Universitas Esa Unggul

Smart, Creative and Entrepreneurial

www.esaunggul.ac.id

Introduction Control and Audit IS

Riya Widayanti
Sistem Informasi - FASILKOM

VISI DAN MISI UNIVERSITAS ESA UNGGUL

VISI

Menjadi perguruan tinggi kelas dunia berbasis intelektualitas, kreatifitas dan kewirausahaan, yang unggul dalam mutu pengelolaan dan hasil pelaksanaan Tridarma Perguruan Tinggi

MISI

1. **Menyelenggarakan pendidikan tinggi yang bermutu dan relevan**
2. **Menciptakan suasana akademik yang kondusif**
3. **Memberikan pelayanan prima kepada seluruh pemangku kepentingan**

Materi Sebelum UTS

01. Introduction Control and Audit IS
02. Areas and Types of Audit IS
03. Control & Audit S Standards
04. Management and Application Control
05. Management Control
06. Application Control
07. Case Study

Universitas Esa Unggul

Materi Setelah UTS

08. Evidence Collection Process
09. Evidence Collection Process
10. Tools CAIS
11. IT Governance and Risk Mangement
12. COBIT
13. ITIL
14. Case Study

Universitas Esa Unggul

KEMAMPUAN AKHIR YANG DIHARAPKAN

1. **Mahasiswa memahami audit sistem informasi dan pengenaliannya, memahami resiko sistem informasi**
2. **Mampu meenggunakn framework untuk mengaudit dan mampu membuat kerangka kerja audit dengan mengacu pada framework tersebut**

Buku Acuan

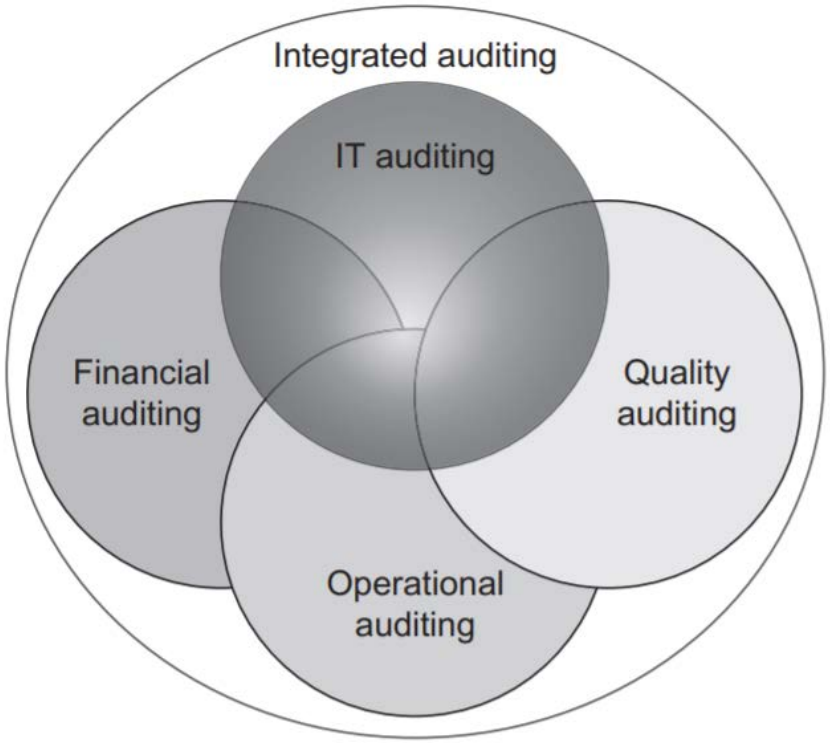
- R. Cascarino, Auditor's Guide to Information System Auditing, John Wiley and Sons: 2007.
- R. Weber, Information System Control and Audit, Prentice Hall: 1999.
- ISACA, COBIT 5 – A Bussiness Framework for Governance and Management of Enterprise IT, 2012.
- ITIL Ver3, 2011

Pengenalan

- Pentingnya Teknolgi Informasi untuk mendukung bisnis proses baik di sektor publik maupun swasta
- TI berperan dalam kesuksesan organisasi, efisiensi proses, daya saing da bahkan untuk keberlanjutan
- Aset informasi dijamin memadai sesuai dengan toleransi resiko organisasi
- Aset tersebut harus
    - beroperasi sebagaimana mestinya
    - bekerja dengan benar
    - berfungsi sesuai dengan peraturan yang berlaku

Overlapping Dalam Audit

- Sumber: The Basic of IT Audit



Auditing

- audit sering didefinisikan sebagai pemeriksaan, pemeriksaan, atau review independen.
- istilah audit untuk berarti "proses yang sistematis, independen dan terdokumentasi untuk mendapatkan bukti audit dan menilainya secara objektif untuk menentukan sejauh mana kriteria audit terpenuhi" [1]
- Library (ITIL) mendefinisikan audit sebagai "pemeriksaan formal dan verifikasi untuk memeriksa apakah seperangkat pedoman diikuti, pencatatannya akurat dan efisiensi/efektivitas dipenuhi.

Complience Audit

- Audit TI mengacu pada standar penilaian dengan membandingkan antara apa yang diharapkan/dibutuhkan organisasi ditunjukkan melalui BUKTI
- Sering disamakan dengan penilaian, evaluasi dan review, namun audit penentuannya lebih biner, yaitu kesesuaian kontrol atau ketidak sesuaian kriteria.

Hasil Audit

- Skala Penilaian (SKOR)→CMM
- Temuan dan rekomendasi untuk perbaikan dari area yang diamati
- Persyaratan audit paham mengenai **baseline**
- Untuk audit eksternal, baseline audit biasanya didefinisikan dalam peraturan atau persyaratan hukum atau peraturan yang berkaitan dengan tujuan dan sasaran audit eksternal.
- Untuk audit internal, organisasi sering memiliki fleksibilitas untuk menentukan garis dasar mereka sendiri atau untuk mengadopsi standar, kerangka kerja, atau persyaratan yang ditentukan oleh organisasi.

Pengendalian Internal

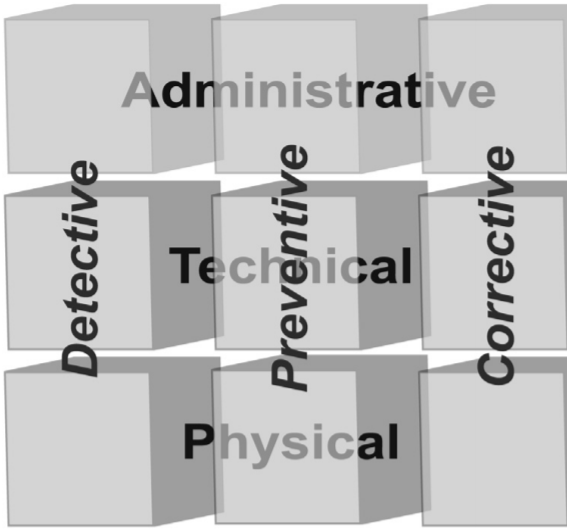
- Audit TI eksternal dan internal memiliki fokus yang sama: pengendalian internal yang dilaksanakan dan dipelihara oleh organisasi yang diaudit.
- **Kontrol** merupakan elemen utama manajemen TI, yang didefinisikan dan dirujuk melalui standar, panduan, metodologi, dan kerangka kerja yang menangani proses bisnis; pemberian layanan dan manajemen; perancangan, implementasi, dan pengoperasian sistem informasi; informasi keamanan; dan tata kelola TI.
- Sumber utama tata kelola TI dan panduan audit TI membedakan antara pengendalian internal dan pengendalian eksternal

Definisi Pengendalian Internal

- "yang dirancang untuk memberikan keyakinan memadai mengenai pencapaian tujuan" – COSO
- kebijakan, rencana dan prosedur, dan struktur organisasi yang dirancang untuk memberikan keyakinan memadai bahwa tujuan bisnis akan tercapai dan kejadian yang tidak diinginkan akan dicegah atau dideteksi dan diperbaiki –COSO
- hasil kebijakan dan prosedur yang dirancang untuk mengendalikan efek --ITGi

Kategori Pengendali Internal

- Preventif: Mencegah hal yang tdk diinginkan
- Detektif: Menemukan hal yang sedang terjadi
- Korektif: Memperbaiki dan memulihkan kejadian yang telah terjadi
- Dan dipisahkan dalam tujuan fungsi yang berbeda yaitu level administratif, teknis dan fisik

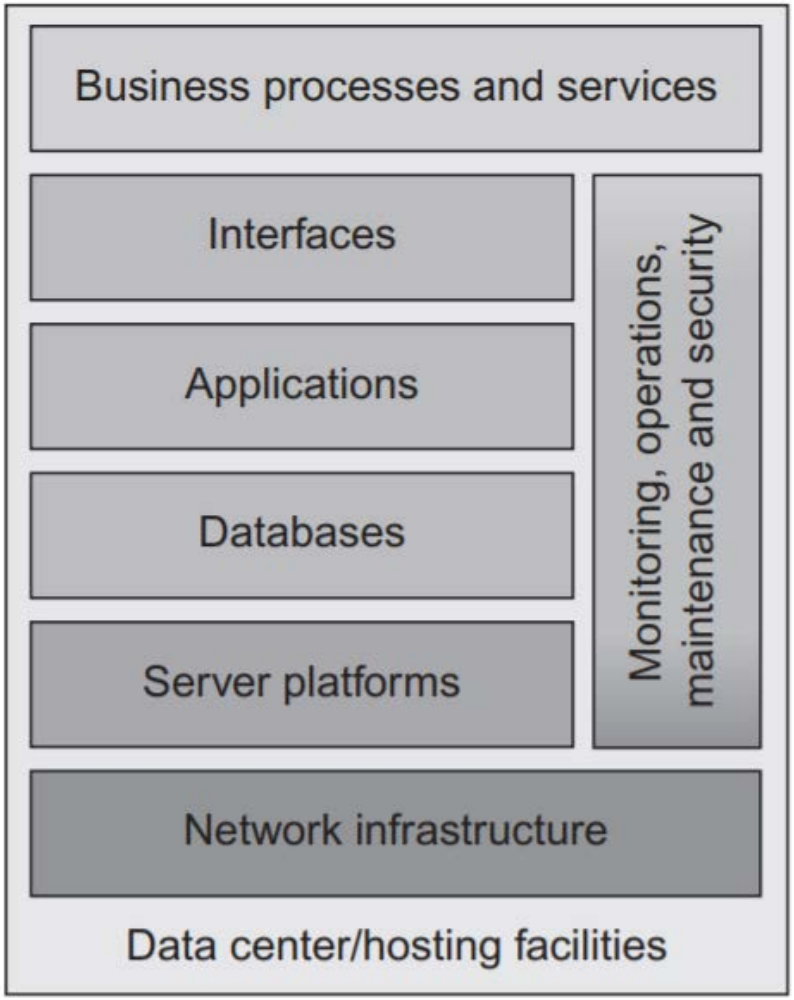


Contoh Pengendalian Internal dari Tipe dan Tujuannya

	Preventive	Detective	Corrective
Administrative	Acceptable use policy; Security awareness training	Audit log review procedures; IT audit program	Disaster recovery plan; Plan of action and milestones
Technical	Application firewall; Logical access control	Network monitoring; Vulnerability scanning	Incident response center; Data and system backup
Physical	Locked doors and server cabinets; Biometric access control	Video surveillance; Burglar alarm	Alternate processing facility; Sprinkler system

Apa yang akan di audit???

- Audit keuangan, kualitas, dan operasional dapat dijalankan secara keseluruhan atau pada tingkat yang berbeda dalam suatu organisasi, audit TI dapat mengevaluasi keseluruhan organisasi, unit bisnis perorangan, fungsi misi dan proses bisnis, layanan, sistem, infrastruktur, atau komponen teknologi.
- Pengendalian internal yang fokus pada elemen TI



Why Audit

Audit TI sering memberikan informasi yang membantu organisasi mengelola risiko, memastikan alokasi sumber daya terkait TI yang efisien, dan mencapai tujuan TI dan bisnis lainnya. Alasan yang digunakan untuk membenarkan audit TI internal mungkin lebih bervariasi antar organisasi, namun mencakup: -

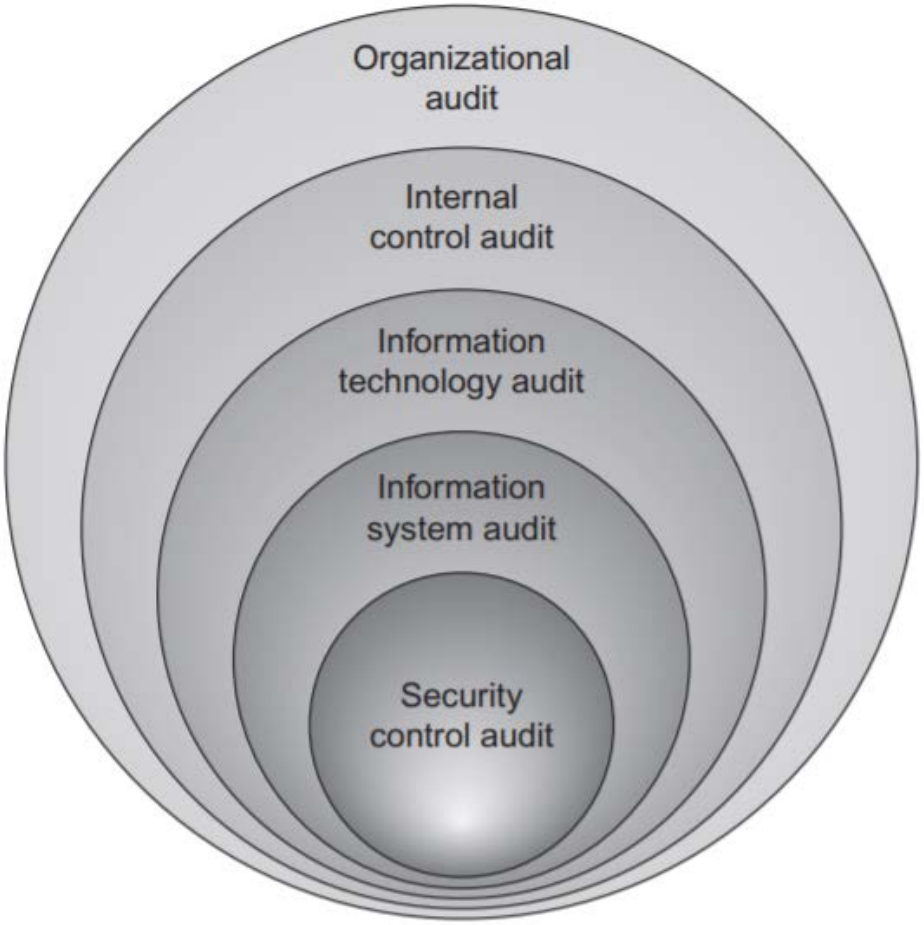
- mematuhi perubahan peraturan bahwa perusahaan memiliki audit internal
- mengevaluasi efektivitas fungsi penerapan kontrol;
- Mengkonfirmasi kepatuhan terhadap kebijakan, proses, dan prosedur internal;
- memeriksa kesesuaian dengan tata kelola atau standar tata kelola atau tata kelola TI;
- menganalisis kerentanan dan pengaturan konfigurasi untuk mendukung pemantauan terus menerus
- mengidentifikasi kelemahan dan kekurangan sebagai bagian dari risiko awal atau yang sedang berlangsung
- mengukur kinerja terhadap tolok ukur mutu atau perjanjian tingkat layanan;
- memverifikasi dan memvalidasi rekayasa sistem atau praktek manajemen proyek TI; dan
- menilai sendiri organisasi terhadap standar atau kriteria yang akan digunakan di Indonesia sebagi antisipasi audit eksternal

External IT Audit Requirement

Sector, Industry, or Type	External IT Audit Drivers
Public corporations	SEC rules; Sarbanes–Oxley Act rules on internal controls (§404) [3] and the PCAOB the law created
Financial institutions	Federal Financial Institutions Examination Council IT Examination Handbook, Audit Booklet [11]
Health care organizations	Revisions to Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Privacy Rule in the Health Information Technology for Economic and Clinical Health (HITECH) Act [12]
Nonprofit organizations	Federal and state audits of internal controls for various types of nonprofits, often tied to sources and amount of funding received
Government agencies	Government Auditing Standards (the "Yellow Book") [13]
Federal funding recipients	Single Audit Act of 1984 [14] and OMB Circular A-133, Audits of states, local governments, and nonprofit organizations [15]
Service providers	ISAE 3402: Assurance reports on controls at a service organization [16]

External Auditor

External IT audits are, by definition, performed by auditors and entities outside the organization subject to the audits



Career IT Audit