleh sistem pengendalian internal.

Kontrol IS terperinci	Kontrol atas akuisisi, implementasi, pengiriman dan dukungan sistem IS dan layanan yang terdiri dari kontrol aplikasi ditambah kontrol umum yang tidak termasuk dalam kontrol meresap
Risiko deteksi	Risiko yang tidak IS audit atau prosedur substantif profesional tidak akan mendeteksi kesalahan yang bisa bersifat material, secara individu atau dalam kombinasi dengan kesalahan lainnya.
Risiko yang melekat	Tingkat risiko atau paparan tanpa memperhitungkan tindakan yang dimiliki manajemen diambil atau mungkin diambil (misalnya, menerapkan kontrol).
Materialitas	Konsep audit mengenai pentingnya item informasi yang berkaitan dengan dampak atau pengaruhnya terhadap subjek yang diaudit. Ekspresi kerabat signifikansi atau pentingnya suatu masalah tertentu dalam konteks pertunangan atau perusahaan secara keseluruhan.
Tugas beresiko	Suatu proses yang digunakan untuk mengidentifikasi dan mengevaluasi risiko dan potensi dampaknya Penilaian risiko digunakan untuk mengidentifikasi item-item atau bidang-bidang yang menghadirkan risiko tertinggi, kerentanan atau paparan terhadap perusahaan untuk dimasukkan dalam rencana audit tahunan SI. Penilaian risiko juga digunakan untuk mengelola pengiriman proyek dan risiko manfaat proyek.
Kontrol IS yang meresap	Kontrol umum yang dirancang untuk mengelola dan memantau lingkungan IS dan yang, oleh karena itu, mempengaruhi semua aktivitas terkait IS
Pengujian substantif	Memperoleh bukti audit tentang kelengkapan, keakuratan atau keberadaan kegiatan atau transaksi selama periode audit

ASSERTION (PENEGASAN)

BAGIAN 1007

Nama kelompok :

Zena Lusi

Try akhyari romadhon

Abi daud

PENGERTIAN ASSERTION (PENEGASAN)

- IS profesional audit dan penjaminan harus meninjau kembali pernyataan yang menjadi dasar subjek masalah akan dinilai untuk menentukan bahwa pernyataan tersebut dapat diaudit dan bahwa pernyataan itu cukup, valid dan relevan.
- IS profesional audit dan jaminan harus menilai, meninjau dan mengevaluasi pekerjaan orang lain ahli sebagai bagian dari perjanjian, dan mendokumentasikan kesimpulan tentang tingkat penggunaan dan mengandalkan pekerjaan mereka.

ASPEK KUNCI ASSERTION (PENEGASAN)

- Mengevaluasi kriteria yang akan dinilai subjeknya untuk memastikan mereka mendukung asersi.
- Menentukan apakah asersi dapat diaudit dan didukung oleh informasi yang menguatkan.
- Menentukan apakah asersi didasarkan pada kriteria yang ditentukan secara tepat dan tunduk pada analisis objektif dan terukur.
- Di mana asersi telah dikembangkan oleh manajemen, pastikan bahwa, bila dibandingkan dengan standar lain dari pernyataan otoritatif bahwa pernyataan tersebut cukup sehubungan dengan apa yang pembaca yang berpengetahuan atau pengguna harapkan.
- Di mana pernyataan telah dikembangkan oleh pihak ketiga yang mengoperasikan kontrol atas nama perusahaan, memastikan bahwa asersi diverifikasi dan diterima oleh manajemen.
- Melaporkan secara langsung terhadap subjek (laporan langsung) atau terhadap pernyataan tentang subjek masalah (laporan tidak langsung).
- Bentuk kesimpulan tentang setiap asersi, berdasarkan pada agregat temuan terhadap kriteria bersama penilaian profesional.

KETENTUAN ASSERTION (PENEGASAN)

- Deklarasi formal atau set deklarasi apa pun yang dibuat oleh manajemen.
- Penegasan biasanya harus secara tertulis dan biasanya berisi daftar spesifik atribut tentang materi pelajaran tertentu atau tentang proses yang melibatkan materi pelajaran.

KRITERIA ASSERTION (PENEGASAN)

IS profesional audit dan penjaminan harus memilih kriteria, di mana materi pelajaran akan dinilai, yang objektif, lengkap, relevan, dapat diukur, dimengerti, diakui secara luas, berwibawa dan dipahami oleh, atau tersedia untuk, semua pembaca dan pengguna laporan.

Materialitas ASSERTION (PENEGASAN)

- Tidak adanya kontrol atau kontrol tidak efektif
- Signifikansi dari defisiensi kontrol
- Kemungkinan kelemahan ini mengakibatkan defisiensi signifikan atau kelemahan material

PEDOMAN ASSERTION (PENEGASAN)

1. Tujuan pedoman dan keterkaitan dengan standar

- Tujuan dari pedoman ini adalah untuk merinci berbagai asersi, panduan IS audit dan profesional penjaminan dalam memastikan bahwa kriteria, yang menjadi dasar penilaian masalah, mendukung pernyataan, dan memberikan panduan untuk merumuskan kesimpulan dan menyusun laporan tentang asersi.
- Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

2. Konten pedoman

3. Keterkaitan dengan standar dan proses COBIT 5

4. Terminologi

5. Tanggal efektif

Standar Pelaporan ASSERTION (PENEGASAN)

- Identifikasi perusahaan, penerima yang dituju dan segala batasan pada konten dan sirkulasi
- Cakupan, tujuan keterlibatan, periode cakupan dan sifat, waktu, dan luasnya pekerjaan yang dilakukan
- Temuan, kesimpulan dan rekomendasi
- Setiap kualifikasi atau batasan dalam ruang lingkup yang dimiliki oleh audit SI dan profesional penjaminan sehubungan dengan pertunangan
- Tanda tangan, tanggal dan distribusi sesuai dengan ketentuan piagam audit atau surat pertunangan

Ketika menerapkan standar dan pedoman, para profesional didorong untuk mencari panduan lain ketika dipertimbangkan perlu. Ini bisa dari audit IS dan jaminan:

- Kolega dari dalam organisasi dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam organisasi, misalnya, komite audit
- Panduan lain (misalnya, buku, makalah, pedoman lainnya)

KETERKAITAN DENGAN PROSES COBIT 5

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam COBIT 5: Proses yang Memampukan.

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pemerintahan pengaturan kerangka kerja dan pemeliharaan.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan keputusan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

TERMININOLOGI ASSERTION (PENEGASAN)

ISTILAH	Definisi
Tuntutan	Deklarasi formal atau set deklarasi apa pun yang dibuat oleh manajemen
Kriteria	Standar dan tolok ukur yang digunakan untuk mengukur dan menyajikan materi pelajaran dan dimana auditor SI mengevaluasi materi pelajaran. Kriteria harus: • Objektif — Bebas dari bias • Lengkap — Sertakan semua faktor yang relevan untuk mencapai kesimpulan • Relevan — Berkaitan dengan pokok pembicaraan • Terukur — Menyediakan pengukuran yang konsisten • Dapat dimengerti Dalam pengikatan pengesahan, tolok ukur terhadap mana pernyataan tertulis manajemen pada materi pelajaran dapat dievaluasi. Praktisi membentuk kesimpulan tentang materi pelajaran dengan mengacu pada kriteria yang sesuai. Penilaian profesional Penerapan pengetahuan dan pengalaman yang relevan dalam membuat keputusan berdasarkan informasi tentang program tindakan yang sesuai dalam keadaan audit IS dan keterlibatan jaminan
Subjek	Informasi spesifik tunduk pada laporan auditor SI dan prosedur terkait, yang dapat mencakup hal-hal seperti desain atau operasi kontrol internal dan kepatuhan praktik atau standar privasi atau hukum dan peraturan tertentu (bidang kegiatan)

IS Audit dan Jaminan Standar
1001 Audit Charter

Sifat khusus dari sistem informasi (IS) audit dan jaminan dan keterampilan yang diperlukan untuk melakukan keterlibatan seperti ini membutuhkan standar yang berlaku secara khusus untuk IS audit dan jaminan.

Pengembangan dan penyebaran audit dan jaminan standar IS adalah landasan ISACA yang® kontribusi profesional untuk masyarakat audit.

IS audit dan jaminan standar menetapkan persyaratan wajib bagi IS audit dan pelaporan dan menginformasikan:

- IS audit dan jaminan profesional dari tingkat minimum kinerja yang dapat diterima yang diperlukan untuk memenuhi tanggung jawab profesional yang ditetapkan dalam Kode ISACA Etik Profesional
- Manajemen dan pihak berkepentingan lainnya dari harapan profesi tentang pekerjaan praktisi
- Pemegang Auditor Bersertifikat Sistem Informasi® (CISA®) Penunjukan persyaratan. Kegagalan untuk mematuhi standar ini dapat mengakibatkan penyelidikan perilaku pemegang CISA oleh ISACA Direksi atau komite yang sesuai dan, pada akhirnya, tindakan disiplin.

IS audit dan jaminan profesional harus mencakup pernyataan dalam pekerjaan mereka, dimana tepat, bahwa pertunangan telah dilakukan sesuai dengan ISACA IS audit dan jaminan standar atau standar profesional yang berlaku lainnya.

The ITAF ™ kerangka kerja untuk IS audit dan jaminan profesional menyediakan beberapa tingkat bimbingan:

- **standar**, Dibagi menjadi tiga kategori:
  - standar umum (1000 series) -Apakah prinsip-prinsip di mana IS audit dan jaminan profesi beroperasi. Mereka berlaku untuk pelaksanaan semua tugas, dan berurusan dengan audit IS dan etika jaminan profesional, independensi, objektivitas dan perawatan karena serta pengetahuan, kompetensi dan keterampilan. Laporan standar (dalam huruf tebal) adalah wajib.
  - standar kinerja (1200 series) -Deal dengan pelaksanaan tugas, seperti perencanaan dan pengawasan, scoping, risiko dan materialitas, mobilisasi sumber daya, pengawasan dan manajemen tugas, audit dan bukti jaminan, dan berolahraga pertimbangan profesional dan perawatan karena
  - standar (1400 series) -Address jenis laporan pelaporan, berarti komunikasi dan informasi yang dikomunikasikan
- **pedoman**, Mendukung standar dan juga dibagi menjadi tiga kategori:
  - Pedoman umum (2000 series)
  - pedoman kinerja (2200 series)
  - pedoman pelaporan (2400 series)
- **Alat dan teknik**, Memberikan bimbingan tambahan untuk IS audit dan jaminan profesional, misalnya, kertas putih, IS audit / program jaminan, COBIT yang® 5 keluarga produk

Sebuah glossary online istilah yang digunakan dalam ITAF disediakan di www.isaca.org/glossary.

Penolakan: ISACA telah merancang pedoman ini sebagai tingkat minimum kinerja yang dapat diterima yang diperlukan untuk memenuhi tanggung jawab profesional diatur dalam Kode Etik ISACA profesional. ISACA tidak membuat klaim yang menggunakan produk ini akan menjamin hasil yang sukses. publikasi tidak harus dianggap termasuk prosedur yang tepat dan tes atau eksklusif prosedur lain dan tes yang cukup diarahkan untuk memperoleh hasil yang sama. Dalam menentukan kepatutan dari setiap prosedur atau tes khusus, kontrol profesional harus menerapkan pertimbangan profesional mereka sendiri dengan keadaan kontrol tertentu disajikan oleh sistem tertentu atau IS lingkungan.

The ISACA Standar Profesional dan Manajemen Karir Komite (PSCMC) berkomitmen untuk konsultasi luas dalam penyusunan standar dan bimbingan. Sebelum mengeluarkan dokumen, sebuah draft eksposur dikeluarkan internasional untuk komentar publik umum. Komentar juga dapat disampaikan kepada perhatian direktur pengembangan standar profesional melalui email (standards@isaca.org), fax (1,847. 253,1443) atau surat pos (ISACA Markas International, 3701 Algonquin Road, Suite 1010, di Rolling Meadows, IL 60008-3105, USA).

laporan

1001,1 IS audit dan jaminan fungsi harus mendokumentasikan fungsi audit secara tepat dalam piagam audit, menunjukkan tujuan, tanggung jawab, wewenang dan akuntabilitas.

1001,2 IS audit dan jaminan fungsi harus memiliki piagam Audit disepakati dan disetujui pada tingkat yang sesuai dalam perusahaan.

Aspek kunci

IS audit dan jaminan fungsi harus:

- Siapkan piagam Audit untuk menentukan kegiatan internal IS audit dan jaminan fungsi dengan cukup detail untuk berkomunikasi:
  - Otoritas, tujuan, tanggung jawab dan keterbatasan audit dan jaminan fungsi IS
  - Kemerdekaan dan akuntabilitas IS audit dan jaminan fungsi
  - Peran dan tanggung jawab dari auditee selama keterlibatan Audit IS atau keterlibatan Jaminan
  - standar profesional yang audit IS dan jaminan profesional akan mengikuti pelaksanaan IS audit dan jaminan keterlibatan
- Tinjau audit charter setidaknya setiap tahun, atau lebih sering jika tanggung jawab berubah.
- Update piagam audit diperlukan untuk memastikan bahwa tujuan dan tanggung jawab telah dan tetap didokumentasikan secara tepat.
- Secara formal berkomunikasi piagam audit untuk auditee untuk setiap IS audit atau jaminan keterlibatan.

Syarat

Istilah	Definisi
Jaminan keterikatan	Pemeriksaan obyektif bukti untuk tujuan memberikan penilaian pada manajemen risiko, mengontrol atau proses tata kelola untuk perusahaan. Lingkup catatan: Contoh mungkin termasuk keuangan, kinerja, kepatuhan dan sistem keterlibatan keamanan
piagam Audit	Sebuah dokumen disetujui oleh pihak yang bertanggung jawab pemerintahan yang mendefinisikan tujuan, wewenang dan tanggung jawab dari internal kegiatan audit. piagam harus: • Menetapkan posisi fungsi audit internal ini dalam perusahaan • Otorisasi akses ke catatan, personil dan sifat fisik relevan dengan kinerja audit IS dan jaminan pertunangan • Mendefinisikan ruang lingkup kegiatan fungsi audit
Audit keterikatan	Sebuah penugasan audit tertentu, tugas atau review kegiatan, seperti audit, kontrol tinjauan self-assessment, pemeriksaan penipuan atau konsultasi. Perikatan audit dapat mencakup beberapa tugas atau kegiatan

	dirancang untuk mencapai satu set spesifik tujuan yang terkait.
Kemerdekaan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. ancaman tersebut ke objektivitas harus dikelola pada auditor individual, keterlibatan, fungsional dan tingkat organisasi. Kemerdekaan meliputi kemerdekaan pikiran dan independensi dalam penampilan.

Keterkaitan dengan Pedoman

Tipe	Judul
garis pedoman	2001 Piagam Audit

operative Tanggal

standar ISACA ini efektif untuk semua IS audit dan jaminan keterlibatan mulai 1 November 2013.

PROFESSIONAL INDEPENDENCE

Information Technology Assurance Framework atau 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.

ITAF dibagi menjadi tiga kategori:

1. Standar Umum (1000 series)

   Prinsip panduan di mana profesi penjamin SI beroperasi. Mereka berlaku untuk perilak semua penugasan, dan berurusan dengan audit SI dan etika profesi, kemandirian, obyektivitas dan perawatan yang wajar serta pengetahuan, kompetensi dan keterampilan

2. Standar kinerja (1200 series)

   Berharap dengan pelaksanaan penugasan, seperti perencanaan dan pengawasan, pelingkupan, risiko dan materialitas, mobilisasi sumber daya, pengawasan dan manajemen penugasan, bukti audit dan jaminan, dan pelaksanaan professional penilaian dan perawatan yang tepat

3. Standar Pelaporan (1400 series)

   Jenis laporan, berarti komunikasi dan informasi yang dikomunikasikan oleh audit dan penjamin SI.

   Ada beberapa hal yang dibahasa dalam dokumen pada bagian standart umum. Dan pada bagian ini, akan dijelakan mengenai professional independen.

1. Standart Umum

1.1 Profesioanal independen

Bahwa seoarang auditor dan penjamin SI harus harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang berkaitan dengan audit dan pemeriksaan.

Auditor dan pemeriksa yang professional harus memiliki sikap sikap yaitu :

1. Melakukan audit atau pemeriksaan dengan kerangka pikir yang adil dan tidak memihak dalam menyikapi masalah jaminan dan mencapai kesimpulan.
2. Harus Independen sebenarnya, walapun terkadang tidak selalu harus independen setiap saat.
3. Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat
4. Menilai independensi secara teratur dengan manajemen dan komite audit, jika ada.
5. Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karenanya peran tersebut dapat merusak independensi di masa depan.

2. Pedoman audit dan penjamin SI

Tujuan pedoman ini adalah untuk menyediakan kerangka kerja yang memungkinkan audit dan penjamin SI profesional untuk:

1. Mengetahui kapan seorang audit dan penjamin merasa dalam kondisi ke-indipenenannya terancam atapun terganggu.
2. Melakukan suatu pendekatan alternative ketika proses audit berjalan dan ke-indipenenannya sedang dan atau mungkin terganggu.
3. Mengurangi atau menghilangkan dampak akibat ke-indipenenan audit SI dan kinerja professional seorang penjamin, peran, fungsi dan layanan non audit
4. Menentukan persyaratan untuk penilaian ketika ke-indipenenan merasa terganggu

2.1 Kerangka kerja konseptual

Pedoman ini menetapkan kerangka kerja konseptual yang membutuhkan profesional untuk mengidentifikasi, mengevaluasi, dan menangani ancaman terhadap independensi. Kerangka kerja konseptual pendekatan membantu dalam mematuhi standar independensi, dan mengakomodasi banyak variasi dalamkeadaan yang menciptakan ancaman bagi kemerdekaan.

2.2 Ancaman dan perlindungan

2.2.1 Ancaman

Ancaman dapat diciptakan oleh berbagai hubungan dan keadaan. Ketika suatu hubungan atau keadaan menciptakan ancaman, ancaman seperti itu dapat merusak, atau bisa dianggap merusak, keprofessionalan independen.

Ancamandapat dikatagorikan kedalam beberapak bentuk yaitu :

1. Kepentingan pribadi

   Ancaman bahwa kepentingan finansial atau lainnya akan memengaruhi penilaian profesional atau perilaku yang tidak tepat

2. Tinjauan diri sendiri

   Ancaman bahwa profesional tidak akan secara tepat mengevaluasi hasil dari mereka lakukan sendiri.

3. Advokasi

   Bahwa seoarang profeisonal akan dipromosikan oleh pihak yang diaudit.

4. Keakraban

   Ancaman yang disebabkan oleh hubungan yang dimiliki oleh auditor dengan pihak yang diaudit.

5. Intimidasi

   Ancaman yang diterima oleh seorang auditor karena dalam keadaan tertekan.

6. Bias

   Ancaman yang akan ditimbulkan oleh para profesional, sebagai akibat dari politik, ideologis, sosial, psikologis, keyakinan aatu lainnya

7. Partisipasi manajemen

   Ancaman yang dihasilkan oleh para profesional yang mengambil peran manajemen atau menjalankan fungsi manajemen atas nama entitas yang menjalani audit atau jaminan keterikatan

2.2.2 Perlindungan

kontrol yang dirancang untuk menghilangkan ancaman terhadap independensi atau menguranginnya.

Contoh perlindungan yang dapat dipertimbangkan oleh para profesional dalam menanggapi ancaman yang diidentifikasi adalah:

1. Sruktur tata kelola di perusahaan dan fungsi audit yang menyediakan pengawasan dan komunikasi mengenai audit SI dan layanan jaminan yang akan dilakukan
2. Memastikan bahwa profesional (dan manajemen audit IS) melapor ke tingkat hierarki yang memadai dalam perusahaan, terutama yang bertanggung jawab atas tata kelola
3. Prosedur internal di perusahaan dan fungsi audit yang memastikan pilihan obyektif dalam penugasan keterlibatan, misalnya, persyaratan pendidikan, pelatihan dan pengalaman yang memadai, melanjutkan professional persyaratan pengembangan
4. Menugaskan manajemen dan staf dari luar fungsi audit, seperti meminjam staf dari yang lain fungsi, divisi, organisasi eksternal, untuk melengkapi para professional

5. Sistem insentif (ganjaran dan penalti) yang memadai yang memberi penghargaan bagi profesional karena kritis dan berpikir objektif dan menghukum bias atau prasangka
6. Rotasi berkala dalam penugasan audit IS dari para profesional yang mengurangi tingkat keakraban dan tinjauan sendiri
7. Praktik perekrutan yang memadai seperti skrining latar belakang dan skrining, yang dapat meningkatkan kemungkinan bahwa profesional bebas dari bias atau kepentingan pribadi
8. Menghapus seseorang dari tim audit IS ketika minat atau hubungan individu tersebut menimbulkan ancaman terhadap kemerdekaan
9. Dokumentasi yang sesuai dan persyaratan pelaporan memastikan penilaian professional independensi didokumentasikan dalam kertas kerja dan secara konsisten dilaporkan dalam hasil
10. Memiliki anggota staf profesional atau manajemen dari dalam fungsi audit yang bukan anggota tim audit IS dengan hati-hati meninjau pekerjaan yang dilakukan
11. Menetapkan sumber daya independen, dari dalam fungsi audit atau sumber lain yang dirujuk sebelumnya, untuk melakukan peer review atau bertindak sebagai pengamat independen selama perencanaan, kerja lapangan dan pelaporan
12. Memiliki peninjauan eksternal atas laporan, komunikasi atau informasi yang dihasilkan oleh para profesional oleh pihak ketiga yang diakui, misalnya, otoritas yang diterima di lapangan atau spesialis independen
13. Mengalihdayakan audit SI dan keterlibatan jaminan ke penyedia layanan eksternal

Mengelola ancaman

Ketika fungsi audit dan profesional mengidentifikasi ancaman terhadap independensi dan, berdasarkan evaluasi

ancaman-ancaman itu, tentukan bahwa ancaman-ancaman itu tidak pada tingkat yang dapat diterima, mereka harus:

• Menentukan apakah perlindungan yang sesuai tersedia dan dapat diterapkan untuk menghilangkan ancaman atau

menguranginya ke tingkat yang dapat diterima.

• Latihan penilaian profesional dalam membuat tekad itu, dan harus mempertimbangkan apakah keduanya

kemandirian pikiran dan kemandirian dalam penampilan dipertahankan.

• Mencari bimbingan dari pihak-pihak yang tepat, seperti dijelaskan dalam 2.1.5, untuk mengidentifikasi dan menerapkan yang sesuai

perlindungan.

2.3.5

Dokumentasi memberikan bukti penilaian profesional dalam membentuk kesimpulan tentang kepatuhan

dengan persyaratan independensi.

2.3.6

Profesional harus mendokumentasikan kesimpulan tentang kepatuhan terhadap persyaratan independensi dan

substansi setiap diskusi yang relevan dengan manajemen audit dan, jika perlu, mereka yang dituduh

pemerintahan, yang mendukung kesimpulan tersebut, termasuk:

• Langkah-langkah yang diambil untuk menganalisis sifat kemerdekaan

• Sifat sebenarnya dari masalah kemerdekaan

• Daftar dan deskripsi ancaman

• Kesimpulan akhir tercapai

• Perlindungan diterapkan untuk menghilangkan atau mengurangi ancaman ke tingkat yang dapat diterima

2.4 Layanan atau peran non-audit

Di banyak perusahaan, harapan manajemen, staf IS dan audit internal adalah bahwa para profesional mungkin

terlibat dalam menyediakan layanan atau peran non-audit seperti:

• Menentukan strategi SI yang berkaitan dengan bidang-bidang seperti teknologi, aplikasi dan sumber daya

• Mengevaluasi, memilih dan mengimplementasikan teknologi

• Mengevaluasi, memilih, menyesuaikan dan mengimplementasikan aplikasi dan solusi IS pihak ketiga

• Merancang, mengembangkan, dan mengimplementasikan aplikasi dan solusi SI yang dibuat khusus

• Menetapkan praktik, kebijakan, dan prosedur yang baik terkait berbagai fungsi TI

• Merancang, mengembangkan, menguji dan menerapkan keamanan TI dan kontrol TI

• Mengelola proyek TI

2.4.2

Menyediakan layanan atau peran non-audit, secara umum, melibatkan partisipasi penuh atau paruh waktu dalam inisiatif TI

dan tim proyek TI untuk menyediakan kemampuan penasehat atau konsultatif. IS dan profesional penjaminan mungkin

memenuhi fungsi non-audit melalui kegiatan seperti:

• Penugasan sementara penuh waktu atau pinjaman staf audit dan penjaminan IS untuk tim proyek TI

• Penugasan paruh waktu dari anggota staf audit dan jaminan SI sebagai anggota berbagai proyek TI

struktur, seperti kelompok pengarah proyek, kelompok kerja proyek, tim evaluasi, negosiasi dan tim kontraktor, tim implementasi, tim jaminan kualitas dan tim penembakan masalah

• Bertindak sebagai penasihat atau peninjau proyek TI atau kontrol TI atas dasar ad hoc

2.4.3 Menyediakan layanan atau peran non-audit dapat menciptakan ancaman terhadap independensi profesional dalam sikap atau

penampilan yang bisa sangat sulit diatasi dengan perlindungan jika area di mana non-audit layanan atau peran yang dilakukan saat ini adalah, atau di masa depan menjadi, subjek audit atau keterlibatan jaminan. Dalam situasi ini, persepsi bisa berupa independensi dan objektivitas profesional telah dirugikan oleh kinerja layanan atau peran non-audit.

2.4.4

Profesional yang menyediakan layanan atau peran non-audit harus mengevaluasi, menggunakan kerangka kerja konseptual, apakah

layanan atau peran non-audit menghasilkan gangguan independensi baik dalam sikap maupun penampilan

untuk audit atau perikatan jaminan saat ini atau di masa depan. Ini berlaku untuk keterlibatan di mana area di mana

layanan atau peran non-audit yang dilakukan signifikan atau materialitas terhadap subjek atau pemangku kepentingan

dari keterlibatan itu. Profesional harus mencari panduan dari rekan audit dan penjaminan IS dan manajemen bila perlu, dan juga, jika perlu, dari pihak yang bertanggung jawab atas tata kelola, untuk menentukan

jika perlindungan yang memadai dapat diterapkan untuk memitigasi secara memadai setiap ancaman aktual atau yang dirasakan

kemerdekaan

2.4.5

Sebelum memulai layanan atau peran non-audit, profesional harus menetapkan dan mendokumentasikannya

pemahaman dengan manajemen audit IS dan / atau pihak yang bertanggung jawab atas tata kelola, sebagaimana mestinya, mengenai:

• Tujuan layanan atau peran non-audit

• Sifat layanan atau peran non-audit yang akan dilakukan

• Penerimaan tanggung jawab entitas yang diaudit terkait dengan layanan atau peran non-audit

• Tanggung jawab profesional terkait dengan layanan atau peran non-audit

• Batasan apa pun dari layanan atau peran non-audit

• Setiap batasan pada ruang lingkup jasa audit profesional di masa depan dapat berikan

2.4.6

Dalam kasus audit SI atau perikatan jaminan di mana ada potensi gangguan independensi di

sikap atau penampilan karena layanan atau peran non-audit yang dilakukan, IS audit dan manajemen jaminan

harus menerapkan perlindungan seperti:

• Memantau pelaksanaan audit dengan cermat

• Mengevaluasi setiap indikasi signifikan dari penurunan independensi dalam sikap atau penampilan yang muncul

layanan atau peran non-audit yang dilakukan dan memulai perlindungan yang diperlukan

• Memberi tahu mereka yang bertanggung jawab atas tata kelola tentang potensi penurunan nilai dalam sikap atau

penampilan dan perlindungan diterapkan

2.5 Layanan atau peran non-audit yang tidak mengganggu independensi

Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggap

tidak menjadi tanggung jawab manajemen dan karenanya tidak akan mengganggu independensi. Selanjutnya, menyediakan

saran dan rekomendasi untuk membantu manajemen dalam melaksanakan tanggung jawabnya tidak dianggap sebagai

memikul tanggung jawab manajemen.

2.5.2

Layanan atau peran non-audit yang juga tidak akan merusak independensi atau objektivitas jika perlindungan memadai

diimplementasikan termasuk memberikan saran rutin tentang risiko dan kontrol TI.

2.5.3

Untuk menghindari risiko memikul tanggung jawab manajemen ketika menyediakan layanan atau peran non-audit dalam suatu

area yang sedang atau bisa menjadi subjek audit atau perikatan jaminan, profesional hanya boleh memberikan layanan atau peran non-audit jika puas bahwa manajemen melakukan atau akan melakukan hal berikut

fungsi sehubungan dengan layanan atau peran non-audit:

• Mengemban semua tanggung jawab manajemen

• Mengawasi layanan dengan menunjuk seorang individu, lebih disukai dalam manajemen senior, yang memiliki

keterampilan, pengetahuan, atau pengalaman yang sesuai

• Mengevaluasi kecukupan dan hasil layanan yang dilakukan

• Menerima tanggung jawab atas hasil layanan

Profesional harus mendokumentasikan pertimbangan kemampuan manajemen untuk secara efektif mengawasi non-audit

layanan atau peran yang harus dilakukan.

2.6 Layanan atau peran non-audit yang merusak independensi

Jika para profesional mengambil tanggung jawab manajemen atau melakukan kegiatan manajemen, ancaman itu

menuju independensi dapat menjadi sangat penting sehingga tidak ada perlindungan yang dapat menguranginya menjadi dapat diterima

tingkat. Apakah suatu kegiatan merupakan tanggung jawab manajemen tergantung pada keadaan dan membutuhkan

latihan penilaian profesional. Contoh kegiatan yang umumnya akan dianggap sebagai manajemen tanggung jawab meliputi:

• Menetapkan kebijakan dan arahan strategis

• Mengarahkan dan bertanggung jawab atas tindakan karyawan entitas

• Otorisasi transaksi

• Memutuskan rekomendasi fungsi audit, fungsi audit internal, organisasi, perusahaan atau lainnya pihak ketiga untuk diimplementasikan

• Bertanggung jawab untuk merancang, mengimplementasikan, atau mempertahankan kontrol internal

• Menerima tanggung jawab atas pengelolaan proyek atau inisiatif TI

2.6.2

Selain memikul tanggung jawab manajemen, layanan atau peran non-audit berikut adalah

dianggap mengganggu independensi dan objektivitas:

• Keterlibatan material para profesional dalam pengawasan atau kinerja merancang, mengembangkan, menguji,

menginstal, mengkonfigurasi atau mengoperasikan sistem informasi yang material atau signifikan bagi subjek

masalah audit atau perikatan jaminan

• Merancang kontrol untuk sistem informasi yang material atau signifikan pada materi pelajaran

audit atau perikatan jaminan

• Melayani dalam peran pemerintahan di mana para profesional bertanggung jawab baik secara mandiri atau bersama-sama

membuat keputusan manajemen atau menyetujui kebijakan dan standar

• Memberikan saran yang membentuk dasar utama keputusan manajemen atau kinerja

fungsi manajemen

2.7 Relevansi independensi ketika memberikan layanan atau peran non-audit

Kecuali dilarang oleh standar eksternal lain atau oleh undang-undang, tidak ada persyaratan untuk profesional

baik menjadi, atau terlihat, independen ketika melakukan tugas-tugas yang berkaitan dengan melakukan non-audit

layanan atau peran; objektivitas masih merupakan persyaratan profesional. Dengan demikian, profesional harus melakukan

tugas yang berkaitan dengan layanan atau peran non-audit secara obyektif dan profesional.

2.7.2

Meskipun tidak ada persyaratan bagi para profesional untuk mandiri saat melakukan non-audit

layanan atau peran, para profesional harus mempertimbangkan apakah independensi dapat dirusak jika memang demikian

ditugaskan untuk melakukan audit atau perikatan jaminan di mana area di mana layanan non-audit atau

peran atau diberikan adalah materi untuk subjek pertunangan. Di mana potensi seperti itu

penurunan nilai dapat diperkirakan sebelumnya (misalnya, di mana audit independen akan diperlukan kemudian dan hanya ada satu

profesional dengan keterampilan yang diperlukan untuk melakukan layanan atau peran non-audit dan selanjutnya

audit), profesional harus mencari bimbingan dari manajemen audit dan, jika perlu, mereka yang dituduh

tata kelola, sebelum menerima atau melakukan layanan atau peran non-audit.

2.7.3

Menentukan apakah profesional harus melakukan layanan atau peran non-audit, saat ini atau

audit atau penjaminan keterlibatan berikutnya dari area di mana layanan atau peran non-audit direncanakan

atau kemungkinan dilakukan oleh profesional yang sama, harus menjadi keputusan manajemen audit IS dengan

persetujuan dari mereka yang didakwa dengan tata kelola. Manajemen audit SI harus menerapkan konseptual

kerangka kerja saat membuat keputusan, dan faktor-faktor berikut juga dapat memengaruhi keputusan:

• Profesional tidak boleh ditempatkan dalam situasi untuk mengaudit pekerjaan mereka sendiri atau menyediakan layanan non-audit

atau peran ke area yang diketahui atau kemungkinan signifikan atau material dengan subjek audit SI atau

keterlibatan jaminan di mana mereka terlibat atau akan terlibat

• Apakah ada sumber daya yang tersedia untuk melakukan audit dan jaminan non-audit dan independen

berfungsi secara terpisah

• Manajemen IS dan pihak yang bertanggung jawab atas persepsi tata kelola tentang nilai atau pentingnya

layanan atau peran non-audit relatif terhadap audit dan perikatan jaminan

• Tingkat risiko terhadap fungsi audit yang terkait dengan layanan atau peran non-audit

• Pengaruh keputusan terhadap persyaratan auditor eksternal atau regulator, jika ada

• Ketentuan piagam audit IS

2.8 Tata kelola penerimaan layanan atau peran non-audit

Piagam audit IS harus menetapkan apakah profesional diizinkan untuk terlibat dalam melakukan layanan atau peran non-audit dan sifat luas, waktu dan tingkat layanan atau peran tersebut, untuk memastikan hal itu

independensi tidak terganggu sehubungan dengan sistem yang mereka audit. Ini bisa menghilangkan atau meminimalkan

kebutuhan untuk mendapatkan mandat khusus untuk setiap layanan atau peran non-audit berdasarkan kasus per kasus.

2.8.2

Profesional harus memberikan jaminan yang masuk akal bahwa kerangka acuan (TOR) non-audit tertentu

layanan atau peran sesuai dengan piagam audit. Di mana ada penyimpangan, hal yang sama juga harus terjadi

secara tegas diuraikan dalam TOR dan disetujui oleh audit SI dan manajemen jaminan dan / atau mereka

dibebankan pemerintahan.

2.8.3 Apabila piagam audit tidak menentukan layanan atau peran non-audit atau di mana tidak ada piagam audit,

profesional harus melaporkan sifat keterlibatan mereka dalam layanan atau peran non-audit untuk audit IS dan

manajemen jaminan dan pihak yang bertanggung jawab atas tata kelola. Waktu dan tingkat profesional

keterlibatan dalam layanan atau peran non-audit harus tunduk pada TOR individu yang ditandatangani oleh manajemen

fungsi di mana layanan atau peran akan dilakukan dan disetujui oleh mereka yang bertanggung jawab atas tata kelola.

2.9 Pelaporan

Di mana kemandirian profesional, dengan mengacu pada audit SI atau keterlibatan jaminan, bisa

bisa tampak, atau terganggu, dan pihak yang bertanggung jawab atas tata kelola telah membuat keputusan untuk melanjutkan

perikatan, audit SI dan laporan perikatan jaminan harus mencakup informasi yang cukup

untuk memungkinkan pengguna laporan untuk memahami sifat potensi penurunan nilai. Informasi itu

profesional harus mempertimbangkan pengungkapan dalam audit SI dan laporan keterlibatan jaminan meliputi:

• Nama dan senioritas profesional yang terlibat dalam audit SI atau keterlibatan jaminan yang mungkin dimiliki, atau
mungkin tampak memiliki, gangguan pada kemandirian

• Analisis dan deskripsi ancaman terhadap kemerdekaan

• Perlindungan diterapkan untuk menghilangkan atau mengurangi ancaman yang berbeda terhadap independensi dan obyektivitas selama
jalannya kerja pelibatan dan proses pelaporan

• Fakta bahwa potensi penurunan independensi telah diungkapkan kepada mereka yang dituduh pemerintahan dan persetujuan mereka untuk melakukan atau melanjutkan perikatan jaminan dan / atau non-audit
layanan atau pera

Saya memilih standar ITIL (***IT Infrastructure Library) Standar ITIL berfokus kepada pelayanan customer, dan sama sekali tidak menyertakan proses penyelarasan strategi perusahaan terhadap strategi TI yang dikembangkan. keterkaitannya dengan COBIT yaitu sama- sama berguna untuk Audit IT atau Tata Kelola IT.***

framework ITIL Terbagi menjadi 2 Bagian Utama yaitu :

1. ***Service Support***
a. ***Service Desk.***
b. ***Incident Management.***
c. ***Problem Management.***
d. ***Configuration Management.***
e. ***Change Management.***
f. ***Release Management.***

2. ***Service Delivery***
a. ***Availability Management.***
b. ***Capacity Management.***
c. ***IT Service Continuity Management.***
d. ***Service Level Management.***
e. ***Financial Management for TI Services.***
f. ***Security Management.***

PROFESIONAL INDEPENDEN

OLEH

AHKMAD IPANDY
ANGGARI AYU P
ARVIAN AGUSAPUTRA
DEDI ZULKARNAIN

ITAF

01 Standar umum

02 Standar kerja

03 Standar pelaporan

Standart Umum

Bahwa seoarang auditor dan penjamin SI harus harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang berkaitan dengan audit dan pemeriksaan

SIKAP AUDITOR DAN PEJAMIN MUTU

1. Melakukan audit atau pemeriksaan dengan kerangka pikir yang adil dan tidak memihak dalam menyikapi masalah jaminan dan mencapai kesimpulan.
2. Harus Independen sebenarnya, walapun terkadang tidak selalu harus independen setiap saat.
3. Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat
4. Menilai independensi secara teratur dengan manajemen dan komite audit, jika ada.
5. Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karenanya peran tersebut dapat merusak independensi di masa depan.

PEDOMAN AUDIT

TUJUAN

1. Mengetahui kapan seorang audit dan penjamin merasa dalam kondisi ke-indipenenannya terancam atapun terganggu.
2. Melakukan suatu pendekatan alternative ketika proses audit berjalan dan ke-indipenenannya sedang dan atau mungkin terganggu.

3. Mengurangi atau menghilangkan dampak akibat ke-indipenenan audit SI dan kinerja professional seorang penjamin, peran, fungsi dan layanan non audit
4. Menentukan persyaratan untuk penilaian ketika ke-indipenenan merasa terganggu

JENIS ANCAMAN

1. Kerangka kerja konseptual
2. Ancaman dan perlindungan
3. Mengelola ancaman
4. Layanan atau peran non-audit
5. Layanan atau peran non-audit yang tidak mengganggu independensi
6. Layanan atau peran non-audit yang merusak independensi
7. Relevans
8. i independensi ketika memberikan layanan atau peran non-auditTata kelola penerimaan layanan atau peran non-audit
9. Pelaporan

KERANGKA KERJA KONSEPTUAL

Pedoman ini menetapkan kerangka kerja konseptual yang membutuhkan profesional untuk mengidentifikasi, mengevaluasi, dan menangani ancaman terhadap independensi. Kerangka kerja konseptual pendekatan membantu dalam mematuhi standar independensi, dan mengakomodasi banyak variasi dalamkeadaan yang menciptakan ancaman bagi kemerdekaan

JENIS ANCAMAN

1. Kepentingan pribadi
2. Tinjauan diri sendiri
3. Advokasi
4. Keakraban
5. Intimidasi
6. Bias
7. Partisipasi manajemen

ANCAMAN DAN PERLINDUNGAN

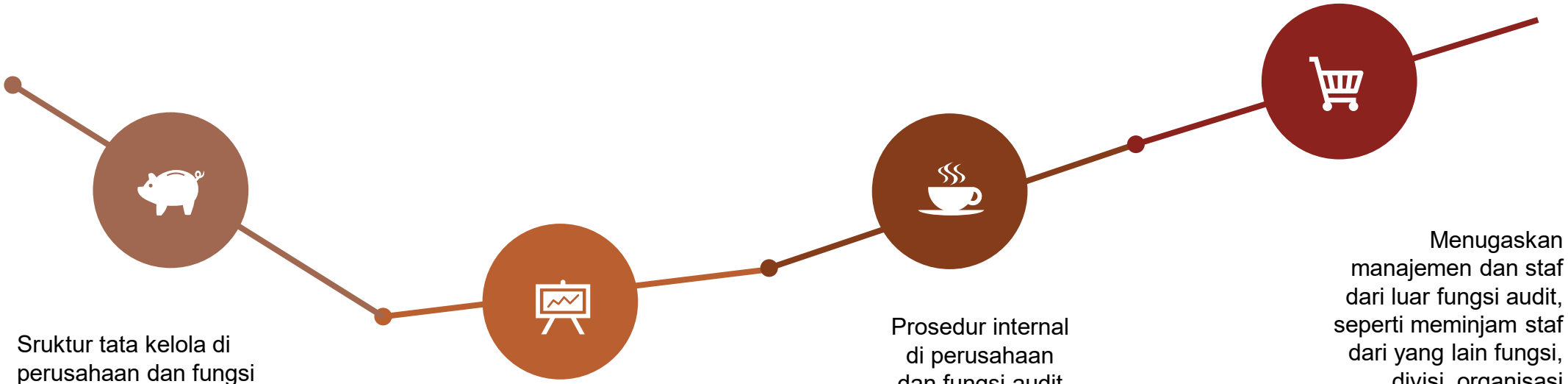
ANCAMAN

Ancaman dapat diciptakan oleh berbagai hubungan dan keadaan. Ketika suatu hubungan atau keadaan menciptakan ancaman, ancaman seperti itu dapat merusak, atau bisa dianggap merusak, keprofessionalan independen.

PERLINDUNGAN

kontrol yang dirancang untuk menghilangkan ancaman terhadap independensi atau menguranginnya.

PERLINDUNGAN



Sruktur tata kelola di perusahaan dan fungsi audit yang menyediakan pengawasan dan komunikasi mengenai audit SI dan layanan jaminan yang akan dilakukan

Memastikan bahwa profesional (dan manajemen audit IS) melapor ke tingkat hierarki yang memadai dalam perusahaan, terutama yang bertanggung jawab atas tata kelola

Prosedur internal di perusahaan dan fungsi audit yang memastikan pilihan obyektif dalam penugasan keterlibatan, misalnya, persyaratan pendidikan, pelatihan dan

Menugaskan manajemen dan staf dari luar fungsi audit, seperti meminjam staf dari yang lain fungsi, divisi, organisasi eksternal, untuk melengkapi para professional

Thank You

Insert the Sub Title of Your Presentation

RESIKO AUDIT

OLEH
AHKMAD IPANDY
ANGGARI AYU P
ARVIAN AGUSAPUTRA
DEDI ZULKARNAIN

RESIKO AUDIT

risiko salah saji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Auditor menyadari bahwa risiko tersebut ada karena adanya hal-hal sebagai berikut, misalnya ketidakpastian mengenai kompetensi bukti, efektivitas struktur pengendalian intern klien, serta ketidakpastian apakah laporan memang telah disajikan secara wajar setelah audit selesai.

Jenis Resiko Audit

RESIKO BAWAAN

Risiko bawaan (Inherent risk) merupakan kerentanan asersi terhadap salah saji (misstatement) yang material, dengan mengasumsikan bahwa tidak ada pengendalian yang berhubungan

RESIKO PENGENDALIAN

risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain

RESIKO DITEKSI

risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud)

AUDITOR SALAH MENETAPKAN LANGKAH PENGUJIANNYA (PROSEDUR AUDIT)

prosedur pengeluaran barang menetapkan bahwa setiap pengeluaran barang harus didasarkan pada permintaan dari pihak yang akan menggunakan. Jadi dalam pelaksanaan pengeluaran barang akan terdapat dua populasi bukti yang saling terkait, bukti permintaan barang dan bukti pengeluaran barang.

prosedur audit “periksa apakah atas setiap bukti permintaan barang terdapat bukti pengeluaran barangnya!” Prosedur ini dipastikan tidak akan menemukan kesalahan seperti kecurangan pihak gudang yang mengeluarkan barang walaupun tidak ada permintaan dari pihak yang membutuhkan barang, karena jika ada permintaan barang dapat dipastikan bagian gudang akan menerbitkan bukti pengeluaran barang

prosedur audit yang ditetapkan adalah: “periksa apakah atas setiap bukti pengeluaran barang terdapat bukti permintaan barangnya!” maka prosedur ini mungkin akan dapat menemukan kecurangan bagian gudang atas pengeluaran barang yang tidak didasarkan pada permintaan barang. Dengan prosedur tersebut, jika seandainya bagian gudang melakukan kecurangan mengeluarkan barang tetapi bukan untuk kepentingan perusahaan, maka akan dapat ditemukan dari sampel pengeluaran barang yang tidak ditemukan bukti permintaan barangnya

CONTOH RESIKO DITEKSI

PENGENDALIAN

Aditor memahami prosedur dan dukumen yang akan di audit.

Menggunakan semua dokumen prosedur sebagai bukti untuk dilakukan audit

control

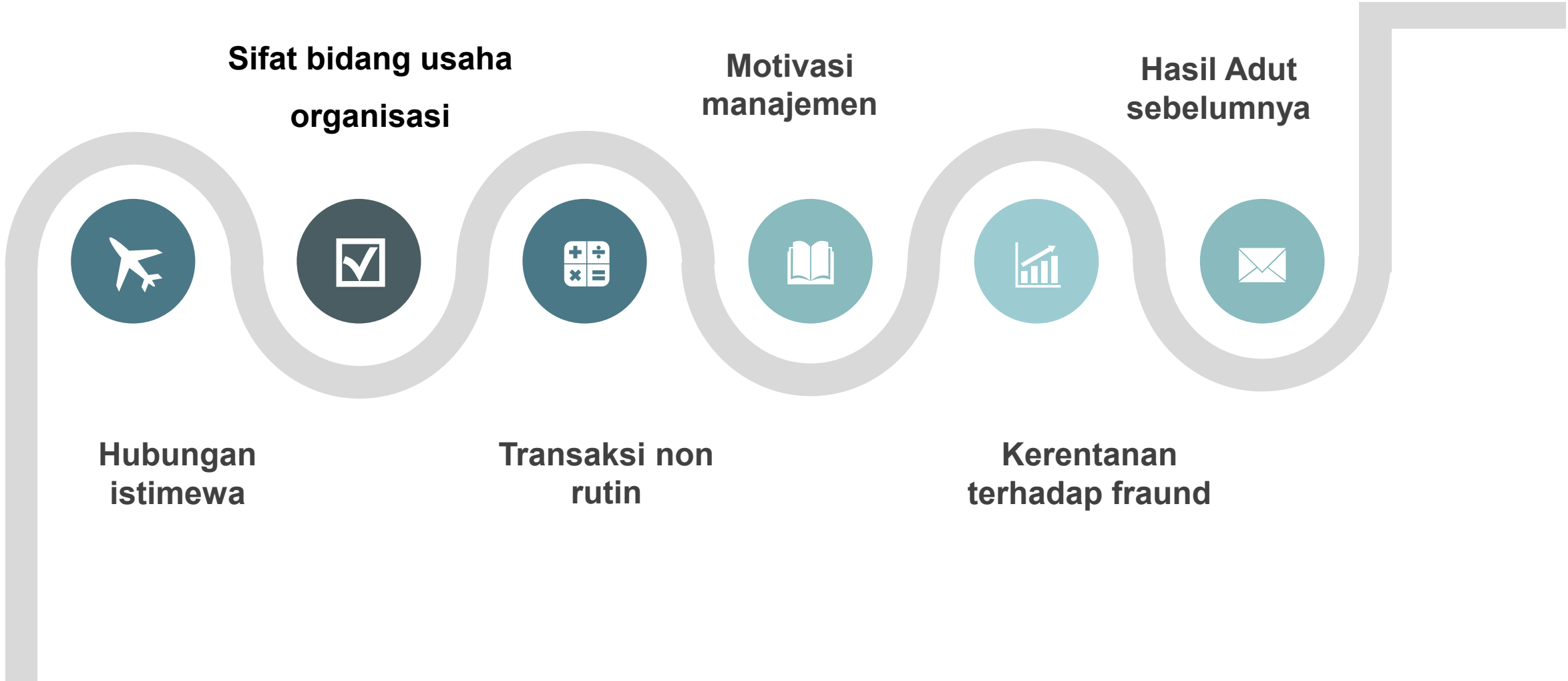
Dilakukan pelatihan bagi auditor, sehingga auditor paham mengenai model risiko audit

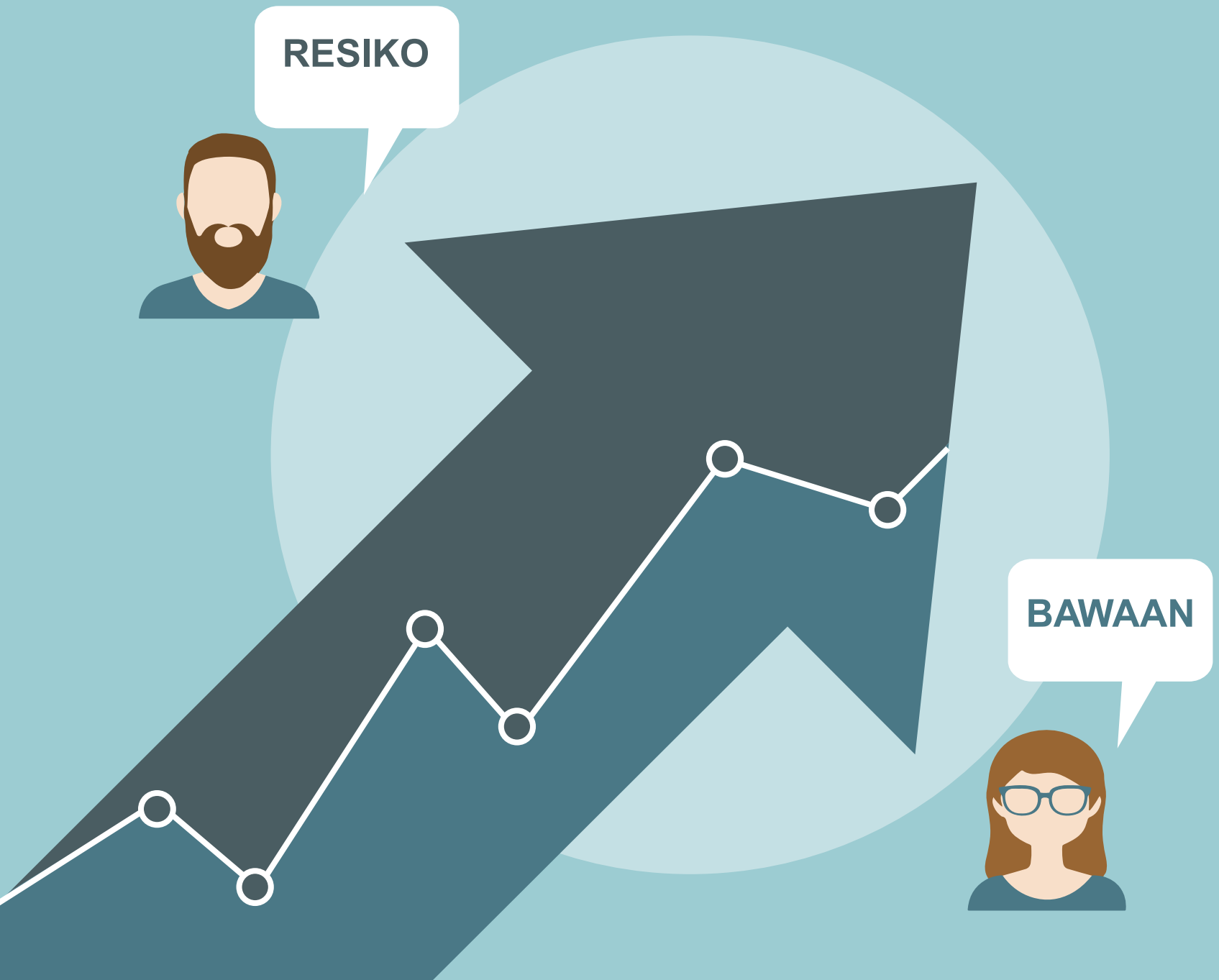
Merancang luasnya pengujian dan menggunakan metode audit yang baik sehingga agar auditor tidak mengalami risiko audit (dalam arti audit menjadi tidak efektif), serta agar audit dapat dilaksanakan secara efisien (dalam arti audit dapat menghindarkan diri, melakukan perluasan pengujian yang tidak perlu).

CONTOH RESIKO BAWAAN

Perhitungan yang rumit lebih mungkin disajikan salah jika dibandingkan dengan perhitungan yang sederhana. Akun yang terdiri dari jumlah yang berasal estimasi akuntansi cenderung mengandung risiko lebih besar dibandingkan dengan akun yang sifatnya rutin dan berisi data berupa fakta.

Faktor-faktor yang perlu ditelaah auditor dalam menetapkan risiko bawaan





Risiko bawaan selalu ada dan tidak pernah mencapai angka nol. Risiko bawaan tidak dapat diubah oleh penerapan prosedur audit yang paling baik sekalipun.

Contoh resiko pengendalian

Audit pada bagian Persediaan.
memeriksa apakah ada 2 pekerjaan terkait atau lebih dirangkap oleh satu orang petugas

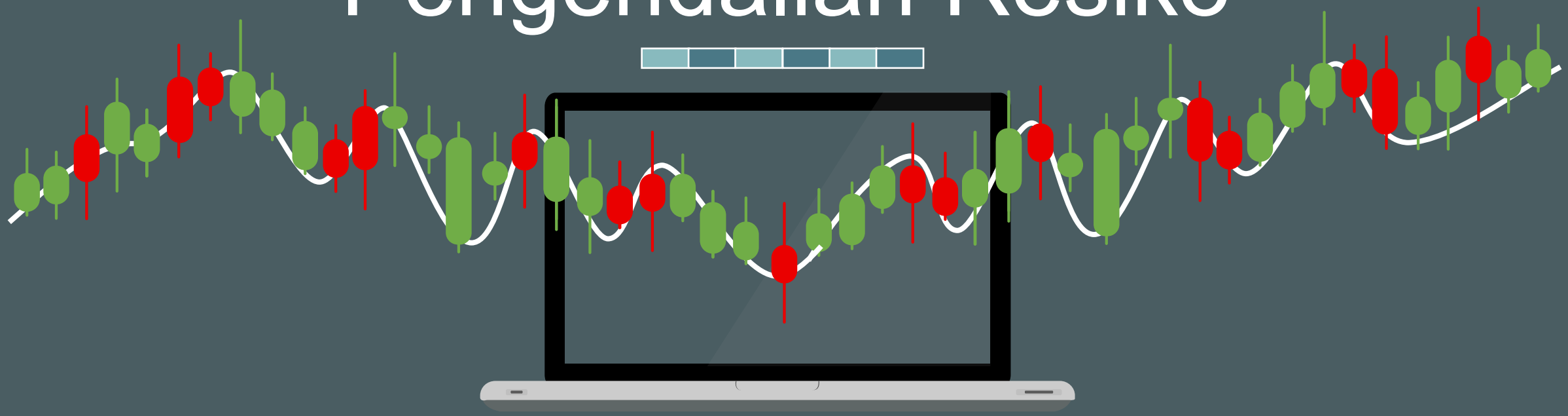
Pegawai Purchasing merangkap sebagai petugas yang penerima barang atau pekerjaan gudang persediaan lainnya (ini buruk); atau Pegawai Shipping merangkap sebagai petugas gudang yang mengurus persediaan barang jadi (ini juga buruk).

Foreman di bagian produksi (yang biasa request persediaan untuk keperluan produksi) diijinkan bebas keluar-masuk gudang persediaan bahan baku atau bahan penolong (ini buruk).

Pegawai admin yang input Receipt of Goods (ROG) memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Payable (Utang)

Pegawai admin yang input picking sheet di Shipping memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Receivable (Piutang).

Pengendalian Resiko



Resiko pengendalian ini tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee

Cara pengedalain resiko :

1. melakukan pembagian tugas yang jelas
2. Melakukan audit internal dan bila diperlukan memiliki bagian audit tersendiri
3. Memperkuat pengawasan manajemen terhadap pegawai


Thank You

IS Audit and Assurance Standards

1202 Risk Assessment in Planning

Standard ini mengharuskan seorang auditor menggunakan pendekatan penilaian risiko yang sesuai dan metodologi pendukung untuk mengembangkan rencana audit SI secara keseluruhan dan menentukan prioritas alokasi sumber daya IT audit yang efektif. Kemudian mengidentifikasi dan menilai risiko yang relevan, dan merencanakan keterlibatan individu. Selain itu juga harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.

Key Aspects

Berikut ini beberapa aspek penting dalam standar ini :

1. Melakukan dan mendokumentasikan audit, setidaknya setiap tahun, memfasilitasi pengembangan rencana audit untuk SI penilaian risiko.
2. Mencari persetujuan penilaian risiko dari pemangku kepentingan audit dan pihak terkait lainnya.
3. Memprioritaskan dan melakukan penjadwalan audit berdasarkan penilaian risiko
4. Identifikasi risiko dan asesmen risiko yang relevan dengan area yang diaudit

Term meliputi *Audit charter, Audit risk, Audit subject matter risk, Control risk, Detection risk, Inherent risk, Materiality, Risk assessment, Substantive testing.*

Linkage to Guidelines

Standar ini terhubung dengan Guideline 2202 Risk Assessment in Planning

IS Audit 1205 Evidence

Kelompok 2
Gina
Defry
Dendi
Erin

1205. Evidence/Bukti

1205.1. IS Audit dan penjaminan professional harus mendapatkan bukti yang cukup dan sesuai untuk menarik kesimpulan yang masuk akal yang menjadi dasar hasil keterlibatan.

1205.2. IS Audit dan penjaminan professional harus mengevaluasi kecukupan bukti yang diperoleh untuk mendukung kesimpulan dan mencapai tujuan keterlibatan

1205. Pernyataan Bukti

Key Aspect

Dalam melakukan keterlibatan, IS Audit dan penjaminan professional harus:

- Dapatkan bukti yang cukup dan tepat, termasuk:
  - Prosedur seperti yang dilakukan.
  - Hasil prosedur dilakukan.
  - Sumber dokumen (baik dalam format elektronik atau kertas), mencatat dan menguatkan informasi yang digunakan untuk mendukung keterlibatan.
  - Temuan dan hasil keterlibatan.
  - Dokumentasi bahwa pekerjaan dilakukan dan mematuhi undang-undang, peraturan, dan kebijakan yang berlaku.

- Siapkan dokumentasi, yang seharusnya:
  - Ditahan dan tersedia untuk jangka waktu tertentu dan dalam format yang sesuai dengan kebijakan organisasi audit atau jaminan dan standar profesional yang relevan, hukum dan peraturan.
  - Dilindungi dari pengungkapan atau modifikasi yang tidak sah selama persiapan dan penyimpanannya.
  - Dibuang dengan benar pada akhir periode retensi.

- Pertimbangkan kecukupan bukti untuk mendukung tingkat risiko pengendalian yang dinilai saat memperoleh bukti dari uji pengendalian.

- Identifikasi secara tepat, referensi silang dan katalog bukti.

- Pertimbangkan properti seperti sumber, jenis (misal., Tulisan, lisan, visual, elektronik) dan keaslian (misal. Tanda tangan digital dan manual, perangko) dari bukti saat mengevaluasi keandalannya.

- Pertimbangkan cara yang paling efektif dan tepat waktu untuk mengumpulkan bukti yang diperlukan untuk memenuhi tujuan dan risiko keterlibatan. Namun, kesulitan atau biaya bukan merupakan dasar yang valid untuk menghilangkan prosedur yang diperlukan.

- Pilih prosedur yang paling tepat untuk mengumpulkan bukti tergantung pada subjek yang diaudit (yaitu, sifatnya, waktu audit, penilaian profesional). Prosedur yang digunakan untuk mendapatkan bukti meliputi:
  - Permintaan dan konfirmasi.
  - Kinerja ulang
  - Perhitungan ulang
  - Komputasi

- Prosedur analitik
- Inspeksi
- Pengamatan
- Metode lain yang diterima secara umum

- Pertimbangkan sumber dan sifat informasi apa pun yang diperoleh untuk mengevaluasi keandalannya dan persyaratan verifikasi lebih lanjut. Secara umum, keandalan bukti lebih besar ketika:
  - Dalam bentuk tertulis, bukan ekspresi lisan
  - Diperoleh dari sumber independen
  - Diperoleh oleh profesional daripada oleh entitas yang diaudit
  - Disertifikasi oleh pihak independen
  - Dipertahankan oleh pihak independen
  - Hasil pemeriksaan
  - Hasil pengamatan

- Dapatkan bukti objektif yang memadai untuk memungkinkan pihak independen yang berkualifikasi untuk melakukan pengujian ulang dan mendapatkan hasil dan kesimpulan yang sama.

- Dapatkan bukti yang sepadan dengan materialitas item dan risiko yang terlibat.

- Tempatkan penekanan pada keakuratan dan kelengkapan informasi ketika informasi yang diperoleh dari perusahaan digunakan oleh audit SI atau profesional penjamin untuk melakukan prosedur audit.

- Bukti aman terhadap akses dan modifikasi yang tidak sah.

- Menyimpan bukti setelah menyelesaikan audit SI atau pekerjaan jaminan selama diperlukan untuk mematuhi semua hukum, peraturan, dan kebijakan yang berlaku.

1205. Bukti Lanjutan

Ketentuan

Ketentuan	Definisi
Bukti yang sesuai	Ukuran kualitas bukti
Bukti yang cukup	Ukuran kuantitas bukti; mendukung semua pertanyaan material untuk tujuan dan ruang lingkup audit. Lihat bukti.

Keterkaitan dengan Standar dan Pedoman

Tipe	Judul
Pedoman	2205 Bukti

IS Audit 1205 Evidence

Kelompok 2
Gina
Defry
Dendi
Erin

1205. Evidence/Bukti

1205.1. IS Audit dan penjaminan professional harus mendapatkan bukti yang cukup dan sesuai untuk menarik kesimpulan yang masuk akal yang menjadi dasar hasil keterlibatan.

1205.2. IS Audit dan penjaminan professional harus mengevaluasi kecukupan bukti yang diperoleh untuk mendukung kesimpulan dan mencapai tujuan keterlibatan

1205. Pernyataan Bukti

Key Aspect

Dalam melakukan keterlibatan, IS Audit dan penjaminan professional harus:

- Dapatkan bukti yang cukup dan tepat, termasuk:
  - Prosedur seperti yang dilakukan.
  - Hasil prosedur dilakukan.
  - Sumber dokumen (baik dalam format elektronik atau kertas), mencatat dan menguatkan informasi yang digunakan untuk mendukung keterlibatan.
  - Temuan dan hasil keterlibatan.
  - Dokumentasi bahwa pekerjaan dilakukan dan mematuhi undang-undang, peraturan, dan kebijakan yang berlaku.

- Siapkan dokumentasi, yang seharusnya:
  - Ditahan dan tersedia untuk jangka waktu tertentu dan dalam format yang sesuai dengan kebijakan organisasi audit atau jaminan dan standar profesional yang relevan, hukum dan peraturan.
  - Dilindungi dari pengungkapan atau modifikasi yang tidak sah selama persiapan dan penyimpanannya.
  - Dibuang dengan benar pada akhir periode retensi.

- Pertimbangkan kecukupan bukti untuk mendukung tingkat risiko pengendalian yang dinilai saat memperoleh bukti dari uji pengendalian.

- Identifikasi secara tepat, referensi silang dan katalog bukti.

- Pertimbangkan properti seperti sumber, jenis (misal., Tulisan, lisan, visual, elektronik) dan keaslian (misal. Tanda tangan digital dan manual, perangko) dari bukti saat mengevaluasi keandalannya.

- Pertimbangkan cara yang paling efektif dan tepat waktu untuk mengumpulkan bukti yang diperlukan untuk memenuhi tujuan dan risiko keterlibatan. Namun, kesulitan atau biaya bukan merupakan dasar yang valid untuk menghilangkan prosedur yang diperlukan.

- Pilih prosedur yang paling tepat untuk mengumpulkan bukti tergantung pada subjek yang diaudit (yaitu, sifatnya, waktu audit, penilaian profesional). Prosedur yang digunakan untuk mendapatkan bukti meliputi:
  - Permintaan dan konfirmasi.
  - Kinerja ulang
  - Perhitungan ulang
  - Komputasi

- Prosedur analitik
- Inspeksi
- Pengamatan
- Metode lain yang diterima secara umum

- Pertimbangkan sumber dan sifat informasi apa pun yang diperoleh untuk mengevaluasi keandalannya dan persyaratan verifikasi lebih lanjut. Secara umum, keandalan bukti lebih besar ketika:
  - Dalam bentuk tertulis, bukan ekspresi lisan
  - Diperoleh dari sumber independen
  - Diperoleh oleh profesional daripada oleh entitas yang diaudit
  - Disertifikasi oleh pihak independen
  - Dipertahankan oleh pihak independen
  - Hasil pemeriksaan
  - Hasil pengamatan

- Dapatkan bukti objektif yang memadai untuk memungkinkan pihak independen yang berkualifikasi untuk melakukan pengujian ulang dan mendapatkan hasil dan kesimpulan yang sama.

- Dapatkan bukti yang sepadan dengan materialitas item dan risiko yang terlibat.

- Tempatkan penekanan pada keakuratan dan kelengkapan informasi ketika informasi yang diperoleh dari perusahaan digunakan oleh audit SI atau profesional penjamin untuk melakukan prosedur audit.

- Bukti aman terhadap akses dan modifikasi yang tidak sah.

- Menyimpan bukti setelah menyelesaikan audit SI atau pekerjaan jaminan selama diperlukan untuk mematuhi semua hukum, peraturan, dan kebijakan yang berlaku.

1205. Bukti Lanjutan

Ketentuan

Ketentuan	Definisi
Bukti yang sesuai	Ukuran kualitas bukti
Bukti yang cukup	Ukuran kuantitas bukti; mendukung semua pertanyaan material untuk tujuan dan ruang lingkup audit. Lihat bukti.

Keterkaitan dengan Standar dan Pedoman

Tipe	Judul
Pedoman	2205 Bukti

Saya memilih standar COSO

COSO – Committee of Sponsoring Organization of the Treadway Commission

COSO merupakan kependekan *dari Committee of Sponsoring Organization of the Treadway Commission*, sebuah organisasi di Amerika yang berdedikasi dalam meningkatkan kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan *corporate governance*. Komite ini didirikan pada tahun 1985 untuk mempelajari faktor-faktor yang menunjukan ketidaksesuaian dalam laporan finansial.

Gambar 2. *COSO Framework*
(COSO Back in The Timelight, 2008)

1. **Komponen kontrol COSO**
   COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal:

a. *Monitoring.*
b. *Information and communications.*
c. *Control activities.*
d. *Risk assessment.*
e. *Control environment.*

2. **Sasaran kontrol internal**
   Sasaran kontrol internal dikategorikan menjadi beberapa area sebagai berikut:

a. *Operations* – efisisensi dan efektifitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan.
b. *Financial reporting* – persiapan pelaporan anggaran finansial yang dapat dipercaya.
c. *Compliance* – pemenuhan hukum dan aturan yang dapat dipercaya.

3. **Unit / Aktifitas Terhadap Organisasi**
   Dimensi ini mengidentifikasikan unit/aktifitas pada organisasi yang menghubungkan kontrol internal. Kontrol internal menyangkut keseluruhan organisasi dan semua bagian-bagiannya. Kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktifitas organisasi.

Kaitannya dengan standar COBIT adalah optimasi kontrol di dalam COSO hanya membahas kontrol dalam suatu sistem informasi perusahaan, kontrol ada di dalam bahasan COBIT.

1002 ORGANISATIONAL INDEPENDENCE

Oleh :

Dwi Septya Putri – Uci Suriani

Fungsi Standar :

Fungsi audit dan jaminan SI harus:

• Melaporkan ke tingkat dalam organisasi yang diaudit yang memberikan independensi organisasi dan memungkinkan IS audit dan fungsi assurance untuk melakukan tanggung jawabnya tanpa gangguan.

• Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika faktanya independensi terganggu atau penampilan.

• Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen sebagai peran tersebut dapat merusak independensi masa depan.

Peranan :

• Mengatasi independensi dan akuntabilitas fungsi audit dalam piagam dan / atau surat perjanjian

Pedoman

Tujuan dari pedoman ini adalah untuk mengatasi independensi fungsi audit dan jaminan IS di Indonesia perusahaan. Tiga aspek penting dipertimbangkan:

• Posisi audit SI dan fungsi jaminan dalam perusahaan

• Tingkat yang dilaporkan oleh audit IS dan fungsi jaminan di dalam perusahaan

• Kinerja layanan non-audit dalam perusahaan oleh audit SI dan manajemen jaminan dan

Gulidline terbagi menjadi 5 bagian :

1. Posisi dalam perusahaan
   Di dalam sebuah perusahaan harus memiliki fungsi audit yang bertanggung jawab penuh untuk mengatasi gangguan.

2. Tingkat Pelaporan

   Fungsi audit harus melaporkan ke tingkat dalam perusahaan yang memungkinkannya

untuk bertindak dengan lengkap kemandirian organisasi. Independensi harus didefinisikan dalam piagam audit dan dikonfirmasi oleh fungsi audit kepada dewan direksi dan mereka yang bertanggung jawab atas tata kelola secara teratur, setidaknya setiap tahun.

3. Layanan Non Audit

2.3.1 Di banyak perusahaan, harapan manajemen dan staf SI adalah bahwa fungsi audit mungkin terlibat dalam menyediakan layanan non-audit. Ini melibatkan, paruh waktu atau paruh waktu, partisipasi para profesional di IS inisiatif dan tim proyek SI untuk memberikan kemampuan penasihat atau konsultatif.

2.3.2 Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggaptidak menjadi tanggung jawab manajemen dan, karenanya, tidak akan mengganggu independensi. Layanan non-audit yang juga tidak akan mengganggu independensi atau objektivitas, jika perlindungan yang memadai diterapkan, termasuk memberikan saran rutin tentang risiko dan kontrol teknologi informasi.

2.3.3 Layanan non-audit berikut ini dianggap merusak independensi dan objektivitas, karena ancaman dibuat akan sangat signifikan sehingga tidak ada perlindungan yang dapat mengurangi mereka ke tingkat yang dapat diterima:

• Menganggap tanggung jawab manajemen atau melakukan kegiatan manajemen

• Keterlibatan material para profesional dalam pengawasan atau kinerja merancang, mengembangkan, menguji, menginstal, mengkonfigurasi atau mengoperasikan sistem informasi yang material atau signifikan bagi subjek masalah audit atau perikatan jaminan

• Merancang kontrol untuk sistem informasi yang material atau signifikan dengan materi terkini atau rencana perikatan audit yang akan datang

• Melayani dalam peran pemerintahan di mana para profesional bertanggung jawab baik secara mandiri atau bersama-sama membuat keputusan manajemen atau menyetujui kebijakan dan standar

• Memberikan saran yang membentuk dasar utama keputusan manajemen

2.3.4 Menyediakan layanan non-audit di bidang-bidang yang saat ini, atau di masa depan akan menjadi, subjek audit keterlibatan juga menciptakan ancaman terhadap kemerdekaan yang akan sulit diatasi dengan perlindungan. Di situasi ini, persepsi mungkin bahwa independensi dan objektivitas fungsi audit dan profesional telah dirugikan dengan melakukan layanan non-audit di bidang tertentu.

Fungsi audit dan para profesional harus menentukan apakah perlindungan yang memadai dapat diimplementasikan untuk memitigasi yang memadai ini ancaman aktual atau yang dirasakan terhadap kemerdekaan.

2.3.5 Pedoman lebih rinci tentang cara menangani ancaman independensi ini dapat ditemukan dalam Standar 1003 Independensi Profesional dan Pedoman terkait 2003.

4. Menilai Independensi

   2.4.1 Independensi harus dinilai secara berkala oleh fungsi audit dan profesional. Penilaian ini perlu terjadi setiap tahun untuk fungsi audit dan sebelum setiap perikatan untuk para profesional, seperti dijelaskan dalam Standar 1003 Independensi Profesional. Penilaian harus mempertimbangkan faktor-faktor seperti:

   • Perubahan dalam hubungan pribadi
   • Kepentingan finansial
   • Penugasan dan tanggung jawab pekerjaan sebelumnya

   2.4.2 Fungsi audit perlu mengungkapkan kemungkinan masalah yang terkait dengan independensi organisasi dan membahasnya mereka dengan dewan direksi atau mereka yang bertanggung jawab atas tata kelola. Resolusi perlu ditemukan dan dikonfirmasi dalam piagam audit atau rencana audit.

5. Audit Charter dan Audit Plan

   2.5.1 Piagam audit harus merinci, di bawah aspek 'tanggung jawab', implementasi organisasi independensi fungsi audit. Selain merinci independensi, piagam audit juga harus mencakup kemungkinan penurunan independensi.

   2.5.2 Independensi organisasi juga harus tercermin dalam rencana audit. Fungsi audit harus mampu menentukan ruang lingkup rencana secara mandiri, tanpa batasan yang diberlakukan oleh eksekutif pengelolaan.

ITAF

ITAF adalah model referensi yang komprehensif dan baik-praktek penetapan bahwa:

- Menetapkan standar yang alamat IS audit dan jaminan peran dan tanggung jawab profesional; pengetahuan dan keterampilan; dan ketekunan, perilaku dan persyaratan pelaporan
- Mendefinisikan istilah dan konsep spesifik untuk jaminan IS
- Memberikan bimbingan dan alat-alat dan teknik pada perencanaan, desain, pelaksanaan dan pelaporan IS audit dan jaminan tugas.

ITAF difokuskan pada materi ISACA dan menyediakan satu sumber di mana IS audit dan jaminan profesional dapat mencari bimbingan, penelitian kebijakan dan prosedur, mendapatkan program audit dan jaminan, dan mengembangkan laporan yang efektif.

Untuk siapakah ITAF berlaku?
ITAF berlaku untuk individu yang bertindak dalam kapasitas IS audit dan jaminan profesional dan terlibat dalam memberikan jaminan atas beberapa komponen dari aplikasi dan infrastruktur IS. Namun, perawatan telah diambil untuk merancang standar ini, pedoman, dan alat-alat dan teknik dengan cara yang juga dapat berguna dan memberikan manfaat bagi khalayak yang lebih luas, termasuk pengguna audit IS dan jaminan laporan.

Kapan ITAF digunakan?
Penerapan kerangka kerja merupakan prasyarat untuk budidaya IS audit dan jaminan kerja. Standar yang wajib. Pedoman, alat dan teknik yang dirancang untuk memberikan bantuan non-wajib dalam melakukan pekerjaan jaminan.

Di mana harus ITAF IS audit dan jaminan standar dan pedoman terkait akan digunakan? Desain ITAF ini mengakui bahwa IS audit dan jaminan profesional dihadapkan dengan kebutuhan yang berbeda dan jenis tugas-mulai dari memimpin audit IS-difokuskan untuk berkontribusi pada keuangan atau operasional audit. ITAF berlaku untuk setiap resmi IS audit atau penilaian pertunangan.

Apakah persyaratan alamat ITAF untuk pekerjaan konsultasi dan penasehat? Selain pekerjaan penilaian, IS audit dan jaminan profesional sering melakukan pertunangan konsultasi dan penasehat untuk majikan mereka atau atas nama klien. Tugas-tugas ini biasanya menghasilkan penilaian daerah tertentu; identifikasi masalah, keprihatinan atau kelemahan; dan pengembangan rekomendasi. Untuk nomor alasan, termasuk sifat pekerjaan, lingkup keterlibatan, kemandirian dan tingkat pengujian, pekerjaan tidak dianggap audit dan, karena itu, IS audit dan jaminan profesional tidak mengeluarkan laporan audit formal. ITAF belum dirancang untuk mengatasi tertentu persyaratan sehubungan dengan pekerjaan konsultasi dan penasehat ini.

Organisasi ITAF IS audit dan jaminan standar dibagi menjadi tiga kategori:

1. Standar Umum (1000 series) -Apakah prinsip-prinsip di mana profesi jaminan IS beroperasi. Mereka berlaku untuk pelaksanaan semua tugas, dan berurusan dengan audit IS dan jaminan profesional etika, independensi, objektivitas dan hati-hati serta pengetahuan, kompetensi dan keterampilan.
2. Standar kinerja (1200 series) -Deal dengan pelaksanaan tugas, seperti perencanaan dan pengawasan, scoping, risiko dan materialitas, mobilisasi sumber daya, pengawasan dan tugas manajemen, audit dan bukti jaminan, dan berolahraga profesional penghakiman dan perawatan karena
3. Standar Pelaporan (1400 series) -Address jenis laporan, berarti komunikasi dan informasi yang dikomunikasikan ITAF IS pedoman audit dan jaminan menyediakan audit IS dan jaminan profesional dengan informasi dan arah tentang audit IS atau daerah jaminan. Sejalan dengan tiga kategori standar yang diuraikan di atas, pedoman fokus pada berbagai pemeriksaan pendekatan, metodologi dan materi yang terkait untuk membantu dalam perencanaan, pelaksanaan, menilai, menguji dan melaporkan IS proses, kontrol dan terkait IS audit atau jaminan inisiatif. Pedoman juga membantu memperjelas hubungan antara kegiatan perusahaan dan inisiatif, dan orang-orang yang dilakukan oleh IT.

IS Audit 1205 Evidence

Kelompok 2
Gina
Defry
Dendi
Erin

1205. Evidence/Bukti

1205.1. IS Audit dan penjaminan professional harus mendapatkan bukti yang cukup dan sesuai untuk menarik kesimpulan yang masuk akal yang menjadi dasar hasil keterlibatan.

1205.2. IS Audit dan penjaminan professional harus mengevaluasi kecukupan bukti yang diperoleh untuk mendukung kesimpulan dan mencapai tujuan keterlibatan

1205. Pernyataan Bukti

Key Aspect

Dalam melakukan keterlibatan, IS Audit dan penjaminan professional harus:

- Dapatkan bukti yang cukup dan tepat, termasuk:
  - Prosedur seperti yang dilakukan.
  - Hasil prosedur dilakukan.
  - Sumber dokumen (baik dalam format elektronik atau kertas), mencatat dan menguatkan informasi yang digunakan untuk mendukung keterlibatan.
  - Temuan dan hasil keterlibatan.
  - Dokumentasi bahwa pekerjaan dilakukan dan mematuhi undang-undang, peraturan, dan kebijakan yang berlaku.

- Siapkan dokumentasi, yang seharusnya:
  - Ditahan dan tersedia untuk jangka waktu tertentu dan dalam format yang sesuai dengan kebijakan organisasi audit atau jaminan dan standar profesional yang relevan, hukum dan peraturan.
  - Dilindungi dari pengungkapan atau modifikasi yang tidak sah selama persiapan dan penyimpanannya.
  - Dibuang dengan benar pada akhir periode retensi.

- Pertimbangkan kecukupan bukti untuk mendukung tingkat risiko pengendalian yang dinilai saat memperoleh bukti dari uji pengendalian.

- Identifikasi secara tepat, referensi silang dan katalog bukti.

- Pertimbangkan properti seperti sumber, jenis (misal., Tulisan, lisan, visual, elektronik) dan keaslian (misal. Tanda tangan digital dan manual, perangko) dari bukti saat mengevaluasi keandalannya.

- Pertimbangkan cara yang paling efektif dan tepat waktu untuk mengumpulkan bukti yang diperlukan untuk memenuhi tujuan dan risiko keterlibatan. Namun, kesulitan atau biaya bukan merupakan dasar yang valid untuk menghilangkan prosedur yang diperlukan.

- Pilih prosedur yang paling tepat untuk mengumpulkan bukti tergantung pada subjek yang diaudit (yaitu, sifatnya, waktu audit, penilaian profesional). Prosedur yang digunakan untuk mendapatkan bukti meliputi:
  - Permintaan dan konfirmasi.
  - Kinerja ulang
  - Perhitungan ulang
  - Komputasi

- Prosedur analitik
- Inspeksi
- Pengamatan
- Metode lain yang diterima secara umum

- Pertimbangkan sumber dan sifat informasi apa pun yang diperoleh untuk mengevaluasi keandalannya dan persyaratan verifikasi lebih lanjut. Secara umum, keandalan bukti lebih besar ketika:
  - Dalam bentuk tertulis, bukan ekspresi lisan
  - Diperoleh dari sumber independen
  - Diperoleh oleh profesional daripada oleh entitas yang diaudit
  - Disertifikasi oleh pihak independen
  - Dipertahankan oleh pihak independen
  - Hasil pemeriksaan
  - Hasil pengamatan

- Dapatkan bukti objektif yang memadai untuk memungkinkan pihak independen yang berkualifikasi untuk melakukan pengujian ulang dan mendapatkan hasil dan kesimpulan yang sama.

- Dapatkan bukti yang sepadan dengan materialitas item dan risiko yang terlibat.

- Tempatkan penekanan pada keakuratan dan kelengkapan informasi ketika informasi yang diperoleh dari perusahaan digunakan oleh audit SI atau profesional penjamin untuk melakukan prosedur audit.

- Bukti aman terhadap akses dan modifikasi yang tidak sah.

- Menyimpan bukti setelah menyelesaikan audit SI atau pekerjaan jaminan selama diperlukan untuk mematuhi semua hukum, peraturan, dan kebijakan yang berlaku.

1205. Bukti Lanjutan

Ketentuan

Ketentuan	Definisi
Bukti yang sesuai	Ukuran kualitas bukti
Bukti yang cukup	Ukuran kuantitas bukti; mendukung semua pertanyaan material untuk tujuan dan ruang lingkup audit. Lihat bukti.

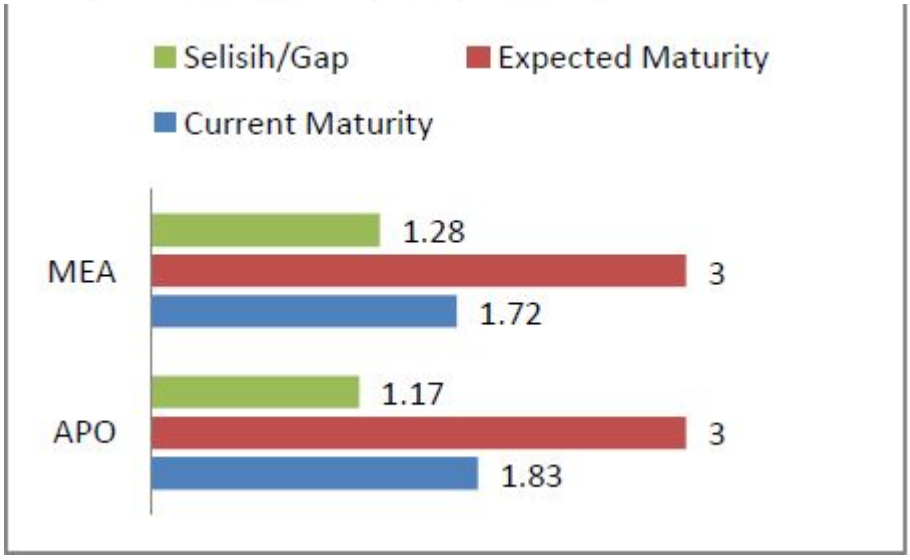
Keterkaitan dengan Standar dan Pedoman

Tipe	Judul
Pedoman	2205 Bukti

Review Jurnal Penerapan Tata Kelola Teknologi Informasi dan Komunikasi Pada Domain APO dan MEA dengan Menggunakan Framework Cobit 5 Studi Kasus : STMIK Pelita Nusantara Medan.

Judul	**Penerapan Tata Kelola Teknologi Informasi dan Komunikasi Pada Domain APO dan MEA dengan Menggunakan Framework Cobit 5 Studi Kasus : STMIK Pelita Nusantara Medan.**
Penulis	Hengki Tamando Sihotang Dan Jijon Raphita Sagala
Topik	Penerapan Tata Kelola IT Pada STMIK Pelita Nusantara Medan
Permasalahan	Setelah Dievaluasi tingkat maturitas tata kelola TI STMIK Pelita Nusantara, masih berada dibawah standar yang telah ditentukan yaitu masih berada pada level lebih kecil dari 3. Artinya dalam tingkat maturitas tata kelola TI STMIK Pelita Nusantara Medan masih perlu perbaikan. Sehingga Untuk mengurangi gap antara capability level saat ini dan capability level yang ingin dicapai, maka STMIK Pelita Nusantara Medan harus memenuhi PA2.1,PA2.2, PA3.1 dan PA3.2.
Tujuan Penelitian	Untuk meningkatkan maturitas tata kelola TI STMIK Pelita Nusantara Medan yang masih dibawah standar ke level 3. Deangan mendapatkan hasil nilai–nilai pada tiap aktifitas yang ada pada domain *Align, Plan and Organise* (APO) dan *Monitor, Evaluate and Assess* (MEA).
Hasil	

MATURITY LEVEL	DOMAIN		
	APO	*MEA*	*APO,MEA*
Expected	3	3	3
Rata-rata	1.83	1.75	1.80
Minimal	1.43	1.46	1.50
Maksimal	1.96	1.90	1.95



	Dari hasil audit yang dilaksanakan, pengukuran *capability level* proses area APO dan MEA STMIK Pelita Nusantara, diperoleh hasil level kapabilitas 1.83 pada domain APO, 1.75 pada Domain MEA, level rata-rata 1,80, artinya MEA dan APO sedang dalam tahap menuju *capability level* 2 dan masih mencapai 0,20 di atas level 1. Pembulatan ke atas dipilih sesuai dengan konsep penentuan *capability level* proses tertentu. Maka dari itu untuk APO dan MEA *capability level* sudah dianggap 2, sehingga *capability level* target yang diinginkan adalah level yang sedang ditujunya yaitu level 3.
Alur Metode	Setelah dilakukan analisis hasil kuisoner maka di dapatkanlah hasil nilai–nilai pada tiap aktifitas yang ada pada domain *Align, Plan and Organise* (APO) dan *Monitor, Evaluate and Assess* (MEA) setelah itu di masukan ke dalam form kerja audit. Tindakan selanjutnya yang dilakukan adalah mencari rata–rata nilai pada tiap proses untuk mengetahui bagaimana kondisi tiap proses yang ada.

PENERAPAN TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI PADA DOMAIN *ALIGN, PLAN AND ORGANISE* (APO) DAN *MONITOR, EVALUATE AND ASSESS* (MEA) DENGAN MENGGUNAKAN FRAMEWORK COBIT 5 STUDI KASUS: STMIK PELITA NUSANTARA MEDAN

Hengki Tamando Sihotang[1], Jijon Raphita Sagala[1]
[1]Program Studi Teknik Informatika
[1]STMIK Pelita Nusantara Medan, Jl. Iskandar Muda No 1 Medan, Sumatera Utara 20154, Indonesia
Hengki_tamando@yahoo.com, *jijonsagala@yahoo.com*

Abstrak

Dalam memasuki persaingan kualitas dan predikat terbaik skala nasional serta kualitas alumni, perguruan tinggi berusaha memanfaatkan TI sebagai alat untuk dapat memenangkan persaingan tersebut. Agar TI dapat dimanfaatkan secara maksimal dan mendukung sistem yang ada di perguruan tinggi, dibutuhkan penilaian kinerja dari TI secara berkala. Salah satu metode untuk melakukan penilaian terhadap kinerja departemen TI adalah dengan memanfaatkan kerangka kerja CobIT 5 sebagai tolak ukur efisiensi dalam pemanfaatan TI saat ini yang terdiri dari 5 (lima) domain yaitu: *Evaluate*, *Direct* and *Organise* (EDM), *Align*, *Plan And Organise* (APO), *Build*, Acquire and *Implement* (BAI), *Deliver*, *Service* and *Support* (DSS), *Monitor*, *Evaluate* and *Assess* (MEA). Sebagai alat ukurnya. Dengan metode tersebut, peneliti mencoba untuk membuat IT Blueprint sebagai hasil akhir dari pemanfaaatan TI diperguruan tinggi, sehingga pihak management dapat merencanakan bagaimana perkembangan TI diperusahaan untuk beberapa tahun mendatang. Dari hasil evaluasi, diketahui level kapabilitas dalam area MEA dan APO secara keseluruhan berada pada level 1 (*Performed*) dengan level target yang ingin dicapai adalah level 3 (*Managed* ProIcess). Kelemahan tata kelola TI di STMIK Pelita Nusantara Medan adalah kurangnya formalisasi aturan dan prosedur manajemen TI. Untuk mengurangi gap antara capability level saat ini dan capability level yang ingin dicapai, maka STMIK Pelita Nusantara Medan harus memenuhi PA2.1,PA2.2, PA3.1 dan PA3.2, agar capability level saat ini yang berada pada level 1 dapat naik ke level 3. Sejalan dengan itu, STMIK Pelita Nusantara Medan semakin mendekati tujuan.

I. PENDAHULUAN

Teknologi informasi secara signifikan telah mempengaruhi dan mengubah cara bisnis yang sedang dikelola dan dipantau saat ini [14] Penerapan teknologi informasi pada proses bisnis suatu perusahaan dipandang sebagai salah satu solusi yang nantinya akan dapat meningkatkan tingkat persaingan perusahaan. Hal ini mengakibatkan pentingnya kerangka kerja untuk memastikan bahwa teknologi informasi memungkinkan bisnis, memaksimalkan keuntungan, resiko teknologi informasi dikelola secara tepat, dan sumber daya teknologi informasi digunakan secara bertanggung jawab [13]. Untuk mencapai tujuan tersebut dibutuhkan perencanan, implementasi, dukungan, pengawasan dan evaluasi yang matang dan optimal. Hal ini disebabkan besarnya biaya investasi yang dikeluarkan dalam peningkatan peran teknologi informasi tersebut. Sehingga kerugian-kerugian yang mungkin bisa terjadi dapat dihindari. Kerugian yang dimaksud dapat terjadi dari kehilangan data, penyalahgunaan data, penyalahgunaan komputer, informasi yang tidak akurat karena kesalahan dalam pemerosesan data sehingga integritas data diragukan, pengadaan investasi perangkat keras dan perangkat lunak yang tinggi tapi tidak diikuti nilai balik, pengelolaan staf teknologi informasi yang tidak terarah. Semua masalah-masalah diatas bisa saja terjadi pada semua perusahaan maka dibutuhkan satu evaluasi teknologi informasi untuk menelusuri bagian mana saja yang harus diperbaiki sehingga tujuan bisnis menjadi tercapai .

Selain perusahaan, Perguruan Tinggi salah satu institusi pendidikan yang sangat membutuhkan dukungan Teknologi informasi dan komunikasi. Perkembangan teknologi informasi menuntut perguruan tinggi mengelola potensi sumberdaya dengan teknologi informasi secara efektif dan efisien untuk menghadapi persaingan.

Pemanfaatan Teknologi Informasi (TI) dalam tata kelola perguruan tinggi khususnya di STMIK Pelita nusantara telah mengikuti perkembangan TI dan telah berjalan sesuai dengan kebutuhan proses bisnis yang ada dan setiap layanan TI yang di berikan oleh STMIK Pelita nusatara selalu dilakukan perubahan secara berkala sesui dengan kebutuhan pengguna layanan tersebut, hal ini membuktikan bahwa STMIK Pelita Nusantara melakukan proses pengawasan dan pengelolaan. Namun dalam pemanfaatan dan tatakelolanya, apakah sudah sesuai dengan standart TI, hal ini perlu dibuktikan melalui proses audit tatakelola teknologi informasi yang mengacu pada sebuah kerangka kerja. Pengukuran kinerja ini nantinya

dapat membatu proses evaluasi implementasi teknologi informasi pada STMIK Pelita Nusantara dan membantu pengambilan putusan untuk menyeimbangkan antara risiko dan manfaat teknologi informasi dalam membangun dan mengembangkan layanan dan fungsi teknologi informasi yang sesuai dengan kebutuhan dan harapan.

Perlunya perancangan tata kelola agar pelayanan yang diberikan dapat meningkat sesuai dengan tujuan strategis instansi, oleh karena itu sejumlah kerangka acuan pengendalian telah diajukan dan dikembangkan untuk membantu perusahaan maupun instansi dalam menciptakan sistem pengendalian yang baik, diantaranya COBIT serta Tata kelola Teknologi Informasi.

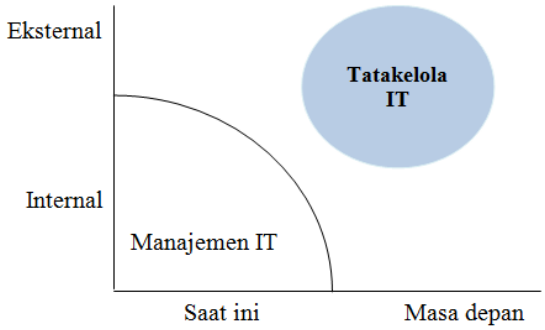
Tata kelola TI adalah suatu struktur dan proses yang saling berhubungan serta mengarahkan dan mengendalikan insatansi dalam pencapaian tujuan perusahaan melalui nilai tambah dan penyeimbangan antara resiko dan manfaat dari teknologi informasi serta prosesnya.

Penggunaan kerangka kerja COBIT terhadap Tata kelola Teknologi Informasi menyediakan struktur yang menyediakan proses TI, sumber daya TI dan informasi bagi STMIK Pelita Nusantara. Tata kelola Teknologi Informasi juga dapat memantau kinerja TI untuk memastikan informasi instansi dan teknologi yang berhubungan mendukung tujuan instansi berdasarkan kerangka kerja COBIT yang memiliki 5 tujuan pengendalian tingkat tinggi yaitu; (1) Evaluate, Direct and Organise (EDM); (2). Align, Plan And Organise (APO); (3). Build, Acquire and Implement (BAI); (4). Deliver, Service and Support; (5). Monitor, Evaluate and Assess[11]. Dengan COBIT, diharapkan penggunaan dan tatakelola IT dapat menghasilkan kerja yang efisien dan efektif serta membuat penggunaan dan pengelolaannya mempertimbangkan integrasi dimana hardware, software dan perangka manusia membangun integrasi.

II. METODOLOGI

IT *governance* merupakan tanggung jawab dari pimpinan puncak dan eksekutif manajemen dari suatu perusahaan. Dijelaskan pula bahwa IT governance merupakan bagian dari pengelolaan perusahaan secara keseluruhan yang terdiri dari kepemimpinan dan struktur organisasi dan proses yang ada adalah untuk memastikan kelanjutan TI organisasi dan pengembangan strategi dan tujuan dari organisasi.[1]

Salah satu kunci fokus tata kelola teknologi informasi adalah untuk menyelaraskan teknologi informasi dengan tujuan bisnis. Sebagai penjelasan dapat dikatakan bahwa tata kelola teknologi informasi adalah perpaduan antara tata kelola perusahaan dan manajemen teknologi informasi. (Grembergen et al. 2005)



Gambar 1. Tata Kelola Teknologi Informasi Dan IT Management.[9]

COBIT (Control Objective for Information and related Technology), dikeluarkan dan disusun oleh IT Governance Institute yang merupakan bagian dari ISACA (Information Systems Audit and Control Association) pada tahun 1996. COBIT merupakan kerangka panduan tata kelola TI atau bisa juga disebut toolset pendukung yang bisa digunakan untuk menjembatani gap antara kebutuhan dan bagaimana teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi.[10]

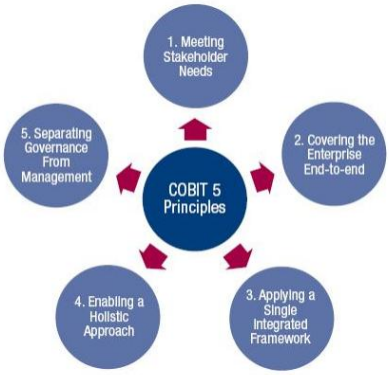
COBIT memungkinkan pengembangan kebijakan yang jelas dan sangat baik digunakan untuk IT kontrol seluruh organisasi, membantu meningkatkan kualitas dan nilai serta menyerdehanakan pelaksanan alur proses sebuah organisasi dari sisi penerapan IT. Adapun salah satu COBIT yang diterbitkan oleh ISACA yaitu COBIT 5. COBIT 5 menyediakan kerangka kerja yang komprehensif yang membantu perusahaan untuk mencapai tujuan mereka dan memberikan nilai melalui pemerintahan yang efektif dan manajemen perusahaan TI.[6]

COBIT 5 didasarkan pada lima prinsip utama untuk tatakelola dan manajemen perusahaan TI [4].

1. Prinsip 1
   Pemenuhan kebutuhan stakeholder setiap perusahaan mempunyai visi dan misi yang berbeda
2. Prinsip 2
   Meliputi enterprise End-to-End menganggap semua tata kelola dan manajemen TI enabler untuk perusahaan
3. Prinsip 3
   Menerapkan Singel Framework yang terpadu Cobit 5 dapat menyesuaikan dengan tatakelola dan manajemen TI pada perusahan
4. Prinsip 4
   Mengaktifkan pendekatan holistik COBIT 5 mendefinisikan satu set enabler untuk mendukung pelaksanaan tata kelola yang

komprehensif dan sistem manajemen TI untuk perusahaan.

5. Prinsip 5
   Pemisahan antara Governance (tata kelola) dengan Manajemen.



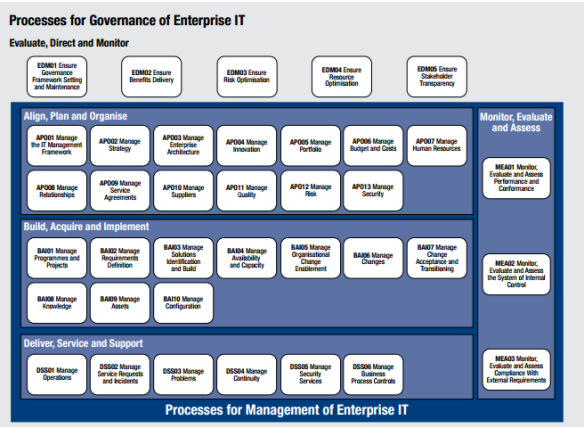
Gambar 2: Cobit 5 principles [Sumber : ISACA, 2012]

Selain ke 5 perinsip tersebut diatas ada 7 *enabler* yang terdapat didalam COBIT 5:[4]-[2]-[12]

1. Prinsip kebijakan dan kerangka kerja
   Adalah kendaraan untuk menerjemahkan perilaku yangdiinginkan menjadi panduan praktis untuk sehari-harimanajemen.
2. Proses
   Menggambarkan set terorganisir praktek dan kegiatanuntuk mencapai tujuan tertentu dan menghasilkan setoutput dalam mendukung pencapaian keseluruhan TI-tujuan yang terkait.
3. Struktur organisasi
   adalah pengambilan keputusan kunci entitas dalamsuatu perusahaan.
4. Budaya etika dan perilaku individu dan perusahaan
   Sangat sering diremehkan sebagai faktor keberhasilandalam kegiatan tata kelola dan manajemen.
5. Informasi
   Diperlukan untuk menjaga organisasi berjalan denganbaik dan diatur, tetapi pada tingkat operasional,informasi sangat sering produk utama dari perusahaanitu sendiri.
6. Layanan infrastruktur dan aplikasi
   Meliputi infrastruktur, teknologi dan aplikasi yangmenyediakan perusahaan dengan pengolahan informasiteknologi dan jasa.
7. Orang keterampilan dan kompetensi
   Diperlukan untuk berhasil menyelesaikan semua kegiatan,dan untuk membuat keputusan yang benar danmengambil tindakan korektif.

COBIT 5 memiliki 5 domain yang terbagi dalam domain *governance* dan *management*, satu domain berasal dari *governance* dan empat lainnya berasal dari *management*.
Domain yang berasal dari area governance of enterprise IT adalah **(Evaluate, Direct, and Monitor) EDM** yang terdiri dari 5 proses. Sedangkan domain yang berasal dari management of enterprise IT sejalan dengan tanggung jawab pada area plan, build, run, and monitor (PBRM). Terdapat 32 proses yang dipecah kedalam masing-masing domain sebagai berikut [2]-[11]:

1. *Align, Plan and Organise* (APO) dengan 13 Proses.
2. *Build, Acquire and Implement* (BAI) dengan 10 proses.
3. *Deliver, Service and Support* (DSS) dengan 6 proses.
4. *Monitor, Evaluate and Assess* (MEA) dengan 3 proses.



Gambar 3 : Cobit 5 Proses [Sumber : ISACA, 2012]

2.1. Proses Capability Model

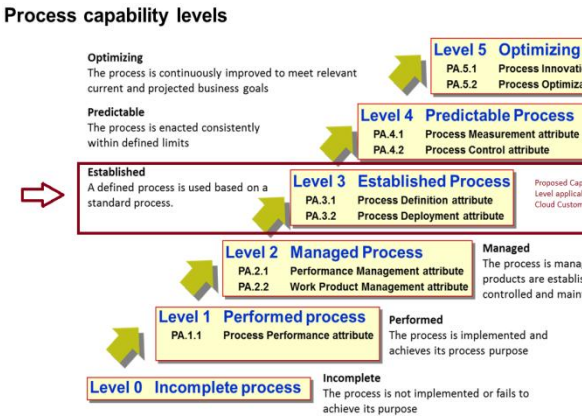
ISO/IEC 15505 mendefinisikan pengukuran untuk penilaian kemampuan proses dari framework COBIT. Process capability didefinisikan pada 6 level poin dari 0 sampai 5, yang mempresentasikan peningkatan capability dari proses yang diimplementasikan [3].

Berikut adalah penjelasan level dari process capability :

TABEL 1. Level Capability

Level	*Value*	Deskripsi
0	*Incomplete*	Tidak dilaksanakan atau gagal mencapai tujuan prosesnya
1	*Performed*	Telah mencapai tujuan prosesnya
2	*Managed*	Level 1 kini diimplementasikan dalam model yang terkelola (direncanakan, dimonitor, dan disesuaikan) dengan kinerja produk tepat didirikan, dikendalikan, dan dipelihara.
3	*Established*	Level 2 kini diimplementasikan menggunakan proses didefinisikan yang mampu mencapai hasil prosesnya

4	*Predictable*	Proses yang dibangun di level 3 kini beroperasi sesuai batas yang ditentukan untuk mencapai hasil prosesnya
5	*Optimized*	Proses yang dapat diprediksi pada level 5 ditingkatkan menerus untuk memenuhi tujuan bisnis terkini yang relevan dan terarah.



Gambar 4 .Process Capability Model [7]

III. HASIL DAN PEMBAHASAN

Setelah dilakukan analisis hasil kuisoner maka di dapatkanlah hasil nilai–nilai pada tiap aktifitas yang ada pada domain *Align, Plan and Organise* (APO) dan *Monitor, Evaluate and Assess* (MEA) setelah itu di masukan ke dalam form kerja audit. Tindakan selanjutnya yang dilakukan adalah mencari rata–rata nilai pada tiap proses untuk mengetahui bagaimana kondisi tiap proses yang ada.

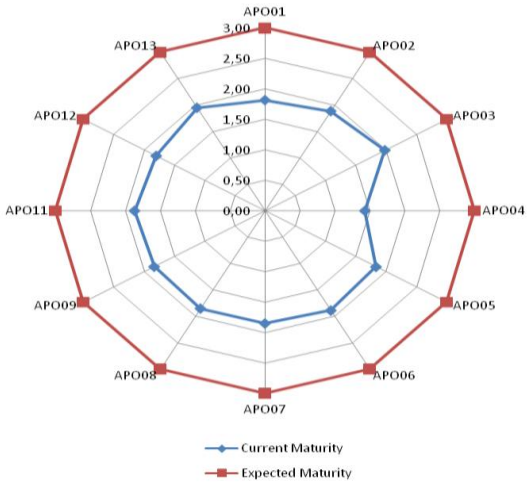
$$Index\ Maturity = \frac{Jumla\ h\ Jawaban}{Jumla\ h\ Soal\ Contr\ ol}$$

Berikut adalah hasil rekapitulasi nilai proses pada domain *Align, Plan and Organise* (APO) dan *Monitor, Evaluate and Assess* (MEA) :

TABEL 2. Rekapitulasi Hasil Perhitungan Tingkat Kematangan TI STMIK PELITA NUSANTARA MEDAN Domain Align, Plan And Organise (APO)

DOMAIN	PROSES	Hasil Pengujian
APO01	Mengelola Kerangka Manajemen TI / Manage the IT Management	1,81
APO02	Mengelola Strategi / Manage Strategy	1,89
APO03	Mengelola Enterprise Architecture/ Manage Enterprise Architecture	1,98
APO04	Mengelola Inovasi / Manage Innovation	1,43
APO05	Mengelola Portofolio / Manage Portfolio	1,84
APO06	Mengelola Anggaran dan Biaya / Manage Budget and Costs	1,89
APO07	Mengelola Sumber Daya Manusia / Manage Human Resources	1,85
APO08	Mengelola Hubungan / Manage Relationships	1,85
APO09	Mengelola Perjanjian Layanan / Manage Service Agreements	1,83
APO11	Mengelola Kualitas /Manage Quality	1,87
APO12	Manage Risk / Manage Risk	1,80
APO13	Mengelola Keamanan / Manage Security	1,95

Dari tabel 2 tingkat kematangan (*maturity level*) domain dapat dibuat representasinya dalam grafik radar, seperti yang terlihat pada gambar 4 berikut ini:

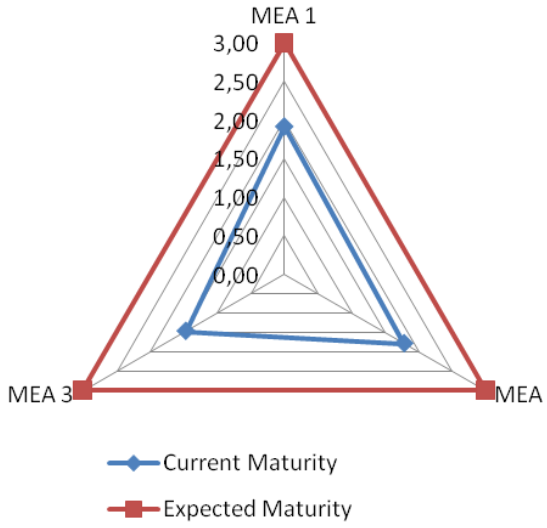


Gambar 5. Grafik *Current maturity* level vs *Expected maturity* level pada domain *Align, Plan and Organise* (APO).

TABEL 3. Rekapitulasi Hasil Perhitungan Tingkat Kematangan TI STMIK PELITA NUSANTARA Medan Domain Monitor, Evaluate and Assess (MEA)

Domain	Proses	Hasil Pengujian
MEA 1	Monitor, Evaluasi dan Menilai Kinerja dan Conformance/Monitor, Evaluate and Assess Performance and Conformance.	1,91
MEA 2	Monitor, Evaluasi dan Asses Sistem Pengendalian Intern/Monitor, Evaluate and Asses the System of Internal Control	1,78
MEA 3	Mengevaluasi dan Menilai Kepatuhan Persyaratan Eksternal/Evaluate and Assess Compliance with External Requirements	1,46

Dari tabel 3 tingkat kematangan (*maturity level*) domain dapat dibuat representasinya dalam grafik radar, seperti yang terlihat pada gambar 5 berikut ini:



Gambar 6. Grafik *Current maturity* level vs *Expected maturity* level pada domain *Monitor, Evaluate and Assess* (MEA).

TABEL 4. Hasil Implikasi Penelitian

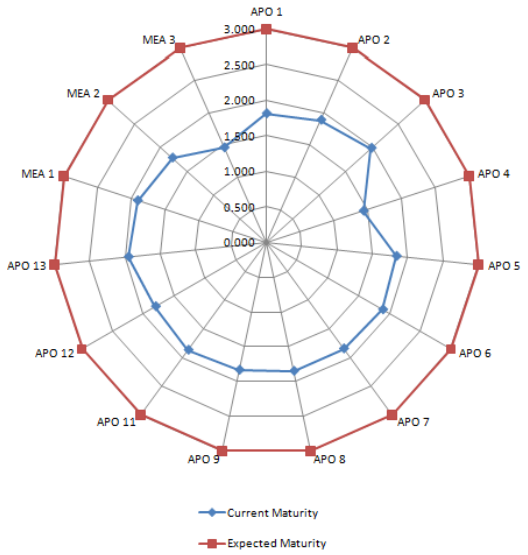
Domain	Proses	Current Maturity	Expected Maturity	Selisih/Gap	Status Perbaikan	
APO 1	Mengelola Kerangka Manajemen TI / Manage the IT Management	1,814	3	1,186	Super prioritas	Diperbaiki
APO 2	Mengelola Strategi / Manage Strategy	1,886	3	1,114	Super prioritas	Diperbaiki
APO 3	Mengelola Enterprise Architecture/ Manage Enterprise Architecture	1,985	3	1,015	Super prioritas	Diperbaiki
APO 4	Mengelola Inovasi / Manage Innovation	1,433	3	1,567	Super prioritas	Diperbaiki
APO 5	Mengelola Portofolio / Manage Portfolio	1,838	3	1,163	Super prioritas	Diperbaiki
APO 6	Mengelola Anggaran dan Biaya / Manage Budget and Costs	1,888	3	1,112	Super prioritas	Diperbaiki
APO 7	Mengelola Sumber Daya Manusia / Manage Human Resources	1,846	3	1,154	Super prioritas	Diperbaiki
APO 8	Mengelola Hubungan / Manage Relationships	1,850	3	1,150	Super prioritas	Diperbaiki
APO 9	Mengelola Perjanjian Layanan / Manage Service Agreements	1,833	3	1,167	Super prioritas	Diperbaiki
APO 11	Mengelola Kualitas /Manage Quality	1,869	3	1,131	Super prioritas	Diperbaiki
APO 12	Manage Risk / Manage Risk	1,800	3	1,200	Super prioritas	Diperbaiki
APO 13	Mengelola Keamanan / Manage Security	1,950	3	1,050	Super prioritas	Diperbaiki
MEA 1	Monitor, Evaluasi dan Menilai Kinerja dan Conformance/Monitor, Evaluate and Assess Performance and Conformance.	1,907	3	1,093	Super prioritas	Diperbaiki
MEA 2	Monitor, Evaluasi dan Asses Sistem Pengendalian Intern/Monitor, Evaluate and Asses the System of Internal Control	1,780	3	1,220	Super prioritas	Diperbaiki
MEA 3	Mengevaluasi dan Menilai Kepatuhan Persyaratan Eksternal/Evaluate and Assess Compliance with External Requirements	1,460	3	1,540	Super prioritas	Diperbaiki

TABEL 5. *GAP* Antara *Current Maturity* Dan *Expected Maturity* Pada Penerapan Sistem Informasi STMIK PELITA NUSANTARA MEDAN Domain *APO* Dan *MEA*

Domain	Proses	Current Maturity	Expected Maturity	Selisih/Gap
APO 1	Mengelola Kerangka Manajemen TI / Manage the IT Management	1,814	3	1,186
APO 2	Mengelola Strategi / Manage Strategy	1,886	3	1,114
APO 3	Mengelola Enterprise Architecture/ Manage Enterprise Architecture	1,985	3	1,015
APO 4	Mengelola Inovasi / Manage Innovation	1,433	3	1,567
APO 5	Mengelola Portofolio / Manage Portfolio	1,838	3	1,163
APO 6	Mengelola Anggaran dan Biaya / Manage Budget and Costs	1,888	3	1,112
APO 7	Mengelola Sumber Daya Manusia / Manage Human Resources	1,846	3	1,154
APO 8	Mengelola Hubungan / Manage Relationships	1,850	3	1,150
APO 9	Mengelola Perjanjian Layanan / Manage Service Agreements	1,833	3	1,167
APO 11	Mengelola Kualitas /Manage Quality	1,869	3	1,131
APO 12	Manage Risk / Manage Risk	1,800	3	1,200

APO 13	Mengelola Keamanan / Manage Security	1,950	3	1,050
MEA 1	Monitor, Evaluasi dan Menilai Kinerja dan Conformance/Monitor, Evaluate and Assess Performance and Conformance.	1,907	3	1,093
MEA 2	Monitor, Evaluasi dan Asses Sistem Pengendalian Intern/Monitor, Evaluate and Asses the System of Internal Control	1,780	3	1,220
MEA 3	Mengevaluasi dan Menilai Kepatuhan Persyaratan Eksternal/Evaluate and Assess Compliance with External Requirements	1,460	3	1,540

Dari tabel 5 tingkat kematangan (*maturity level*) domain dapat dibuat representasinya dalam grafik radar, seperti yang terlihat pada gambar 4 berikut ini:

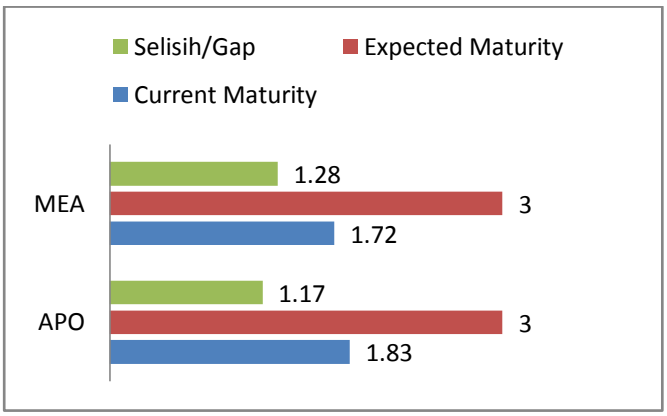


Gambar 6. Grafik rexume *Current maturity* level vs *Expected maturity* level pada domain *MEA dan APO*.

TABEL 6
Rexume Current Maturity Dan *Expected Maturity* Pada Penerapan Sistem Informasi STMIK PELITA NUSANTARA MEDAN Domain *APO* Dan *MEA*

MATURITY LEVEL	**DOMAIN**		
	APO	***MEA***	***APO,MEA***
Expected	3	3	3
Rata-rata	1.83	1.75	1.80
Minimal	1.43	1.46	1.50
Maksimal	1.96	1.90	1.95

Dari tabel VI tingkat kematangan (*maturity level*) domain dapat dibuat representasinya dalam grafik radar, seperti yang terlihat pada gambar 4 berikut ini:



Gambar 7. Grafik Rexume *Current maturity* level vs *Expected maturity* level pada domain *MEA dan* APO.

Dari hasil audit yang dilaksanakan, pengukuran *capability level* proses area APO dan MEA STMIK Pelita Nusantara, diperoleh hasil level kapabilitas 1.83 pada domain APO, 1.75 pada Domain MEA, level rata-rata 1,80, artinya MEA dan APO sedang dalam tahap menuju *capability level* 2 dan masih mencapai 0,20 di atas level 1. Pembulatan ke atas dipilih sesuai dengan konsep penentuan *capability level* proses tertentu. Maka dari itu untuk APO dan MEA *capability level* sudah dianggap 2, sehingga *capability level* target yang diinginkan adalah level yang sedang ditujunya yaitu level 3.

IV.KESIMPULAN

Berdasarkan audit yang dilakukan pada STMIK Pelita Nusantara Medan dengan framework COBIT 5 Domain Align, Plan And Organise (APO) dan domain *Monitor, Evaluate and Assess* (MEA) maka kesimpulan adalah :

1. Berdasarkan hasil pengukuran tingkat maturitas IT pada STMIK Pelita Nusantara Medan dengan menggunakan kerangka kerja CobIT 5, didapatkan tingkat maturitas masih berada dibawah standar yang telah ditentukan yaitu masih berada pada level lebih kecil dari 3. Artinya tingkat maturitas tata kelola TI STMIK Pelita Nusantara Medan masih banyak perlu perbaikan.

2. Dari hasil evaluasi *capability level* pada area domain MEA dan APO, STMIK Pelita Nusantara berada pada level 1 (performed) dari kesuluruhan proses Align, Plan And Organise (APO) dan domain *Monitor, Evaluate and Assess* (MEA).
3. Dari hasil audit yang dilaksanakan, pengukuran capability level proses area APO dan MEA pada STMIK Pelita Nusantara Medan, diperoleh hasil level kapabilitas 1, level rata-rata 1,80 , artinya APO11 sedang dalam tahap menuju capability level 2 dan masih mencapai 0,80 di atas level 1. Pembulatan ke keatas dipilih sesuai dengan konsep penentuan capability levelproses tertentu. Maka dari itu untuk APO dan MEA capability level masih dianggap 1, sehingga capability level target yang diinginkan adalah level yang sedang ditujunya yaitu level 3.
4. Berdasarkan hasil analisa *gap* yang diperoleh, didapatkan jarak *gap* semuanya berada pada level diatas 1, hal ini berarti masih banyak yang harus diperbaiki oleh STMIK Pelita Nusantara dan harus secepat mungkin tindakan perbaikannya.
5. Menurut *capability level* masing-masing proses, ditentukan level target masing-masing proses yaitu 2 level di atas *capability level* STMIK Pelita Nusantara Medan saat dinilai, sehingga target *capability level* yang ingin dicapai adalah level 3 (*Estabilished process*) untuk masing-masing proses MEA dan APO.
6. Untuk mengurangi gap antara capability level saat ini dan capability level yang ingin dicapai, maka STMIK Pelita Nusantara Medan harus memenuhi PA2.1,PA2.2, PA3.1 dan PA3.2, agar capability level saat ini yang berada pada level 1 dapat naik ke level 3. Sejalan dengan itu, STMIK Pelita Nusantara Medan semakin mendekati tujuan.

Hal ini dapat dikatakan secara menyeluruh proses tata kelola TI di STMIK Pelita Nusantara Medan belum memenuhi standar internasional sesuai dengan yang ditetapkan oleh CobIT (Control Objectives for Information and related Technology) dalam tata kelola teknologi informasi.

REFERENCES

[1].COBIT Steering Committee and the IT Governance Institute, 2000, COBIT (3rd Edition) Implementation Tool Set, IT Governance Institute, http://www.isaca.org.

[2].ISACA. 2012. COBIT 5: A Business Framework for Governance & Management IT.

[3].Jung, Ho-Won, Robin Hunter. 2001. The Relationship Between ISO/IEC 15504 Process Capability Levels, ISO 9001 Certification and Organization Size: An Empirical Study. Elsevi

[4].M.Garsoux.2013.COBIT 5 ISACA's new framework for IT Governance, Risk,Security and Auditing *http://www.qualified-audit-partners.be/user_files/QECB_GLC_COBIT_5_ISACA_s_new_framework_201303.pdf*

[5].Capability-Levels *http://www.tutorialspoint.com/cmmi/pdf/cmmi-capability-levels.pdf*

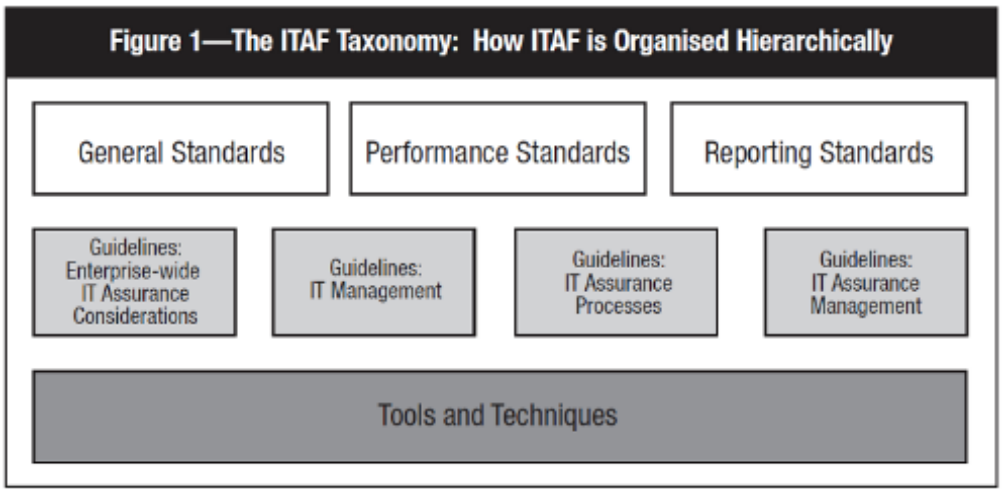
[6].IT Governance Institute. 2007. COBIT 4.1: Framework Control Objectives Management Guidelines Maturity Model. USA: Rolling Meadow.

[7].Ben Martin. 2013.Cloud Services and the definition of a Target Operating Model. *Information Technology Infrastructure Library* (ITIL)

ITAF adalah model yang komprehensif dan memberikan panduan praktek tentang penerapan nya, meliputi :

- Memberikan bimbingan pada desain, pelaksanaan dan pelaporan IS audit dan jaminan tugas
- Mendefinisikan istilah dan konsep spesifik untuk jaminan IS
- Menetapkan standar bahwa alamat IS audit dan jaminan peran dan tanggung jawab profesional; pengetahuan dan keterampilan dan ketekunan, perilaku dan persyaratan pelaporan

ITAF menyediakan satu sumber di mana IS audit dan jaminan profesional dapat mencari bimbingan, kebijakan dan prosedur penelitian, mendapatkan program audit dan jaminan, dan mengembangkan laporan yang efektif.



Standar Umum dalam ITAF

Standar umum adalah prinsip-prinsip di mana IS audit dan jaminan profesional beroperasi. Prinsip dan jaminan tersebut berlaku untuk pelaksanaan semua tugas dan penanganan audit IS dan jaminan profesional etika, kemandirian, objektivitas dan perawatan karena, serta pengetahuan, kompetensi dan keterampilan. Standar umum ini mencakup audit charter, independensi organisasi, independensi tenaga profesional, ekspektasi yang logis, perlindungan tenaga profesional, profil, pernyataan tegas dan kriteria. Audit charter memastikan adanya fungsi audit yang jelas mencakup tujuan, tanggung jawab dan akuntabilitas audit. Independensi organisasi memastikan fungsi audit berlaku objektif pada seluruh bagian organisasi dan selurh proses di dalamnya. Independensi tenaga profesional memastikan auditor berperilaku sama kepada seluruh auditee termasuk sikap perilaku dalam proses audit.

Ekspektasi yang logis memastikan ekspektasi audit yang rasional dengan standar peraturan yang berlaku dan opini tenaga audit profesional. Perlindungan tenaga profesional dalam arti ketaatan terhadap standar audit yang berlaku dalam perencanaan, proses hingga pelaporan. Profil terkait hasil audit atau penilaian lain yang sebelumnya telah dilakukan dan kompetensi auditor yang melakukan tugas audit di perusahaan. Pernyataan tegas yang menegaskan bahwa proses audit telah dilakukan pada bagian tertentu dengan memberikan hasil audit yang dikategorikan sebagai mencukupi, valid dan relevan. Kriteria yang digunakan harus menjawab kebutuhan informasi audit seperti asasaran audit, keutuhan, relevan, terukur, dapat dimengerti, dikenal umum (penggunaan standar) dan sesuai dengan pengguna hasil audit.

Standar ITAF adalah standar yang berfokus dan mengacu pada ISACA, dimana setiap perkembangannya menyesuaikan dengan perkembangan ISACA, sedangkan COBIT adalah satu metode pengelolaan teknologi informasi yang digunakan secara luas adalah IT governance yang terdapat pada COBIT (Control Objectives for Information and Related Technology). COBIT dapat dikatakan sebagai kerangka kerja teknologi informasi yang dipublikasikan oleh ISACA (Information System Audit and Control Association). COBIT berfungsi mempertemukan semua bisnis kebutuhan kontrol dan isu-isu teknik. Di samping itu, COBIT juga dirancang agar dapat menjadi alat bantu yang dapat memecahkan permasalahan pada IT governance dalam memahami dan mengelola resiko serta keuntungan yang behubungan dengan sumber daya informasi perusahaan.

TUGAS KELOMPOK

IS AUDIT AND ASSURANCE STANDARDS

"1002 Organisational Independence"

Mata Kuliah : IT Audit

Dosen Pengasuh : Dr. Widya Cholil, S.Kom., M.IT.

Disusun oleh :

1. **Reni Septiyanti**
2. **Evan Apriadi Dilatama**
3. **Fero Triando**
4. **Fitrianto Puja Kesuma**

Reguler B Angkatan 19 (Sembilan Belas)

Program Pascasarjana Magister Teknik Informatika

Universitas Bina Darma Palembang

2019

AUDIT SISTEM INFORMASI DAN STANDAR JAMINAN

Audit Sistem Informasi dan Standar Jaminan merupakan aspek-aspek utama yang dirancang untuk membantu audit Sistem Informasi, salah satunya adalah **Standar 1002 Organisational Independence (Kemandirian Organisasi).**

1002 Organisational Independence (Kemandirian Organisasi).

1002.1 Fungsi audit dan jaminan IS harus independen dari area atau aktivitas yang ditinjau untuk memungkinkan penyelesaian obyektif audit dan perikatan jaminan.

Aspek Utama Fungsi audit dan penjaminan IS harus:

- Melaporkan ke tingkat dalam organisasi yang diaudit yang memberikan independensi organisasi dan memungkinkan fungsi audit dan penjaminan IS untuk melakukan tanggung jawabnya tanpa campur tangan.
- Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika independensi mengalami gangguan dalam penampilan atau penampilan.
- Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karena peran tersebut dapat merusak independensi di masa depan.
- Mengatasi independensi dan akuntabilitas fungsi audit dalam piagam dan / atau surat perjanjian.

Istilah	Definisi
Kerusakan	Suatu kondisi yang menyebabkan kelemahan atau berkurangnya kemampuan untuk melaksanakan tujuan audit. Kerusakan pada independensi organisasi dan obyektivitas individu dapat mencakup konflik kepentingan pribadi; batasan ruang lingkup; pembatasan akses ke catatan, personel, peralatan, atau fasilitas; dan keterbatasan sumber daya (seperti pendanaan atau penempatan staf).
Kebebasan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup Kemandirian pikiran dan Kemandirian dalam penampilan.
Kemandirian dalam penampilan	Menghindari fakta dan keadaan yang begitu signifikan sehingga pihak ketiga yang berpengetahuan akan cenderung menyimpulkan, menimbang semua fakta dan keadaan tertentu, bahwa perusahaan, fungsi audit atau anggota integritas, objektivitas atau skeptisisme profesional tim audit telah disepakati.
Kemandirian pikiran	Keadaan pikiran yang memungkinkan ekspresi kesimpulan tanpa dipengaruhi oleh pengaruh yang membahayakan penilaian profesional, dengan demikian memungkinkan individu untuk bertindak dengan integritas dan menjalankan obyektivitas dan skeptisisme profesional
Objektivitas	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi tanpa memihak.

Tautan ke Pedoman

Tipe	Judul
Pedoman	2002 Kemandirian Organisasi

Tanggal Operatif — Standar ISACA ini berlaku untuk semua audit SI dan perjanjian jaminan mulai 1 November 2013.

2002 Kemandirian Organisasi

Pedoman disajikan dalam bagian berikut:

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman
3. Keterkaitan dengan standar dan proses COBIT 5
4. Terminologi
5. Tanggal berlaku

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan Bagian ini mengklarifikasi:

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tujuan dari pedoman ini adalah untuk membahas independensi fungsi audit dan jaminan IS di perusahaan. Tiga aspek penting dipertimbangkan:

- Posisi audit SI dan fungsi jaminan dalam perusahaan
- Tingkat yang dilaporkan oleh audit IS dan fungsi jaminan di dalam perusahaan
- Kinerja layanan non-audit dalam perusahaan oleh audit SI dan manajemen jaminan serta audit SI dan profesional jaminan

1.1.2 Pedoman ini memberikan panduan untuk menilai independensi organisasi dan merinci hubungan antara independensi organisasi dan piagam audit serta rencana audit.

1.1.3 IS profesional audit dan jaminan harus mempertimbangkan pedoman ini ketika menentukan bagaimana menerapkan standar, menggunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan mencari panduan tambahan jika dianggap perlu.

1.2 Keterkaitan dengan Standar

1.2.1 Standar 1001 Piagam Audit

1.2.2 Standar 1002 Kemandirian Organisasi

1.2.3 Standar 1003 Independensi Profesional

1.2.4 Standar 1004 Harapan yang Wajar

1.2.5 Standar 1006 Kemahiran

1.3 Istilah Penggunaan 1.3.1 Selanjutnya:

- 'Fungsi audit dan penjaminan IS' disebut sebagai 'fungsi audit'
- 'Profesional audit dan penjaminan' disebut sebagai 'profesional'

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang topik utama audit IS dan keterlibatan asuransi:

2.1 Posisi dalam perusahaan

2.2 Tingkat pelaporan

2.3 Layanan non-audit

2.4 Menilai independensi

2.5 Piagam audit dan rencana audit

2002 Kemandirian Organisasi (lanjutan)

2.1 Posisi dalam Perusahaan

2.1.1 Untuk memungkinkan kemandirian organisasi, fungsi audit perlu memiliki posisi di perusahaan yang memungkinkannya untuk melakukan tanggung jawabnya tanpa campur tangan. Ini dapat dicapai dengan:

- Menetapkan fungsi audit dalam piagam audit sebagai fungsi atau departemen independen, di luar departemen operasional. Fungsi audit tidak boleh diberi tanggung jawab atau kegiatan operasional apa pun.
- Memastikan bahwa fungsi audit melapor ke tingkat dalam perusahaan yang memungkinkannya mencapai independensi organisasi. Pelaporan ke kepala departemen operasional dapat membahayakan independensi organisasi, seperti yang dijelaskan secara lebih rinci di bagian 2.2.

2.1.2 Fungsi audit harus menghindari pelaksanaan peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen, karena peran tersebut dapat merusak independensi di masa depan. Independensi dan akuntabilitas fungsi audit harus dialamatkan dalam piagam audit, sebagaimana dijelaskan dalam Piagam Audit Standar 1001.

2.2 Tingkat Pelaporan

2.2.1 Fungsi audit harus melaporkan ke tingkat dalam perusahaan yang memungkinkannya untuk bertindak dengan independensi organisasi yang lengkap. Independensi harus didefinisikan dalam piagam audit dan dikonfirmasi oleh fungsi audit kepada dewan direksi dan pihak yang bertanggung jawab atas tata kelola secara teratur, setidaknya setiap tahun.

2.2.2 Untuk memastikan independensi organisasi dalam fungsi audit, hal-hal berikut harus dilaporkan kepada pihak yang bertanggung jawab atas tata kelola (misalnya, dewan direksi) untuk masukan dan / atau persetujuan mereka:

- Rencana dan anggaran sumber daya audit
- Rencana audit (berbasis risiko)
- Tindak lanjut kinerja yang dilakukan oleh fungsi audit pada aktivitas audit IS
- Tindak lanjut dari ruang lingkup yang signifikan atau keterbatasan sumber daya

2.2.3 Untuk memastikan independensi organisasi dalam fungsi audit, diperlukan dukungan eksplisit dari dewan dan manajemen eksekutif.

2.3 Layanan Non-audit

2.3.1 Di banyak perusahaan, harapan manajemen dan staf IS adalah bahwa fungsi audit dapat terlibat dalam menyediakan layanan non-audit. Ini melibatkan, paruh waktu atau paruh waktu, partisipasi para profesional dalam inisiatif SI dan tim proyek SI untuk menyediakan kemampuan penasehat atau konsultatif.

2.3.2 Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggap bukan tanggung jawab manajemen dan, karenanya, tidak akan mengganggu independensi. Layanan non-audit yang juga tidak akan merusak independensi atau objektivitas, jika pengamanan yang memadai dilaksanakan, termasuk memberikan saran rutin tentang risiko dan kontrol teknologi informasi.

2.3.3 Layanan non-audit berikut ini dianggap merusak independensi dan objektivitas, karena ancaman yang dibuat akan sangat signifikan sehingga tidak ada perlindungan yang dapat mengurangi mereka ke tingkat yang dapat diterima:

- Menganggap tanggung jawab manajemen atau melakukan kegiatan manajemen
- Keterlibatan material para profesional dalam pengawasan atau kinerja merancang, mengembangkan, menguji, memasang, mengonfigurasikan atau mengoperasikan sistem informasi yang material atau signifikan dengan subjek audit atau perikatan jaminan.
- Merancang kontrol untuk sistem informasi yang material atau signifikan dengan subjek perikatan audit saat ini atau yang akan datang
- Melayani dalam peran tata kelola di mana para profesional bertanggung jawab baik secara mandiri atau bersama-sama membuat keputusan manajemen atau menyetujui kebijakan dan standar
- Memberikan saran yang membentuk dasar utama keputusan manajemen

2.3.4 Menyediakan layanan non-audit di bidang-bidang yang saat ini, atau di masa depan, masalah perikatan audit juga menciptakan ancaman terhadap independensi yang akan sulit diatasi dengan perlindungan. Dalam situasi ini, persepsi mungkin bahwa

independensi dan obyektivitas fungsi audit dan profesional telah dirugikan dengan melakukan layanan non-audit di bidang tertentu. Fungsi audit dan profesional harus menentukan apakah pengamanan yang memadai dapat diimplementasikan untuk memitigasi ancaman aktual atau yang dirasakan ini terhadap independensi secara memadai.

2.3.5 Pedoman lebih rinci tentang cara menangani ancaman independensi ini dapat ditemukan dalam Standar 1003 Kemandirian Profesional dan Pedoman terkait 2003.

2.4 Menilai Independensi

2.4.1 Independensi harus dinilai secara berkala oleh fungsi audit dan profesional. Penilaian ini perlu terjadi setiap tahun untuk fungsi audit dan sebelum setiap perikatan untuk para profesional, sebagaimana dijelaskan dalam Standar 1003 Independensi Profesional. Penilaian harus mempertimbangkan faktor-faktor seperti:

- Perubahan dalam hubungan pribadi
- Kepentingan finansial
- Penugasan dan tanggung jawab pekerjaan sebelumnya

2.4.2 Fungsi audit perlu mengungkapkan kemungkinan masalah terkait independensi organisasi dan mendiskusikannya dengan dewan direksi atau pihak yang bertanggung jawab atas tata kelola. Resolusi perlu ditemukan dan dikonfirmasi dalam piagam audit atau rencana audit.

2.5 Piagam Audit dan Rencana Audit

2.5.1 Piagam audit harus merinci, di bawah aspek 'tanggung jawab', implementasi independensi organisasi dari fungsi audit. Selain merinci independensi, piagam audit juga harus mencakup kemungkinan penurunan independensi.

2.5.2 Independensi organisasi juga harus tercermin dalam rencana audit. Fungsi audit harus dapat menentukan ruang lingkup rencana secara independen, tanpa batasan yang diberlakukan oleh manajemen eksekutif.

3. Keterkaitan dengan Standar dan Proses COBIT 5

3.0 Pendahuluan

Bagian ini memberikan ikhtisar yang relevan:

3.1 Keterkaitan dengan standar

3.2 Keterkaitan dengan proses COBIT 5

3.3 Pedoman lain

3.1 Keterkaitan dengan Standar

Tabel ini memberikan ikhtisar tentang:

- Standar audit dan jaminan ISACA IS yang paling relevan yang didukung langsung oleh pedoman ini
- Pernyataan standar yang paling relevan dengan pedoman ini Catatan: Hanya pernyataan standar yang relevan dengan pedoman ini yang terdaftar

Judul Standar	Pernyataan Standar yang Relevan
1001 Piagam Audit	Fungsi audit dan penjaminan IS harus mendokumentasikan fungsi audit dengan tepat dalam piagam audit, yang menunjukkan tujuan, tanggung jawab, wewenang, dan akuntabilitas. Fungsi audit dan jaminan SI harus memiliki piagam audit yang disepakati dan disetujui pada tingkat yang sesuai dalam perusahaan.
1002 Kemandirian Organisasi	Fungsi audit dan jaminan IS harus independen dari area atau aktivitas yang ditinjau untuk memungkinkan penyelesaian obyektif audit dan perikatan jaminan.
1003 Independensi Profesional	Profesional audit dan penjaminan IS harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang terkait dengan audit dan perikatan assurance.
1004 Harapan yang Wajar	Profesional audit dan penjaminan IS harus memiliki ekspektasi yang masuk akal bahwa ruang lingkup perikatan memungkinkan kesimpulan atas pokok permasalahan dan mengatasi segala pembatasan.
1006 Kemahiran	Profesional audit dan penjaminan IS, bersama-sama dengan orang lain yang membantu penugasan, harus memiliki keterampilan dan kecakapan yang memadai dalam melakukan audit SI dan keterlibatan penjaminan serta kompeten secara profesional untuk melakukan pekerjaan yang diperlukan.

3.2 Keterkaitan dengan Proses COBIT 5

Tabel ini memberikan ikhtisar yang paling relevan:

- Proses cobit 5
- Tujuan proses cobit 5 aktivitas spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini tercantum dalam cobit 5: proses yang memungkinkan

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pengaturan dan pemeliharaan kerangka tata kelola.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan strategi dan tujuan perusahaan, pastikan bahwa proses terkait TI diawasi secara efektif dan transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
APO01 Kelola kerangka kerja manajemen TI.	Memberikan pendekatan manajemen yang konsisten untuk memungkinkan terpenuhinya persyaratan tata kelola perusahaan, yang mencakup proses manajemen, struktur organisasi, peran dan tanggung jawab, kegiatan yang andal dan dapat diulang, serta keterampilan dan kompetensi.
MEA02 Memantau,	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan

mengevaluasi dan menilai sistem pengendalian internal.	kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

3.3 Panduan Lain

Ketika menerapkan standar dan pedoman, profesional didorong untuk mencari panduan lain bila dianggap perlu. Ini bisa dari audit IS dan jaminan:

- Kolega di dalam dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam perusahaan, misalnya, komite audit
- Panduan profesional lainnya (mis. Buku, makalah, pedoman lain)

4. Terminologi

Istilah	Definisi
Kemerdekaan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup kemandirian pikiran dan kemandirian dalam penampilan.
Objektivitas	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi tanpa memihak

5. Tanggal Efektif

5.1 Tanggal Efektif Pedoman ini berlaku untuk semua audit SI dan perjanjian jaminan yang dimulai pada atau setelah 1 September 2014.

IT AUDIT

Nama : Fido Rizki (182420060)

Program Studi Teknik Informatika S-2

Pascasarjana Universitas Bina Darma

SOAL

Pilih salah satu Standard yang ada pada dokumen ITAF (materi), dan jelaskan secara ringkas fungsi dari standard tersebut pada Audit TI dan jelaskan keterkaitannya dengan COBIT atau framework lain.

JAWABAN :

Standard yang dipilih ialah **1001 (*Audit Charter*)**

Piagam Audit Internal (Internal Audit Charter) adalah pedoman bagi Auditor/Internal Controller agar dapat melaksanakan tugasnya secara profesional, memperoleh hasil Audit yang sesuai dengan standar mutu, dan dapat diterima oleh berbagai pihak baik internal maupun external. Piagam Audit Internal menjelaskan tujuan, wewenang, tanggung jawab dan keorganisasian Satuan Audit & Kontrol Internal.

Fungsi dan Tujuan dari *Audit Charter*:

- Audit & Kontrol Internal berfungsi untuk membantu Manajemen dalam merencanakan dan mengimplementasikan prinsip-prinsip pengawasan manajerial dan fungsi-fungsi operasional Perusahaan.
- Tujuan Audit & Kontrol Internal adalah memberi nilai tambah pada kinerja operasional Perusahaan baik dari faktor efisiensi maupun efektivitas operasional sesuai dengan standar mutu yang berlaku

Hubungan Cobit dengan Framework

Audit Teknologi adalah evaluasi secara sistematis dan objektif yang dilakukan oleh Auditor Teknologi terhadap aset teknologi untuk mencapai tujuan Audit Teknologi sehingga memberikan nilai tambah dan meningkatkan kinerja pihak yang diaudit (auditee) atau pemilik kepentingan. Audit Teknologi tidak dimaksudkan untuk mencari kesalahan, namun dimaksudkan untuk melakukan perbaikan. Audit Teknologi merupakan mata rantai dari prinsip "Rencana–Pelaksanaan– Evaluasi–Perbaikan" (PDCA cycle), dimana Audit Teknologi merupakan mata rantai evaluasi.

Framework Audit Teknologi adalah model kerangka kerja yang memberikan acuan dalam perancangan, pelaksanaan dan pelaporan audit teknologi, mendefinisikan terminologi dan konsep

spesifik bagi audit teknologi, menetapkan standar persyaratan bagi peran, tanggung jawab, pengetahuan dan keahlian auditor teknologi, kepatuhan, pelaksanaan dan pelaporan. Demikian luasnya spektrum dan cakupan audit tekologi, yang mencakup berbagai sektor teknologi, sehingga keberadaan Framework Audit Teknologi menjadi kebutuhan yang vital bagi pelaksanaan audit teknologi yang berkualitas. Framework Audit Teknologi secara umum mengadopsi model yang serupa yang diterapkan pada Framework Audit Internal dan Framework Audit Teknologi Informasi (ITAF – Information Technology Assurance Framework). Framework memberikan gambaran hubungan antara standar dan kode etik audit teknologi, pedoman umum audit teknologi dan panduan audit teknologi, serta kerangka penggunaannya.

Framework Audit Teknologi dan semua dokumen yang tercakup didalamnya merupakan dokumen yang dinamis, hidup, dan akan selalu dikembangkan dan diperbaiki di masa mendatang untuk memastikan bahwa best practice akan diadopsi dalam audit teknologi.

Framework Audit Teknologi terdiri dari beberapa tingkatan/ hirarki dokumen yang masing-masing memiliki fungsi berbeda. Setiap tingkatan memiliki kode dokumen yang unik dan berbeda, sehingga dari kode dokumen dapat dipahami fungsi dari dokumen tersebut.

-16- Struktur dan hubungan antara bagian-bagian dalam Framework Audit Teknologi digambarkan dalam diagram dibawah dan dapat dijelaskan sebagai berikut. Dokumen dengan daftar istilah dan definisi yang menjelaskan pemahaman umum tentang hal-hal terkait dengan audit teknologi yang digunakan dalam dokumen tersebut, baik yang bersifat umum maupun khusus terkait sektor atau tujuan audit teknologi. Diagram struktur kaitan berbagai dokumen audit teknologi dalam framework dapat dilihat di bawah:

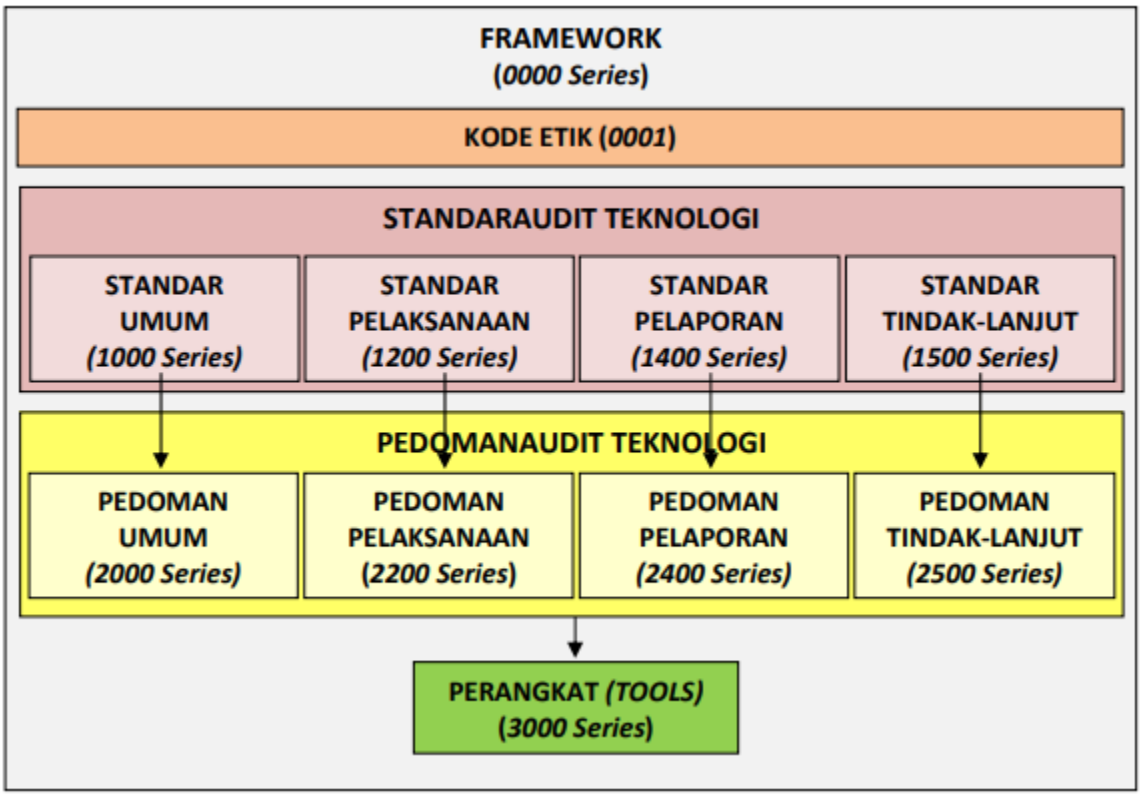


Diagram Struktur Dokumen Audit Teknologi dalam Framework

Standar Umum (1000 Series)

Standar Umum menjelaskan tentang kualifikasi dari auditor teknologi dan atau institusi yang memberikan layanan jasa audit teknologi sehingga pekerjaan audit teknologi sampai pelaporannya dapat terlaksana dengan baik dan efektif.

1001. Tujuan, Wewenang dan Tanggung-jawab

Tujuan, wewenang dan tanggung jawab suatu aktivitas audit teknologi harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa Piagam Audit Teknologi (TechnologyAudit Charter), surat tugas atau dokumen yang setara.

Penjelasan:

Piagam Audit Tekhnologi (Technology Audit Charter), surat tugas atau dokumen yang setara harus mencantumkan hal-hal sebagai berikut:

- tujuan, sasaran dan lingkup audit teknologi yang dilaksanakan;
- wewenang, tanggung jawab, dan akuntabilitas dari auditor teknologi;

- hubungan yang jelas antara auditor teknologi dengan klien, kemudahan akses terhadap data dan informasi, personil serta properti yang terkait dengan pencapaian tujuan audit teknologi.

1001

Audit Charter (Piagam Audit)

DISUSUN OLEH:

1. FIDO RIZKI
2. MUHAMMAD DIAH MAULIDIN

KELAS : REGULER A R1

MATA KULIAH : IT AUDIT

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

Fungsi 1001 Audit Charter

- Menyiapkan dokumen audit untuk mendefinisikan kegiatan audit sistem informasi internal dan fungsi penjaminan dengan cukup detail;
- Sebagai wewewang, tujuan, tanggung jawab dan batasan audit sistem informasi dan fungsi jaminan;
- Rahasia dan akurat dalam penjaminan audit sistem informasi;
- Peran dan tanggung jawab pihak yang diaudit;
- Standar professional yang akan diikuti oleh audit Sistem Informasi dan profesional penjaminan dalam pelaksanaan audit Sistem Informasi dan perjanjian jaminan;

Fungsi 1001 Audit Charter

- Tinjau dokumen audit setidaknya setiap tahun atau lebih sering jika tanggung jawab berubah;
- Memperbarui dokumen audit sesuai kebutuhan untuk memastikan bahwa tujuan dan tanggung jawab telah dan tetap didokumentasikan dengan tepat. Secara formal mengkomunikasikan audit charter kepada pihak yang diaudit untuk setiap audit Sistem Informasi atau perikatan jaminan.

Peranan 1001 Audit Charter

- Untuk membantu profesional audit dan penjaminan Sistem informasi dalam menyiapkan dokumen audit;
- Untuk membantu dalam mendefinisikan tujuan, tanggung jawab, wewenang dan akuntabilitas audit Sistem Informasi dan fungsi jaminan;
- Sebagai pedoman saat menentukan cara menerapkan standar, penilaian dan penerapannya, membantu dalam membenarkan setiap kegiatan dan pencarian pedoman tambahan jika dianggap perlu.

Pedoman 1001 Audit Charter

- Pedoman 1001 Audit Charter mengacu kepada 2001 Audit Charter
- Tujuan pedoman 2001 Audit Charter untuk membantu audit Sistem Informasi dan profesional penjaminan dalam menyiapkan Audit Charter. Audit Charter mendefinisikan tujuan, tanggung jawab, wewenang dan akuntabilitas audit IS dan fungsi jaminan.
- Audit Sistem Informasi dan professional penjaminan harus mempertimbangkan pedoman 2001 Audit Charter ketika menentukan bagaimana menerapkan standar dan menggunakan penilaian profesional dalam penerapan.

Pedoman 2001 Audit Charter

- Pedoman 2001 Audit Charter membahas empat aspek yaitu tujuan, tanggung jawab, wewenang dan akuntabilitas.
- Tujuan Pedoman 2001 Audit Charter berisi tentang tujuan, penjelasan objektivitas fungsi audit, cakupan audit dan wewenang isi fungsi audit charter.
- Tanggung jawab Pedoman 2001 Audit Chater berisi prinsip operasi, independen, hubungan audit eksternal, expetasi auditor, kemampuan auditor dan komunikasi auditor.

Pedoman 2001 Audit Charter

- Wewenang Pedoman 2001 Audit Charter berisi akses yang relevan, pembatasan wewenang dan proses audit.
- Akuntanbilitas Pedoman 2001 Audit Charter berisi struktur organisasi, laporan tentang detail format, performa fungsi audit, kepatuhan dengan standar yang detail, proses penjaminan kualitas, aturan kepegawaian untuk perikatan audit, komitmen pendidikan berkelanjutan dari fungsi audit dan tindakan yang disetujui terkait fungsi audit.

1001 Audit Charter Link ke Proses COBIT 5

- Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses yang terdapat dalam COBIT 5 yaitu

  COBIT 5: Enabling Processes

Proses COBIT 5	Tujuan Proses
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Memperoleh transparansi bagi para pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

TERIMA KASIH

Nama : Fitrianto Puja Kesuma

NIM : 182420082

AUDIT SISTEM INFORMASI DAN STANDAR JAMINAN

Audit Sistem Informasi dan Standar Jaminan merupakan aspek-aspek utama yang dirancang untuk membantu audit Sistem Informasi, salah satunya adalah **Standar 1002 Organisational Independence (Kemandirian Organisasi).**

1002 Organisational Independence (Kemandirian Organisasi).

1002.1 Fungsi audit dan jaminan IS harus independen dari area atau aktivitas yang ditinjau untuk memungkinkan penyelesaian obyektif audit dan perikatan jaminan.

Aspek Utama Fungsi audit dan penjaminan IS harus:

- Melaporkan ke tingkat dalam organisasi yang diaudit yang memberikan independensi organisasi dan memungkinkan fungsi audit dan penjaminan IS untuk melakukan tanggung jawabnya tanpa campur tangan.
- Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika independensi mengalami gangguan dalam penampilan atau penampilan.
- Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karena peran tersebut dapat merusak independensi di masa depan.
- Mengatasi independensi dan akuntabilitas fungsi audit dalam piagam dan / atau surat perjanjian.

Istilah	Definisi
Kerusakan	Suatu kondisi yang menyebabkan kelemahan atau berkurangnya kemampuan untuk melaksanakan tujuan audit. Kerusakan pada independensi organisasi dan obyektivitas individu dapat mencakup konflik kepentingan pribadi; batasan ruang lingkup; pembatasan akses ke catatan, personel, peralatan, atau fasilitas; dan keterbatasan sumber daya (seperti pendanaan atau penempatan staf).
Kebebasan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup Kemandirian pikiran dan Kemandirian dalam penampilan.
Kemandirian dalam penampilan	Menghindari fakta dan keadaan yang begitu signifikan sehingga pihak ketiga yang berpengetahuan akan cenderung menyimpulkan, menimbang semua fakta dan keadaan tertentu, bahwa perusahaan, fungsi audit atau anggota integritas, objektivitas atau skeptisisme profesional tim audit telah disepakati.
Kemandirian pikiran	Keadaan pikiran yang memungkinkan ekspresi kesimpulan tanpa dipengaruhi oleh pengaruh yang membahayakan penilaian profesional, dengan demikian memungkinkan individu untuk bertindak dengan integritas dan menjalankan obyektivitas dan skeptisisme profesional
Objektivitas	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi tanpa memihak.

Tautan ke Pedoman

Tipe	Judul
Pedoman	2002 Kemandirian Organisasi

Tanggal Operatif — Standar ISACA ini berlaku untuk semua audit SI dan perjanjian jaminan mulai 1 November 2013.

2002 Kemandirian Organisasi

Pedoman disajikan dalam bagian berikut:

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman
3. Keterkaitan dengan standar dan proses COBIT 5
4. Terminologi
5. Tanggal berlaku

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan Bagian ini mengklarifikasi:

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tujuan dari pedoman ini adalah untuk membahas independensi fungsi audit dan jaminan IS di perusahaan. Tiga aspek penting dipertimbangkan:

- Posisi audit SI dan fungsi jaminan dalam perusahaan
- Tingkat yang dilaporkan oleh audit IS dan fungsi jaminan di dalam perusahaan
- Kinerja layanan non-audit dalam perusahaan oleh audit SI dan manajemen jaminan serta audit SI dan profesional jaminan

1.1.2 Pedoman ini memberikan panduan untuk menilai independensi organisasi dan merinci hubungan antara independensi organisasi dan piagam audit serta rencana audit.

1.1.3 IS profesional audit dan jaminan harus mempertimbangkan pedoman ini ketika menentukan bagaimana menerapkan standar, menggunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan mencari panduan tambahan jika dianggap perlu.

1.2 Keterkaitan dengan Standar

1.2.1 Standar 1001 Piagam Audit

1.2.2 Standar 1002 Kemandirian Organisasi

1.2.3 Standar 1003 Independensi Profesional

1.2.4 Standar 1004 Harapan yang Wajar

1.2.5 Standar 1006 Kemahiran

1.3 Istilah Penggunaan 1.3.1 Selanjutnya:

- 'Fungsi audit dan penjaminan IS' disebut sebagai 'fungsi audit'
- 'Profesional audit dan penjaminan' disebut sebagai 'profesional'

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang topik utama audit IS dan keterlibatan asuransi:

2.1 Posisi dalam perusahaan

2.2 Tingkat pelaporan

2.3 Layanan non-audit

2.4 Menilai independensi

2.5 Piagam audit dan rencana audit

2002 Kemandirian Organisasi (lanjutan)

2.1 Posisi dalam Perusahaan

2.1.1 Untuk memungkinkan kemandirian organisasi, fungsi audit perlu memiliki posisi di perusahaan yang memungkinkannya untuk melakukan tanggung jawabnya tanpa campur tangan. Ini dapat dicapai dengan:

- Menetapkan fungsi audit dalam piagam audit sebagai fungsi atau departemen independen, di luar departemen operasional. Fungsi audit tidak boleh diberi tanggung jawab atau kegiatan operasional apa pun.
- Memastikan bahwa fungsi audit melapor ke tingkat dalam perusahaan yang memungkinkannya mencapai independensi organisasi. Pelaporan ke kepala departemen operasional dapat membahayakan independensi organisasi, seperti yang dijelaskan secara lebih rinci di bagian 2.2.

2.1.2 Fungsi audit harus menghindari pelaksanaan peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen, karena peran tersebut dapat merusak independensi di masa depan. Independensi dan akuntabilitas fungsi audit harus dialamatkan dalam piagam audit, sebagaimana dijelaskan dalam Piagam Audit Standar 1001.

2.2 Tingkat Pelaporan

2.2.1 Fungsi audit harus melaporkan ke tingkat dalam perusahaan yang memungkinkannya untuk bertindak dengan independensi organisasi yang lengkap. Independensi harus didefinisikan dalam piagam audit dan dikonfirmasi oleh fungsi audit kepada dewan direksi dan pihak yang bertanggung jawab atas tata kelola secara teratur, setidaknya setiap tahun.

2.2.2 Untuk memastikan independensi organisasi dalam fungsi audit, hal-hal berikut harus dilaporkan kepada pihak yang bertanggung jawab atas tata kelola (misalnya, dewan direksi) untuk masukan dan / atau persetujuan mereka:

- Rencana dan anggaran sumber daya audit
- Rencana audit (berbasis risiko)
- Tindak lanjut kinerja yang dilakukan oleh fungsi audit pada aktivitas audit IS
- Tindak lanjut dari ruang lingkup yang signifikan atau keterbatasan sumber daya

2.2.3 Untuk memastikan independensi organisasi dalam fungsi audit, diperlukan dukungan eksplisit dari dewan dan manajemen eksekutif.

2.3 Layanan Non-audit

2.3.1 Di banyak perusahaan, harapan manajemen dan staf IS adalah bahwa fungsi audit dapat terlibat dalam menyediakan layanan non-audit. Ini melibatkan, paruh waktu atau paruh waktu, partisipasi para profesional dalam inisiatif SI dan tim proyek SI untuk menyediakan kemampuan penasehat atau konsultatif.

2.3.2 Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggap bukan tanggung jawab manajemen dan, karenanya, tidak akan mengganggu independensi. Layanan non-audit yang juga tidak akan merusak independensi atau objektivitas, jika pengamanan yang memadai dilaksanakan, termasuk memberikan saran rutin tentang risiko dan kontrol teknologi informasi.

2.3.3 Layanan non-audit berikut ini dianggap merusak independensi dan objektivitas, karena ancaman yang dibuat akan sangat signifikan sehingga tidak ada perlindungan yang dapat mengurangi mereka ke tingkat yang dapat diterima:

- Menganggap tanggung jawab manajemen atau melakukan kegiatan manajemen
- Keterlibatan material para profesional dalam pengawasan atau kinerja merancang, mengembangkan, menguji, memasang, mengonfigurasikan atau mengoperasikan sistem informasi yang material atau signifikan dengan subjek audit atau perikatan jaminan.
- Merancang kontrol untuk sistem informasi yang material atau signifikan dengan subjek perikatan audit saat ini atau yang akan datang
- Melayani dalam peran tata kelola di mana para profesional bertanggung jawab baik secara mandiri atau bersama-sama membuat keputusan manajemen atau menyetujui kebijakan dan standar
- Memberikan saran yang membentuk dasar utama keputusan manajemen

2.3.4 Menyediakan layanan non-audit di bidang-bidang yang saat ini, atau di masa depan, masalah perikatan audit juga menciptakan ancaman terhadap independensi yang akan sulit diatasi dengan perlindungan. Dalam situasi ini, persepsi mungkin bahwa independensi dan obyektivitas fungsi audit dan profesional telah dirugikan dengan melakukan layanan non-audit di bidang tertentu. Fungsi audit dan profesional harus menentukan apakah pengamanan yang memadai dapat diimplementasikan untuk memitigasi ancaman aktual atau yang dirasakan ini terhadap independensi secara memadai.

2.3.5 Pedoman lebih rinci tentang cara menangani ancaman independensi ini dapat ditemukan dalam Standar 1003 Kemandirian Profesional dan Pedoman terkait 2003.

2.4 Menilai Independensi

2.4.1 Independensi harus dinilai secara berkala oleh fungsi audit dan profesional. Penilaian ini perlu terjadi setiap tahun untuk fungsi audit dan sebelum setiap perikatan untuk para profesional, sebagaimana dijelaskan dalam Standar 1003 Independensi Profesional. Penilaian harus mempertimbangkan faktor-faktor seperti:

- Perubahan dalam hubungan pribadi
- Kepentingan finansial
- Penugasan dan tanggung jawab pekerjaan sebelumnya

2.4.2 Fungsi audit perlu mengungkapkan kemungkinan masalah terkait independensi organisasi dan mendiskusikannya dengan dewan direksi atau pihak yang bertanggung jawab atas tata kelola. Resolusi perlu ditemukan dan dikonfirmasi dalam piagam audit atau rencana audit.

2.5 Piagam Audit dan Rencana Audit

2.5.1 Piagam audit harus merinci, di bawah aspek 'tanggung jawab', implementasi independensi organisasi dari fungsi audit. Selain merinci independensi, piagam audit juga harus mencakup kemungkinan penurunan independensi.

2.5.2 Independensi organisasi juga harus tercermin dalam rencana audit. Fungsi audit harus dapat menentukan ruang lingkup rencana secara independen, tanpa batasan yang diberlakukan oleh manajemen eksekutif.

3. Keterkaitan dengan Standar dan Proses COBIT 5

3.0 Pendahuluan

Bagian ini memberikan ikhtisar yang relevan:

3.1 Keterkaitan dengan standar

3.2 Keterkaitan dengan proses COBIT 5

3.3 Pedoman lain

3.1 Keterkaitan dengan Standar

Tabel ini memberikan ikhtisar tentang:

- Standar audit dan jaminan ISACA IS yang paling relevan yang didukung langsung oleh pedoman ini
- Pernyataan standar yang paling relevan dengan pedoman ini Catatan: Hanya pernyataan standar yang relevan dengan pedoman ini yang terdaftar

Judul Standar	Pernyataan Standar yang Relevan
1001 Piagam Audit	Fungsi audit dan penjaminan IS harus mendokumentasikan fungsi audit dengan tepat dalam piagam audit, yang menunjukkan tujuan, tanggung jawab, wewenang, dan akuntabilitas. Fungsi audit dan jaminan SI harus memiliki

	piagam audit yang disepakati dan disetujui pada tingkat yang sesuai dalam perusahaan.
1002 Kemandirian Organisasi	Fungsi audit dan jaminan IS harus independen dari area atau aktivitas yang ditinjau untuk memungkinkan penyelesaian obyektif audit dan perikatan jaminan.
1003 Independensi Profesional	Profesional audit dan penjaminan IS harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang terkait dengan audit dan perikatan assurance.
1004 Harapan yang Wajar	Profesional audit dan penjaminan IS harus memiliki ekspektasi yang masuk akal bahwa ruang lingkup perikatan memungkinkan kesimpulan atas pokok permasalahan dan mengatasi segala pembatasan.
1006 Kemahiran	Profesional audit dan penjaminan IS, bersama-sama dengan orang lain yang membantu penugasan, harus memiliki keterampilan dan kecakapan yang memadai dalam melakukan audit SI dan keterlibatan penjaminan serta kompeten secara profesional untuk melakukan pekerjaan yang diperlukan.

3.2 Keterkaitan dengan Proses COBIT 5

Tabel ini memberikan ikhtisar yang paling relevan:

- Proses cobit 5
- Tujuan proses cobit 5 aktivitas spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini tercantum dalam cobit 5: proses yang memungkinkan

Proses COBIT 5	**Tujuan proses**
EDM01 Pastikan pengaturan dan pemeliharaan kerangka tata kelola.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan strategi dan tujuan perusahaan, pastikan bahwa proses terkait TI diawasi secara efektif dan transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
APO01 Kelola kerangka kerja manajemen TI.	Memberikan pendekatan manajemen yang konsisten untuk memungkinkan terpenuhinya persyaratan tata kelola perusahaan, yang mencakup proses manajemen, struktur organisasi, peran dan tanggung jawab, kegiatan yang andal dan dapat diulang, serta keterampilan dan kompetensi.
MEA02 Memantau, mengevaluasi dan menilai sistem pengendalian internal.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

3.3 Panduan Lain

Ketika menerapkan standar dan pedoman, profesional didorong untuk mencari panduan lain bila dianggap perlu. Ini bisa dari audit IS dan jaminan:

- Kolega di dalam dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam perusahaan, misalnya, komite audit
- Panduan profesional lainnya (mis. Buku, makalah, pedoman lain)

4. Terminologi

Istilah	Definisi
Kemerdekaan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup kemandirian pikiran dan kemandirian dalam penampilan.
Objektivitas	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi tanpa memihak

5. Tanggal Efektif

5.1 Tanggal Efektif Pedoman ini berlaku untuk semua audit SI dan perjanjian jaminan yang dimulai pada atau setelah 1 September 2014.

IS Audit 1205 Evidence

Kelompok 2
Gina
Defry
Dendi
Erin

1205. Evidence/Bukti

1205.1. IS Audit dan penjaminan professional harus mendapatkan bukti yang cukup dan sesuai untuk menarik kesimpulan yang masuk akal yang menjadi dasar hasil keterlibatan.

1205.2. IS Audit dan penjaminan professional harus mengevaluasi kecukupan bukti yang diperoleh untuk mendukung kesimpulan dan mencapai tujuan keterlibatan

1205. Pernyataan Bukti

Key Aspect

Dalam melakukan keterlibatan, IS Audit dan penjaminan professional harus:

- Dapatkan bukti yang cukup dan tepat, termasuk:
  - Prosedur seperti yang dilakukan.
  - Hasil prosedur dilakukan.
  - Sumber dokumen (baik dalam format elektronik atau kertas), mencatat dan menguatkan informasi yang digunakan untuk mendukung keterlibatan.
  - Temuan dan hasil keterlibatan.
  - Dokumentasi bahwa pekerjaan dilakukan dan mematuhi undang-undang, peraturan, dan kebijakan yang berlaku.

- Siapkan dokumentasi, yang seharusnya:
  - Ditahan dan tersedia untuk jangka waktu tertentu dan dalam format yang sesuai dengan kebijakan organisasi audit atau jaminan dan standar profesional yang relevan, hukum dan peraturan.
  - Dilindungi dari pengungkapan atau modifikasi yang tidak sah selama persiapan dan penyimpanannya.
  - Dibuang dengan benar pada akhir periode retensi.

- Pertimbangkan kecukupan bukti untuk mendukung tingkat risiko pengendalian yang dinilai saat memperoleh bukti dari uji pengendalian.

- Identifikasi secara tepat, referensi silang dan katalog bukti.

- Pertimbangkan properti seperti sumber, jenis (misal., Tulisan, lisan, visual, elektronik) dan keaslian (misal. Tanda tangan digital dan manual, perangko) dari bukti saat mengevaluasi keandalannya.

- Pertimbangkan cara yang paling efektif dan tepat waktu untuk mengumpulkan bukti yang diperlukan untuk memenuhi tujuan dan risiko keterlibatan. Namun, kesulitan atau biaya bukan merupakan dasar yang valid untuk menghilangkan prosedur yang diperlukan.

- Pilih prosedur yang paling tepat untuk mengumpulkan bukti tergantung pada subjek yang diaudit (yaitu, sifatnya, waktu audit, penilaian profesional). Prosedur yang digunakan untuk mendapatkan bukti meliputi:
  - Permintaan dan konfirmasi.
  - Kinerja ulang
  - Perhitungan ulang
  - Komputasi

- Prosedur analitik
- Inspeksi
- Pengamatan
- Metode lain yang diterima secara umum

- Pertimbangkan sumber dan sifat informasi apa pun yang diperoleh untuk mengevaluasi keandalannya dan persyaratan verifikasi lebih lanjut. Secara umum, keandalan bukti lebih besar ketika:
  - Dalam bentuk tertulis, bukan ekspresi lisan
  - Diperoleh dari sumber independen
  - Diperoleh oleh profesional daripada oleh entitas yang diaudit
  - Disertifikasi oleh pihak independen
  - Dipertahankan oleh pihak independen
  - Hasil pemeriksaan
  - Hasil pengamatan

- Dapatkan bukti objektif yang memadai untuk memungkinkan pihak independen yang berkualifikasi untuk melakukan pengujian ulang dan mendapatkan hasil dan kesimpulan yang sama.

- Dapatkan bukti yang sepadan dengan materialitas item dan risiko yang terlibat.

- Tempatkan penekanan pada keakuratan dan kelengkapan informasi ketika informasi yang diperoleh dari perusahaan digunakan oleh audit SI atau profesional penjamin untuk melakukan prosedur audit.

- Bukti aman terhadap akses dan modifikasi yang tidak sah.

- Menyimpan bukti setelah menyelesaikan audit SI atau pekerjaan jaminan selama diperlukan untuk mematuhi semua hukum, peraturan, dan kebijakan yang berlaku.

1205. Bukti Lanjutan

Ketentuan

Ketentuan	Definisi
Bukti yang sesuai	Ukuran kualitas bukti
Bukti yang cukup	Ukuran kuantitas bukti; mendukung semua pertanyaan material untuk tujuan dan ruang lingkup audit. Lihat bukti.

Keterkaitan dengan Standar dan Pedoman

Tipe	Judul
Pedoman	2205 Bukti

IT AUDIT

1202 Risk Assessment in Planning

Kelompok 4 (Empat)

1. Yuniarti Denita Sari
2. Raju Septa Wijaya
3. Hendri

Dosen Pengampuh : Dr. Widya Cholil, S.Kom., M.IT.

Kelas : MTI 19 Reguler **B**

Magister Teknik Informatika
PASCASARJANA
Universitas Bina Darma Palembang

2019

1202. Risk Assessment in Planning

1202.1 Fungsi audit dan penjaminan IS harus menggunakan pendekatan penilaian risiko yang sesuai dan metodologi pendukung untuk dikembangkan rencana audit SI keseluruhan dan menentukan prioritas untuk alokasi sumber daya audit SI yang efektif.

1202.2 IS audit dan jaminan profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area yang dikaji, ketika merencanakan keterlibatan individu.

1202.3 Profesional audit dan penjaminan IS harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.

Key Aspects (Aspek Kunci)

Saat merencanakan kegiatan yang sedang berlangsung, fungsi audit dan jaminan SI harus:

- Melakukan dan mendokumentasikan, setidaknya setiap tahun, penilaian risiko untuk memfasilitasi pengembangan rencana audit SI.
- Sertakan, sebagai bagian dari penilaian risiko, rencana dan sasaran strategis organisasi dan perusahaan kerangka kerja dan inisiatif manajemen risiko.
- Untuk setiap audit SI dan perikatan jaminan, menghitung dan membenarkan jumlah sumber daya audit SI yang diperlukan untuk memenuhi persyaratan keterlibatan.
- Gunakan penilaian risiko dalam pemilihan area dan item yang menjadi minat audit dan keputusan untuk merancang dan melakukan audit IS dan keterlibatan jaminan tertentu.
- Mencari persetujuan penilaian risiko dari pemangku kepentingan audit dan pihak terkait lainnya.
- Prioritaskan dan jadwalkan pekerjaan audit dan penjaminan IS berdasarkan penilaian risiko.
- Berdasarkan penilaian risiko, kembangkan sebuah rencana yang:
    - Bertindak sebagai kerangka kerja untuk aktivitas audit dan penjaminan IS
    - Mempertimbangkan persyaratan dan kegiatan audit dan jaminan non-IS
    - Diperbarui setidaknya setiap tahun dan disetujui oleh pihak yang bertanggung jawab atas tata kelola
    - Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

Saat merencanakan keterlibatan individu, profesional audit dan penjaminan IS harus:

- Identifikasi dan nilai risiko yang relevan dengan area yang dikaji.

- Melakukan penilaian awal terhadap risiko yang relevan dengan area yang dikaji untuk setiap keterlibatan. Tujuan untuk setiap keterlibatan spesifik harus mencerminkan hasil penilaian risiko awal.
- Dalam mempertimbangkan bidang-bidang risiko dan merencanakan perikatan khusus, pertimbangkan audit, tinjauan, dan temuan sebelumnya, termasuk setiap kegiatan perbaikan. Juga pertimbangkan proses penilaian risiko menyeluruh dewan.
- Berusaha untuk mengurangi risiko audit ke tingkat yang dapat diterima, dan memenuhi tujuan audit dengan tepat penilaian materi IS dan kontrol terkait, saat merencanakan dan melakukan audit IS.
- Saat merencanakan prosedur audit IS spesifik, kenali bahwa semakin rendah ambang materialitas, semakin banyak tepatkan harapan audit dan semakin besar risiko audit.
- Untuk mengurangi risiko materialitas yang lebih tinggi, ganti rugi dengan memperpanjang uji kontrol (kurangi risiko kontrol) dan / atau memperluas prosedur pengujian substantif (mengurangi risiko deteksi) untuk mendapatkan jaminan tambahan.

Terms (ISTILAH)	**Definition(DEFINISI)**
Audit risk (Risiko audit)	Risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah: • Kontrol risiko • Risiko deteksi • Risiko yang melekat
Audit subject matter risk (Risiko materi pelajaran audit)	Risiko relevan dengan area yang sedang ditinjau: • Risiko bisnis (kemampuan pelanggan untuk membayar, kelayakan kredit, faktor pasar, dll.) • Risiko kontrak (kewajiban, harga, jenis, penalti, dll.) • Risiko negara (politik, lingkungan, keamanan, dll.) • Risiko proyek (sumber daya, keahlian, metodologi, stabilitas produk, dll.) • Risiko teknologi (solusi, arsitektur, perangkat keras, dan infrastruktur perangkat lunak jaringan, saluran pengiriman, dll.)
Control risk	Risiko bahwa ada kesalahan materi yang tidak akan dicegah atau

(Kendalikan risiko)	terdeteksi pada dasar tepat waktu oleh sistem pengendalian internal.
Detection risk (Risiko deteksi)	Risiko bahwa IS akan mengaudit atau prosedur substantif profesional jaminan akan tidak mendeteksi kesalahan yang bisa bersifat material, secara individu atau dalam kombinasi dengan lainnya kesalahan.
Inherent risk (Risiko yang melekat)	Tingkat risiko atau paparan tanpa memperhitungkan tindakan yang dilakukan manajemen telah mengambil atau mungkin mengambil (mis., menerapkan kontrol).
Materiality (Materialitas)	Konsep audit mengenai pentingnya item informasi yang berkaitan dengan dampak atau pengaruhnya terhadap fungsi entitas yang diaudit. Ekspresi dari signifikansi relatif atau pentingnya suatu hal tertentu dalam konteks perusahaan secara keseluruhan.
Risk assessment (Tugas beresiko)	Suatu proses yang digunakan untuk mengidentifikasi dan mengevaluasi risiko dan potensi dampaknya. Penilaian risiko digunakan untuk mengidentifikasi item-item atau area yang menyajikan risiko tertinggi, kerentanan atau paparan terhadap perusahaan untuk dimasukkan dalam IS rencana audit tahunan. Penilaian risiko juga digunakan untuk mengelola pengiriman proyek dan proyek risiko manfaat.
Substantive testing (Pengujian substantif)	Memperoleh bukti audit tentang kelengkapan, keakuratan, atau keberadaan kegiatan atau transaksi selama periode audit

Linkage to Guidelines **(Tautan ke Pedoman)**

Tipe	Judul
Guideline(Pedoman)	2202 Penilaian Risiko dalam Perencanaan

2202 Penilaian Risiko dan Perencanaan Audit

Pedoman disajikan dalam bagian berikut:

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman

3. Keterkaitan dengan standar dan proses COBIT 5

4. Terminologi

5. Tanggal efektif

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan

Bagian ini mengklarifikasi:

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tingkat pekerjaan audit yang diperlukan untuk memenuhi tujuan audit adalah keputusan subyektif yang dibuat oleh audit IS dan profesional penjaminan. Tujuan pedoman ini adalah untuk mengurangi risiko mencapai kesalahan kesimpulan berdasarkan temuan audit dan untuk mengurangi adanya kesalahan dalam area yang diaudit.

1.1.2 Pedoman ini memberikan panduan dalam menerapkan pendekatan penilaian risiko untuk mengembangkan:

• IS rencana audit yang mencakup semua perikatan audit tahunan

• Rencana proyek perikatan audit yang berfokus pada satu perikatan audit tertentu

1.1.3 Pedoman ini memberikan perincian tentang berbagai jenis risiko audit dan jaminan IS pertemuan profesional.

1.1.4 Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

1.2 Tautan ke

Standar

1.2.1 Perencanaan Keterlibatan Standar 1201

1.2.2 Standar 1202 Penilaian Risiko dalam Perencanaan

1.2.3 Standar 1203 Kinerja dan Pengawasan

1.2.4 Material 1204 Standar

1.2.5 Standar 1207 Penyimpangan dan Tindakan Ilegal

1.3 Penggunaan Jangka

1.3.1 Selanjutnya:

- 'Fungsi audit dan penjaminan IS' disebut sebagai 'fungsi audit'
- 'Profesional audit dan penjaminan' disebut sebagai 'profesional'

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang audit dan jaminan utama berikut topik keterlibatan:

2.1 Penilaian risiko dari rencana audit SI

2.2 Metodologi penilaian risiko

2.3 Penilaian risiko perikatan audit perorangan

2.4 Risiko audit

2.5 Risiko yang melekat

2.6 Mengontrol risiko

2.7 Risiko deteksi

2.1 Risiko Penilaian atas IS Rencana Audit

2.1.1 Ketika mengembangkan rencana audit SI secara keseluruhan, pendekatan penilaian risiko yang sesuai harus diikuti. Sebuah resiko penilaian harus dilakukan dan didokumentasikan setidaknya setiap tahun untuk memfasilitasi proses pengembangan dari rencana audit IS. Ini harus mempertimbangkan rencana dan sasaran strategis organisasi dan kerangka kerja dan inisiatif manajemen risiko perusahaan.

2.1.2 Untuk menilai dengan benar dan lengkap risiko yang terkait dengan cakupan lengkap area audit IS, profesional harus mempertimbangkan elemen-elemen berikut ketika mengembangkan rencana audit SI:

- Cakupan penuh semua area dalam lingkup semesta audit IS, yang mewakili kisaran semua kemungkinan kegiatan audit
- Keandalan dan kesesuaian penilaian risiko yang disediakan oleh manajemen
- Proses diikuti oleh manajemen untuk mengawasi, memeriksa, dan melaporkan risiko atau masalah yang mungkin terjadi

- Menutup risiko dalam kegiatan terkait yang relevan dengan kegiatan yang sedang ditinjau

2.1.3 Pendekatan penilaian risiko yang diterapkan harus membantu proses penentuan prioritas dan penjadwalan IS audit dan assurance berfungsi. Ini harus mendukung pemilihan bidang dan item kepentingan audit dan proses pengambilan keputusan untuk merancang dan melakukan perikatan audit IS tertentu.

2.1.4 Profesional harus memastikan bahwa pendekatan penilaian risiko yang diterapkan disetujui oleh mereka yang dituduh pemerintahan dan didistribusikan ke berbagai pemangku kepentingan pelibatan

2.1.5 Profesional harus menggunakan penilaian risiko untuk mengukur dan membenarkan jumlah sumber daya audit SI yang dibutuhkan untuk menyelesaikan rencana audit IS dan persyaratan untuk keterlibatan khusus

2.1.6 Berdasarkan penilaian risiko, para profesional harus mengembangkan rencana audit IS yang bertindak sebagai kerangka kerja untuk kegiatan audit dan penjaminan IS. Itu harus:

- Mempertimbangkan audit dan persyaratan serta kegiatan non-SI audit
- Diperbarui setidaknya setiap tahun
- Disetujui oleh mereka yang bertanggung jawab atas tata kelola
- Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

2.2 Risiko Penilaian Metodologi

2.2.1 Profesional harus mempertimbangkan metodologi penilaian risiko yang tepat untuk memastikan lengkap dan cakupan yang akurat dari perikatan audit dalam rencana audit SI.

2.2.2 Profesional harus setidaknya menyertakan analisis, dalam metodologi, risiko yang terkait dengan perusahaan untuk ketersediaan sistem, integritas data, dan kerahasiaan informasi bisnis.

2.2.3 Banyak metodologi penilaian risiko tersedia untuk mendukung proses penilaian risiko. Ini mulai dari klasifikasi sederhana tinggi, sedang dan rendah, berdasarkan penilaian profesional, hingga lebih banyak lagi perhitungan kuantitatif dan ilmiah memberikan peringkat risiko numerik, dan lainnya yang merupakan kombinasi di antara dua. Profesional harus mempertimbangkan tingkat kompleksitas dan detail yang sesuai untuk perusahaan atau subjek yang diaudit. Panduan khusus tentang melakukan penilaian risiko dapat ditemukan di ISACA publikasi *COBIT 5 untuk Risiko* .

2.2.4 Semua metodologi penilaian risiko bergantung pada penilaian subyektif di beberapa titik dalam proses (misalnya, untuk menugaskan bobot ke berbagai parameter). Profesional harus mengidentifikasi keputusan subjektif yang diperlukan untuk menggunakan metodologi tertentu dan mempertimbangkan apakah penilaian ini dapat dibuat dan divalidasi menjadi tingkat akurasi yang sesuai.

2.2.5 Dalam memutuskan metodologi penilaian risiko mana yang paling tepat, para profesional harus mempertimbangkannya hal-hal sebagai:

- Jenis informasi yang harus dikumpulkan (beberapa sistem menggunakan efek finansial sebagai satu-satunya ukuran ini tidak selalu sesuai untuk perikatan audit IS)
- Biaya perangkat lunak atau lisensi lain yang diperlukan untuk menggunakan metodologi ini
- Sejauh mana informasi yang diperlukan sudah tersedia
- Jumlah informasi tambahan yang harus dikumpulkan sebelum hasil yang andal dapat diperoleh, dan biaya pengumpulan informasi ini (termasuk waktu yang diperlukan untuk diinvestasikan dalam latihan pengumpulan)
- Pendapat dari pengguna lain dari metodologi, dan pandangan mereka tentang seberapa baik telah membantu mereka dalam meningkatkan efisiensi dan / atau efektivitas audit mereka
- Kesediaan mereka yang bertanggung jawab atas tata kelola area audit IS untuk menerima metodologi sebagai sarana untuk menentukan jenis dan tingkat pekerjaan audit yang dilakukan

2.2.6 Tidak ada metodologi penilaian risiko tunggal yang diharapkan sesuai dalam semua situasi. Kondisi mempengaruhi audit dapat berubah seiring waktu. Secara berkala, profesional harus mengevaluasi kembali kesesuaian metodologi penilaian risiko yang dipilih.

2.2.7 Para profesional harus menggunakan teknik penilaian risiko yang dipilih dalam mengembangkan rencana audit SI keseluruhan dan dalam perencanaan pengikatan audit khusus. Penilaian risiko, dalam kombinasi dengan teknik audit lainnya, harus dipertimbangkan dalam membuat keputusan perencanaan seperti:

- Area atau fungsi bisnis yang akan diaudit
- Jumlah waktu dan sumber daya yang akan dialokasikan untuk audit

• Sifat, luas dan waktu prosedur audit

2.2.8 Metodologi penilaian risiko yang diadopsi harus menghasilkan yang konsisten, valid, dapat dibandingkan, dan dapat diulang hasil. Penilaian risiko yang keluar dari metodologi harus konsisten (selama periode), valid, sebanding (dengan penilaian awal / nanti menggunakan metodologi penilaian yang sama) dan berulang (diberikan seperangkat fakta yang serupa, menggunakan metodologi penilaian yang sama akan menghasilkan hasil yang serupa).

2.3 Risiko Penilaian terhadap Audit Hubungan Perorangan

2.3.1 Ketika merencanakan keterlibatan individu, profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area tersebut sedang ditinjau. Hasil penilaian risiko ini harus tercermin dalam tujuan perikatan audit. Selama penilaian risiko, para profesional harus mempertimbangkan:

• Hasil dari perikatan audit sebelumnya, ulasan dan temuan, termasuk kegiatan perbaikan

• Proses penilaian risiko menyeluruh perusahaan

• Kemungkinan terjadinya risiko tertentu

• Dampak risiko tertentu (dalam ukuran nilai moneter atau lainnya) jika itu terjadi

2.3.2 Profesional harus memastikan pemahaman penuh tentang kegiatan dalam ruang lingkup sebelum menilai risiko. Mereka harus meminta komentar dan saran dari pemangku kepentingan dan pihak terkait lainnya. Ini diperlukan untuk menentukan dengan benar dan memeriksa dampak dari risiko yang mungkin terjadi dalam perikatan audit.

2.3.3 Tujuan dari penilaian risiko adalah pengurangan risiko audit ke tingkat yang dapat diterima, dan mengidentifikasi bagian-bagian dari suatu kegiatan yang harus menerima lebih banyak fokus audit. Ini perlu dilakukan oleh seorang penilaian yang tepat dari masalah IS dan kontrol terkait, sambil merencanakan dan melakukan IS audit.

2.3.4 Ketika merencanakan audit IS dan prosedur jaminan tertentu, profesional harus mengenali fakta itu semakin rendah ambang materialitas, semakin tepat ekspektasi audit dan semakin besar risiko audit.

2.3.5 Ketika merencanakan audit IS dan prosedur jaminan tertentu, profesional harus mempertimbangkan kemungkinan illegal tindakan yang dapat memerlukan modifikasi sifat, waktu, atau luas prosedur yang ada. Untuk lebih informasi mengacu pada Standar 1207 Penyimpangan dan Tindakan Ilegal dan Pedoman 2207.

2.3.6 Untuk mendapatkan jaminan tambahan dalam kasus di mana ada risiko audit tinggi atau ambang batas materialitas yang lebih rendah, profesional harus memberikan kompensasi dengan memperluas ruang lingkup atau sifat tes audit IS atau meningkatkan atau memperluas pengujian substantif.

2.4 Risiko Audit

2.4.1 Risiko audit mengacu pada risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah:

- Kontrol risiko
- Risiko deteksi
- Risiko yang melekat

2.4.2 Profesional harus mempertimbangkan masing-masing komponen risiko untuk menentukan tingkat risiko secara keseluruhan. Ini termasuk risiko materi, yang mencakup risiko bawaan dan risiko kontrol; bersama dengan risiko deteksi itu kemudian disebut sebagai risiko audit. Penjelasan lebih lanjut tentang berbagai komponen risiko audit dapat ditemukan di bagian 2.5 hingga 2.7.

2.5 Risiko Inheren

2.5.1 Risiko yang melekat adalah kerentanan area audit untuk melakukan kesalahan yang dapat bersifat material, secara individu atau dalam kombinasi dengan kesalahan lain, dengan asumsi bahwa tidak ada kontrol internal terkait. Sebagai contoh, risiko inheren yang terkait dengan sistem operasi tanpa kontrol yang sesuai biasanya tinggi, karena perubahan, atau bahkan pengungkapan, data atau program melalui kelemahan keamanan sistem operasi dapat mengakibatkan informasi manajemen yang salah atau kerugian kompetitif. Sebaliknya, risiko yang melekat terkait dengan keamanan untuk PC yang berdiri sendiri tanpa kontrol, ketika analisis yang tepat menunjukkan itu tidak digunakan untuk keperluan bisnis yang kritis, biasanya rendah.

2.5.2 Risiko yang melekat untuk sebagian besar area audit IS adalah tinggi karena potensi dampak kesalahan biasanya mencakup beberapa area sistem bisnis dan banyak pengguna.

2.6 Mengontrol Risiko

2.6.1 Risiko pengendalian adalah risiko kesalahan yang dapat terjadi di area audit dan dapat bersifat material, secara individu atau dalam kombinasi dengan kesalahan lain, tidak akan dicegah atau dideteksi dan diperbaiki tepat waktu oleh sistem kontrol internal. Misalnya, risiko kontrol yang terkait dengan tinjauan manual terhadap log komputer dapat menjadi tinggi karena volume informasi yang dicatat. Risiko kontrol terkait dengan data yang terkomputerisasi prosedur validasi biasanya rendah karena proses diterapkan secara konsisten.

2.6.2 Profesional harus menilai risiko kontrol setinggi kecuali kontrol internal yang relevan adalah:

- Diidentifikasi
- Dievaluasi sebagai efektif
- Diuji dan terbukti beroperasi dengan tepat

2.6.3 Para profesional harus mempertimbangkan kontrol IS yang meresap dan terperinci:

- Kontrol IS yang meresap dianggap sebagai bagian dari kontrol umum; mereka adalah kontrol-kontrol umum itu fokus pada manajemen dan pemantauan lingkungan IS. Karena itu mereka mempengaruhi semua yang terkait IS kegiatan. Efek dari kontrol IS yang meresap pada pekerjaan profesional tidak terbatas pada keandalan kontrol aplikasi dalam sistem proses bisnis. Mereka juga mempengaruhi keandalan IS rinci mengendalikan, misalnya, pengembangan program aplikasi, implementasi sistem, administrasi keamanan dan prosedur pencadangan. Lemahnya kontrol IS yang tersebar, dan dengan demikian manajemen dan pemantauan yang lemah Lingkungan IS, harus memberi tahu para profesional tentang kemungkinan risiko tinggi yang dirancang oleh control beroperasi pada level terperinci mungkin tidak efektif.

- Kontrol IS terperinci terdiri dari kontrol aplikasi ditambah kontrol umum yang tidak termasuk dalam kontrol IS meresap. Mengikuti kerangka COBIT, mereka adalah kontrol atas akuisisi, implementasi, pengiriman dan dukungan sistem dan layanan IS.

2.6.4 Risiko yang harus dipertimbangkan oleh para profesional adalah keterbatasan dan kekurangan dalam IS rinci yang mengontrolnya diinduksi oleh ketidakcukupan kontrol IS meresap.

2.7 Risiko Deteksi

2.7.1 Risiko deteksi adalah risiko bahwa prosedur substantif profesional tidak akan mendeteksi kesalahan yang mungkin terjadi materi, secara individu atau dalam kombinasi dengan kesalahan lain. Misalnya, risiko deteksi terkait dengan mengidentifikasi pelanggaran keamanan dalam sistem aplikasi biasanya tinggi karena log untuk seluruh periode audit tidak tersedia pada saat audit. Risiko deteksi terkait dengan mengidentifikasi kekurangan rencana pemulihan bencana biasanya rendah, karena keberadaannya mudah diverifikasi.

2.7.2 Dalam menentukan tingkat pengujian substantif yang diperlukan, para profesional harus mempertimbangkan:

• Penilaian risiko yang melekat

• Kesimpulan dicapai pada risiko kontrol setelah pengujian kepatuhan

2.7.3 Semakin tinggi penilaian risiko bawaan dan risiko kontrol, semakin banyak bukti audit yang harus dimiliki oleh para professional biasanya diperoleh dari kinerja prosedur audit substantif.

3. Keterkaitan dengan Standar dan Proses COBIT 5

3.0 Pendahuluan

Bagian ini memberikan ikhtisar yang relevan:

3.1 Keterkaitan dengan standar

3.2 Keterkaitan dengan proses COBIT 5

3.3 Pedoman lain

3.1 Tautan ke

Standar

Tabel ini memberikan gambaran umum tentang:

• Standar ISACA paling relevan yang secara langsung didukung oleh pedoman ini

• Pernyataan standar yang paling relevan dengan pedoman ini

Catatan: Hanya pernyataan standar yang relevan dengan pedoman ini yang terdaftar.

Judul Standar	Pernyataan Standar yang Relevan
1201 Keterlibatan Perencanaan	Profesional audit dan penjaminan IS harus merencanakan setiap audit dan perikatan jaminan IS untuk mengatasi: • Tujuan, cakupan, garis waktu, dan hasil • Kepatuhan terhadap hukum yang berlaku dan standar audit profesional • Penggunaan pendekatan berbasis risiko, jika perlu • Masalah khusus keterlibatan • Persyaratan dokumentasi dan pelaporan
1202 Penilaian Risiko dalam Perencanaan	Fungsi audit dan penjaminan IS harus menggunakan pendekatan penilaian risiko yang tepat dan mendukung metodologi untuk mengembangkan rencana audit SI keseluruhan dan menentukan prioritas untuk alokasi efektif sumber daya audit IS. IS audit dan jaminan profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area tersebut sedang ditinjau, saat merencanakan keterlibatan individu. Profesional audit dan penjaminan IS harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.
1203 Kinerja dan	IS profesional audit dan jaminan akan melakukan pekerjaan sesuai

Pengawasan	dengan rencana audit SI yang disetujui untuk mencakup risiko yang teridentifikasi dan dalam jadwal yang disepakati.
1204 Materialitas	Profesional audit dan penjaminan IS harus mempertimbangkan potensi kelemahan atau ketidakhadiran mengontrol sementara merencanakan suatu pertunangan, dan apakah kelemahan atau ketidakhadiran tersebut kontrol dapat menyebabkan defisiensi signifikan atau kelemahan material. Profesional audit dan penjaminan IS harus mempertimbangkan materialitas dan hubungannya dengan audit risiko sambil menentukan sifat, waktu dan tingkat prosedur audit. Profesional audit dan penjaminan IS harus mempertimbangkan efek kumulatif minor mengendalikan kekurangan atau kelemahan dan apakah tidak adanya kendali diterjemahkan menjadi defisiensi signifikan atau kelemahan material. IS profesional audit dan jaminan harus mengungkapkan hal berikut dalam laporan: • Tidak adanya kontrol atau kontrol tidak efektif • Signifikansi dari defisiensi control • Kemungkinan kelemahan ini mengakibatkan defisiensi signifikan atau kelemahan material
1207 Penyimpangan dan Tindakan Ilegal	IS profesional audit dan penjaminan akan mempertimbangkan risiko penyimpangan dan tindakan ilegal selama pertunangan.

3.2 Tautan ke

COBIT 5

Proses

Tabel ini memberikan ikhtisar yang paling relevan:

• proses COBIT 5

• Tujuan proses COBIT 5

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam *COBIT 5: Proses yang Memampukan.*

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pemerintahan pengaturan kerangka kerja dan pemeliharaan.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan keputusan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
EDM03 Pastikan risiko optimasi.	Pastikan bahwa risiko perusahaan yang terkait dengan TI tidak melebihi selera risiko dan toleransi risiko, dampak risiko IT terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi untuk kegagalan kepatuhan diminimalkan.
APO12 Kelola risiko.	Mengintegrasikan manajemen risiko perusahaan terkait TI dengan ERM secara keseluruhan, dan menyeimbangkannya biaya dan manfaat mengelola risiko perusahaan terkait TI.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.
MEA03 Monitor, mengevaluasi dan menilai kepatuhan dengan persyaratan eksternal.	Pastikan perusahaan mematuhi semua persyaratan eksternal yang berlaku.

3.3 Panduan Lain

Ketika menerapkan standar dan pedoman, para profesional didorong untuk mencari panduan lain, ketika dipertimbangkan perlu. Ini bisa dari audit IS dan jaminan:

- Kolega dari dalam organisasi dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau
- kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam organisasi, misalnya, komite audit
- Panduan lain (misalnya, buku, makalah, pedoman lainnya)

4. Terminologi

Istilah	Definisi
Piagam audit	Dokumen yang disetujui oleh pihak yang bertanggung jawab atas tata kelola yang mendefinisikan tujuan, wewenang dan tanggung jawab audit IS internal dan kegiatan penjaminan Piagam tersebut harus: • Menetapkan posisi audit IS dan fungsi jaminan internal di dalam perusahaan • Mengesahkan akses ke catatan, personel, dan properti fisik yang relevan dengan kinerja audit SI dan keterlibatan jaminan • Menentukan ruang lingkup kegiatan audit IS dan fungsi jaminan
Risiko audit	Risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah: • Kontrol risiko • Risiko deteksi • Risiko yang melekat
Kendalikan risiko	Risiko bahwa ada kesalahan materi yang tidak dapat dicegah atau terdeteksi pada waktu yang tepat dasar oleh sistem pengendalian internal.

Kontrol IS terperinci	Kontrol atas akuisisi, implementasi, pengiriman dan dukungan sistem IS dan layanan yang terdiri dari kontrol aplikasi ditambah kontrol umum yang tidak termasuk dalam kontrol meresap
Risiko deteksi	Risiko yang tidak IS audit atau prosedur substantif profesional tidak akan mendeteksi kesalahan yang bisa bersifat material, secara individu atau dalam kombinasi dengan kesalahan lainnya.
Risiko yang melekat	Tingkat risiko atau paparan tanpa memperhitungkan tindakan yang dimiliki manajemen diambil atau mungkin diambil (misalnya, menerapkan kontrol).
Materialitas	Konsep audit mengenai pentingnya item informasi yang berkaitan dengan dampak atau pengaruhnya terhadap subjek yang diaudit. Ekspresi kerabat signifikansi atau pentingnya suatu masalah tertentu dalam konteks pertunangan atau perusahaan secara keseluruhan.
Tugas beresiko	Suatu proses yang digunakan untuk mengidentifikasi dan mengevaluasi risiko dan potensi dampaknya Penilaian risiko digunakan untuk mengidentifikasi item-item atau bidang-bidang yang menghadirkan risiko tertinggi, kerentanan atau paparan terhadap perusahaan untuk dimasukkan dalam rencana audit tahunan SI. Penilaian risiko juga digunakan untuk mengelola pengiriman proyek dan risiko manfaat proyek.
Kontrol IS yang meresap	Kontrol umum yang dirancang untuk mengelola dan memantau lingkungan IS dan yang, oleh karena itu, mempengaruhi semua aktivitas terkait IS
Pengujian substantif	Memperoleh bukti audit tentang kelengkapan, keakuratan atau keberadaan kegiatan atau transaksi selama periode audit

IT AUDIT

Nama : Ilsa Palingga Ninditama (182420061)

Program Studi Teknik Informatika S-2

Pascasarjana Universitas Bina Darma

SOAL

Pilih salah satu Standard yang ada pada dokumen ITAF (materi), dan jelaskan secara ringkas fungsi dari standard tersebut pada Audit TI dan jelaskan keterkaitannya dengan COBIT atau framework lain.

JAWABAN :

Standard yang dipilih ialah **1005 (*Due Professional Care*)**

Due Professional Care (Kecermatan professional) berarti kecermatan dan kompetensi yang sewajarnya, tidak berarti kesempurnaan atau kinerja yang luar biasa. Dengan demikian, kecermatan professional **hanya** menuntut auditor internal untuk melakukan pemeriksaan dan verifikasi sampai batas-batas yang wajar. Sekaligus, auditor internal tidak dapat memberikan jaminan mutlak bahwa ketidakpatuhan atau penyimpangan tidak ada. Namun demikian, kemungkinan penyimpangan material atau ketidakpatuhan perlu selalu diperhatikan oleh auditor internal setiap kali melakukan penugasan audit internal.

Fungsi dari *Due Professional Care*:

- Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan.
- Mengoptimalkan kemampuan sumber daya manusia untuk memenuhi tujuan perusahaan.
- Memantau, mengevaluasi, dan menilai sistem pengendalian internal.
- Berkomunikasi dengan anggota tim tentang peran dan tanggung jawab mereka dan memastikan kepatuhan tim terhadap standar yang tepat dalam melakukan perikatan.
- Memahami kompetensi yang memadai untuk mencapai tujuan keterlibatan.
- Menjaga komunikasi yang efektif dengan para pemangku kepentingan yang relevan selama keterlibatan.

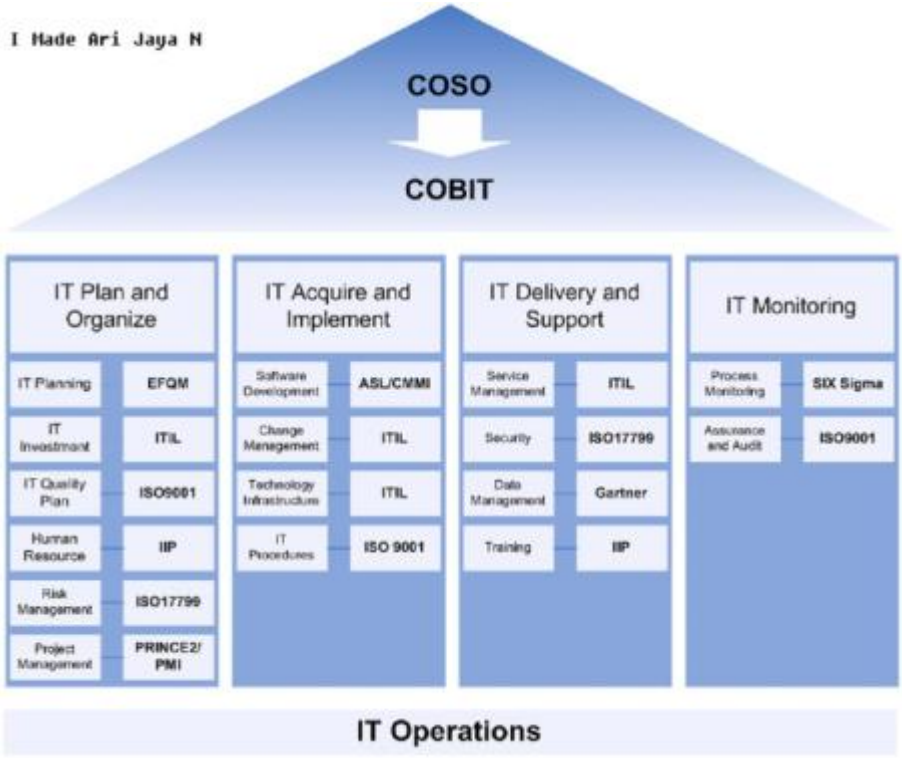
Hubungan Cobit dengan Framework

Secara umum, kerangka kerja IT Governance serta control yang dibutuhkan untuk mencapainya disediakan oleh **COBIT** *(Control Objectives for Information and Related Technology)*. Dimana didalamnya terdapat panduan bagaimana organisasi harus mengendalikan pengelolaan IT dalam pencapaian governance.

Namun COBIT hanya memberikan panduan control dan tidak memberikan panduan implementasi operasional. Dalam memenuhi kebutuhan **COBIT** dalam lingkungan operasional, maka perlu diadopsi berbagai kerangka governance operasional. Dalam implementasi IT Governance di lingkungan operasi, ada beberapa framework governance yang bisa diterapkan, antara lain:

- EFQM *(European Foundation for Quality Management)*, EFQM adalah yayasan non-profit yang berhubungan dengan pengembangan standard an prosedur pemasaran
- ITIL *(IT Infrastructure Library)*, merupakan sebuah panduan pengelolaan layanan IT yang mencakup service delivery dan sevice support.
- ISO9001, merupakan standarisasi manajemen kualitas
- IIP *(Investor in People)*, merupakan standar *de-facto* dari proses pengembangan SDM.
- ISO17799, merupakan standar dalam pengembangan keamanan IT.
- PRINCE2/PMI *(Project Management Institute)*, merupakan standar dalam pengelolaan proyek.
- ASL *(Application Service Library)*, merupakan standar dalam pengembangan software
- CMMI *(Capability Maturity Model Institute)*, merupakan standar dalam pengembangan software
- Gartner, Gartner mengeluarkan sebuah standar dalam pengelolaan data dan informasi
- Six Sigma, merupakan standar dalam pengawasan proses operasi

Gambar berikut menjelaskan bagaimana hubungan framework governance IT operasional tersebut dalam domain COBIT:



Tugas Audit Charter : Indri Endang Lestari & Sulistiyani

MTI19AR2

1. Standard 1001 - Audit Charter :

Audit Charter adalah sebuah dokumen formal yang menyatakan tujuan, wewenang, dan tanggung jawab unit audit intern pada suatu organisasi. Piagam Audit merupakan penegasan komitmen dari para pemangku kepentingan (*stakeholders*) terhadap arti pentingnya fungsi pengawasan di organisasinya. Adapun ketentuan dari piagram ini harus :

- Menetapkan posisi fungsi audit internal dalam perusahaan
- Memberikan Otorisasi akses ke catatan, personel dan properti fisik yang relevan dengan kinerja audit dan jaminan IS
- Tentukan ruang lingkup kegiatan fungsi audit

Adapun manfaat piagam audit adalah menjadi salah satu alat untuk mempertegas independensi. Penegasan itu nampak dari pengaturan posisi unit audit intern dalam struktur organisasi dan kepada siapa pimpinan unit tersebut bertanggung jawab secara fungsional. Penegasan tersebut sekaligus juga berguna untuk meningkatkan trust semua unsur organisasi terhadap fungsi audit intern.

adapun guideline yang digunakan dalam audit charter adalah **2001 Audit Charter**

2. Guideline 2001 – Audit Charter

a. Tujuan Guideline – 2001 Audit Charter :
   - Membantu professional audit dan penjaminan IS dalam menyiapkan piagam audit
   - Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

b. Guideline 2001 Audit charter selain digunakan untuk standard 1001 audit charter, juga bias digunakan untuk 1002 Organisational Independence, dan 1003 Professional Independence.

c. Contents of Audit Charter

Piagam audit harus dengan jelas membahas empat aspek, yaitu tujuan, tanggung jawab, wewenang dan akuntabilitas.

- **Tujuan** piagam audit dan fungsi audit harus berisi bagian-bagian berikut:
    - Maksud / tujuan piagam audit memberikan kerangka kerja fungsional dan organisasi di mana audit fungsi beroperasi.
    - Pernyataan misi dan tujuan fungsi audit membawa pendekatan terstruktur untuk mengevaluasi dan meningkatkan desain dan efektivitas operasional dari proses manajemen risiko, pengendalian internal sistem dan struktur tata kelola sistem informasi.
    - Lingkup fungsi audit adalah untuk seluruh perusahaan atau organisasi tertentu dalam perusahaan.
    - Tata kelola merinci badan otorisasi untuk piagam audit dan fungsi audit.
- **Tanggung jawab** fungsi audit harus berisi bagian-bagian berikut:
    - Prinsip operasi memberikan penghitungan yang lebih rinci dan kuantitatif dari berbagai tujuan fungsi audit.
    - Independensi merinci pelaksanaan persyaratan independensi untuk fungsi audit dan profesional, sebagaimana dijelaskan dalam Standar 1002 Organisational Independence, dan 1003 Professional Independence.
    - Hubungan dengan audit eksternal untuk merinci hubungan fungsi audit dengan auditor eksternal, adapun pertemuannya untuk mengoordinasikan upaya kerja untuk meminimalkan upaya duplikasi, Menyediakan akses ke kertas kerja, dokumentasi, dan bukti professional, dan Mempertimbangkan pekerjaan yang direncanakan oleh auditor eksternal ketika menyusun rencana audit untuk periode mendatang
    - Harapan audit merinci layanan dan hasil yang dapat diaudit dari fungsi audit dan professional, meliputi deskripsi masalah yang teridentifikasi, konsekuensi dan kemungkinan resolusi yang berkaitan dengan bidang tanggung jawab pihak yang diaudit
    - Kemungkinan untuk memasukkan respons manajemen dan tindakan korektif yang diambil atas temuan dalam audit, termasuk referensi untuk perjanjian tingkat layanan terkait (SLA) untuk barang-barang seperti

pengiriman laporan, tanggapan terhadap keluhan yang diaudit, kualitas layanan, tinjauan kinerja, proses pelaporan dan persetujuan temuan.

  - Persyaratan audit merinci tanggung jawab audit.
  - Komunikasi dengan auditee merinci frekuensi dan saluran komunikasi yang melaluinya audit fungsi akan berkomunikasi dengan pihak yang diaudit.

- **Otoritas** fungsi audit harus berisi bagian-bagian berikut:
  - Hak akses ke informasi yang relevan, sistem, personel dan lokasi oleh para profesional ketika melakukan perikatan audit. Fungsi audit, diwakili oleh para professional.
  - Keterbatasan kewenangan fungsi audit dan profesional, jika ada
  - Proses yang akan diaudit, di mana fungsi audit berwenang untuk mengaudit.
- **Akuntabilitas** fungsi audit harus berisi bagian-bagian berikut:
  - Struktur organisasi, termasuk jalur pelaporan ke dewan dan manajemen senior, dari fungsi audit, mis., fungsi audit harus memiliki akses terbuka dan tidak terbatas ke dewan dan anggotanya.
  - Pelaporan yang merinci format, konten, dan penerima komunikasi pada hasil setiap perikatan audit, mis., laporan audit tertulis akan dikeluarkan oleh fungsi audit setelah setiap audit keterlibatan dan didistribusikan kepada pemangku kepentingan yang tepat.
  - kinerja fungsi audit dibandingkan dengan rencana audit dan anggaran,
  - Kepatuhan terhadap standar yang merinci standar yang akan digunakan fungsi audit dan professional. mematuhi, mis., fungsi audit dan profesional akan mematuhi dan bertindak sesuai dengan semua Audit ISACA IS dan Standar dan Pedoman Jaminan.
  - Proses penjaminan kualitas
  - Aturan kepegawaian untuk perikatan audit
  - Komitmen pendidikan berkelanjutan dari fungsi audit terhadap para professional

- Tindakan yang disetujui mengenai fungsi fungsi audit dan perilaku profesional, mis., Hukuman saat salah satu pihak gagal melaksanakan tanggung jawabnya

- Aspek lain yang harus dipertimbangkan untuk ditambahkan dalam piagam audit adalah:
  - Meninjau dan mengubah piagam, yang merupakan tanggung jawab fungsi audit. Seharusnya secara berkala menilai apakah tujuan, tanggung jawab, wewenang dan akuntabilitas, sebagaimana didefinisikan dalam piagam audit, terus menjadi memadai dan mengomunikasikan hasil penilaian kepada komite audit.
  - Memperoleh persetujuan amandemen terhadap piagam audit dari pihak yang bertanggung jawab atas tata kelola.
  - Termasuk dokumen terkait seperti referensi standar terkait, pedoman, kebijakan, kerangka kerja, manual, dll.

3. Linkage to COBIT 5 Processes

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam COBIT 5

Proses Cobit 5 : MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.

Tujuannya : Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem internal mengendalikan dan, dengan demikian, memberikan kepercayaan dalam operasi, kepercayaan pada pencapaian perusahaan tujuan dan pemahaman yang memadai tentang risiko residual.

4 Contoh Piagam Audit Charter

PIAGAM AUDIT INTERNAL
(INTERNAL AUDIT CHARTER)
PT SINAR MAS AGRO RESOURCES & TECHNOLOGY Tbk.

smart
agribusiness and food

BAB I
DASAR DAN TUJUAN PEMBENTUKAN

1.1. PT Sinar Mas Agro Resources & Technology Tbk (selanjutnya disebut "PT SMART Tbk" atau "Perseroan"), sebagai perusahaan publik harus mematuhi peraturan perundangan di bidang pasar modal.

1.2 PT SMART Tbk wajib memiliki Unit Audit Internal ("AI") yaitu unit kerja yang menjalankan fungsi Audit Internal. Audit Internal adalah suatu kegiatan pemberian keyakinan dan konsultasi yang bersifat independen dan objektif, dengan tujuan untuk meningkatkan nilai dan memperbaiki operasional Perseroan dan anak perusahaannya, melalui pendekatan yang sistematis, dengan cara mengevaluasi dan meningkatkan efektivitas manajemen risiko, pengendalian, dan proses tata kelola perusahaan.

1.3 Sehubungan dengan itu, AI wajib menyusun Piagam Audit Internal (selanjutnya disebut "Piagam"). Piagam ini disusun agar AI dapat melaksanakan tugas dan tanggung jawabnya secara efisien, transparan, kompeten, independen, dan dapat dipertanggungjawabkan sehingga dapat diterima oleh semua pihak yang berkepentingan. Piagam ini ditetapkan oleh Direksi setelah mendapat persetujuan Dewan Komisaris.

1.4 Dasar hukum Piagam ini adalah:

1.4.1 Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal;

1.4.2 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan; dan

1.4.3 Peraturan Otoritas Jasa Keuangan Nomor 56/POJK.04/2015 tentang Pembentukan dan Pedoman Penyusunan Piagam Unit Audit Internal.

BAB II
STRUKTUR, KEDUDUKAN DAN SYARAT KEANGGOTAAN

2.1 Struktur dan Kedudukan

2.1.1 AI dipimpin oleh seorang Kepala AI.

2.1.2 Kepala AI diangkat dan diberhentikan oleh Direktur Utama atas persetujuan Dewan Komisaris.

2.1.3 Direktur Utama dapat memberhentikan Kepala AI, setelah mendapat persetujuan Dewan Komisaris, jika tidak memenuhi persyaratan sebagai auditor internal sebagaimana diatur dalam piagam ini dan/atau gagal atau dianggap tidak cakap dalam menjalankan tugas terkait.

2.1.4 Kepala AI bertanggung jawab kepada Direktur Utama dan secara fungsional kepada Dewan Komisaris atau melalui Komite Audit.

2.1.5 Auditor internal atau anggota dalam AI bertanggung jawab secara langsung kepada Kepala AI.

2.1.6 Dalam melaksanakan tugasnya, manajemen dan Dewan Komisaris memberikan dukungan sepenuhnya kepada AI agar dapat bekerja dengan bebas dan obyektif tanpa campur tangan pihak manapun.

2.2 Syarat Keanggotaan

Auditor internal dalam AI wajib memenuhi persyaratan sebagai berikut:

2.2.1 memiliki integritas dan perilaku yang profesional, independen, jujur dan objektif;

2.2.2 berkompeten di bidangnya, baik mengenai teknis audit, disiplin ilmu lain yang relevan, peraturan perundang-undangan di bidang pasar modal dan peraturan perundang-undangan terkait lainnya, prinsip tata kelola perusahaan yang baik, maupun manajemen risiko;

2.2.3 memiliki kecakapan untuk berinteraksi dan berkomunikasi baik secara lisan maupun tertulis secara efektif;

2.2.4 mematuhi standar profesi yang dikeluarkan oleh asosiasi Audit Internal;

2.2.5 mematuhi Kode Etik AI;

2.2.6 menjaga kerahasiaan informasi dan/atau data Perseroan dan anak perusahaan terkait dengan pelaksanaan tugas dan tanggung jawab AI kecuali diwajibkan berdasarkan peraturan perundang-undangan atau penetapan atau putusan pengadilan; dan

2.2.7 bersedia meningkatkan pengetahuan, keahlian dan kemampuan profesionalismenya secara terus menerus.

BAB III
TUGAS, TANGGUNG JAWAB DAN WEWENANG

3.1 Tugas dan Tanggung Jawab

3.1.1 Menyiapkan dan melaksanakan rencana dan anggaran aktivitas audit internal tahunan berdasarkan prioritas risiko sesuai dengan tujuan Perseroan.

3.1.2 Menguji dan mengevaluasi pelaksanaan pengendalian internal dan sistem manajemen risiko sesuai dengan kebijakan Perseroan.

3.1.3 Melakukan pemeriksaan dan penilaian atas efisiensi dan efektivitas di seluruh bidang kegiatan Perseroan dan anak perusahaan.

3.1.4 Memberikan saran perbaikan dan informasi yang obyektif tentang kegiatan yang diperiksa pada semua tingkatan manajemen.

3.1.5 Membuat laporan hasil audit dan menyampaikan laporan tersebut kepada Manajemen terkait, Direktur Utama dan Dewan Komisaris atau Komite Audit.

3.1.6 Memantau, menganalisis dan melaporkan pelaksanaan tindak lanjut perbaikan yang telah disarankan.

3.1.7 Menyusun program untuk mengevaluasi mutu kegiatan audit yang dilakukannya.

3.1.8 Melakukan pemeriksaan khusus apabila diperlukan.

3.2. Wewenang

3.2.1 Mengakses seluruh informasi yang relevan tentang Perseroan dan anak perusahaan terkait dengan tugas dan fungsinya.

3.2.2 Berkomunikasi langsung dan/atau mengadakan rapat secara berkala maupun insidentil dengan Direksi, Dewan Komisaris, dan/atau Komite Audit serta anggota dari Direksi, Dewan Komisaris, dan/atau Komite Audit.

3.2.3 Melakukan koordinasi kegiatannya dengan kegiatan auditor eksternal.

BAB IV
KODE ETIK

4.1 Prinsip-prinsip

Dalam melaksanakan tugas dan tanggung jawabnya, auditor internal harus menerapkan dan menegakkan prinsip-prinsip berikut ini:

4.1.1 **Integritas**

Integritas yang dimiliki auditor internal membentuk kepercayaan, dan berdasarkan kepercayaan inilah maka pertimbangan mereka dapat diandalkan.

4.1.2 **Obyektivitas**

Auditor internal memperlihatkan tingkat obyektifitas tertinggi dalam mengumpulkan, mengevaluasi dan mengkomunikasikan informasi tentang aktivitas atau proses yang diperiksa. Auditor internal membuat penilaian yang seimbang atas segala kondisi yang terkait dan tidak dipengaruhi oleh kepentingan pribadi atau pihak lain dalam memberikan pertimbangan.

4.1.3 **Kerahasiaan**

Auditor internal menghormati nilai dan kepemilikan dari informasi yang diterimanya dan tidak mengungkapkan informasi tersebut tanpa kewenangan yang sah, kecuali diharuskan oleh hukum atau profesi.

4.1.4 **Kompetensi**

Auditor internal menggunakan pengetahuan, keterampilan dan pengalaman yang diperlukan dalam melakukan tugas/jasa audit internal.

4.2. Aturan pelaksanaan

4.2.1 **Integritas**

- Melakukan pekerjaannya dengan jujur, tekun dan penuh tanggung jawab.
- Mematuhi hukum/peraturan/kebijakan yang berlaku dan membuat pengungkapan sesuai dengan hukum/peraturan/kebijakan serta aturan profesi yang berlaku tersebut.
- Tidak secara sengaja terlibat dalam kegiatan terlarang atau melakukan tindakan yang mencemarkan nama baik profesi maupun Perseroan.
- Menghormati dan memberikan kontribusi pada tujuan Perseroan yang sah dan etis.

4.2.2 **Obyektivitas**

- Tidak ikut serta dalam segala kegiatan atau hubungan yang dapat mengganggu dalam memberikan penilaian yang tidak memihak. Keikutsertaan tersebut mencakup keikutsertaan dalam kegiatan atau hubungan yang bertentangan dengan kepentingan Perseroan.
- Tidak menerima apapun yang dapat membahayakan pertimbangan profesionalnya.
- Mengungkapkan seluruh fakta material yang diketahuinya, yang apabila tidak diungkapkan dapat menimbulkan distorsi atas pelaporan kegiatan yang diperiksa.

4.2.3 **Kerahasiaan**

- Berhati-hati dalam menggunakan dan menjaga informasi yang diperoleh selama menjalankan tugasnya.
- Tidak menggunakan informasi untuk keuntungan pribadi, atau dengan cara apapun yang bertentangan dengan hukum atau merusak tujuan Perseroan yang sah dan etis.

4.2.4 **Kompetensi**

- Hanya terlibat dalam pemberian jasa dimana mereka memiliki pengetahuan, keterampilan dan pengalaman yang dibutuhkan.
- Melaksanakan jasa audit internal yang sesuai dengan standar profesional untuk audit internal.
- Senantiasa meningkatkan keahlian, keefektifan dan kualitas jasanya secara berkelanjutan.

BAB V
PERTANGGUNGJAWABAN

AI akan menyiapkan dan menerbitkan laporan hasil audit secara tertulis setelah penugasan audit selesai, dan laporan hasil audit tersebut akan didistribusikan sebagaimana mestinya. Laporan audit internal juga akan disampaikan kepada Dewan Komisaris atau melalui Komite Audit.

Laporan hasil audit tersebut memuat respon manajemen dan tindakan/rencana tindakan perbaikan yang akan dilakukan manajemen terkait dengan temuan-temuan audit dan rekomendasinya. Respon manajemen harus memuat jadwal penyelesaian tindakan perbaikan oleh manajemen dan penjelasan jika suatu tindakan perbaikan tidak dapat dilakukan.

BAB VI
KEMANDIRIAN FUNGSIONAL

Auditor internal tidak memiliki tanggung jawab atau wewenang operasional atas apa yang mereka audit. Sesuai dengan hal tersebut, auditor internal juga tidak mengimplementasikan pengendalian internal, membuat prosedur, merancang sistem, membukukan transaksi atau terlibat dalam kegiatan-kegiatan lainnya yang dapat mempengaruhi penilaian mereka.

Piagam AI PT SMART Tbk ini mulai berlaku sejak tanggal ditetapkan dan selanjutnya Piagam AI dan Kode Etik AI yang ditetapkan tanggal 30 April 2009 dicabut dan dinyatakan tidak berlaku.

Disetujui oleh Dewan Komisaris melalui Rapat Dewan Komisaris tanggal 22 Desember 2016 dan selanjutnya ditetapkan oleh Direksi tanggal : 23 Desember 2016

Standar 1401 Report

standar tersebut memiliki beberapa fungsi

- memberikan informasi yang relevan
- informasi yang terpercaya
- informasi yang cukup atau layak
- informasi yang nyaman
- informasi yang tepat waktu

untuk framework lebih cocok ke cobit 5, karena cobit 5 adalah layanan kerangka kerja yang mengatur hal – hal yang terkait dengan informasi dan teknologi di dalam perusahaan, pengaturan dilakukan secara holistik berdasarkan fungsi dan tanggung jawab.

Tugas IT Audit Standards dan Guideline pada ITAF

M APRILIANSYAH R

MEGITER TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA
PALEMBANG
2019

SOAL

Pilih salah satu Standard yang ada pada dokumen ITAF (materi), dan jelaskan secara ringkas fungsi dari standard tersebut pada Audit TI dan jelaskan keterkaitannya dengan COBIT atau framework lain.

JAWABAN

Standard yang dipilih ialah 1005 (*Due Professional Care*) karena menurut saya Due Professional Care Due professional merupakan kemahiran profesioanal yang cermat dan seksama dalam menjalankan tanggung jawabnya dan hanya menuntut auditor internal untuk melakukan pemeriksaan dan verifikasi sampai batas-batas yang wajar. Sekaligus, auditor internal tidak dapat memberikan jaminan mutlak bahwa ketidakpatuhan atau penyimpangan tidak ada. dilapangan.Beberapa indikator untuk menentukan due professional care

1. Skeptisme Professional merupakan sikap yang mencangkup pikiran yang selalu mempertanyakan dan melakukan evaluasi secara kritis bukti audit.

2. Keyakinan yang memadai Merupakan persepsi auditor atas simpulan bahwa laporan keuangan bebas dari salah saji material, baik karena kekeliruan maupun kecurangan

terdapat beberapa indikator yang dapat digunakan untuk mengukur kualitas audit, dengan Standard yang dipilih 1005 (*Due Professional Care*) diantaranya :

Standar Umum.
a.Audit harus dilaksanakan oleh seseorang atau lebih yang memiliki keahlian dan pelatihan teknis yang cukup sebagai auditor.
b.Dalam semua hal yang berhubungan dengan perikatan, independensi dalam sikap mental harus dipertahankan oleh auditor. c.Dalam pelaksanaan audit dan penyusunan laporannya, auditor wajib menggunakan kemahiran profesionalnya dengan cermat dan seksama.

Standar Pekerjaan Lapangana.
A.Pekerjaan harus direncanakan sebaik-baiknya dan jika digunakan asisten harus disupervisi dengan semestinya.
B.Pemahaman memadai atas pengendalian intern harus diperoleh untuk merencanakan audit dan menentukan sifat, saat, dan lingkup pengujian yang akan dilakukan.

C.Bukti audit kompeten yang cukup harus diperoleh melalui inspeksi, pengamatan, permintaan keterangan, dan konfirmasi sebagai dasar memadai untuk menyatakan pendapat atas laporan keuangan yang diaudit

Fungsi *Due Professional Care*:

1. Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan.
2. Mengoptimalkan kemampuan sumber daya manusia untuk memenuhi tujuan perusahaan.
3. Memantau, mengevaluasi, dan menilai sistem pengendalian internal.
4. Berkomunikasi dengan anggota tim tentang peran dan tanggung jawab mereka dan memastikan kepatuhan tim terhadap standar yang tepat dalam melakukan perikatan.
5. Memahami kompetensi yang memadai untuk mencapai tujuan keterlibatan.
6. Menjaga komunikasi yang efektif dengan para pemangku kepentingan yang relevan selama keterlibatan.

Hubungan Cobit dengan Framework

Secara umum, kerangka kerja IT Governance serta control yang dibutuhkan untuk mencapainya disediakan oleh COBIT *(Control Objectives for Information and Related Technology)*. Dimana didalamnya terdapat panduan bagaimana organisasi harus mengendalikan pengelolaan IT dalam pencapaian governance.Namun COBIT hanya memberikan panduan control dan tidak memberikan panduan implementasi operasional. Dalam memenuhi kebutuhan COBIT dalam lingkungan operasional, maka perlu diadopsi berbagai kerangka governance operasional. Dalam implementasi IT Governance di lingkungan operasi,

1001

Audit Charter (Piagam Audit)

DISUSUN OLEH:

1. FIDO RIZKI
2. MUHAMMAD DIAH MAULIDIN

KELAS : REGULER A R1

MATA KULIAH : IT AUDIT

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

Fungsi 1001 Audit Charter

- Menyiapkan dokumen audit untuk mendefinisikan kegiatan audit sistem informasi internal dan fungsi penjaminan dengan cukup detail;
- Sebagai wewewang, tujuan, tanggung jawab dan batasan audit sistem informasi dan fungsi jaminan;
- Rahasia dan akurat dalam penjaminan audit sistem informasi;
- Peran dan tanggung jawab pihak yang diaudit;
- Standar professional yang akan diikuti oleh audit Sistem Informasi dan profesional penjaminan dalam pelaksanaan audit Sistem Informasi dan perjanjian jaminan;

Fungsi 1001 Audit Charter

- Tinjau dokumen audit setidaknya setiap tahun atau lebih sering jika tanggung jawab berubah;
- Memperbarui dokumen audit sesuai kebutuhan untuk memastikan bahwa tujuan dan tanggung jawab telah dan tetap didokumentasikan dengan tepat. Secara formal mengkomunikasikan audit charter kepada pihak yang diaudit untuk setiap audit Sistem Informasi atau perikatan jaminan.

Peranan 1001 Audit Charter

- Untuk membantu profesional audit dan penjaminan Sistem informasi dalam menyiapkan dokumen audit;
- Untuk membantu dalam mendefinisikan tujuan, tanggung jawab, wewenang dan akuntabilitas audit Sistem Informasi dan fungsi jaminan;
- Sebagai pedoman saat menentukan cara menerapkan standar, penilaian dan penerapannya, membantu dalam membenarkan setiap kegiatan dan pencarian pedoman tambahan jika dianggap perlu.

Pedoman 1001 Audit Charter

- Pedoman 1001 Audit Charter mengacu kepada 2001 Audit Charter
- Tujuan pedoman 2001 Audit Charter untuk membantu audit Sistem Informasi dan profesional penjaminan dalam menyiapkan Audit Charter. Audit Charter mendefinisikan tujuan, tanggung jawab, wewenang dan akuntabilitas audit IS dan fungsi jaminan.
- Audit Sistem Informasi dan professional penjaminan harus mempertimbangkan pedoman 2001 Audit Charter ketika menentukan bagaimana menerapkan standar dan menggunakan penilaian profesional dalam penerapan.

Pedoman 2001 Audit Charter

- Pedoman 2001 Audit Charter membahas empat aspek yaitu tujuan, tanggung jawab, wewenang dan akuntabilitas.
- Tujuan Pedoman 2001 Audit Charter berisi tentang tujuan, penjelasan objektivitas fungsi audit, cakupan audit dan wewenang isi fungsi audit charter.
- Tanggung jawab Pedoman 2001 Audit Chater berisi prinsip operasi, independen, hubungan audit eksternal, expetasi auditor, kemampuan auditor dan komunikasi auditor.

Pedoman 2001 Audit Charter

- Wewenang Pedoman 2001 Audit Charter berisi akses yang relevan, pembatasan wewenang dan proses audit.
- Akuntanbilitas Pedoman 2001 Audit Charter berisi struktur organisasi, laporan tentang detail format, performa fungsi audit, kepatuhan dengan standar yang detail, proses penjaminan kualitas, aturan kepegawaian untuk perikatan audit, komitmen pendidikan berkelanjutan dari fungsi audit dan tindakan yang disetujui terkait fungsi audit.

1001 Audit Charter Link ke Proses COBIT 5

- Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses yang terdapat dalam COBIT 5 yaitu

  COBIT 5: Enabling Processes

Proses COBIT 5	Tujuan Proses
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Memperoleh transparansi bagi para pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

TERIMA KASIH

Review IT Audit Standards dan Guideline pada ITAF

Oleh:

Muhammad Irvai (182420063)

Mata Kuliah : IT Audit

Dosen Pengampu: Dr. Widya Cholil., M.IT

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

Review IT Audit Standards dan Guideline pada ITAF

Pada review IT Audit standards yang saya ambil kali ini mengenai standar : *IS Audit and Assurance Standard 1002 Organisational Independence* (kemandirian organisasi).

1002.1 Fungsi audit dan jaminan Sistem Informasi (SI) harus independen dari area atau aktivitas ditinjau untuk memungkinkan penyelesaian obyektif audit dan jaminan keterikatan.

Fungsi audit dan jaminan SI pada standar *Organisational Independen* harus:

a. Melaporkan ke tingkat dalam organisasi yang diaudit yang menyediakan sistem organisasi Independensi dan memungkinkan fungsi audit dan penjaminan SI untuk menjalankan fungsinya tanggung jawab tanpa gangguan.
b. Mengungkapkan atau menjelaskan rincian penurunan nilai kepada pihak-pihak yang tepat jika independen fakta atau penampilan terganggu.
c. menghindari peran non-audit dalam inisiatif SI yang memerlukan asumsi manajemen tanggung jawab karena peran tersebut dapat merusak independensi untuk masa depan organisasi tersebut
d. Mengatasi independensi dan akuntabilitas fungsi audit terhadap sertifikat audit dan / atau surat perjanjian.

Keterkaitan dari 1002 *Organisational independence* ke 2002 *Organisational independence.*

Tujuan dari pedoman ini adalah untuk mengatasi independensi fungsi audit dan jaminan IS di perusahaan Indonesia. Tiga aspek penting dipertimbangkan:

a. Posisi audit SI dan fungsi jaminan dalam perusahaan
b. Tingkat yang dilaporkan oleh audit IS dan fungsi jaminan di dalam perusahaan
c. Kinerja layanan non-audit dalam perusahaan oleh audit SI dan manajemen jaminan dan IS profesional audit dan penjaminan

Pedoman ini memberikan panduan untuk menilai independensi organisasi dan merinci hubungannya antara independensi organisasi dan piagam audit dan rencana audit. Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

1. **Posisi dalam perusahaan**
   a. Untuk mengaktifkan independensi organisasi, fungsi audit perlu memiliki posisi dalam perusahaan itu memungkinkannya untuk melakukan tanggung jawabnya tanpa gangguan. Ini dapat dicapai dengan:
      - Menetapkan fungsi audit dalam piagam audit sebagai fungsi atau departemen independen, di luardepartemen operasional. Fungsi audit tidak boleh diberi tanggung jawab operasional apa pun atau kegiatan.
      - Memastikan bahwa fungsi audit melapor ke tingkat dalam perusahaan yang memungkinkannya untuk mencapai kemandirian organisasi
   b. Fungsi audit harus menghindari pelaksanaan peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen, karena peran tersebut dapat merusak independensi di masa depan

2. **Tingkat Pelaporan**
   a. Fungsi audit harus melaporkan ke tingkat dalam perusahaan yang memungkinkannya untuk bertindak dengan lengkap kemandirian organisasi. Independensi harus didefinisikan dalam piagam audit dan dikonfirmasi oleh fungsi audit kepada dewan direksi dan mereka yang bertanggung jawab atas tata kelola secara teratur, setidaknya setiap tahun.
   b. Untuk memastikan independensi organisasi dalam fungsi audit, hal-hal berikut harus dilaporkan kepada mereka dibebankan dengan tata kelola (mis., dewan direksi) untuk masukan dan / atau persetujuan mereka:
      - Rencana dan anggaran sumber daya audit
      - Rencana audit (berbasis risiko)

- Tindak lanjut kinerja yang dilakukan oleh fungsi audit pada aktivitas audit SI
- Tindak lanjut dari ruang lingkup yang signifikan atau keterbatasan sumber daya

c. Untuk memastikan independensi organisasi dari fungsi audit, diperlukan dukungan eksplisit dari kedua dewan dan manajemen eksekutif.

3. Servis Non-Audit

a. Di banyak perusahaan, harapan manajemen dan staf IS adalah bahwa fungsi audit mungkin terlibat dalam menyediakan layanan non-audit. Ini melibatkan, paruh waktu atau paruh waktu, partisipasi para profesional di IS inisiatif dan tim proyek SI untuk memberikan kemampuan penasihat atau konsultatif

b. Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggap tidak menjadi tanggung jawab manajemen dan, karenanya, tidak akan mengganggu independensi. Layanan non-audit yang juga tidak akan mengganggu independensi atau objektivitas, jika perlindungan yang memadai diterapkan, termasuk memberikan saran rutin tentang risiko dan kontrol teknologi informasi

c. Layanan non-audit berikut dianggap mengganggu independensi dan objektivitas, karena ancaman dibuat akan sangat signifikan sehingga tidak ada perlindungan yang dapat mengurangi mereka ke tingkat yang dapat diterima:

- Menganggap tanggung jawab manajemen atau melakukan kegiatan manajemen
- Keterlibatan material para profesional dalam pengawasan atau kinerja merancang, mengembangkan, menguji, menginstal, mengkonfigurasi atau mengoperasikan sistem informasi yang material atau signifikan bagi subjek masalah audit atau perikatan jaminan
- Merancang kontrol untuk sistem informasi yang material atau signifikan dengan materi terkini atau rencana perikatan audit yang akan datang

- Melayani dalam peran pemerintahan di mana para profesional bertanggung jawab baik secara mandiri atau bersama-sama membuat keputusan manajemen atau menyetujui kebijakan dan standar
- Memberikan saran yang membentuk dasar utama keputusan manajemen

4. Menilai Independence

a. Independensi harus dinilai secara berkala oleh fungsi audit dan profesional. Penilaian ini perlu terjadi setiap tahun untuk fungsi audit dan sebelum setiap perikatan untuk para profesional, seperti dijelaskan dalam Standar 1003 Independensi Profesional. Penilaian harus mempertimbangkan faktor-faktor seperti:
   - Perubahan dalam hubungan pribadi
   - Kepentingan finansial
   - Penugasan dan tanggung jawab pekerjaan sebelumnya

b. Fungsi audit perlu mengungkapkan kemungkinan masalah yang terkait dengan independensi organisasi dan membahasnya mereka dengan dewan direksi atau mereka yang bertanggung jawab atas tata kelola. Resolusi perlu ditemukan dan dikonfirmasi dalam piagam audit atau rencana audit.

5. Piagam Audit dan Rencana Audit

a. Piagam audit harus merinci, di bawah aspek 'tanggung jawab', implementasi organisasi independensi fungsi audit. Selain merinci independensi, piagam audit juga harus mencakup kemungkinan penurunan independensi.

b. Independensi organisasi juga harus tercermin dalam rencana audit. Fungsi audit harus mampu menentukan ruang lingkup rencana secara mandiri, tanpa batasan yang diberlakukan oleh eksekutif pengelolaan.

TUGAS ITAF TASK 3

Nama : Nurhachita

Kelas : MTi Reguler A

NIK : 182420065

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PASCASARJANA UNIVERSITAS BINA DARMA

PALEMBANG

201

IS AUDIT AND ASSURANCE STANDARDS CONTOH KASUS : AUDIT CHARTER

Standar Audit dan Jaminan IS berfungsi untuk :

- Landasan kontribusi profesionalnya bagi komunitas audit dan jaminan
- Terdiri dari level pertama panduan ITAF
- Memberikan informasi yang diperlukan untuk memenuhi kebutuhan kepatuhan
- Memberikan panduan penting untuk meningkatkan efektivitas dan efisiensi
- Menawarkan pendekatan berbasis risiko yang selaras dengan metodologi ISACA
- Berlaku untuk individu yang memberikan jaminan atas beberapa komponen sistem IS, aplikasi, dan infrastruktur
- Semoga juga memberikan manfaat kepada khalayak yang lebih luas, termasuk pengguna audit IS dan laporan jaminan
- Standar ISACA menyediakan informasi yang diperlukan untuk memenuhi kebutuhan kepatuhan profesional audit dan penjaminan IS, serta memberikan panduan penting untuk meningkatkan efektivitas dan efisiensi. Pengetahuan dan kepatuhan terhadap standar ISACA memungkinkan profesional audit dan penjaminan IS untuk mendekati tantangan mereka dengan pendekatan berbasis risiko yang selaras dengan metodologi ISACA.

AUDIT CHARTER

Piagam **Audit** Internal (Internal **Audit Charter**) adalah pedoman bagi **Auditor**/Internal Controller agar dapat melaksanakan tugasnya secara profesional, memperoleh hasil **Audit** yang sesuai dengan standar mutu, dan dapat diterima oleh berbagai pihak baik internal maupun external. Audit charter bisa juga diartikan sebagai Dokumen yang disetujui oleh pihak yang bertanggung jawab atas tata kelola yang mendefinisikan tujuan, wewenang dan tanggung jawab kegiatan audit internal.

Audit charter tersebut berfungsi untuk :

- Menetapkan posisi fungsi audit internal dalam perusahaan
- Otorisasi akses ke catatan, personel, dan properti fisik yang relevan dengan kinerja audit SI dan keterlibatan jaminan
- Tentukan ruang lingkup kegiatan fungsi audit

Audit Charter Hubungan dengan frame work lain dalam cobit :

Sebagai mandat dokumen formal bagi audit IT yang menyatakan tujuan, wewenang, dan tanggung jawab audit intern untuk mengontrol frame work lainnya yang dirancang untuk mencapai serangkaian tujuan spesifik terkait.

Review IT Audit Standards dan Guideline pada ITAF1003 Professional Independence

Statements :

Profesional Audit dan Audit IS harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang terkait dengan audit dan perikatan jaminan.

Key Aspects

Profesional Audit dan Audit IS harus :

- Melakukan Audit SI atau keterlibatan jaminan dengan kerangka pikir yang adil dan tidak memihak dalam menyikapi masalah jaminan dan mencapai kesimpulan.
- Independen sebenarnya, tetapi juga tampak independen setiap saat.
- Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika independensi terganggu pada kenyataannya atau penampilan.
- Menilai independensi secara teratur dengan manajemen dan komite audit, jika ada.
- Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karenanya peran dapat merusak independensi masa depan.

Terms

Term	Definition
Impairment	Suatu kondisi yang menyebabkan kelemahan atau berkurangnya kemampuan untuk melaksanakan tujuan audit Kerusakan independensi organisasi dan objektivitas individu dapat termasuk konflik kepentingan pribadi; batasan ruang lingkup; pembatasan akses ke catatan, personel, peralatan, atau fasilitas; dan keterbatasan sumber daya (seperti pendanaan atau penempatan staf).
Independence	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup Kemandirian pikiran dan Kemandirian dalam penampilan.
Independence in appearance	Menghindari fakta dan keadaan yang begitu

Term	Definition
	signifikan sehingga pihak ketiga yang masuk akal dan berpengetahuan akan cenderung menyimpulkan, menimbang semua fakta dan keadaan tertentu, bahwa perusahaan, fungsi audit atau anggota integritas, objektivitas atau skeptisisme profesional tim audit telah dikompromikan.
Independence of mind	Keadaan pikiran yang memungkinkan ekspresi kesimpulan tanpa dipengaruhi oleh pengaruh yang membahayakan penilaian profesional, dengan demikian memungkinkan individu untuk bertindak dengan integritas dan menjalankan obyektivitas dan skeptisisme profesional.
Objectivity	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi dengan tidak memihak

Review IT Audit Guidelines

2003 Professional Independence

Pedoman disajikan dalam bagian berikut :

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman
3. Referensi dan pemetaan
4. Terminologi
5. Tanggal efektif

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tujuan dari pedoman ini adalah untuk memberikan kerangka kerja yang memungkinkan audit SI dan profesional penjaminan untuk :

- Menetapkan kapan kemerdekaan mungkin, atau mungkin tampak, terganggu
- Pertimbangkan pendekatan alternatif yang potensial untuk proses audit ketika independensi sedang, atau mungkin tampak, terganggu
- Mengurangi atau menghilangkan dampak pada independensi audit IS dan profesional penjamin yang menjalankan peran, fungsi, dan layanan non-audit
- Menentukan persyaratan pengungkapan ketika independensi yang disyaratkan mungkin, atau mungkin tampak, terganggu

1.1.2 IS audit dan jaminan profesional harus mempertimbangkan pedoman ini ketika menentukan bagaimana menerapkan standar, menggunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan mencari panduan tambahan jika dianggap perlu.

1.2 Keterkaitan dengan Standar

1.2.1 Standard 1002 Organisational Independence

1.2.2 Standard 1003 Professional Independence

1.2.3 Standard 1005 Due Professional Care

1.3.1 Selanjutnya :

- 'Fungsi audit dan jaminan IS' disebut sebagai 'fungsi audit'
- ‘IS audit dan assurance profesional’ disebut sebagai ‘profesional’

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang topik utama audit IS dan keterlibatan asuransi:

2.1 Kerangka kerja konseptual

2.2 Ancaman dan perlindungan

2.3 Mengelola ancaman

2.4 Layanan atau peran non-audit

2.5 Layanan atau peran non-audit yang tidak mengganggu independensi

2.6 Layanan atau peran non-audit yang merusak independensi

2.7 Relevansi independensi ketika memberikan layanan atau peran non-audit

2.8 Tata kelola penerimaan layanan atau peran non-audit

2.9 Pelaporan

Fungsi dari Standard tersebut pada Audit TI dan Keterkaitan dengan Cobit

Fungsi Balanced Scorecard menurut Sayekti (2007) adalah:

1. Sebagai sistem pengukuran kinerja yang melihat organisasi secara keseluruhan melalui empat perspektif.

2. Sebagai sistem manajemen strategik yang menyelaraskan antara tujuan jangka pendek dengan strategi tujuan jangka panjang.

3. Sebagai sarana komunikasi bagi perusahaan dengan menerjemahkan strategi kedalam tindakan-tindakan yang seharusnya diambil oleh organisasi.

Secara jelas, COBIT membagi proses pengelolaan teknologi informasi menjadi empat domain utama dengan total tiga puluh empat proses teknologi informasi. Masing-masing domain dalam COBIT mempunyai beberapa rincian sebagai berikut (Sarno, 2009: 31-42): 1.

Plan and Oganise (PO) Dalam perencanaan dan organisasi perusahaan ini sudah Mencakup strategi, taktik dan perhatian atas identifikasi bagaimana IT secara maksimal dapat berkontribusi dalam pencapaian tujuan bisnis. Tetapi disini , startegis perlu direncanakan, dikomunikasikan, dan dikelola untuk berbagai perspektif yang berbeda. Disini sebuah pengorganisasian serta infrastruktur teknologi sudah ditempatkan di tempat yang semestinya. Domain PO ini terdiri dari 10 (sepuluh) proses teknologi informasi seperti terlihat pada tabel F.3. Tabel F.3 Proses Teknologi Informasi dalam Domain PO PO1 Mendefinisikan rencana strategis TI PO2 Mendefinisikan arsitektur informasi PO3 Menentukan arahan teknologi PO4 Mendefinisikan proses TI, organisasi dan keterhubungannya PO5 Mengelola investasi TI PO6 Mengkomunikasikan tujuan dan arahan manajemen PO7 Mengelola sumber daya TI PO8 Mengelola kualitas PO9 Menaksir dan mengelola resiko TI PO10 Mengelola proyek 2. Acquire and Implement (AI) Solusi IT sudah diidentifikasi dan dikembangkan serta diimplementasikan, namun belum diimplementasikan dan terintegrasi ke dalam proses bisnis, tetapi sudah ada perubahan serta pemeliharaan system yang mencakup di dalam domain ini. Pada domain Acquire and Implement sebuah solusi teknologi informasi perlu diidentifikasikan,

dikembangkan, diimplementasikan dan diintegrasikan ke dalam proses bisnis. Domain AI ini terdiri dari 7 (tujuh) proses teknologi informasi seperti terlihat pada tabel F.4. Tabel F.4 Proses Teknologi Informasi dalam Domain AI AI1 Mengidentifikasi solusi otomatis AI2 Memperoleh dan memelihara software aplikasi AI3 Memperoleh dan memelihara infrastruktur teknologi AI4 Memungkinkan operasional dan penggunaan AI5 Memenuhi sumber daya TI AI6 Mengelola perubahan AI7 Instalasi dan akreditasi solusi beserta perubahaannya 3. Deliver and Support (DS) Domain ini berfokus utama pada aspek penyampaian/pengiriman dari IT. Domain ini mencakup area-area seperti pengoperasian aplikasi-aplikasi dalam sistem IT dan hasilnya, serta proses dukungan yang memungkinkan pengoperasian sistem IT tersebut dengan efektif dan efisien. Proses dukungan ini termasuk isu/ masalah keamanan dan juga pelatihan. Domain DS ini terdiri dari 13 (tiga belas) proses teknologi informasi seperti terlihat pada tabel F.5. Tabel F.5 Proses Teknologi Informasi dalam Domain DS DS1 Mendefinisikan dan mengelola tingkat layanan DS2 Mengelola layanan pihak ketiga DS3 Mengelola kinerja dan kapasitas DS4 Memastikan layanan yang berkelanjutan DS5 Memastikan keamanan system DS6 Mengidentifikasikan dan mengalokasikan biaya DS7 Mendidik dan melatih pengguna DS8 Mengelola service desk dan insiden DS9 Mengelola konfigurasi DS10 Mengelola permasalahan DS11 Mengelola data DS12 Mengelola lingkungan fisik DS13 Mengelola operasi 4. Monitor and Evaluate (ME) Menyelenggarakan audit TI yang dilakukan oleh pihak Independent untuk meningkatkan kepercayaan dan memastikan kesesuaian penerapan dan pengelolaan TI dalam mendukung pencapaian tujuan organisasi. Pada domain ini akan ditekankan kepada pentingnya semua proses teknologi informasi perlu diakses secara berkala untuk menjaga kualitas dan kesesuaian dengan standar yang telah ditetapkan. Domain ME ini terdiri dari 4 (empat) proses teknologi informasi seperti terlihat pada tabel F.6. Tabel F.6 Proses Teknologi Informasi dalam Domain ME ME1 Mengawasi dan mengevaluasi kinerja TI ME2 Mengawasi dan mengevaluasi kontrol internal ME3 Memastikan pemenuhan terhadap kebutuhan eksternal ME4 Menyediakan tata kelola TI COBIT memberikan satu langkah praktis melalui domain dan framework yang menggambarkan aktivitas teknologi informasi dalam suatu struktur dan proses yang disesuaikan. Gambaran kerangka kerja (framework) COBIT secara keseluruhan dapat dilihat pada gambar F.3. ITGI (Information Technology Governance Institue, 2007) memberikan pemetaan tujuan teknologi informasi dan tujuan bisnis berdasarkan standar COBIT menjadi 28

tujuan teknologi informasi dan 17 tujuan bisnis. Tabel F.7 Pemetaan Tujuan Bisnis dan Tujuan Teknologi Informasi berdasarkan COBIT No. Tujuan Bisnis Tujuan Teknologi Informasi

1. Penyediaan pengembalian investasi yang baik dari bisnis yang dibangkitkan teknologi informasi.

2. Pengelolaan resiko bisnis yang terkait dengan teknologi informasi.

3. Peningkatan transparansi dan tata kelola perusahaan.

4. Peningkatan layanan dan orientasi terhadap pelanggan.

5. Penawaran produk dan jasa yang kompetitif.

6. Penentuan ketersediaan dan kelancaran layanan.

7. Penciptaan ketangkasan (agility) untuk menjawab permintaan bisnis yang berubah.

8. Pencapaian optimasi biaya dari penyampaian layanan.

9. Perolehan informasi yang bermanfaat dan handal untuk pembuatan keputusan strategis.
10. Peningkatan dan pemeliharaan fungsionalitas proses bisnis.

11. Penurunan biaya proses.

12. Penyediaan kepatutan terhadap hukum eksternal, regulasi dan kontrak.

13. Penyediaan kepatutan terhadap kebijakan internal.

14. Pengelolaan perubahan bisnis.

15. Peningkatan dan pengelolaan produktivitas operasional dan staf.

16. Pengelolaan inovasi produk dan bisnis.

17. Perolehan dan pemeliharaan karyawan yang cakap dan termotivasi.

Sumber: Sarno, 2009: 57-59

Mine coins - make money: http://bit.ly/money_crypto Secara jelas, COBIT membagi proses pengelolaan teknologi informasi menjadi empat domain utama dengan total tiga puluh empat proses teknologi informasi. Masing-masing domain dalam COBIT mempunyai beberapa rincian sebagai berikut (Sarno, 2009: 31-42): 1.

IT AUDIT

Nama : Rahma Fitriyani (182420066)

Program Studi Teknik Informatika S-2

Pascasarjana Universitas Bina Darma

SOAL

Pilih salah satu Standard yang ada pada dokumen ITAF (materi), dan jelaskan secara ringkas fungsi dari standard tersebut pada Audit TI dan jelaskan keterkaitannya dengan COBIT atau framework lain.

JAWABAN :

Standard yang dipilih ialah **1005 (*Due Professional Care*)**

Due Professional Care (Kecermatan professional) berarti kecermatan dan kompetensi yang sewajarnya, tidak berarti kesempurnaan atau kinerja yang luar biasa. Dengan demikian, kecermatan professional **hanya** menuntut auditor internal untuk melakukan pemeriksaan dan verifikasi sampai batas-batas yang wajar. Sekaligus, auditor internal tidak dapat memberikan jaminan mutlak bahwa ketidakpatuhan atau penyimpangan tidak ada. Namun demikian, kemungkinan penyimpangan material atau ketidakpatuhan perlu selalu diperhatikan oleh auditor internal setiap kali melakukan penugasan audit internal.

Fungsi dari *Due Professional Care*:

- Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan.
- Mengoptimalkan kemampuan sumber daya manusia untuk memenuhi tujuan perusahaan.
- Memantau, mengevaluasi, dan menilai sistem pengendalian internal.
- Berkomunikasi dengan anggota tim tentang peran dan tanggung jawab mereka dan memastikan kepatuhan tim terhadap standar yang tepat dalam melakukan perikatan.
- Memahami kompetensi yang memadai untuk mencapai tujuan keterlibatan.
- Menjaga komunikasi yang efektif dengan para pemangku kepentingan yang relevan selama keterlibatan.

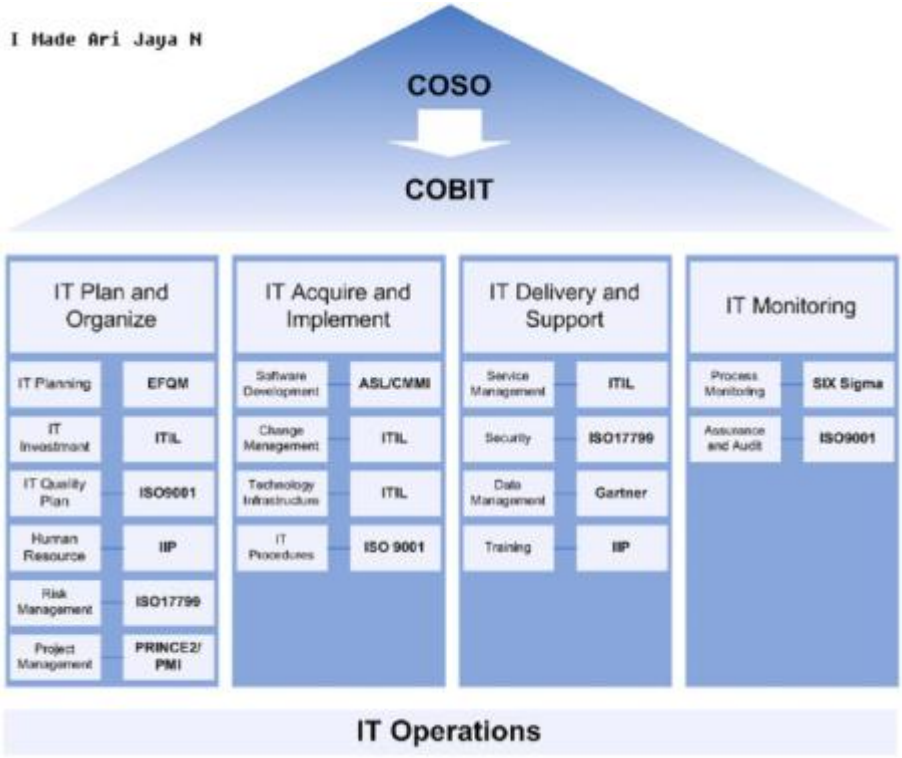
Hubungan Cobit dengan Framework

Secara umum, kerangka kerja IT Governance serta control yang dibutuhkan untuk mencapainya disediakan oleh **COBIT** *(Control Objectives for Information and Related Technology)*. Dimana didalamnya terdapat panduan bagaimana organisasi harus mengendalikan pengelolaan IT dalam pencapaian governance.

Namun COBIT hanya memberikan panduan control dan tidak memberikan panduan implementasi operasional. Dalam memenuhi kebutuhan **COBIT** dalam lingkungan operasional, maka perlu diadopsi berbagai kerangka governance operasional. Dalam implementasi IT Governance di lingkungan operasi, ada beberapa framework governance yang bisa diterapkan, antara lain:

- EFQM *(European Foundation for Quality Management)*, EFQM adalah yayasan non-profit yang berhubungan dengan pengembangan standard an prosedur pemasaran
- ITIL *(IT Infrastructure Library)*, merupakan sebuah panduan pengelolaan layanan IT yang mencakup service delivery dan sevice support.
- ISO9001, merupakan standarisasi manajemen kualitas
- IIP *(Investor in People)*, merupakan standar *de-facto* dari proses pengembangan SDM.
- ISO17799, merupakan standar dalam pengembangan keamanan IT.
- PRINCE2/PMI *(Project Management Institute)*, merupakan standar dalam pengelolaan proyek.
- ASL *(Application Service Library)*, merupakan standar dalam pengembangan software
- CMMI *(Capability Maturity Model Institute)*, merupakan standar dalam pengembangan software
- Gartner, Gartner mengeluarkan sebuah standar dalam pengelolaan data dan informasi
- Six Sigma, merupakan standar dalam pengawasan proses operasi

Gambar berikut menjelaskan bagaimana hubungan framework governance IT operasional tersebut dalam domain COBIT:



Fungsi dari *Due Professional Care*:

- Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan.
- Mengoptimalkan kemampuan sumber daya manusia untuk memenuhi tujuan perusahaan.
- Memantau, mengevaluasi, dan menilai sistem pengendalian internal.
- Berkomunikasi dengan anggota tim tentang peran dan tanggung jawab mereka dan memastikan kepatuhan tim terhadap standar yang tepat dalam melakukan perikatan.
- Memahami kompetensi yang memadai untuk mencapai tujuan keterlibatan.
- Menjaga komunikasi yang efektif dengan para pemangku kepentingan yang relevan selama keterlibatan.

IT AUDIT

1202 Risk Assessment in Planning

Kelompok 4 (Empat)

1. Yuniarti Denita Sari
2. Raju Septa Wijaya
3. Hendri

Dosen Pengampuh : Dr. Widya Cholil, S.Kom., M.IT.

Kelas : MTI 19 Reguler **B**

Magister Teknik Informatika
PASCASARJANA
Universitas Bina Darma Palembang

2019

1202. Risk Assessment in Planning

1202.1 Fungsi audit dan penjaminan IS harus menggunakan pendekatan penilaian risiko yang sesuai dan metodologi pendukung untuk dikembangkan rencana audit SI keseluruhan dan menentukan prioritas untuk alokasi sumber daya audit SI yang efektif.

1202.2 IS audit dan jaminan profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area yang dikaji, ketika merencanakan keterlibatan individu.

1202.3 Profesional audit dan penjaminan IS harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.

Key Aspects (Aspek Kunci)

Saat merencanakan kegiatan yang sedang berlangsung, fungsi audit dan jaminan SI harus:

- Melakukan dan mendokumentasikan, setidaknya setiap tahun, penilaian risiko untuk memfasilitasi pengembangan rencana audit SI.
- Sertakan, sebagai bagian dari penilaian risiko, rencana dan sasaran strategis organisasi dan perusahaan kerangka kerja dan inisiatif manajemen risiko.
- Untuk setiap audit SI dan perikatan jaminan, menghitung dan membenarkan jumlah sumber daya audit SI yang diperlukan untuk memenuhi persyaratan keterlibatan.
- Gunakan penilaian risiko dalam pemilihan area dan item yang menjadi minat audit dan keputusan untuk merancang dan melakukan audit IS dan keterlibatan jaminan tertentu.
- Mencari persetujuan penilaian risiko dari pemangku kepentingan audit dan pihak terkait lainnya.
- Prioritaskan dan jadwalkan pekerjaan audit dan penjaminan IS berdasarkan penilaian risiko.
- Berdasarkan penilaian risiko, kembangkan sebuah rencana yang:
    - Bertindak sebagai kerangka kerja untuk aktivitas audit dan penjaminan IS
    - Mempertimbangkan persyaratan dan kegiatan audit dan jaminan non-IS
    - Diperbarui setidaknya setiap tahun dan disetujui oleh pihak yang bertanggung jawab atas tata kelola
    - Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

Saat merencanakan keterlibatan individu, profesional audit dan penjaminan IS harus:

- Identifikasi dan nilai risiko yang relevan dengan area yang dikaji.

- Melakukan penilaian awal terhadap risiko yang relevan dengan area yang dikaji untuk setiap keterlibatan. Tujuan untuk setiap keterlibatan spesifik harus mencerminkan hasil penilaian risiko awal.
- Dalam mempertimbangkan bidang-bidang risiko dan merencanakan perikatan khusus, pertimbangkan audit, tinjauan, dan temuan sebelumnya, termasuk setiap kegiatan perbaikan. Juga pertimbangkan proses penilaian risiko menyeluruh dewan.
- Berusaha untuk mengurangi risiko audit ke tingkat yang dapat diterima, dan memenuhi tujuan audit dengan tepat penilaian materi IS dan kontrol terkait, saat merencanakan dan melakukan audit IS.
- Saat merencanakan prosedur audit IS spesifik, kenali bahwa semakin rendah ambang materialitas, semakin banyak tepatkan harapan audit dan semakin besar risiko audit.
- Untuk mengurangi risiko materialitas yang lebih tinggi, ganti rugi dengan memperpanjang uji kontrol (kurangi risiko kontrol) dan / atau memperluas prosedur pengujian substantif (mengurangi risiko deteksi) untuk mendapatkan jaminan tambahan.

Terms (ISTILAH)	**Definition(DEFINISI)**
Audit risk (Risiko audit)	Risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah: • Kontrol risiko • Risiko deteksi • Risiko yang melekat
Audit subject matter risk (Risiko materi pelajaran audit)	Risiko relevan dengan area yang sedang ditinjau: • Risiko bisnis (kemampuan pelanggan untuk membayar, kelayakan kredit, faktor pasar, dll.) • Risiko kontrak (kewajiban, harga, jenis, penalti, dll.) • Risiko negara (politik, lingkungan, keamanan, dll.) • Risiko proyek (sumber daya, keahlian, metodologi, stabilitas produk, dll.) • Risiko teknologi (solusi, arsitektur, perangkat keras, dan infrastruktur perangkat lunak jaringan, saluran pengiriman, dll.)
Control risk	Risiko bahwa ada kesalahan materi yang tidak akan dicegah atau

(Kendalikan risiko)	terdeteksi pada dasar tepat waktu oleh sistem pengendalian internal.
Detection risk (Risiko deteksi)	Risiko bahwa IS akan mengaudit atau prosedur substantif profesional jaminan akan tidak mendeteksi kesalahan yang bisa bersifat material, secara individu atau dalam kombinasi dengan lainnya kesalahan.
Inherent risk (Risiko yang melekat)	Tingkat risiko atau paparan tanpa memperhitungkan tindakan yang dilakukan manajemen telah mengambil atau mungkin mengambil (mis., menerapkan kontrol).
Materiality (Materialitas)	Konsep audit mengenai pentingnya item informasi yang berkaitan dengan dampak atau pengaruhnya terhadap fungsi entitas yang diaudit. Ekspresi dari signifikansi relatif atau pentingnya suatu hal tertentu dalam konteks perusahaan secara keseluruhan.
Risk assessment (Tugas beresiko)	Suatu proses yang digunakan untuk mengidentifikasi dan mengevaluasi risiko dan potensi dampaknya. Penilaian risiko digunakan untuk mengidentifikasi item-item atau area yang menyajikan risiko tertinggi, kerentanan atau paparan terhadap perusahaan untuk dimasukkan dalam IS rencana audit tahunan. Penilaian risiko juga digunakan untuk mengelola pengiriman proyek dan proyek risiko manfaat.
Substantive testing (Pengujian substantif)	Memperoleh bukti audit tentang kelengkapan, keakuratan, atau keberadaan kegiatan atau transaksi selama periode audit

Linkage to Guidelines **(Tautan ke Pedoman)**

Tipe	Judul
Guideline(Pedoman)	2202 Penilaian Risiko dalam Perencanaan

2202 Penilaian Risiko dan Perencanaan Audit

Pedoman disajikan dalam bagian berikut:

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman

3. Keterkaitan dengan standar dan proses COBIT 5

4. Terminologi

5. Tanggal efektif

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan

Bagian ini mengklarifikasi:

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tingkat pekerjaan audit yang diperlukan untuk memenuhi tujuan audit adalah keputusan subyektif yang dibuat oleh audit IS dan profesional penjaminan. Tujuan pedoman ini adalah untuk mengurangi risiko mencapai kesalahan kesimpulan berdasarkan temuan audit dan untuk mengurangi adanya kesalahan dalam area yang diaudit.

1.1.2 Pedoman ini memberikan panduan dalam menerapkan pendekatan penilaian risiko untuk mengembangkan:

• IS rencana audit yang mencakup semua perikatan audit tahunan

• Rencana proyek perikatan audit yang berfokus pada satu perikatan audit tertentu

1.1.3 Pedoman ini memberikan perincian tentang berbagai jenis risiko audit dan jaminan IS pertemuan profesional.

1.1.4 Profesional audit dan penjaminan IS harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.

1.2 Tautan ke

Standar

1.2.1 Perencanaan Keterlibatan Standar 1201

1.2.2 Standar 1202 Penilaian Risiko dalam Perencanaan

1.2.3 Standar 1203 Kinerja dan Pengawasan

1.2.4 Material 1204 Standar

1.2.5 Standar 1207 Penyimpangan dan Tindakan Ilegal

1.3 Penggunaan Jangka

1.3.1 Selanjutnya:

- 'Fungsi audit dan penjaminan IS' disebut sebagai 'fungsi audit'
- 'Profesional audit dan penjaminan' disebut sebagai 'profesional'

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang audit dan jaminan utama berikut topik keterlibatan:

2.1 Penilaian risiko dari rencana audit SI

2.2 Metodologi penilaian risiko

2.3 Penilaian risiko perikatan audit perorangan

2.4 Risiko audit

2.5 Risiko yang melekat

2.6 Mengontrol risiko

2.7 Risiko deteksi

2.1 Risiko Penilaian atas IS Rencana Audit

2.1.1 Ketika mengembangkan rencana audit SI secara keseluruhan, pendekatan penilaian risiko yang sesuai harus diikuti. Sebuah resiko penilaian harus dilakukan dan didokumentasikan setidaknya setiap tahun untuk memfasilitasi proses pengembangan dari rencana audit IS. Ini harus mempertimbangkan rencana dan sasaran strategis organisasi dan kerangka kerja dan inisiatif manajemen risiko perusahaan.

2.1.2 Untuk menilai dengan benar dan lengkap risiko yang terkait dengan cakupan lengkap area audit IS, profesional harus mempertimbangkan elemen-elemen berikut ketika mengembangkan rencana audit SI:

- Cakupan penuh semua area dalam lingkup semesta audit IS, yang mewakili kisaran semua kemungkinan kegiatan audit
- Keandalan dan kesesuaian penilaian risiko yang disediakan oleh manajemen
- Proses diikuti oleh manajemen untuk mengawasi, memeriksa, dan melaporkan risiko atau masalah yang mungkin terjadi

- Menutup risiko dalam kegiatan terkait yang relevan dengan kegiatan yang sedang ditinjau

2.1.3 Pendekatan penilaian risiko yang diterapkan harus membantu proses penentuan prioritas dan penjadwalan IS audit dan assurance berfungsi. Ini harus mendukung pemilihan bidang dan item kepentingan audit dan proses pengambilan keputusan untuk merancang dan melakukan perikatan audit IS tertentu.

2.1.4 Profesional harus memastikan bahwa pendekatan penilaian risiko yang diterapkan disetujui oleh mereka yang dituduh pemerintahan dan didistribusikan ke berbagai pemangku kepentingan pelibatan

2.1.5 Profesional harus menggunakan penilaian risiko untuk mengukur dan membenarkan jumlah sumber daya audit SI yang dibutuhkan untuk menyelesaikan rencana audit IS dan persyaratan untuk keterlibatan khusus

2.1.6 Berdasarkan penilaian risiko, para profesional harus mengembangkan rencana audit IS yang bertindak sebagai kerangka kerja untuk kegiatan audit dan penjaminan IS. Itu harus:

- Mempertimbangkan audit dan persyaratan serta kegiatan non-SI audit
- Diperbarui setidaknya setiap tahun
- Disetujui oleh mereka yang bertanggung jawab atas tata kelola
- Mengatasi tanggung jawab yang ditetapkan oleh piagam audit

2.2 Risiko Penilaian Metodologi

2.2.1 Profesional harus mempertimbangkan metodologi penilaian risiko yang tepat untuk memastikan lengkap dan cakupan yang akurat dari perikatan audit dalam rencana audit SI.

2.2.2 Profesional harus setidaknya menyertakan analisis, dalam metodologi, risiko yang terkait dengan perusahaan untuk ketersediaan sistem, integritas data, dan kerahasiaan informasi bisnis.

2.2.3 Banyak metodologi penilaian risiko tersedia untuk mendukung proses penilaian risiko. Ini mulai dari klasifikasi sederhana tinggi, sedang dan rendah, berdasarkan penilaian profesional, hingga lebih banyak lagi perhitungan kuantitatif dan ilmiah memberikan peringkat risiko numerik, dan lainnya yang merupakan kombinasi di antara dua. Profesional harus mempertimbangkan tingkat kompleksitas dan detail yang sesuai untuk perusahaan atau subjek yang diaudit. Panduan khusus tentang melakukan penilaian risiko dapat ditemukan di ISACA publikasi *COBIT 5 untuk Risiko* .

2.2.4 Semua metodologi penilaian risiko bergantung pada penilaian subyektif di beberapa titik dalam proses (misalnya, untuk menugaskan bobot ke berbagai parameter). Profesional harus mengidentifikasi keputusan subjektif yang diperlukan untuk menggunakan metodologi tertentu dan mempertimbangkan apakah penilaian ini dapat dibuat dan divalidasi menjadi tingkat akurasi yang sesuai.

2.2.5 Dalam memutuskan metodologi penilaian risiko mana yang paling tepat, para profesional harus mempertimbangkannya hal-hal sebagai:

- Jenis informasi yang harus dikumpulkan (beberapa sistem menggunakan efek finansial sebagai satu-satunya ukuran ini tidak selalu sesuai untuk perikatan audit IS)
- Biaya perangkat lunak atau lisensi lain yang diperlukan untuk menggunakan metodologi ini
- Sejauh mana informasi yang diperlukan sudah tersedia
- Jumlah informasi tambahan yang harus dikumpulkan sebelum hasil yang andal dapat diperoleh, dan biaya pengumpulan informasi ini (termasuk waktu yang diperlukan untuk diinvestasikan dalam latihan pengumpulan)
- Pendapat dari pengguna lain dari metodologi, dan pandangan mereka tentang seberapa baik telah membantu mereka dalam meningkatkan efisiensi dan / atau efektivitas audit mereka
- Kesediaan mereka yang bertanggung jawab atas tata kelola area audit IS untuk menerima metodologi sebagai sarana untuk menentukan jenis dan tingkat pekerjaan audit yang dilakukan

2.2.6 Tidak ada metodologi penilaian risiko tunggal yang diharapkan sesuai dalam semua situasi. Kondisi mempengaruhi audit dapat berubah seiring waktu. Secara berkala, profesional harus mengevaluasi kembali kesesuaian metodologi penilaian risiko yang dipilih.

2.2.7 Para profesional harus menggunakan teknik penilaian risiko yang dipilih dalam mengembangkan rencana audit SI keseluruhan dan dalam perencanaan pengikatan audit khusus. Penilaian risiko, dalam kombinasi dengan teknik audit lainnya, harus dipertimbangkan dalam membuat keputusan perencanaan seperti:

- Area atau fungsi bisnis yang akan diaudit
- Jumlah waktu dan sumber daya yang akan dialokasikan untuk audit

• Sifat, luas dan waktu prosedur audit

2.2.8 Metodologi penilaian risiko yang diadopsi harus menghasilkan yang konsisten, valid, dapat dibandingkan, dan dapat diulang hasil. Penilaian risiko yang keluar dari metodologi harus konsisten (selama periode), valid, sebanding (dengan penilaian awal / nanti menggunakan metodologi penilaian yang sama) dan berulang (diberikan seperangkat fakta yang serupa, menggunakan metodologi penilaian yang sama akan menghasilkan hasil yang serupa).

2.3 Risiko Penilaian terhadap Audit Hubungan Perorangan

2.3.1 Ketika merencanakan keterlibatan individu, profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area tersebut sedang ditinjau. Hasil penilaian risiko ini harus tercermin dalam tujuan perikatan audit. Selama penilaian risiko, para profesional harus mempertimbangkan:

• Hasil dari perikatan audit sebelumnya, ulasan dan temuan, termasuk kegiatan perbaikan

• Proses penilaian risiko menyeluruh perusahaan

• Kemungkinan terjadinya risiko tertentu

• Dampak risiko tertentu (dalam ukuran nilai moneter atau lainnya) jika itu terjadi

2.3.2 Profesional harus memastikan pemahaman penuh tentang kegiatan dalam ruang lingkup sebelum menilai risiko. Mereka harus meminta komentar dan saran dari pemangku kepentingan dan pihak terkait lainnya. Ini diperlukan untuk menentukan dengan benar dan memeriksa dampak dari risiko yang mungkin terjadi dalam perikatan audit.

2.3.3 Tujuan dari penilaian risiko adalah pengurangan risiko audit ke tingkat yang dapat diterima, dan mengidentifikasi bagian-bagian dari suatu kegiatan yang harus menerima lebih banyak fokus audit. Ini perlu dilakukan oleh seorang penilaian yang tepat dari masalah IS dan kontrol terkait, sambil merencanakan dan melakukan IS audit.

2.3.4 Ketika merencanakan audit IS dan prosedur jaminan tertentu, profesional harus mengenali fakta itu semakin rendah ambang materialitas, semakin tepat ekspektasi audit dan semakin besar risiko audit.

2.3.5 Ketika merencanakan audit IS dan prosedur jaminan tertentu, profesional harus mempertimbangkan kemungkinan illegal tindakan yang dapat memerlukan modifikasi sifat, waktu, atau luas prosedur yang ada. Untuk lebih informasi mengacu pada Standar 1207 Penyimpangan dan Tindakan Ilegal dan Pedoman 2207.

2.3.6 Untuk mendapatkan jaminan tambahan dalam kasus di mana ada risiko audit tinggi atau ambang batas materialitas yang lebih rendah, profesional harus memberikan kompensasi dengan memperluas ruang lingkup atau sifat tes audit IS atau meningkatkan atau memperluas pengujian substantif.

2.4 Risiko Audit

2.4.1 Risiko audit mengacu pada risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah:

- Kontrol risiko
- Risiko deteksi
- Risiko yang melekat

2.4.2 Profesional harus mempertimbangkan masing-masing komponen risiko untuk menentukan tingkat risiko secara keseluruhan. Ini termasuk risiko materi, yang mencakup risiko bawaan dan risiko kontrol; bersama dengan risiko deteksi itu kemudian disebut sebagai risiko audit. Penjelasan lebih lanjut tentang berbagai komponen risiko audit dapat ditemukan di bagian 2.5 hingga 2.7.

2.5 Risiko Inheren

2.5.1 Risiko yang melekat adalah kerentanan area audit untuk melakukan kesalahan yang dapat bersifat material, secara individu atau dalam kombinasi dengan kesalahan lain, dengan asumsi bahwa tidak ada kontrol internal terkait. Sebagai contoh, risiko inheren yang terkait dengan sistem operasi tanpa kontrol yang sesuai biasanya tinggi, karena perubahan, atau bahkan pengungkapan, data atau program melalui kelemahan keamanan sistem operasi dapat mengakibatkan informasi manajemen yang salah atau kerugian kompetitif. Sebaliknya, risiko yang melekat terkait dengan keamanan untuk PC yang berdiri sendiri tanpa kontrol, ketika analisis yang tepat menunjukkan itu tidak digunakan untuk keperluan bisnis yang kritis, biasanya rendah.

2.5.2 Risiko yang melekat untuk sebagian besar area audit IS adalah tinggi karena potensi dampak kesalahan biasanya mencakup beberapa area sistem bisnis dan banyak pengguna.

2.6 Mengontrol Risiko

2.6.1 Risiko pengendalian adalah risiko kesalahan yang dapat terjadi di area audit dan dapat bersifat material, secara individu atau dalam kombinasi dengan kesalahan lain, tidak akan dicegah atau dideteksi dan diperbaiki tepat waktu oleh sistem kontrol internal. Misalnya, risiko kontrol yang terkait dengan tinjauan manual terhadap log komputer dapat menjadi tinggi karena volume informasi yang dicatat. Risiko kontrol terkait dengan data yang terkomputerisasi prosedur validasi biasanya rendah karena proses diterapkan secara konsisten.

2.6.2 Profesional harus menilai risiko kontrol setinggi kecuali kontrol internal yang relevan adalah:

- Diidentifikasi
- Dievaluasi sebagai efektif
- Diuji dan terbukti beroperasi dengan tepat

2.6.3 Para profesional harus mempertimbangkan kontrol IS yang meresap dan terperinci:

- Kontrol IS yang meresap dianggap sebagai bagian dari kontrol umum; mereka adalah kontrol-kontrol umum itu fokus pada manajemen dan pemantauan lingkungan IS. Karena itu mereka mempengaruhi semua yang terkait IS kegiatan. Efek dari kontrol IS yang meresap pada pekerjaan profesional tidak terbatas pada keandalan kontrol aplikasi dalam sistem proses bisnis. Mereka juga mempengaruhi keandalan IS rinci mengendalikan, misalnya, pengembangan program aplikasi, implementasi sistem, administrasi keamanan dan prosedur pencadangan. Lemahnya kontrol IS yang tersebar, dan dengan demikian manajemen dan pemantauan yang lemah Lingkungan IS, harus memberi tahu para profesional tentang kemungkinan risiko tinggi yang dirancang oleh control beroperasi pada level terperinci mungkin tidak efektif.

- Kontrol IS terperinci terdiri dari kontrol aplikasi ditambah kontrol umum yang tidak termasuk dalam kontrol IS meresap. Mengikuti kerangka COBIT, mereka adalah kontrol atas akuisisi, implementasi, pengiriman dan dukungan sistem dan layanan IS.

2.6.4 Risiko yang harus dipertimbangkan oleh para profesional adalah keterbatasan dan kekurangan dalam IS rinci yang mengontrolnya diinduksi oleh ketidakcukupan kontrol IS meresap.

2.7 Risiko Deteksi

2.7.1 Risiko deteksi adalah risiko bahwa prosedur substantif profesional tidak akan mendeteksi kesalahan yang mungkin terjadi materi, secara individu atau dalam kombinasi dengan kesalahan lain. Misalnya, risiko deteksi terkait dengan mengidentifikasi pelanggaran keamanan dalam sistem aplikasi biasanya tinggi karena log untuk seluruh periode audit tidak tersedia pada saat audit. Risiko deteksi terkait dengan mengidentifikasi kekurangan rencana pemulihan bencana biasanya rendah, karena keberadaannya mudah diverifikasi.

2.7.2 Dalam menentukan tingkat pengujian substantif yang diperlukan, para profesional harus mempertimbangkan:

• Penilaian risiko yang melekat

• Kesimpulan dicapai pada risiko kontrol setelah pengujian kepatuhan

2.7.3 Semakin tinggi penilaian risiko bawaan dan risiko kontrol, semakin banyak bukti audit yang harus dimiliki oleh para professional biasanya diperoleh dari kinerja prosedur audit substantif.

3. Keterkaitan dengan Standar dan Proses COBIT 5

3.0 Pendahuluan

Bagian ini memberikan ikhtisar yang relevan:

3.1 Keterkaitan dengan standar

3.2 Keterkaitan dengan proses COBIT 5

3.3 Pedoman lain

3.1 Tautan ke

Standar

Tabel ini memberikan gambaran umum tentang:

• Standar ISACA paling relevan yang secara langsung didukung oleh pedoman ini

• Pernyataan standar yang paling relevan dengan pedoman ini

Catatan: Hanya pernyataan standar yang relevan dengan pedoman ini yang terdaftar.

Judul Standar	Pernyataan Standar yang Relevan
1201 Keterlibatan Perencanaan	Profesional audit dan penjaminan IS harus merencanakan setiap audit dan perikatan jaminan IS untuk mengatasi: • Tujuan, cakupan, garis waktu, dan hasil • Kepatuhan terhadap hukum yang berlaku dan standar audit profesional • Penggunaan pendekatan berbasis risiko, jika perlu • Masalah khusus keterlibatan • Persyaratan dokumentasi dan pelaporan
1202 Penilaian Risiko dalam Perencanaan	Fungsi audit dan penjaminan IS harus menggunakan pendekatan penilaian risiko yang tepat dan mendukung metodologi untuk mengembangkan rencana audit SI keseluruhan dan menentukan prioritas untuk alokasi efektif sumber daya audit IS. IS audit dan jaminan profesional harus mengidentifikasi dan menilai risiko yang relevan dengan area tersebut sedang ditinjau, saat merencanakan keterlibatan individu. Profesional audit dan penjaminan IS harus mempertimbangkan risiko materi, risiko audit, dan paparan terkait dengan perusahaan.
1203 Kinerja dan	IS profesional audit dan jaminan akan melakukan pekerjaan sesuai

Pengawasan	dengan rencana audit SI yang disetujui untuk mencakup risiko yang teridentifikasi dan dalam jadwal yang disepakati.
1204 Materialitas	Profesional audit dan penjaminan IS harus mempertimbangkan potensi kelemahan atau ketidakhadiran mengontrol sementara merencanakan suatu pertunangan, dan apakah kelemahan atau ketidakhadiran tersebut kontrol dapat menyebabkan defisiensi signifikan atau kelemahan material. Profesional audit dan penjaminan IS harus mempertimbangkan materialitas dan hubungannya dengan audit risiko sambil menentukan sifat, waktu dan tingkat prosedur audit. Profesional audit dan penjaminan IS harus mempertimbangkan efek kumulatif minor mengendalikan kekurangan atau kelemahan dan apakah tidak adanya kendali diterjemahkan menjadi defisiensi signifikan atau kelemahan material. IS profesional audit dan jaminan harus mengungkapkan hal berikut dalam laporan: • Tidak adanya kontrol atau kontrol tidak efektif • Signifikansi dari defisiensi control • Kemungkinan kelemahan ini mengakibatkan defisiensi signifikan atau kelemahan material
1207 Penyimpangan dan Tindakan Ilegal	IS profesional audit dan penjaminan akan mempertimbangkan risiko penyimpangan dan tindakan ilegal selama pertunangan.

3.2 Tautan ke

COBIT 5

Proses

Tabel ini memberikan ikhtisar yang paling relevan:

• proses COBIT 5

• Tujuan proses COBIT 5

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam *COBIT 5: Proses yang Memampukan.*

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pemerintahan pengaturan kerangka kerja dan pemeliharaan.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan keputusan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
EDM03 Pastikan risiko optimasi.	Pastikan bahwa risiko perusahaan yang terkait dengan TI tidak melebihi selera risiko dan toleransi risiko, dampak risiko IT terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi untuk kegagalan kepatuhan diminimalkan.
APO12 Kelola risiko.	Mengintegrasikan manajemen risiko perusahaan terkait TI dengan ERM secara keseluruhan, dan menyeimbangkannya biaya dan manfaat mengelola risiko perusahaan terkait TI.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.
MEA03 Monitor, mengevaluasi dan menilai kepatuhan dengan persyaratan eksternal.	Pastikan perusahaan mematuhi semua persyaratan eksternal yang berlaku.

3.3 Panduan Lain

Ketika menerapkan standar dan pedoman, para profesional didorong untuk mencari panduan lain, ketika dipertimbangkan perlu. Ini bisa dari audit IS dan jaminan:

- Kolega dari dalam organisasi dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau
- kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam organisasi, misalnya, komite audit
- Panduan lain (misalnya, buku, makalah, pedoman lainnya)

4. Terminologi

Istilah	Definisi
Piagam audit	Dokumen yang disetujui oleh pihak yang bertanggung jawab atas tata kelola yang mendefinisikan tujuan, wewenang dan tanggung jawab audit IS internal dan kegiatan penjaminan Piagam tersebut harus: • Menetapkan posisi audit IS dan fungsi jaminan internal di dalam perusahaan • Mengesahkan akses ke catatan, personel, dan properti fisik yang relevan dengan kinerja audit SI dan keterlibatan jaminan • Menentukan ruang lingkup kegiatan audit IS dan fungsi jaminan
Risiko audit	Risiko mencapai kesimpulan yang salah berdasarkan temuan audit. Tiga komponen risiko audit adalah: • Kontrol risiko • Risiko deteksi • Risiko yang melekat
Kendalikan risiko	Risiko bahwa ada kesalahan materi yang tidak dapat dicegah atau terdeteksi pada waktu yang tepat dasar oleh sistem pengendalian internal.

Kontrol IS terperinci	Kontrol atas akuisisi, implementasi, pengiriman dan dukungan sistem IS dan layanan yang terdiri dari kontrol aplikasi ditambah kontrol umum yang tidak termasuk dalam kontrol meresap
Risiko deteksi	Risiko yang tidak IS audit atau prosedur substantif profesional tidak akan mendeteksi kesalahan yang bisa bersifat material, secara individu atau dalam kombinasi dengan kesalahan lainnya.
Risiko yang melekat	Tingkat risiko atau paparan tanpa memperhitungkan tindakan yang dimiliki manajemen diambil atau mungkin diambil (misalnya, menerapkan kontrol).
Materialitas	Konsep audit mengenai pentingnya item informasi yang berkaitan dengan dampak atau pengaruhnya terhadap subjek yang diaudit. Ekspresi kerabat signifikansi atau pentingnya suatu masalah tertentu dalam konteks pertunangan atau perusahaan secara keseluruhan.
Tugas beresiko	Suatu proses yang digunakan untuk mengidentifikasi dan mengevaluasi risiko dan potensi dampaknya Penilaian risiko digunakan untuk mengidentifikasi item-item atau bidang-bidang yang menghadirkan risiko tertinggi, kerentanan atau paparan terhadap perusahaan untuk dimasukkan dalam rencana audit tahunan SI. Penilaian risiko juga digunakan untuk mengelola pengiriman proyek dan risiko manfaat proyek.
Kontrol IS yang meresap	Kontrol umum yang dirancang untuk mengelola dan memantau lingkungan IS dan yang, oleh karena itu, mempengaruhi semua aktivitas terkait IS
Pengujian substantif	Memperoleh bukti audit tentang kelengkapan, keakuratan atau keberadaan kegiatan atau transaksi selama periode audit

TUGAS KELOMPOK

IS AUDIT AND ASSURANCE STANDARDS

“1002 Organisational Independence”

Mata Kuliah : IT Audit

Dosen Pengasuh : Dr. Widya Cholil, S.Kom., M.IT.

Disusun oleh :

1. **Reni Septiyanti**
2. **Evan Apriadi Dilatama**
3. **Fero Triando**
4. **Fitrianto Puja Kesuma**

Reguler B Angkatan 19 (Sembilan Belas)

Program Pascasarjana Magister Teknik Informatika

Universitas Bina Darma Palembang

2019

AUDIT SISTEM INFORMASI DAN STANDAR JAMINAN

Audit Sistem Informasi dan Standar Jaminan merupakan aspek-aspek utama yang dirancang untuk membantu audit Sistem Informasi, salah satunya adalah **Standar 1002 Organisational Independence (Kemandirian Organisasi).**

1002 Organisational Independence (Kemandirian Organisasi).

1002.1 Fungsi audit dan jaminan IS harus independen dari area atau aktivitas yang ditinjau untuk memungkinkan penyelesaian obyektif audit dan perikatan jaminan.

Aspek Utama Fungsi audit dan penjaminan IS harus:

- Melaporkan ke tingkat dalam organisasi yang diaudit yang memberikan independensi organisasi dan memungkinkan fungsi audit dan penjaminan IS untuk melakukan tanggung jawabnya tanpa campur tangan.
- Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika independensi mengalami gangguan dalam penampilan atau penampilan.
- Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karena peran tersebut dapat merusak independensi di masa depan.
- Mengatasi independensi dan akuntabilitas fungsi audit dalam piagam dan / atau surat perjanjian.

Istilah	Definisi
Kerusakan	Suatu kondisi yang menyebabkan kelemahan atau berkurangnya kemampuan untuk melaksanakan tujuan audit. Kerusakan pada independensi organisasi dan obyektivitas individu dapat mencakup konflik kepentingan pribadi; batasan ruang lingkup; pembatasan akses ke catatan, personel, peralatan, atau fasilitas; dan keterbatasan sumber daya (seperti pendanaan atau penempatan staf).
Kebebasan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup Kemandirian pikiran dan Kemandirian dalam penampilan.
Kemandirian dalam penampilan	Menghindari fakta dan keadaan yang begitu signifikan sehingga pihak ketiga yang berpengetahuan akan cenderung menyimpulkan, menimbang semua fakta dan keadaan tertentu, bahwa perusahaan, fungsi audit atau anggota integritas, objektivitas atau skeptisisme profesional tim audit telah disepakati.
Kemandirian pikiran	Keadaan pikiran yang memungkinkan ekspresi kesimpulan tanpa dipengaruhi oleh pengaruh yang membahayakan penilaian profesional, dengan demikian memungkinkan individu untuk bertindak dengan integritas dan menjalankan obyektivitas dan skeptisisme profesional
Objektivitas	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi tanpa memihak.

Tautan ke Pedoman

Tipe	Judul
Pedoman	2002 Kemandirian Organisasi

Tanggal Operatif — Standar ISACA ini berlaku untuk semua audit SI dan perjanjian jaminan mulai 1 November 2013.

2002 Kemandirian Organisasi

Pedoman disajikan dalam bagian berikut:

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman
3. Keterkaitan dengan standar dan proses COBIT 5
4. Terminologi
5. Tanggal berlaku

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan Bagian ini mengklarifikasi:

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tujuan dari pedoman ini adalah untuk membahas independensi fungsi audit dan jaminan IS di perusahaan. Tiga aspek penting dipertimbangkan:

- Posisi audit SI dan fungsi jaminan dalam perusahaan
- Tingkat yang dilaporkan oleh audit IS dan fungsi jaminan di dalam perusahaan
- Kinerja layanan non-audit dalam perusahaan oleh audit SI dan manajemen jaminan serta audit SI dan profesional jaminan

1.1.2 Pedoman ini memberikan panduan untuk menilai independensi organisasi dan merinci hubungan antara independensi organisasi dan piagam audit serta rencana audit.

1.1.3 IS profesional audit dan jaminan harus mempertimbangkan pedoman ini ketika menentukan bagaimana menerapkan standar, menggunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan mencari panduan tambahan jika dianggap perlu.

1.2 Keterkaitan dengan Standar

1.2.1 Standar 1001 Piagam Audit

1.2.2 Standar 1002 Kemandirian Organisasi

1.2.3 Standar 1003 Independensi Profesional

1.2.4 Standar 1004 Harapan yang Wajar

1.2.5 Standar 1006 Kemahiran

1.3 Istilah Penggunaan 1.3.1 Selanjutnya:

- 'Fungsi audit dan penjaminan IS' disebut sebagai 'fungsi audit'
- 'Profesional audit dan penjaminan' disebut sebagai 'profesional'

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang topik utama audit IS dan keterlibatan asuransi:

2.1 Posisi dalam perusahaan

2.2 Tingkat pelaporan

2.3 Layanan non-audit

2.4 Menilai independensi

2.5 Piagam audit dan rencana audit

2002 Kemandirian Organisasi (lanjutan)

2.1 Posisi dalam Perusahaan

2.1.1 Untuk memungkinkan kemandirian organisasi, fungsi audit perlu memiliki posisi di perusahaan yang memungkinkannya untuk melakukan tanggung jawabnya tanpa campur tangan. Ini dapat dicapai dengan:

- Menetapkan fungsi audit dalam piagam audit sebagai fungsi atau departemen independen, di luar departemen operasional. Fungsi audit tidak boleh diberi tanggung jawab atau kegiatan operasional apa pun.
- Memastikan bahwa fungsi audit melapor ke tingkat dalam perusahaan yang memungkinkannya mencapai independensi organisasi. Pelaporan ke kepala departemen operasional dapat membahayakan independensi organisasi, seperti yang dijelaskan secara lebih rinci di bagian 2.2.

2.1.2 Fungsi audit harus menghindari pelaksanaan peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen, karena peran tersebut dapat merusak independensi di masa depan. Independensi dan akuntabilitas fungsi audit harus dialamatkan dalam piagam audit, sebagaimana dijelaskan dalam Piagam Audit Standar 1001.

2.2 Tingkat Pelaporan

2.2.1 Fungsi audit harus melaporkan ke tingkat dalam perusahaan yang memungkinkannya untuk bertindak dengan independensi organisasi yang lengkap. Independensi harus didefinisikan dalam piagam audit dan dikonfirmasi oleh fungsi audit kepada dewan direksi dan pihak yang bertanggung jawab atas tata kelola secara teratur, setidaknya setiap tahun.

2.2.2 Untuk memastikan independensi organisasi dalam fungsi audit, hal-hal berikut harus dilaporkan kepada pihak yang bertanggung jawab atas tata kelola (misalnya, dewan direksi) untuk masukan dan / atau persetujuan mereka:

- Rencana dan anggaran sumber daya audit
- Rencana audit (berbasis risiko)
- Tindak lanjut kinerja yang dilakukan oleh fungsi audit pada aktivitas audit IS
- Tindak lanjut dari ruang lingkup yang signifikan atau keterbatasan sumber daya

2.2.3 Untuk memastikan independensi organisasi dalam fungsi audit, diperlukan dukungan eksplisit dari dewan dan manajemen eksekutif.

2.3 Layanan Non-audit

2.3.1 Di banyak perusahaan, harapan manajemen dan staf IS adalah bahwa fungsi audit dapat terlibat dalam menyediakan layanan non-audit. Ini melibatkan, paruh waktu atau paruh waktu, partisipasi para profesional dalam inisiatif SI dan tim proyek SI untuk menyediakan kemampuan penasehat atau konsultatif.

2.3.2 Kegiatan yang bersifat rutin dan administratif atau melibatkan hal-hal yang tidak penting umumnya dianggap bukan tanggung jawab manajemen dan, karenanya, tidak akan mengganggu independensi. Layanan non-audit yang juga tidak akan merusak independensi atau objektivitas, jika pengamanan yang memadai dilaksanakan, termasuk memberikan saran rutin tentang risiko dan kontrol teknologi informasi.

2.3.3 Layanan non-audit berikut ini dianggap merusak independensi dan objektivitas, karena ancaman yang dibuat akan sangat signifikan sehingga tidak ada perlindungan yang dapat mengurangi mereka ke tingkat yang dapat diterima:

- Menganggap tanggung jawab manajemen atau melakukan kegiatan manajemen
- Keterlibatan material para profesional dalam pengawasan atau kinerja merancang, mengembangkan, menguji, memasang, mengonfigurasikan atau mengoperasikan sistem informasi yang material atau signifikan dengan subjek audit atau perikatan jaminan.
- Merancang kontrol untuk sistem informasi yang material atau signifikan dengan subjek perikatan audit saat ini atau yang akan datang
- Melayani dalam peran tata kelola di mana para profesional bertanggung jawab baik secara mandiri atau bersama-sama membuat keputusan manajemen atau menyetujui kebijakan dan standar
- Memberikan saran yang membentuk dasar utama keputusan manajemen

2.3.4 Menyediakan layanan non-audit di bidang-bidang yang saat ini, atau di masa depan, masalah perikatan audit juga menciptakan ancaman terhadap independensi yang akan sulit diatasi dengan perlindungan. Dalam situasi ini, persepsi mungkin bahwa independensi dan obyektivitas fungsi audit dan profesional telah dirugikan dengan melakukan layanan non-audit di bidang tertentu. Fungsi audit dan profesional harus menentukan apakah pengamanan yang memadai dapat diimplementasikan untuk memitigasi ancaman aktual atau yang dirasakan ini terhadap independensi secara memadai.

2.3.5 Pedoman lebih rinci tentang cara menangani ancaman independensi ini dapat ditemukan dalam Standar 1003 Kemandirian Profesional dan Pedoman terkait 2003.

2.4 Menilai Independensi

2.4.1 Independensi harus dinilai secara berkala oleh fungsi audit dan profesional. Penilaian ini perlu terjadi setiap tahun untuk fungsi audit dan sebelum setiap perikatan untuk para profesional, sebagaimana dijelaskan dalam Standar 1003 Independensi Profesional. Penilaian harus mempertimbangkan faktor-faktor seperti:

- Perubahan dalam hubungan pribadi
- Kepentingan finansial
- Penugasan dan tanggung jawab pekerjaan sebelumnya

2.4.2 Fungsi audit perlu mengungkapkan kemungkinan masalah terkait independensi organisasi dan mendiskusikannya dengan dewan direksi atau pihak yang bertanggung jawab atas tata kelola. Resolusi perlu ditemukan dan dikonfirmasi dalam piagam audit atau rencana audit.

2.5 Piagam Audit dan Rencana Audit

2.5.1 Piagam audit harus merinci, di bawah aspek 'tanggung jawab', implementasi independensi organisasi dari fungsi audit. Selain merinci independensi, piagam audit juga harus mencakup kemungkinan penurunan independensi.

2.5.2 Independensi organisasi juga harus tercermin dalam rencana audit. Fungsi audit harus dapat menentukan ruang lingkup rencana secara independen, tanpa batasan yang diberlakukan oleh manajemen eksekutif.

3. Keterkaitan dengan Standar dan Proses COBIT 5

3.0 Pendahuluan

Bagian ini memberikan ikhtisar yang relevan:

3.1 Keterkaitan dengan standar

3.2 Keterkaitan dengan proses COBIT 5

3.3 Pedoman lain

3.1 Keterkaitan dengan Standar

Tabel ini memberikan ikhtisar tentang:

- Standar audit dan jaminan ISACA IS yang paling relevan yang didukung langsung oleh pedoman ini
- Pernyataan standar yang paling relevan dengan pedoman ini Catatan: Hanya pernyataan standar yang relevan dengan pedoman ini yang terdaftar

Judul Standar	Pernyataan Standar yang Relevan
1001 Piagam Audit	Fungsi audit dan penjaminan IS harus mendokumentasikan fungsi audit dengan tepat dalam piagam audit, yang menunjukkan tujuan, tanggung jawab, wewenang, dan akuntabilitas. Fungsi audit dan jaminan SI harus memiliki piagam audit yang disepakati dan disetujui pada tingkat yang sesuai dalam perusahaan.
1002 Kemandirian Organisasi	Fungsi audit dan jaminan IS harus independen dari area atau aktivitas yang ditinjau untuk memungkinkan penyelesaian obyektif audit dan perikatan jaminan.
1003 Independensi Profesional	Profesional audit dan penjaminan IS harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang terkait dengan audit dan perikatan assurance.
1004 Harapan yang Wajar	Profesional audit dan penjaminan IS harus memiliki ekspektasi yang masuk akal bahwa ruang lingkup perikatan memungkinkan kesimpulan atas pokok permasalahan dan mengatasi segala pembatasan.
1006 Kemahiran	Profesional audit dan penjaminan IS, bersama-sama dengan orang lain yang membantu penugasan, harus memiliki keterampilan dan kecakapan yang memadai dalam melakukan audit SI dan keterlibatan penjaminan serta kompeten secara profesional untuk melakukan pekerjaan yang diperlukan.

3.2 Keterkaitan dengan Proses COBIT 5

Tabel ini memberikan ikhtisar yang paling relevan:

- Proses cobit 5
- Tujuan proses cobit 5 aktivitas spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini tercantum dalam cobit 5: proses yang memungkinkan

Proses COBIT 5	Tujuan proses
EDM01 Pastikan pengaturan dan pemeliharaan kerangka tata kelola.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan pendekatan tata kelola perusahaan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan strategi dan tujuan perusahaan, pastikan bahwa proses terkait TI diawasi secara efektif dan transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
APO01 Kelola kerangka kerja manajemen TI.	Memberikan pendekatan manajemen yang konsisten untuk memungkinkan terpenuhinya persyaratan tata kelola perusahaan, yang mencakup proses manajemen, struktur organisasi, peran dan

	tanggung jawab, kegiatan yang andal dan dapat diulang, serta keterampilan dan kompetensi.
MEA02 Memantau, mengevaluasi dan menilai sistem pengendalian internal.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

3.3 Panduan Lain

Ketika menerapkan standar dan pedoman, profesional didorong untuk mencari panduan lain bila dianggap perlu. Ini bisa dari audit IS dan jaminan:

- Kolega di dalam dan / atau di luar perusahaan, misalnya, melalui asosiasi profesional atau kelompok media sosial profesional
- Manajemen
- Badan tata kelola dalam perusahaan, misalnya, komite audit
- Panduan profesional lainnya (mis. Buku, makalah, pedoman lain)

4. Terminologi

Istilah	Definisi
Kemerdekaan	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup kemandirian pikiran dan kemandirian dalam penampilan.
Objektivitas	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi tanpa memihak

5. Tanggal Efektif

5.1 Tanggal Efektif Pedoman ini berlaku untuk semua audit SI dan perjanjian jaminan yang dimulai pada atau setelah 1 September 2014.

TUGAS ITAF TASK 3

Nama : RiccaVerana Sari

Kelas : MTi Reguler A

NIK : 182420067

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

PASCASARJANA UNIVERSITAS BINA DARMA

PALEMBANG

201

IS AUDIT AND ASSURANCE STANDARDS CONTOH KASUS : AUDIT CHARTER

Standar Audit dan Jaminan IS berfungsi untuk :

- Landasan kontribusi profesionalnya bagi komunitas audit dan jaminan
- Terdiri dari level pertama panduan ITAF
- Memberikan informasi yang diperlukan untuk memenuhi kebutuhan kepatuhan
- Memberikan panduan penting untuk meningkatkan efektivitas dan efisiensi
- Menawarkan pendekatan berbasis risiko yang selaras dengan metodologi ISACA
- Berlaku untuk individu yang memberikan jaminan atas beberapa komponen sistem IS, aplikasi, dan infrastruktur
- Semoga juga memberikan manfaat kepada khalayak yang lebih luas, termasuk pengguna audit IS dan laporan jaminan
- Standar ISACA menyediakan informasi yang diperlukan untuk memenuhi kebutuhan kepatuhan profesional audit dan penjaminan IS, serta memberikan panduan penting untuk meningkatkan efektivitas dan efisiensi. Pengetahuan dan kepatuhan terhadap standar ISACA memungkinkan profesional audit dan penjaminan IS untuk mendekati tantangan mereka dengan pendekatan berbasis risiko yang selaras dengan metodologi ISACA.

AUDIT CHARTER

Piagam **Audit** Internal (Internal **Audit Charter**) adalah pedoman bagi **Auditor**/Internal Controller agar dapat melaksanakan tugasnya secara profesional, memperoleh hasil **Audit** yang sesuai dengan standar mutu, dan dapat diterima oleh berbagai pihak baik internal maupun external. Audit charter bisa juga diartikan sebagai Dokumen yang disetujui oleh pihak yang bertanggung jawab atas tata kelola yang mendefinisikan tujuan, wewenang dan tanggung jawab kegiatan audit internal.

Audit charter tersebut berfungsi untuk :

- Menetapkan posisi fungsi audit internal dalam perusahaan
- Otorisasi akses ke catatan, personel, dan properti fisik yang relevan dengan kinerja audit SI dan keterlibatan jaminan
- Tentukan ruang lingkup kegiatan fungsi audit

Audit Charter Hubungan dengan frame work lain dalam cobit :

Sebagai mandat dokumen formal bagi audit IT yang menyatakan tujuan, wewenang, dan tanggung jawab audit intern untuk mengontrol frame work lainnya yang dirancang untuk mencapai serangkaian tujuan spesifik terkait.

Review IT Audit Standards

1003 Professional Independence

Statements :

Profesional Audit dan Audit IS harus independen dan obyektif dalam sikap dan penampilan dalam semua hal yang terkait dengan audit dan perikatan jaminan.

Key Aspects

Profesional Audit dan Audit IS harus :

- Melakukan Audit SI atau keterlibatan jaminan dengan kerangka pikir yang adil dan tidak memihak dalam menyikapi masalah jaminan dan mencapai kesimpulan.
- Independen sebenarnya, tetapi juga tampak independen setiap saat.
- Mengungkapkan rincian penurunan nilai kepada pihak-pihak yang tepat jika independensi terganggu pada kenyataannya atau penampilan.
- Menilai independensi secara teratur dengan manajemen dan komite audit, jika ada.
- Hindari peran non-audit dalam inisiatif SI yang memerlukan asumsi tanggung jawab manajemen karenanya peran dapat merusak independensi masa depan.

Terms

Term	Definition
Impairment	Suatu kondisi yang menyebabkan kelemahan atau berkurangnya kemampuan untuk melaksanakan tujuan audit Kerusakan independensi organisasi dan objektivitas individu dapat termasuk konflik kepentingan pribadi; batasan ruang lingkup; pembatasan akses ke catatan, personel, peralatan, atau fasilitas; dan keterbatasan sumber daya (seperti pendanaan atau penempatan staf).
Independence	Kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Ancaman terhadap obyektivitas seperti itu harus dikelola pada tingkat individu auditor, keterlibatan, fungsional, dan organisasi. Kemandirian mencakup Kemandirian pikiran dan Kemandirian dalam penampilan.

Term	Definition
Independence in appearance	Menghindari fakta dan keadaan yang begitu signifikan sehingga pihak ketiga yang masuk akal dan berpengetahuan akan cenderung menyimpulkan, menimbang semua fakta dan keadaan tertentu, bahwa perusahaan, fungsi audit atau anggota integritas, objektivitas atau skeptisisme profesional tim audit telah dikompromikan.
Independence of mind	Keadaan pikiran yang memungkinkan ekspresi kesimpulan tanpa dipengaruhi oleh pengaruh yang membahayakan penilaian profesional, dengan demikian memungkinkan individu untuk bertindak dengan integritas dan menjalankan obyektivitas dan skeptisisme profesional.
Objectivity	Kemampuan untuk melakukan penilaian, mengemukakan pendapat, dan menyajikan rekomendasi dengan tidak memihak

Review IT Audit Guidelines

2003 Professional Independence

Pedoman disajikan dalam bagian berikut :

1. Tujuan pedoman dan keterkaitan dengan standar
2. Konten pedoman
3. Referensi dan pemetaan
4. Terminologi
5. Tanggal efektif

1. Tujuan Pedoman dan Keterkaitan dengan Standar

1.0 Pendahuluan

1.1 Tujuan pedoman ini

1.2 Keterkaitan dengan standar

1.3 Penggunaan istilah 'fungsi audit' dan 'profesional'

1.1 Tujuan

1.1.1 Tujuan dari pedoman ini adalah untuk memberikan kerangka kerja yang memungkinkan audit SI dan profesional penjaminan untuk :

- Menetapkan kapan kemerdekaan mungkin, atau mungkin tampak, terganggu
- Pertimbangkan pendekatan alternatif yang potensial untuk proses audit ketika independensi sedang, atau mungkin tampak, terganggu
- Mengurangi atau menghilangkan dampak pada independensi audit IS dan profesional penjamin yang menjalankan peran, fungsi, dan layanan non-audit
- Menentukan persyaratan pengungkapan ketika independensi yang disyaratkan mungkin, atau mungkin tampak, terganggu

1.1.2 IS audit dan jaminan profesional harus mempertimbangkan pedoman ini ketika menentukan bagaimana menerapkan standar, menggunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan mencari panduan tambahan jika dianggap perlu.

1.2 Keterkaitan dengan Standar

1.2.1 Standard 1002 Organisational Independence

1.2.2 Standard 1003 Professional Independence

1.2.3 Standard 1005 Due Professional Care

1.3.1 Selanjutnya :

- 'Fungsi audit dan jaminan IS' disebut sebagai 'fungsi audit'
- ‘IS audit dan assurance profesional’ disebut sebagai ‘profesional’

2. Konten Pedoman

2.0 Pendahuluan

Bagian konten pedoman disusun untuk memberikan informasi tentang topik utama audit IS dan keterlibatan asuransi:

2.1 Kerangka kerja konseptual

2.2 Ancaman dan perlindungan

2.3 Mengelola ancaman

2.4 Layanan atau peran non-audit

2.5 Layanan atau peran non-audit yang tidak mengganggu independensi

2.6 Layanan atau peran non-audit yang merusak independensi

2.7 Relevansi independensi ketika memberikan layanan atau peran non-audit

2.8 Tata kelola penerimaan layanan atau peran non-audit

2.9 Pelaporan

TASK 3: REVIEW IT AUDIT STANDARDS DAN GUIDELINE PADA ITAF

NAMA : Rumondang Martha A

NIM : 182420069

KELAS : MTI 19 A

REVIEW ITAF STANDARD

ITAF didesain dan diciptakan oleh ISACA, ITAF merupakan sebuah Framework Praktek Profesional Audit / Assurance SI yang bertujuan sebagai sumber daya pendidikan untuk para profesional yang bekerja pada bidang audit/assurance SI. ITAF memiliki standar-standar audit SI salah satunya adalah Standar Umum (*General Standard*).

Standar umum adalah prinsip-prinsip di mana IS audit dan jaminan profesional beroperasi. Prinsip dan jaminan tersebut berlaku untuk pelaksanaan semua tugas dan penanganan audit IS dan jaminan profesional etika, kemandirian, objektivitas dan perawatan karena, serta pengetahuan, kompetensi dan keterampilan. Standar umum ini mencakup audit charter, independensi organisasi, independensi tenaga profesional, ekspektasi yang logis, perlindungan tenaga profesional, profil, pernyataan tegas dan kriteria. Audit charter memastikan adanya fungsi audit yang jelas mencakup tujuan, tanggung jawab dan akuntabilitas audit. Independensi organisasi memastikan fungsi audit berlaku objektif pada seluruh bagian organisasi dan selurh proses di dalamnya. Independensi tenaga profesional memastikan auditor berperilaku sama kepada seluruh auditee termasuk sikap perilaku dalam proses audit. Ekspektasi yang logis memastikan ekspektasi audit yang rasional dengan standar peraturan yang berlaku dan opini tenaga audit profesional. Perlindungan tenaga profesional dalam arti ketaatan terhadap standar audit yang berlaku dalam perencanaan, proses hingga pelaporan. Profil terkait hasil audit atau penilaian lain yang sebelumnya telah dilakukan dan kompetensi auditor yang melakukan tugas audit di perusahaan. Pernyataan tegas yang menegaskan bahwa proses audit telah dilakukan pada bagian tertentu dengan memberikan hasil audit yang dikategorikan sebagai mencukupi, valid dan relevan. Kriteria yang digunakan harus menjawab kebutuhan informasi audit seperti asasaran audit, keutuhan, relevan, terukur, dapat dimengerti, dikenal umum (penggunaan standar) dan sesuai dengan pengguna hasil audit.

ITAF difokuskan pada materi ISACA dan menyediakan satu sumber di mana IS audit dan jaminan profesional dapat mencari bimbingan, penelitian kebijakan dan prosedur, mendapatkan program audit dan jaminan, dan mengembangkan laporan yang efektif.

Berbeda dengan COBIT yang lebih fokus kepada tata kelola TI, ITAF lebih menitikberatkan pada proses audit.

TUGAS TOPIC 3

IT AUDIT

OLEH:

SAFTA HASTINI

(NIM : 18240084)

DOSEN:

Dr. WIDYA CHOLIL, S.Kom., M.I.T

PROGRAM PASCASARJANA

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA PALEMBANG

TAHUN 2019

PERTANYAAN:

Pilih salah satu Standard yang ada pada dokumen ITAF (materi), dan jelaskan secara ringkas fungsi dari standard tersebut pada Audit TI dan jelaskan keterkaitannya dengan COBIT atau framework lain.

JAWABAN:

1007 ASSERTIONS (PENEGASAN)

Profesional IS audit dan assurance harus meninjau kembali pernyataan yang menjadi dasar subjek masalah akan dinilai untuk menentukan bahwa pernyataan tersebut dapat diaudit dan bahwa pernyataan itu cukup, valid dan relevan.

Profesional IS audit dan assurance harus:

- ✓ Mengevaluasi kriteria yang akan dinilai subjeknya untuk memastikan mereka mendukung asersi.
- ✓ Menentukan apakah asersi dapat diaudit dan didukung oleh informasi yang menguatkan.
- ✓ Menentukan apakah asersi didasarkan pada kriteria yang ditentukan secara tepat dan tunduk pada analisis objektif dan terukur.
- ✓ Di mana asersi telah dikembangkan oleh manajemen, pastikan bahwa, bila dibandingkan dengan standar lain dari pernyataan otoritatif bahwa pernyataan tersebut cukup sehubungan dengan apa yang pembaca yang berpengetahuan atau pengguna harapkan.
- ✓ Di mana pernyataan telah dikembangkan oleh pihak ketiga yang mengoperasikan kontrol atas nama perusahaan, memastikan bahwa asersi diverifikasi dan diterima oleh manajemen.
- ✓ Melaporkan secara langsung terhadap subjek (laporan langsung) atau terhadap pernyataan tentang subjek masalah (laporan tidak langsung).
- ✓ Bentuk kesimpulan tentang setiap asersi, berdasarkan pada agregat temuan terhadap kriteria bersama penilaian profesional.

Kriteria Assertions:

Profesional IS audit dan assurance harus memilih kriteria, di mana materi pelajaran akan dinilai, yang objektif, lengkap, relevan, dapat diukur, dimengerti, diakui secara luas, berwibawa dan dipahami oleh, atau tersedia untuk, semua pembaca dan pengguna laporan.

Ketentuan Assertions:

- ✓ Deklarasi formal atau set deklarasi apa pun yang dibuat oleh manajemen.
- ✓ Penegasan biasanya harus secara tertulis dan biasanya berisi daftar spesifik atribut tentang materi pelajaran tertentu atau tentang proses yang melibatkan materi pelajaran.

Panduan Assertion

- ✓ Tujuan panduan dan keterkaitan dengan standar, yaitu:
  1. Untuk merinci berbagai asersi, panduan Profesional IS audit dan assurance dalam memastikan bahwa kriteria, yang menjadi dasar penilaian masalah, mendukung pernyataan, dan memberikan panduan untuk merumuskan kesimpulan dan menyusun laporan tentang asersi.
  2. Profesional IS audit dan assurance harus mempertimbangkan pedoman ini saat menentukan cara menerapkan standar, gunakan penilaian profesional dalam penerapannya, bersiaplah untuk membenarkan setiap keberangkatan dan pencarian pedoman tambahan jika dianggap perlu.
- ✓ Konten pedoman
- ✓ Keterkaitan dengan standar dan proses COBIT 5
- ✓ Terminologi
- ✓ Tanggal efektif

Standar Pelaporan Assertions

- ✓ Identifikasi perusahaan, penerima yang dituju dan segala batasan pada konten dan sirkulasi
- ✓ Cakupan, tujuan keterlibatan, periode cakupan dan sifat, waktu, dan luasnya pekerjaan yang dilakukan
- ✓ Temuan, kesimpulan dan rekomendasi
- ✓ Setiap kualifikasi atau batasan dalam ruang lingkup yang dimiliki oleh Profesional IS audit dan assurance sehubungan dengan pertunangan
- ✓ Tanda tangan, tanggal dan distribusi sesuai dengan ketentuan piagam audit atau surat pertunangan

TERMININOLOGI ASSERTION

Istilah	Definisi
Tuntutan	Deklarasi formal atau set deklarasi apa pun yang dibuat oleh manajemen
Kriteria	Standar dan tolok ukur yang digunakan untuk mengukur dan menyajikan materi pelajaran dan dimana auditor SI mengevaluasi materi pelajaran. Kriteria harus: ✓ Objektif — Bebas dari bias ✓ Lengkap — Sertakan semua faktor yang relevan untuk mencapai kesimpulan ✓ Relevan — Berkaitan dengan pokok pembicaraan ✓ Terukur — Menyediakan pengukuran yang konsisten ✓ Dapat dimengerti: dalam pengikatan pengesahan, tolok ukur terhadap mana pernyataan tertulis manajemen pada materi pelajaran dapat dievaluasi. Praktisi membentuk kesimpulan tentang materi pelajaran dengan mengacu pada kriteria yang sesuai. Penilaian profesional Penerapan pengetahuan dan pengalaman yang relevan dalam membuat keputusan berdasarkan informasi tentang program tindakan yang sesuai dalam keadaan audit IS dan keterlibatan jaminan
Subjek	Informasi spesifik tunduk pada laporan auditor SI dan prosedur terkait, yang dapat mencakup hal-hal seperti desain atau operasi kontrol internal dan kepatuhan praktik atau standar privasi atau hukum dan peraturan tertentu (bidang kegiatan)

KETERKAITAN ASSERTIONS DENGAN FRAMEWORK COBIT 5

Kegiatan spesifik yang dilakukan sebagai bagian dari pelaksanaan proses ini terdapat dalam COBIT 5

Proses COBIT 5	Tujuan Proses
EDM01 Pastikan pemerintahan pengaturan kerangka kerja dan pemeliharaan	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan keputusan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Dapatkan transparansi untuk pemangku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.