**1,4,8,16**: **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. Berikut adalah 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.

**2,5,13: 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.

**3: 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.

**6: 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*)‏

**7: 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.

**9: 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

**10: 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

**11: 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.): B**ertanggung jawab atas implementasi, pemeliharaan, dan pengembangan teknis sistem informasi.
4. **User: B**erinteraksi langsung dengan aplikasi & data, sehingga penggunaan yang tepat dan aman penting untuk keberhasilan sistem.

**12: 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**: **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.

**15**: **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*).