**1: Tujuan ASI** mencakup mencakup berbagai aspek yang mendukung keberhasilan dan keamanan pengelolaan sistem informasi. Beberapa tujuannya ada di nomor 7

**2,6,9**: **Audit sistem informasi** adalah proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien.

**Ruang lingkup Audit Sistem Informasi (8,16)** mencakup berbagai aspek yang dievaluasi oleh auditor untuk memastikan keamanan, integritas, ketersediaan, dan efektivitas sistem informasi

**Beberapa aspek lingkup Audit Sistem Informasi**:

1. Keamanan Informasi: Evaluasi kontrol keamanan untuk melindungi informasi dari akses yang tidak sah, perusakan, atau modifikasi yang tidak sah.
2. Integritas Data: Pemeriksaan terhadap kebenaran dan ketepatan data yang disimpan dan diproses oleh sistem.
3. Ketersediaan Sistem: Pemastian bahwa sistem informasi dapat diakses dan digunakan sesuai kebutuhan organisasi.
4. Efisiensi Operasional: Evaluasi efisiensi dan efektivitas sistem dalam memenuhi tujuan bisnis.
5. Manajemen Risiko: Penilaian terhadap kemampuan sistem untuk mengidentifikasi, mengelola, dan mengurangi risiko informasi.
6. Kepatuhan Hukum dan Peraturan: Pemeriksaan terhadap kepatuhan terhadap regulasi dan perundang-undangan yang berlaku terkait pengelolaan informasi.

**Beberapa perbedaan antara Audit Sistem Informasi dan audit-audit lainnya meliputi:**

1. Fokus pada Teknologi Informasi: Audit Sistem Informasi secara khusus berfokus pada teknologi informasi, termasuk infrastruktur teknologi, perangkat lunak, dan data.
2. Aspek Keamanan yang Mencolok: Keamanan informasi menjadi perhatian utama dalam Audit Sistem Informasi, sedangkan audit lain mungkin lebih menekankan pada aspek keuangan atau operasional.
3. Penekanan pada Pengelolaan Risiko Informasi: Audit Sistem Informasi sering kali lebih menekankan pada pengelolaan risiko terkait dengan keamanan dan integritas informasi.
4. Penggunaan Teknik Audit Berbasis IT: Audit Sistem Informasi sering melibatkan penggunaan teknik audit berbasis teknologi informasi, seperti uji penetrasi, pemindaian keamanan, dan evaluasi kontrol keamanan IT.

**3: Proses pelaporan ASI & langkah" pembuatan laporan ASI**

Berikut adalah langkah-langkah umum dalam membuat laporan audit sistem informasi:

1. *Persiapan Laporan:*

Identifikasi Penerima Laporan: Tentukan pihak-pihak yang akan menerima laporan audit, termasuk manajemen senior, pemilik bisnis, dan mungkin regulator atau otoritas terkait.

Pengumpulan Temuan Audit: Kumpulkan temuan audit dari hasil penilaian dan pengujian sistem informasi, termasuk identifikasi kelemahan, pelanggaran kebijakan, dan rekomendasi perbaikan.

1. *Penyusunan Ringkasan Eksekutif:*

Deskripsi Tujuan Audit: Jelaskan tujuan audit sistem informasi dan ruang lingkup penilaian yang telah dilakukan.

Temuan Kunci: Sertakan ringkasan temuan kunci yang mencakup aspek-aspek signifikan yang ditemukan selama audit.

1. *Pengantar dan Latar Belakang:*

Pengantar: Sertakan pengantar yang menjelaskan alasan pelaksanaan audit dan kepentingan bisnis atau keamanan informasi yang terlibat.

Latar Belakang Sistem: Berikan latar belakang tentang sistem informasi yang diaudit, termasuk arsitektur, aplikasi yang digunakan, dan infrastruktur pendukung.

1. *Metodologi Audit:*

Penjelasan Pendekatan Audit: Jelaskan metode dan pendekatan yang digunakan selama audit, termasuk teknik pengujian, sumber data yang digunakan, dan proses evaluasi keamanan.

1. *Hasil Temuan:*

Presentasi Temuan: Jelaskan temuan audit secara rinci, termasuk kelemahan sistem, pelanggaran kebijakan keamanan, dan risiko yang diidentifikasi.

Bukti Pendukung: Sertakan bukti pendukung seperti hasil pengujian, catatan wawancara, atau dokumentasi lainnya untuk mendukung temuan.

1. *Penilaian Risiko:*

Identifikasi Risiko: Tinjau dan nilai risiko yang terkait dengan temuan audit.

Prioritaskan Risiko: Prioritaskan risiko berdasarkan tingkat urgensi dan dampaknya terhadap keamanan dan kinerja sistem.

1. *Rekomendasi Perbaikan:*

Rekomendasi: Ajukan rekomendasi konkret untuk mengatasi kelemahan dan risiko yang diidentifikasi selama audit.

Prioritas Tindakan: Prioritaskan rekomendasi berdasarkan urgensi dan kepentingan strategis.

1. *Tinjauan Manajemen:*

Presentasi Laporan ke Manajemen: Sajikan laporan kepada manajemen dan pihak terkait, dengan memberikan kesempatan untuk memberikan masukan atau klarifikasi.

Diskusi dan Persetujuan: Diskusikan hasil audit dan rekomendasi dengan manajemen untuk mendapatkan persetujuan dan pemahaman yang mendalam.

1. *Penyusunan Laporan Akhir:*

Penyusunan Laporan: Sempurnakan laporan audit berdasarkan umpan balik dari manajemen dan pihak-pihak terkait.

Penyusunan Laporan Akhir: Susun laporan audit akhir yang mencakup semua elemen yang telah disebutkan sebelumnya.

1. *Distribusi dan Tindak Lanjut:*

Distribusi Laporan: Bagikan laporan audit kepada pihak-pihak yang berkepentingan.

Tindak Lanjut: Pantau dan tindak lanjuti implementasi rekomendasi yang telah diajukan dalam laporan. Pastikan bahwa manajemen mengambil langkah-langkah yang diperlukan untuk memperbaiki kelemahan dan mengurangi risiko.

**4: Audit Mutu Eksternal Bidang Umum** adalah proses penilaian independen dan sistematis terhadap kegiatan atau produk suatu organisasi oleh pihak eksternal yang tidak terlibat langsung dalam operasional organisasi tersebut. Tujuan utama dari audit mutu eksternal adalah untuk menilai sejauh mana organisasi telah mematuhi standar kualitas tertentu dan apakah sistem manajemen mutu yang diterapkan telah efektif.

**Audit Mutu Eksternal di bidang IT** merujuk pada proses penilaian independen yang dilakukan oleh pihak eksternal terhadap sistem, aplikasi, atau proyek TI suatu organisasi untuk memastikan bahwa standar kualitas tertentu dipatuhi. Tujuan utama dari Audit Mutu Eksternal di bidang IT adalah untuk memastikan bahwa produk atau layanan TI memenuhi standar mutu yang ditentukan sebelumnya.

**5,16: Hal-hal yang dilakukan seorang auditor dalam melaksanakan tugasnya**

1. Persiapan: Auditor melakukan persiapan awal audit, termasuk pemahaman tujuan, ruang lingkup, dan risiko yang terkait dengan sistem informasi yang akan diaudit.
2. Review Dokumen: Auditor meninjau dokumen terkait sistem informasi, seperti kebijakan, prosedur, dan dokumentasi teknis.
3. Persiapan kegiatan on-site audit: Persiapan untuk melakukan audit secara langsung di lokasi organisasi yang diaudit.
4. Melakukan kegiatan on-site audit: Auditor menjalankan kegiatan audit secara langsung di lokasi organisasi
5. Persiapan, persetujuan dan distribusi laporan audit: Auditor menyusun laporan audit berdasarkan temuan dan hasil kegiatan audit.
6. **Follow up audit**: Melibatkan tindak lanjut terhadap temuan dan rekomendasi dari laporan audit sebelumnya.

**7**: **4 Tujuan Audit Sistem Informasi**

1. Mengamankan Asset: Memastikan bahwa semua aset sistem informasi, baik itu berupa perangkat keras, perangkat lunak, data, atau sumber daya lainnya, dilindungi dengan langkah-langkah keamanan yang sesuai. Ini termasuk pencegahan akses yang tidak sah dan melindungi informasi sensitif.
2. Menjaga Integritas Data: Memastikan bahwa data yang disimpan dan diolah oleh sistem informasi tetap akurat, konsisten, dan tidak diubah secara tidak sah. Integritas data menjadi kritis untuk keputusan bisnis yang benar dan dapat diandalkan.
3. Menjaga Efektivitas Sistem: Memastikan bahwa sistem informasi beroperasi sesuai dengan tujuan dan kebutuhan perusahaan. Ini mencakup pengoptimalan kinerja sistem, peningkatan fungsionalitas, dan pemenuhan kebutuhan bisnis secara efektif.
4. Mencapai Efisiensi Sumber Daya: Memastikan bahwa sumber daya yang digunakan dalam operasi sistem informasi dimanfaatkan secara efisien. Ini mencakup pengelolaan perangkat keras, perangkat lunak, dan sumber daya lainnya sehingga biaya operasional dapat ditekan tanpa mengorbankan kualitas layanan.

**8**: **Pendekatan Audit Sistem Informasi**

1. Pendekatan temuan (*Exposures Approach*), fokus utama ditekankan pada jenis kesalahan (*losses*) yang terjadi dalam suatu sistem informasi. Setelah itu ditentukan kendali (*controls*) yang dapat digunakan untuk mengurangi kesalahan tersebut sampai pada batas yang dapat diterima (*acceptable levels*).
2. Pendekatan kendali (*Control Approach*), fokus utamanya adalah kendali-kendali di dalam suatu sistem informasi yang dapat digunakan untuk mengurangi kesalahan sampai pada level yang dapat diterima (*acceptable* *levels*).

**10: Keuntungan Audit**

1. Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
2. Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
3. Mengukur tingkat efektifitas dari sistem
4. Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang
5. Menyediakan informasi untuk proses peningkatan
6. Meningkatkan saling memahami antar departemen dan antar individu
7. Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

**11: Jenis Audit** = umum: Compliance, Kinerja, Kecurangan, Sertifikasi

IT: System Audit, Compliance Audit, Product / Service Audit

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

**12: Siapa Saja Yang Akan Di Audit**

1. Management: Bertanggung jawab atas kebijakan, strategi, dan pengambilan keputusan terkait dengan sistem informasi
2. IT Manager: memiliki peran kunci dalam merancang, menerapkan, dan menjaga sistem informasi
3. IT Specialist (network, database, system analyst, programmer, dll.): Bertanggung jawab atas implementasi, pemeliharaan, dan pengembangan teknis sistem informasi.
4. User: Berinteraksi langsung dengan aplikasi & data, sehingga penggunaan yang tepat dan aman penting untuk keberhasilan sistem.

**13: Langkah menjadi Auditor Sistem Informasi:**

Pendidikan & kualifikasi: Gelar Pendidikan & sertifikasi; Pengalaman Kerja: P di bidang It, P Audit; Menguasai Keterampilan Teknis & Nonteknis; Pemahaman Hukum dan Regulasi; Profesional: Bukti Sertifikasi

**14: Tahapan Audit SI, menurut Ron Weber terdapat 5 yaitu:**

Perencanaan Audit (*Planning the Audits*)‏; Pengetesan Kendali (*Tests of Controls*); Pengetesan Transaksi (*Tests of Transactions*); Pengetesan Keseimbangan / Keseluruhan Hasil (*Tests of Balances or Overall Results*); Pengakhiran / penyelesaian Audit (*Completion of the Audit*)‏

**Menurut Gallegos Cs. tahapan Audit SI mencakup 4 aktivitas:**

Perencanaan (*Planning*)‏, Pemeriksaan Lapangan (*Fieldwork*)‏, Pelaporan (*Reporting*), Tindak Lanjut (*Follow Up*)‏

**15: Auditor Eksternal Sistem Informasi**

Audit TI eksternal, menurut definisi, dilakukan oleh auditor dan entitas luar subjek organisasi untuk audit. Tergantung pada ukuran organisasi dan ruang lingkup dan kompleksitas audit TI, audit eksternal dapat dilakukan oleh auditor tunggal atau tim. Auditor mandiri penting bagi audit internal dan eksternal, tetapi dalam konteks audit eksternal mandiri tersebut sering tidak diperlukan. Sementara perusahaan yang menyediakan jasa audit eksternal tunduk peraturan organisasi dan pengawasan, auditor individu melakukan audit eksternal biasanya harus menunjukkan pengetahuan yang memadai dan keahlian dan kualifikasi yang sesuai. Sertifikasi profesional menyediakan satu indikator kualifikasi auditor, terutama di mana sertifikasi yang spesifik sesuai dengan jenis audit eksternal yang dilakukan.

**17: Kasus**. Seorang Wirausaha mempunyai usaha perdagangan dengan berbasis IT menggunakan media on-line yaitu memanfaatkan media on-line (facebook, WA dan Instagram), usaha tersebut berkembang sangat pesat, hal itu dibuktikan dengan banyaknya pemesanan dan transaksi penjualan secara on-line. Seiring dengan kemajuan teknologi maka muncul teknologi dengan berbasis mobile, yang semakin menjadikan komptesi semakin meningkat. Untuk itu wirausahan tersebut menginginkan adanya pengembangan sistem dari yang sudah berjalan ke sistem yang juga menggunakan basis mobile. Buatlah:

a. **Manajemen Risiko:**

1. Identifikasi Risiko: Identifikasi risiko-risiko yang mungkin muncul sehubungan dengan pengembangan sistem dari berbasis web ke berbasis mobile.
2. Analisis Risiko: Lakukan analisis mendalam terhadap setiap risiko yang teridentifikasi untuk menentukan dampak dan probabilitasnya.
3. Evaluasi Risiko: Evaluasi risiko-risiko yang telah diidentifikasi untuk menentukan tingkat risiko yang dapat diterima oleh wirausahawan.
4. PengembanganStrategi**:** Pengembangan strategi manajemen risiko untuk mengurangi atau mengatasi risiko-risiko yang mungkin terjadi.

**b. Risiko-risiko yang Mungkin Terjadi:**

* Inkompatibilitas platform mobile.
* Keamanan data yang kurang pada aplikasi mobile.
* Biaya pengembangan sistem yang lebih tinggi dari perkiraan.
* Potensial penurunan penjualan selama transisi.
* Ketergantungan pada platform pihak ketiga (Facebook, WA, Instagram).
* Persaingan yang semakin meningkat di pasar mobile.
* Kehilangan pangsa pasar kepada pesaing yang lebih adaptif.

**c. Klasifikasi Risiko:**

**1) Resiko Reaktif:**

* Inkompatibilitas Platform Mobile
* Keamanan Data yang Kurang pada Aplikasi Mobile:

**2) Resiko Proaktif:**

* Biaya Pengembangan Sistem yang Lebih Tinggi dari Perkiraan
* Potensial Penurunan Penjualan Selama Transisi
* Ketergantungan pada Platform Pihak Ketiga (Facebook, WA, Instagram)
* Ketidakmampuan Staf untuk Beradaptasi dengan Perubahan
* Persaingan yang Semakin Meningkat di Pasar Mobile
* Kehilangan Pangsa Pasar kepada Pesaing yang Lebih Adaptif

**d. Penyelesaian Risiko:**

* Melibatkan tim pengembang dan uji coba ekstensif sebelum peluncuran.
* Mengadopsi praktik keamanan terbaik untuk melindungi data pelanggan.
* Memiliki anggaran yang jelas dan pemantauan biaya yang ketat.
* Melakukan analisis pasar untuk memahami potensial perubahan dalam pola pembelian pelanggan.
* Membuat rencana kontinuitas bisnis untuk mengatasi ketergantungan pada platform pihak ketiga.
* Melibatkan karyawan dalam tahap perencanaan dan implementasi untuk mengurangi resistansi perubahan.
* Melakukan survei pasar untuk memahami tren dan kebutuhan pelanggan.
* Mengembangkan fitur unik pada aplikasi mobile untuk membedakan dari pesaing.