Universitas Komputer Indonesia

Chap 7 – IT Control

Dr. Ir. Yeffry Handoko Putra

MAGISTER SISTEM INFORMASI

What is IT Control

- In a governance or risk management context, controls are any measures such as actions, policies, processes, procedures, practices, devices, or organizational structures—used to manage or mitigate risk.
- Controls—especially internal controls—are the primary focus of many types of IT audits

What is IT Control

- the controls applicable to an organization's information technology not only technical controls, but also the administrative controls used by the processes that leverage or support IT and the physical controls associated with people, facilities, equipment, and infrastructure

Control Category

Basis	Representative Categorizations
Control purpose	• Preventive, detective, corrective
Control objective	• Operations, reporting, compliance • Governance, risk management, compliance
Control function	• Administrative, technical, physical • Management, operational, technical
Nature of implementation	• Centralized, shared, decentralized
Level of applicability	• Organization, division, business unit, function • Program, project, system, component

Control categorization is primarily intended to introduce consistency in the way controls are referenced and applied in different contexts and for different purposes. There is no single accepted standard for categorizing controls

Example of IT Control

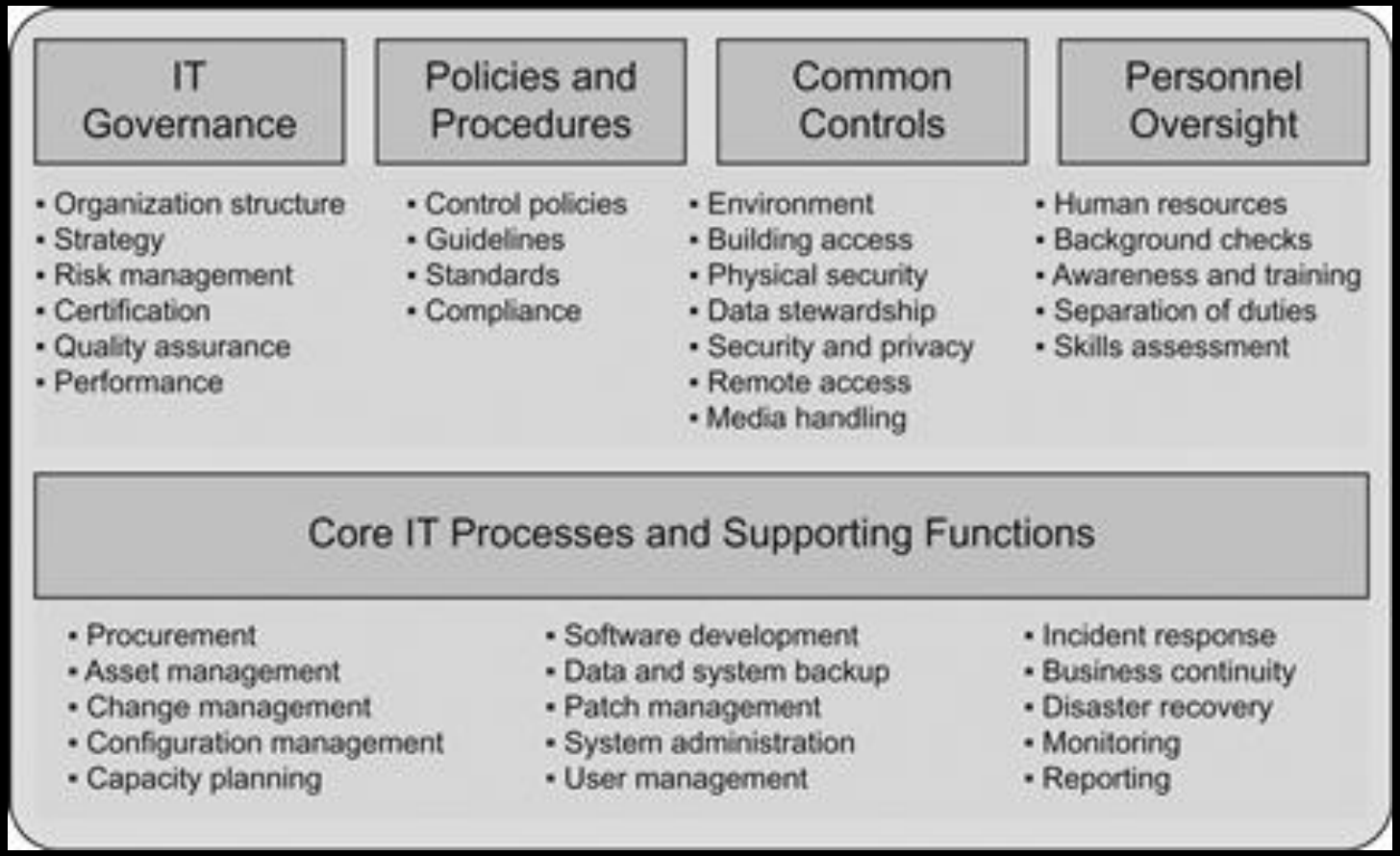
Information Security Management (ISO/IEC 27002) identify :

- 39 control objectives
- 100 controls grouped
- 12 security domains

Organizational controls

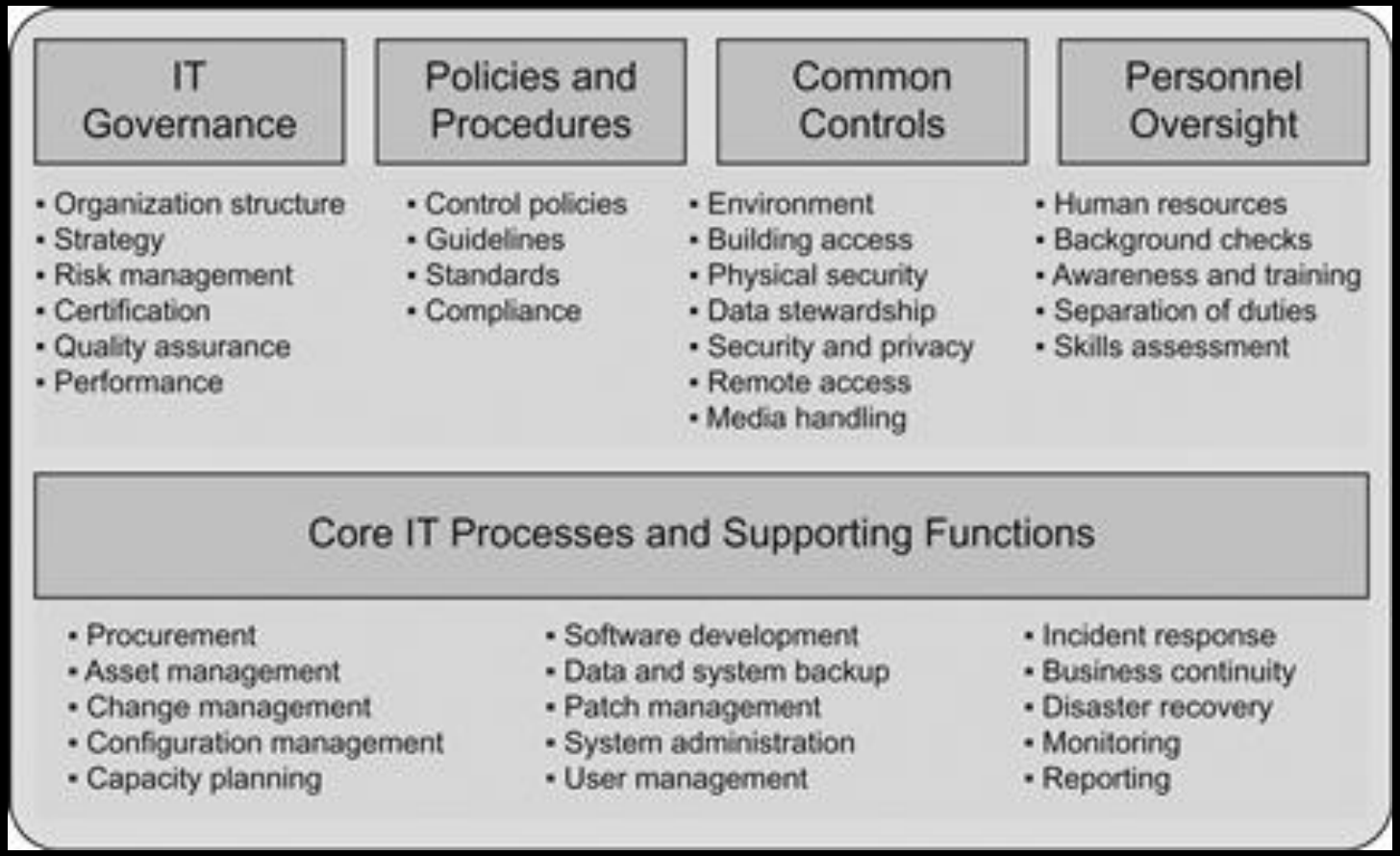
- are selected and implemented once with applicability across the entire enterprise.
- Entity-level controls are important as a focus area for internal and external audits because they provide the foundation for how organizations manage control-supported functions.

Entity-level controls subjected to audit



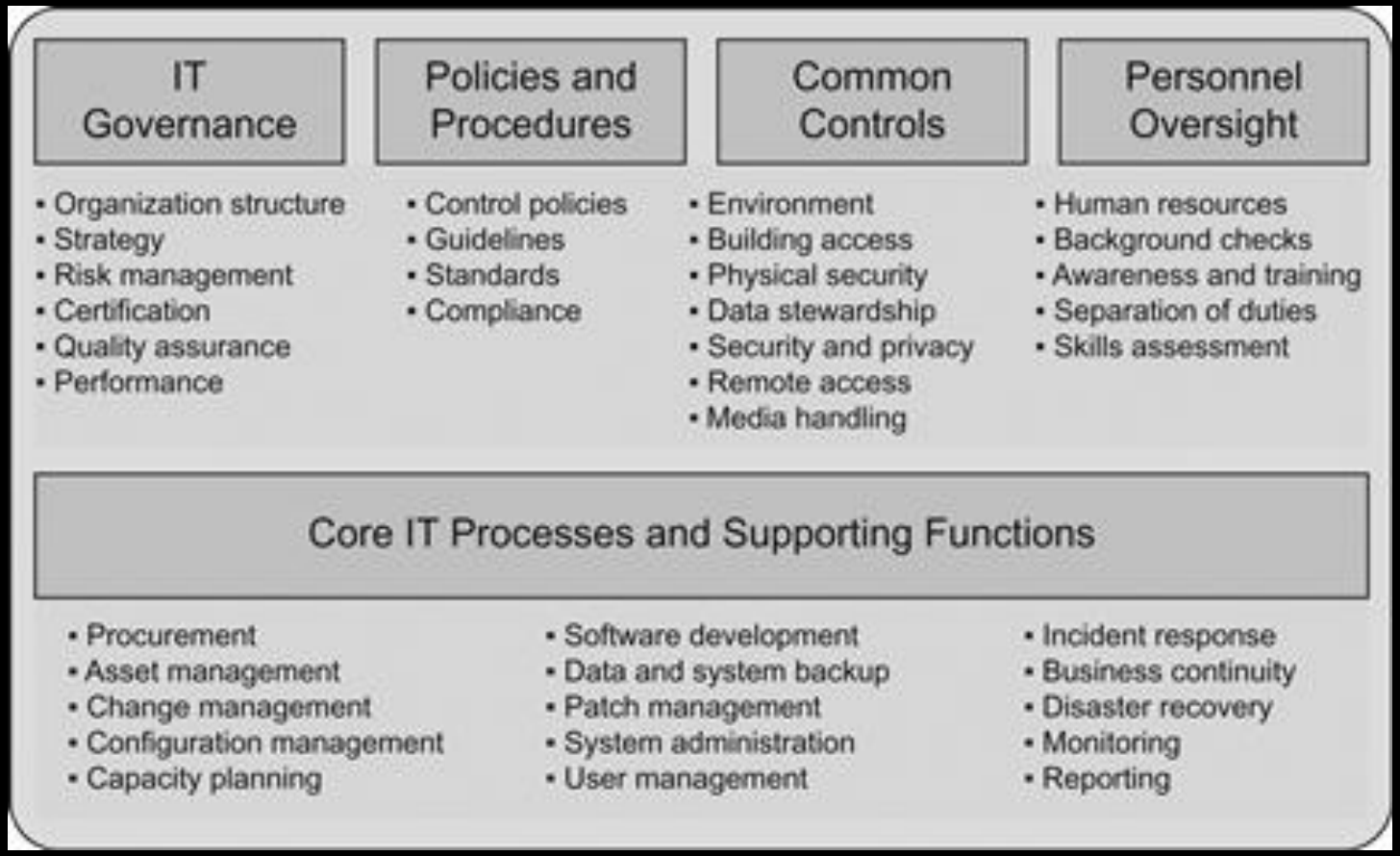
Entity-level controls include any policies, processes and procedures, standards, or measures specified for organization-wide use.

Entity-level controls subjected to audit



IT governance, policies and procedures, common controls, and personnel oversight—each reflect at least some functions or management activities that are likely to be performed similarly across different business units or operational areas

Entity-level controls subjected to audit



Greater variation may be expected for core IT processes and support functions in organizations with different data centers, facilities, service providers, or types of systems, or in organizations with decentralized management structures

Auditing different IT assets

- IT audits require the examination of IT assets as a primary focus in IT-centric auditing or in the context of auditing management functions, business processes, and operational programs and projects supported by IT assets
- The questions IT auditors seek to answer also vary so auditors must have applicable technical knowledge about the IT components and technical controls they audit

IT component decomposition

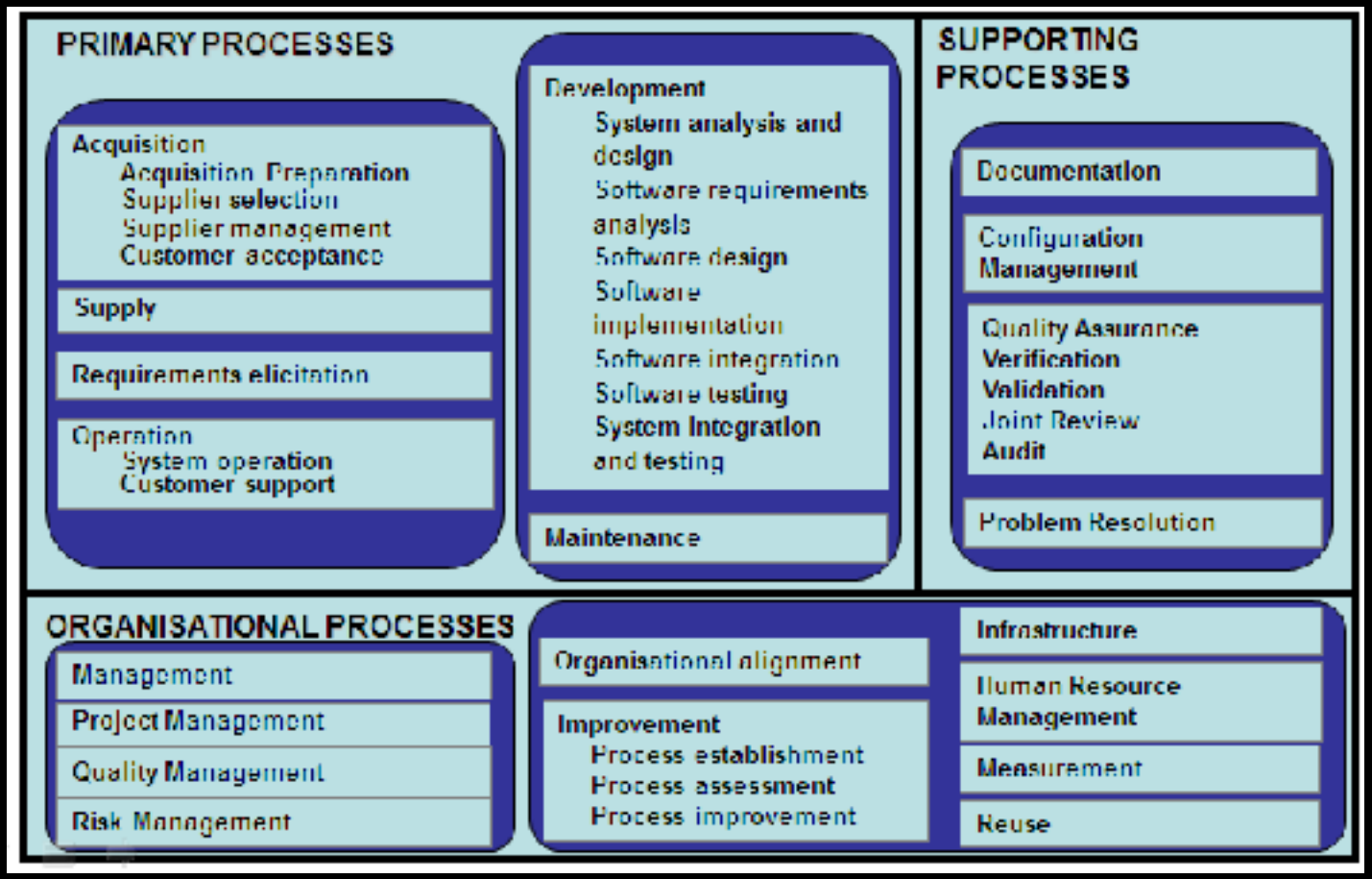
- Organizations clearly identifying IT assets and technical controls to be addressed within each type of audit.
- Decomposing IT audit subject areas into individual technologies
- IT audit plans reflect the IT components it will examine, and the procedures, protocols, standards, or criteria auditors will use

THERE IS NO SINGLE STANDARD OR "BEST" METHOD TO EVALUATING SYSTEMS OR TECHNICAL ENVIRONMENTS

System architecture standards or models as a guide for decomposing IT Component :

- seven-layer Open Systems Interconnection model described in ISO/IEC 7498-1 → OSI Layer
- the software architecture design specified in ISO/IEC 12207 → Software Life Cycle Process
- software architecture description languages conforming to ISO/IEC/ IEEE 42010
- Open Distributed Processing ISO/ IEC 19501:2005 → UML

Software Life Cycle Process



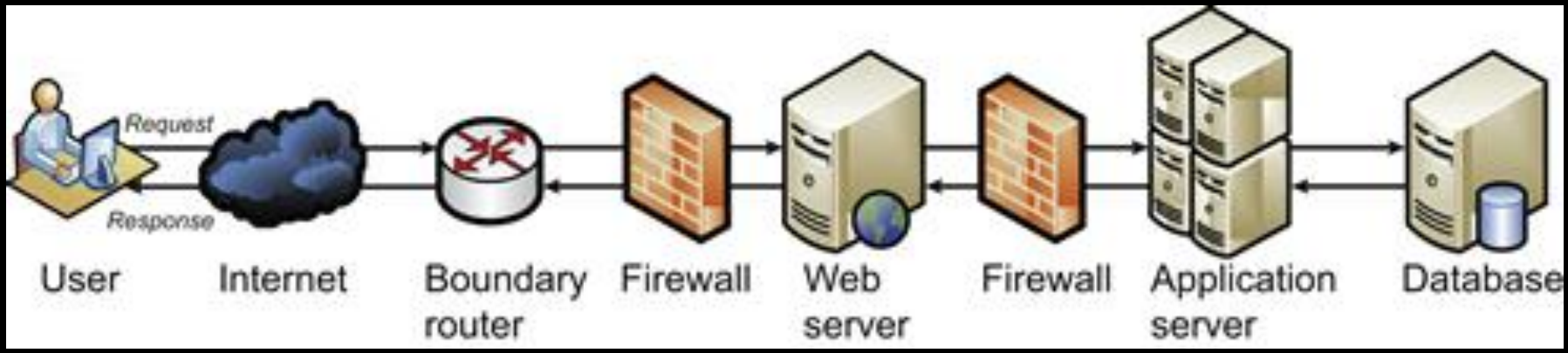
Conceptual foundations: Architecture descriptions

- To audit a typical n-tier architected system, for example, an auditor using such an approach might separately examine the web server, application server, database, middleware or other integration technology as well as the administrators, support personnel, and end users who access the system

Path Analysis
(or critical path analysis, or transaction path analysis)

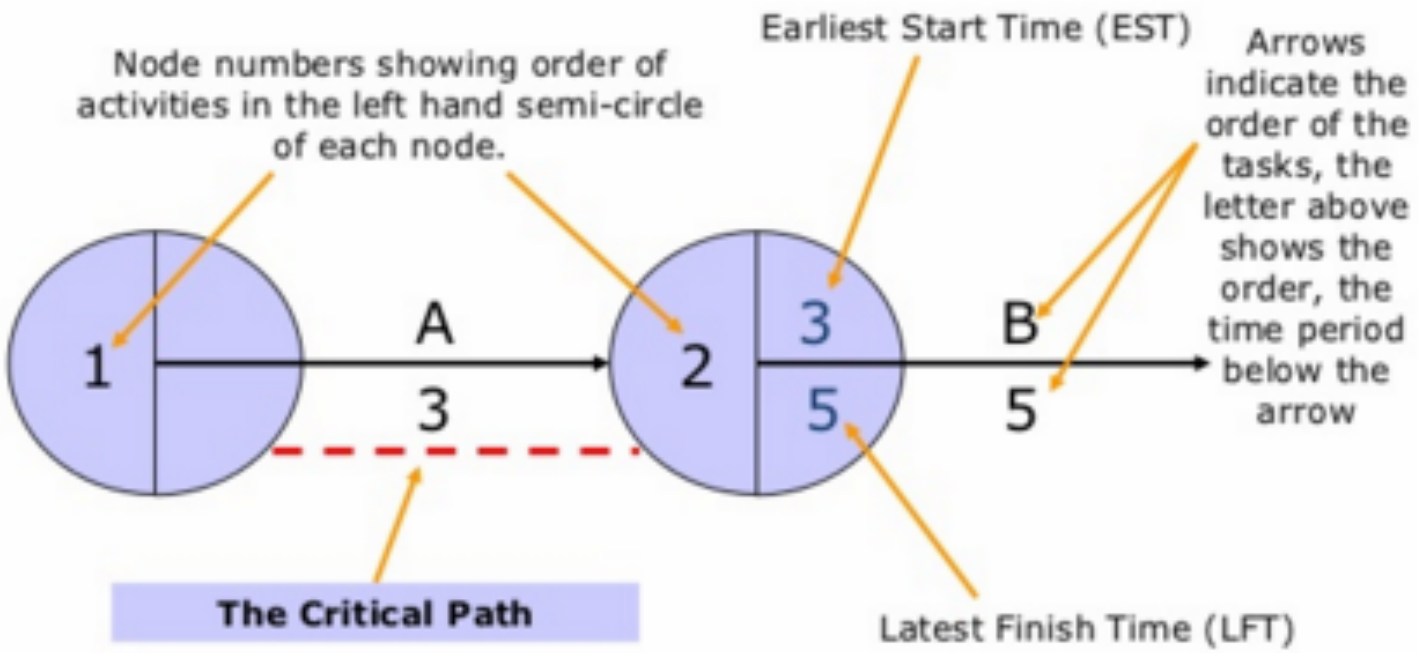
- An alternative approach to auditing systems at the individual component level considers all components, points of integration, and data flows together as the basis for an end-to-end examination

Path Analysis
(or critical path analysis, or transaction path analysis)



defines the system scope by tracing the flow of information from initiation by a user or other system through all points of interaction

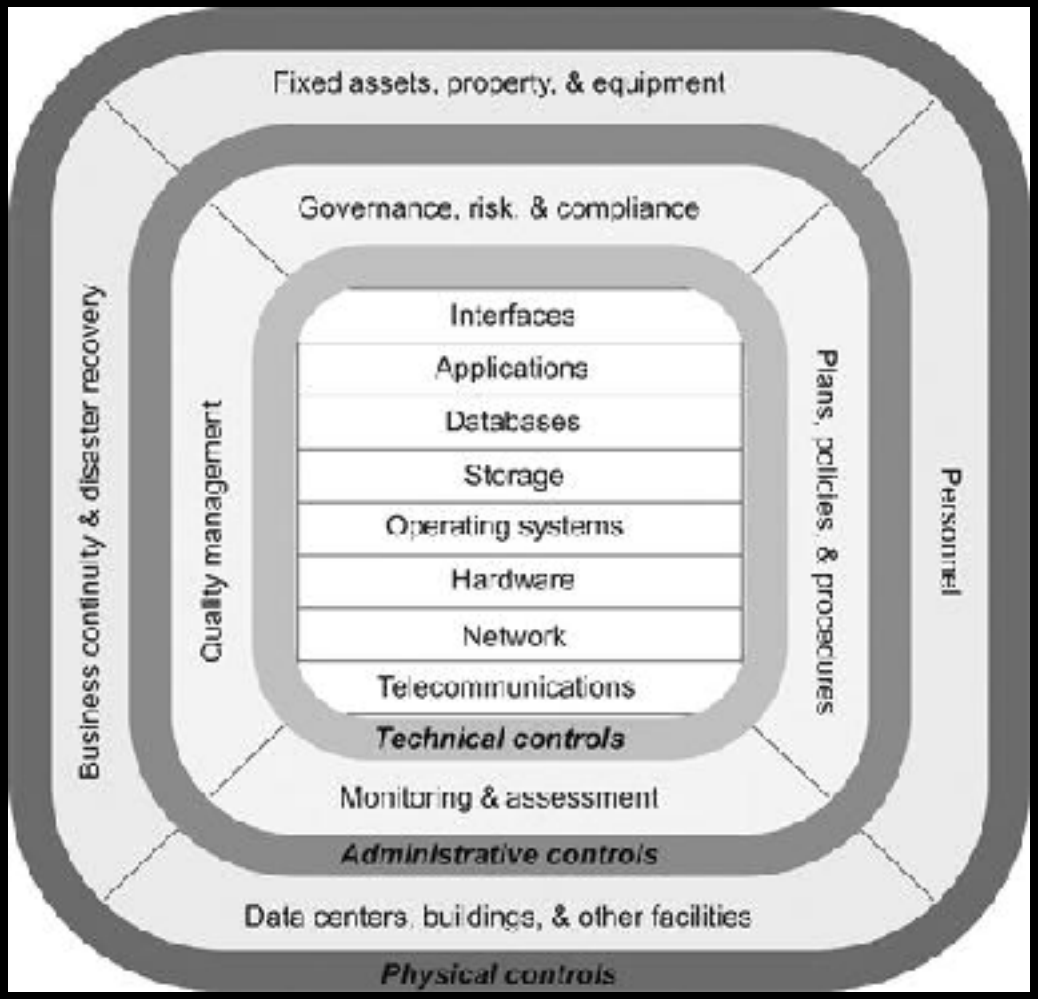
Critical Path Analysis



Nodes: Show the start and finish of a task

ANY QUESTION?

Eight IT Component



Eight IT Component

- Systems and applications
  - The terms system and application are used interchangeably refer to the software and computing capabilities
  - The audit procedures depends on their architecture
  - Audit often focus on fully operational or other phases of the system development life cycle
  - focus on functional and nonfunctional capabilities and controls. Nonfunctional aspects include performance, usability, reliability, and security,

Eight IT Component

- Databases
  - means any collection or repository of information also a specific type of technology that stores and provides access to data
  - Audit focus on The nature and sensitivity of the data, security or privacy controls, confidentiality, integrity, and availability
- Interfaces
  - Audit focus on confirming that system interconnections are authorized, conform to technical specifications, and satisfy functional and technical requirements

Eight IT Component

- Operating systems
  - Operating system audits confirm the use and appropriate configuration of operating systems on different computing platforms deployed within organizations.
- Hardware
  - Audits focus on consistent and correct configuration and adherence to internal policies and standards
  - Compared to software, hardware audits also consider the vendors and internal processes used to acquire hardware.

Eight IT Component

- Networks
  - Network audits examine the implementation and configuration of hardware devices, services and protocols running on the network, and security controls such as firewalls and network intrusion detection systems.
  - Also consider the nature of the communication within the network so that auditors can select appropriate audit procedures to address the use of wireless, satellite, cellular, frame relay, and other network technologies.

Eight IT Component

- Storage
  - Audit procedures storage depend both on the specific types of storage technology and the nature and sensitivity of the data housed in storage environments
  - may be audited in isolation or in a broader operational context
  - May include alternate data storage locations or third-party providers of off-site data backup services

Eight IT Component

- Virtualized environments
  - provides an alternative technical approach to delivering infrastructure, platforms and operating systems, servers, software, and systems and applications
  - employ high-performing hardware and specialized software that enables a single physical server to function as multiple concurrently running instances e.g. Cloud Computing
  - cloud service Distinctions include on-demand service provisioning, ubiquitous network access, resource pooling, elastic capabilities and services, and metered usage and associated billing and payment models
  - Available frameworks developed by Cloud Security Alliance and the Federal Risk and Authorization Management Program (FedRAMP)

Auditing procedural controls or processes

- auditors may examine process-based or procedural controls in conjunction with the IT assets and components
- Influenced by IT framework
  - COBIT for IT Governance
  - ITIL or CMMI for IT Service Management
- Can be found from IT operation

Relevant Process in IT Audit

- Strategic and tactical planning
- Risk management
- Quality management
- Financial management
- Human resources management
- Acquisition or procurement
- Supply chain management

- Program and project management
- Change management
- Service management
- Customer and technical support
- Security management
- Facilities management
- Vendor management

Program and project management

ISO 12207 [12]	ISO 15288 [24]	SP 800-64 [25]	PMBOK [21]
Software development	System development	System development	Project management
Acquisition	Concept	Initiation	Initiating
Supply	Development	Development/acquisition	Planning
Development	Production	Implementation/assessment	Executing
Operation	Utilization	Operations and maintenance	Monitoring and controlling
Maintenance	Support		
Disposal	Retirement	Disposal	Closing