CIA Test Preparation
Part III : Unit 8

Information Technology I

March 17, 2012

By Mr. Manit Panichakul, MBA, CIA, CISA, CISM, CRISC

Outline

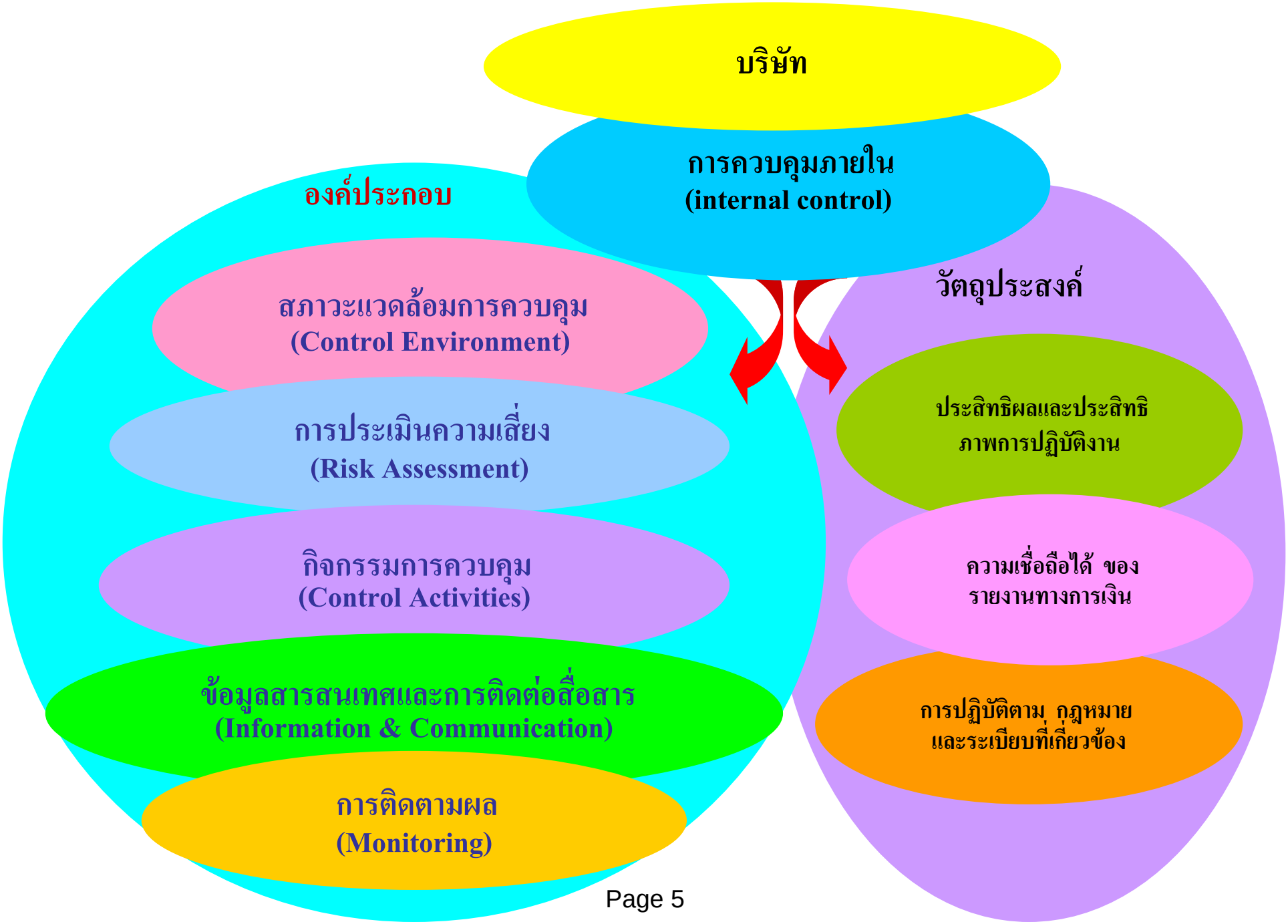
1. Control Frameworks
   a) Committee of Sponsoring Organizations of the Tradeway Commission (COSO) Framework
   b) Electronic Systems Assurance and Control (eSAC)
   c) Control Objectives for Information and Related Technology (CobiT)
   d) Global Technology Audit Guide (GTAG)
2. Aspects of Automated Information processing including IT Controls
3. Data Communications, Networks, and Client-Server Systems
4. EFT, E-Commerce and EDI
5. Questions

1a. Committee of Sponsoring Organizations of the Tradeway Commission (COSO) Framework

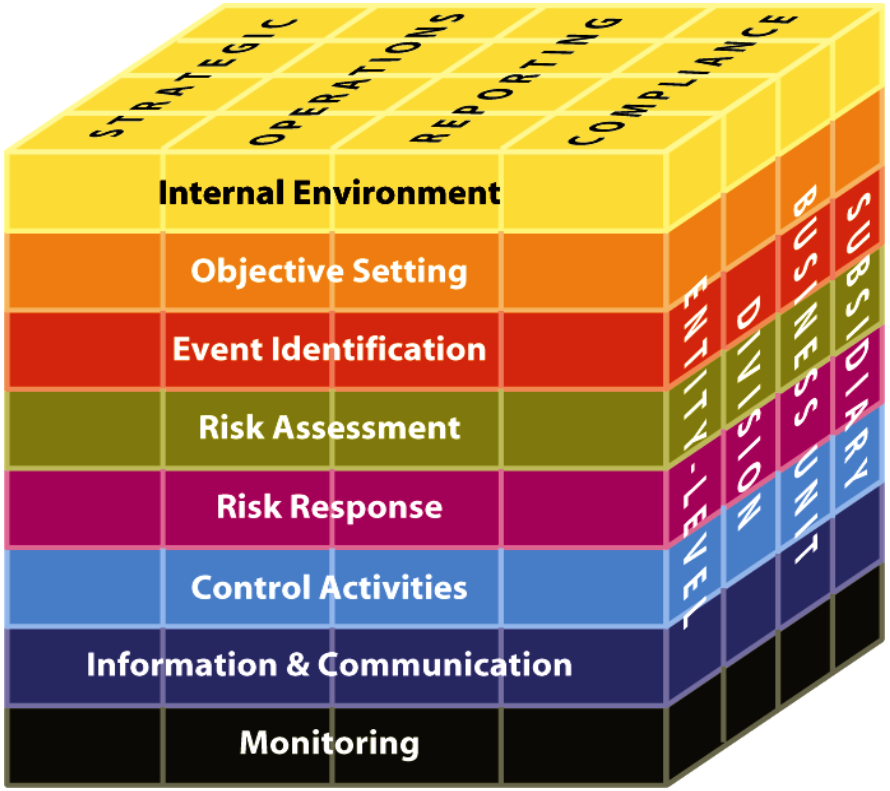
COSO Framework:
Internal Control - Integrated Framework, published 1992

COSO's simple and straightforward definition has proved extremely useful
The important and durability of COSO was reinforced by US SEC under the requirement of Sarbanes-Oxley Act 2002


วิธีการดำเนินทางธุรกิจ
(The way management
run a business)
กระบวนการ
บริหารธุรกิจ
(Management
Process)
องค์ประกอบ
การควบคุมภายใน
(Internal Control
Components)


บริษัท
การควบคุมภายใน
(internal control)
องค์ประกอบ
สภาวะแวดล้อมการควบคุม
(Control Environment)
การประเมินความเสี่ยง
(Risk Assessment)
กิจกรรมการควบคุม
(Control Activities)
ข้อมูลสารสนเทศและการติดต่อสื่อสาร
(Information & Communication)
การติดตามผล
(Monitoring)
วัตถุประสงค์
ประสิทธิผลและประสิทธิ
ภาพการปฏิบัติงาน
ความเชื่อถือได้ ของ
รายงานทางการเงิน
การปฏิบัติตาม กฎหมาย
และระเบียบที่เกี่ยวข้อง

COSO Control Framework vs. *COSO ERM*



Summary of Updates

What's changed…

The experienced reader will find much familiar in the updated *Framework*, which builds on what has proven effective in the original version.

What is not changing...

1. Definition of internal control
2. Five components of internal control
3. The fundamental criteria used to assess effectiveness of systems of internal control
4. Use of judgment in evaluating the effectiveness of systems of internal control

What is changing...

1. Codification of principles with universal application for use in developing and evaluating the effectiveness of systems of internal control
2. Expanded financial reporting objective to address internal and external, financial and non-financial reporting objectives
3. Increased focus on operations, compliance and non-financial reporting objectives based on user input

Summary of Updates

A changing business environment...	***Drives updates to the Framework...***
Expectations for governance oversight	
Globalization of markets and operations	
Changes in business models	
Demands and complexity of rules, regulations and standards	
Expectations for competencies and accountabilities	
Use and reliance on evolving technology	
Expectations for preventing and detecting fraud	

Updated COSO Cube

1b. Electronic Systems Assurance and Control (eSAC)

eSAC

Tool produced by IIA in 2002 to update the SAC

- Understand, monitor,assess, and mitigate technology risks
- Address risk that accompany each organizational component including customers, competitors, regulators,communities, infrastructures, and owners
- A framework for evaluating business controls

•Major IT changes

- IT is in every aspect of operations
- Distributed data processing
- Broadband and wireless communication
- Decreased cost, increased capacity and processing power
- Evolution of enterprise-wide planning (ERP) software

1b. Electronic Systems Assurance and Control (eSAC)

eSAC response to technology challenges

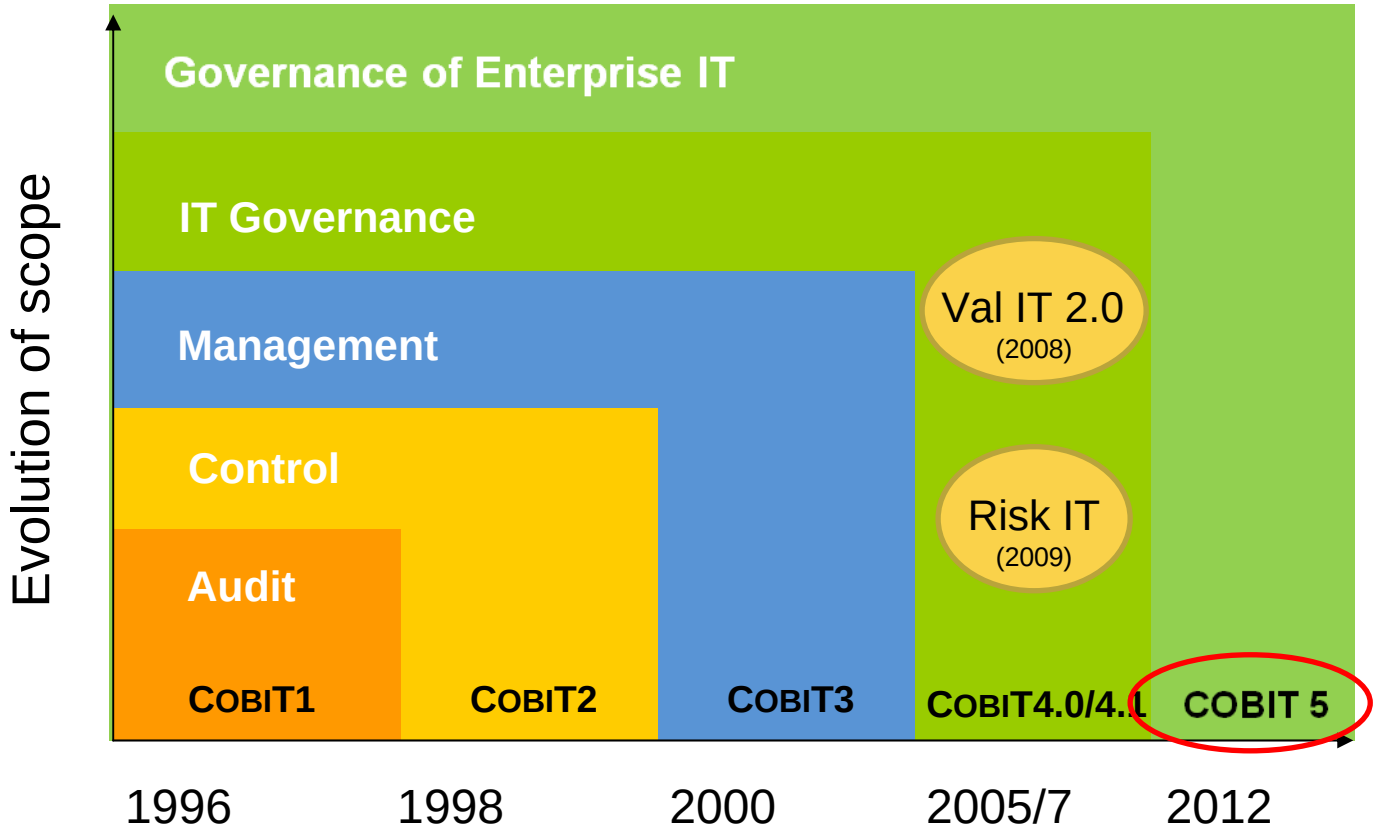
- Risk assessment
  - Identify risk
  - Measure exposures
  - Determine whether controls are in place and effective
  - Specify threats to survival
  - Consider cost of mitigating risks
- Internal control (COSO control model)
- E-assurance services
  - Agreed-upon criteria for measuring assertion
  - Improvement in IT controls (firewalls, routers, 3rd party certification, digital signature, public-key encryption
- Internal and external assurance
  - 5 Objectives: Availability, Capability, Functionability, Protectability and Accountability

1c. Control Objectives for Information and Related Technology (CobiT)

History

- Launched in 1994
- 1st/2nd Edition — 1996/1998
  - CobiT "IT Governance" framework defined
  - Control Objectives & Audit Guidelines developed
  - by using international standards, best practices, and controls & security research
- 3rd Edition — Jul-2000
  - CobiT framework revised and enhanced
  - Management Guidelines developed
  - Maturity Model added (KGIs, KPIs, CSFs)
- 4th Edition — Web Edition (Oct 1, 2003)
- 4.1th Edition — Include Application control
- 5th Edition – coming soon. Schedule to release in 2012, COBIT 5 will consolidate and integrate the COBIT 4.1, Val IT 2.0 and Risk IT frameworks and also draw significantly from the Business Model for Information Security (BMIS) and ITAF.

By ITG- IT Governance Institute

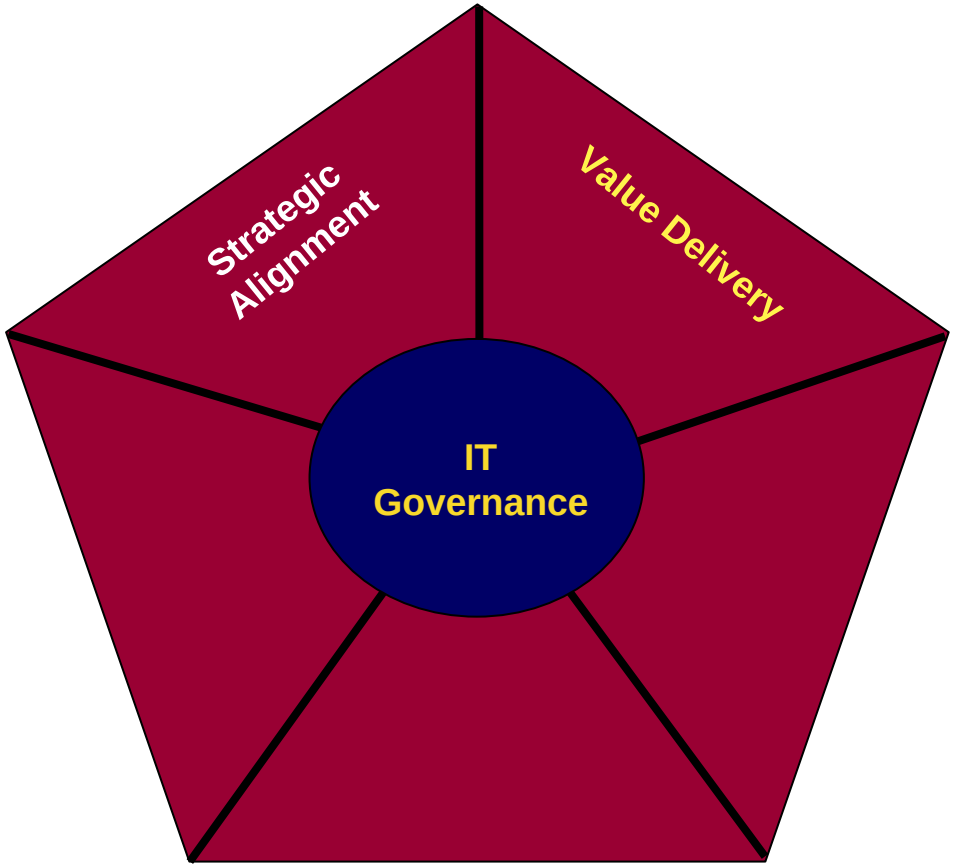


An business framework from ISACA, at www.isaca.org/cobit

Benefits of implementing COBIT as a governance framework over IT

- Better alignment, based on a business focus
- A view, understandable to management, of what IT does
- Clear ownership and responsibilities, based on process orientation
- General acceptability with third parties and regulators
- Shared understanding amongst all stakeholders, based on a common language
- Fulfillment of the COSO requirements for the IT control environment
- Characteristics: Business-focused, Process-oriented, Controls-based, and Measurement-driven

IT Governance Focus Areas



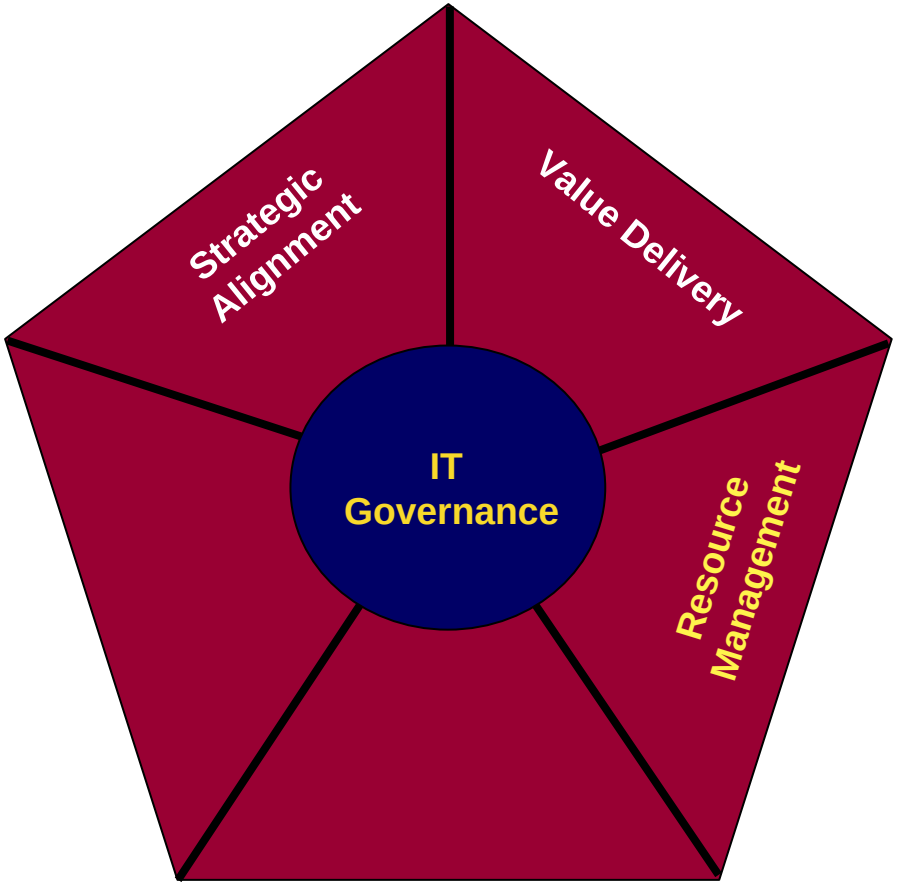
Strategic Alignment

- Linking business and IT plan
- Defining, maintaining and validating the IT value proposition
- Aligning IT operations with the enterprise operations
- Adding value and competitive positioning to the enterprise's products and services
- Containing costs while improving administrative efficiency and managerial effectiveness

Value Delivery

- Executing the value proposition throughout the delivery cycle
- Ensuring that IT delivers the promised benefits against the strategy
- Concentrating on optimizing expenses and proving the value of IT
- Controlling projects and operational processes with practices that increase the probability of success (quality, risk, time, budget, cost, etc.).

IT Governance Focus Areas

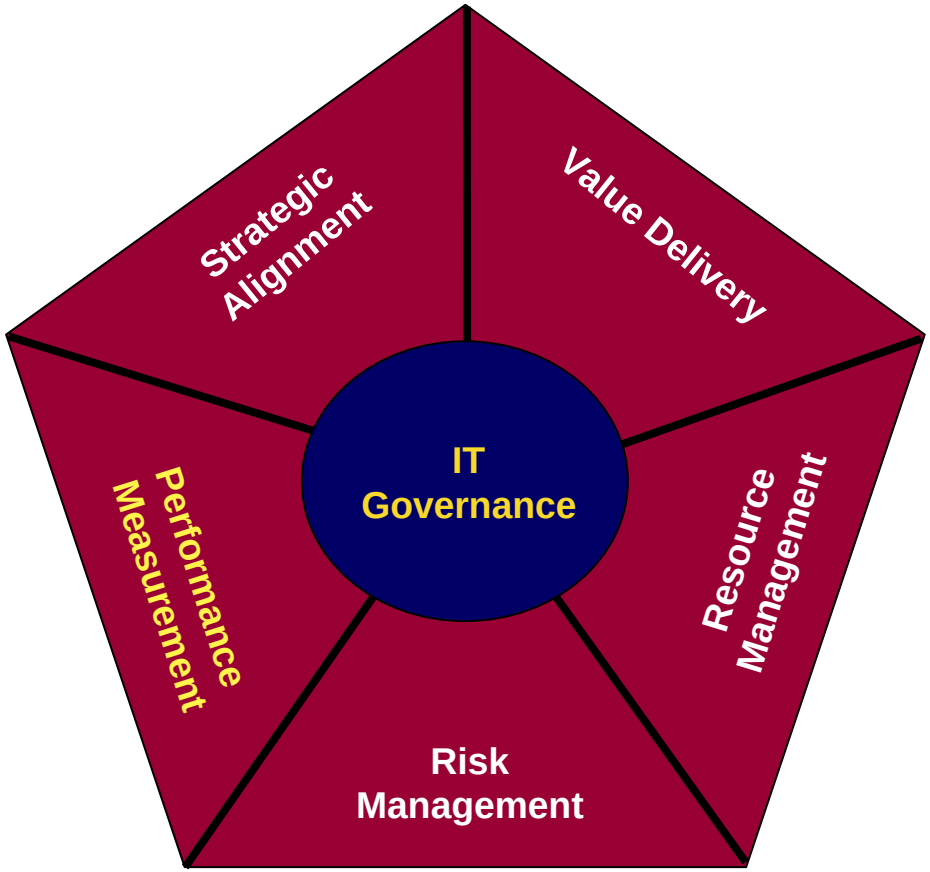


Resource Management

- Optimal investment, use and allocation of IT resources and capabilities (people, applications, technology, facilities, data) in servicing the needs of the enterprise
- Maximizing the efficiency of these assets and optimizing their costs
- Optimizing knowledge and the IT infrastructure and on where and how to outsource

75% of respondents have implemented, are considering implementing or are in the process of implementing this phase of IT governance.

IT Governance Focus Areas



Risk Management

- Requires risk awareness of senior corporate officers, a clear understanding of the enterprise's appetite for risk and transparency about the significant risks to the enterprise
- Embeds risk management responsibilities in the operation of the enterprise
- Addresses the safeguarding of IT assets, disaster recovery and continuity of operations

Performance Measurement

- Tracking project delivery and monitoring IT services
- Using balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting
- Measuring those relationships and knowledge-based assets necessary to compete in the information age: customer focus, process efficiency and the ability to learn and grow

คุณลักษณะสารสนเทศที่ดี

ความต้องการบรรลุวัตถุประสงค์ทางธุรกิจที่เกี่ยวข้องกับสารสนเทศจำเป็นต้องมี

คุณสมบัติของสารสนเทศที่ดีแบ่งเป็น 3 ด้าน:

ความต้องการด้านคุณภาพ (Quality Requirement)	-คุณภาพ - ต้นทุน - การส่งมอบ
ความต้องการด้านความไว้วางใจ (Fiduciary Requirement)	- การมีประสิทธิภาพและประสิทธิผลในการดำเนินงาน - ความเชื่อถือได้ของข้อมูล - การปฏิบัติตามกฎหมายและข้อบังคับต่างๆ
ความต้องการด้านการรักษาความปลอดภัย (Security Requirement)	- การรักษาความลับของข้อมูล - ความครบถ้วนถูกต้อง - สภาพพร้อมใช้งาน

What is GTAG?

GTAG - **Global Technology Audit Guide**

Started in 2005, IIA replaced PA on IT topics

- To provide easy-to-understand information technology audit guides to Chief Audit Executives, Audit Committees and Executive Management
- To provide a mechanism to quickly address new IT Issues
- To produce technical audit guides on a global scale

1d. Global Technology Audit Guide (GTAG)

16 GTAGs

- 1: IT Controls , 2005 (3 families of controls)
- 2: Change and Patch Management Controls, 2005
- 3: Continuous Auditing, 2005
- 4: Management of IT Auditing, 2006
- 5: Managing and Auditing Privacy Risks, 2006
- 6: Managing and Auditing IT Vulnerabilities, 2006
- 7: Information Technology Outsourcing, 2007
- 8: Auditing Application Controls, 2007

1d. Global Technology Audit Guide (GTAG)

16 GTAGs

- 9: Identity and Access Management, 2007
- 10: Business Continuity Management, 2008
- 11: Developing the IT Audit Plan, 2008
- 12: Auditing IT Projects, 2009
- 13:Fraud Prevention and Detection in an Automated World, 2009
- 14: Auditing User-developed Applications, 2009
- 15: Information Security Governance, 2009
- 16. Data Analysis Technologies, 2011

2. Aspects of Automated Information processing

- Characteristics
- Classification of controls
- Functional areas of IT operations
- Responsibilities of IT personnel
- Data center operations

2. Aspects of Automated Information processing

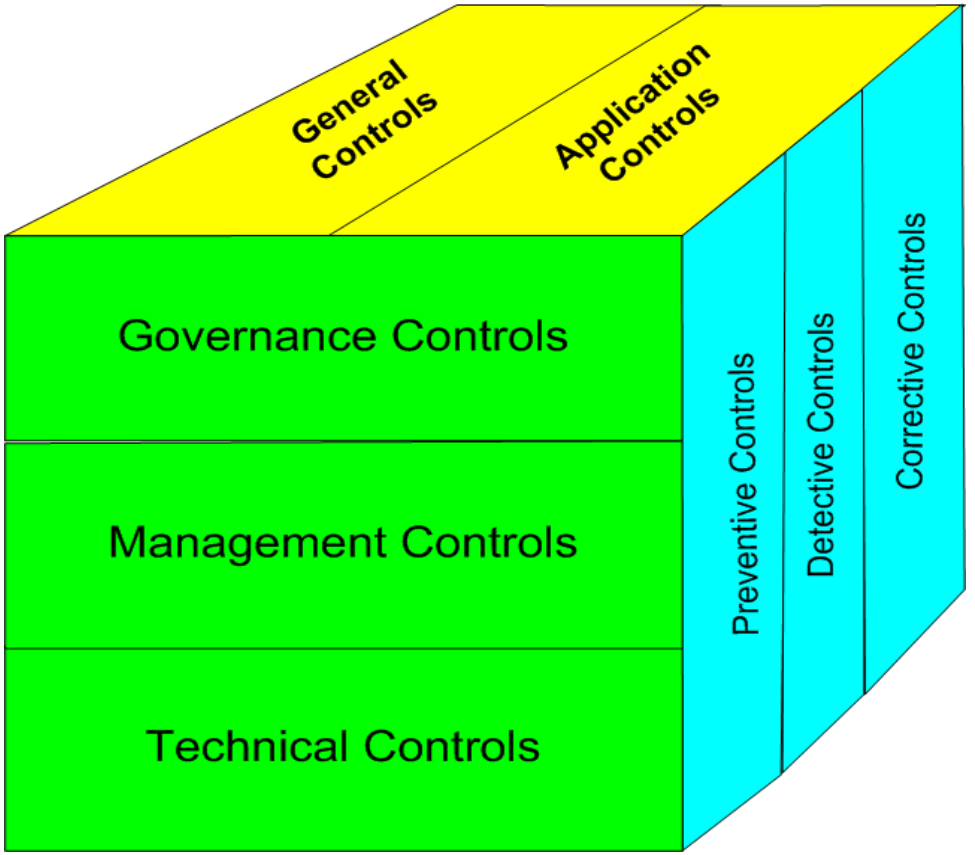
Characteristics:

These effects flow from the characteristics that distinguish computer-based from manual processing:

- Transaction trails,>depend on transaction mode
- Uniform processing of transactions,virtually eliminate clerical error but may have systematic error
- Segregation of functions,incl. dual control (4 eyes) principle
- Potential for efforts and fraud,>STP-Straight-Through-Processing
- Potential for increased management supervision>with analytical tool can enhance internal controls
- Initiation or subsequent execution of transactions by computer>paperless
- Dependence of controls in order areas on controls over computer processing>pervasive issues

Understanding Controls

- Classification
  - General Controls
  - Application Controls
- Classification
  - Preventative
  - Detective
  - Corrective
- Classification
  - Governance controls
  - Management controls
  - Technical controls



Control families by GTAG

Key Controls - General Category

- **Preventive** Controls (Procedures, policies, standards, documentation, continuous audit software)
- **Detective** Controls (logs, reports, CCTV)
- **Corrective** Controls (error corrections, discharge of personnel, change management procedures)

>>>Manual V.S. Automated>>>

2. Aspects of Automated Information processing

Classification of controls:

The broad categories are General controls or Application controls.

- General controls:
  - The plan of organization and operation of the computer activity,
  - The procedures for documenting, reviewing, testing, and approving systems or programs and changes in them,
  - Controls built into the equipment by the manufacturer (hardware controls),incl. Parity checks, echo checks, read-after-write checks to assure data integrity
  - Controls over access to equipment and data files,
  - Other data and procedural controls affecting overall computer operations.

2. Aspects of Automated Information processing

Classification of controls: (cont.)

Application controls: preventive, corrective and detective control

- Input controls
- Processing controls
- Output controls

การควบคุม Batch

- การควบคุม Batch เพื่อให้แน่ใจว่า
  - ทุกเอกสารใน Batch ได้มีการประมวลผล
  - ไม่มีเอกสารใดที่ประมวลผลมากกว่า 1 ครั้ง
  - มีร่องรอยการตรวจสอบ (Audit Trail) ตลอดการทำงาน ตั้งแต่ข้อมูลนำเข้า การประมวลผล จนถึงข้อมูลส่งออก
- การควบคุม Batch ไม่ใช่เป็นเพียงการควบคุมข้อมูลนำเข้าเท่านั้น แต่ยังเป็นการควบคุมข้อมูลจนกระทั่งประมวลผลด้วย

การควบคุม Batch (ต่อ)

- มีเอกสารใบส่ง Batch จากผู้ใช้ฝ่ายต่าง ๆ ให้หน่วยงานคีย์ข้อมูล ซึ่งเรียกว่า “Batch transmittal sheet” ซึ่งประกอบด้วย
  - เลขที่ Batch ในแบบ Running number
  - วันที่ Batch
  - เลขที่รหัสรายการ
  - จำนวนของเอกสารใน Batch (Record counts)
  - ยอดรวมจำนวนตัวเลขที่เป็นตัวเงิน (Amount control total or Financial totals)
  - ยอดรวมจำนวนตัวเลขที่ไม่ใช่ตัวเงิน (Hash totals)

การควบคุมความถูกต้อง

- การควบคุมความถูกต้องของข้อมูลนำเข้ามี 3 ระดับคือ
    1. การควบคุมระดับ Field
    2. การควบคุมระดับ Record
    3. การควบคุมระดับ File

การควบคุมระดับ **field**

- การทำงานของโปรแกรมที่ตรวจสอบความถูกต้องของข้อมูลนำเข้าใน field ต่าง ๆ เช่น การตรวจสอบต่อไปนี้:
    - Validity check
    - Filed check หรือ Type check
    - Limit check
    - Range check
    - Self-checking digits for primary key/index (detect manual error but can not protect frauds)

Validity Check

เป็นการควบคุมโดยใช้โปรแกรมตรวจสอบข้อมูลที่นำเข้าในรูปรหัส หรือตัวอักษรย่อ หรือ คำต่าง ๆ ว่ามีอยู่จริงในระบบ ซึ่งได้รับการบันทึกเก็บไว้ในระบบงานคอมพิวเตอร์ ให้เป็นรหัสที่ใช้ทำรายการต่างๆกับระบบงานนั้นได้ เช่น รหัสลูกค้า

Field Check

เป็นการควบคุมโดยใช้โปรแกรมตรวจสอบฟิลด์ (Field) ว่าข้อมูลที่นำเข้าอยู่ในรูปแบบที่ถูกต้องเหมาะสมหรือไม่ เช่น ฟิลด์จำนวนเงิน ข้อมูลที่นำเข้าต้องเป็นตัวเลขเท่านั้น

Limit Check

เป็นการควบคุมโดยโปรแกรมใช้ค่าของข้อมูลนำเข้า หรือค่าของข้อมูลที่ได้จากการคำนวณโดยโปรแกรม เปรียบเทียบกับหลักเกณฑ์หรือข้อจำกัดเกี่ยวกับค่าของข้อมูลที่กำหนดไว้ โดยหลักเกณฑ์หรือข้อจำกัดค่าสูงสุดที่กำหนดไว้ เช่น การตรวจว่าค่าขายเชื่อต้องไม่เกินวงเงินสินเชื่อ ข้อจำกัด คือ จำนวนวงเงินสินเชื่อ ถ้าใส่จำนวนเงินเกินระบบจะส่งข้อความเตือนให้

Range Check

เป็นการควบคุมโดยโปรแกรมใช้ค่าของข้อมูลนำเข้า เปรียบเทียบกับช่วงของค่าที่ควรจะเป็นที่ได้กำหนดไว้ล่วงหน้า เช่น อายุของพนักงานควรอยู่ในช่วง 20-60 ปี

การควบคุมระดับ Record

- การทำงานของโปรแกรมที่ตรวจสอบความถูกต้องของข้อมูลนำเข้าใน Field มากกว่า 1 Field โดยลักษณะการตรวจสอบ:
  - การตรวจสอบความสมเหตุสมผลของข้อมูล (Reasonableness checks)
  - การตรวจสอบเครื่องหมายของข้อมูลในระดับ Record (Sign checks)
  - การตรวจสอบความถูกต้องของการเรียงลำดับข้อมูลใน Transaction file กับ Master file (Sequence checks)

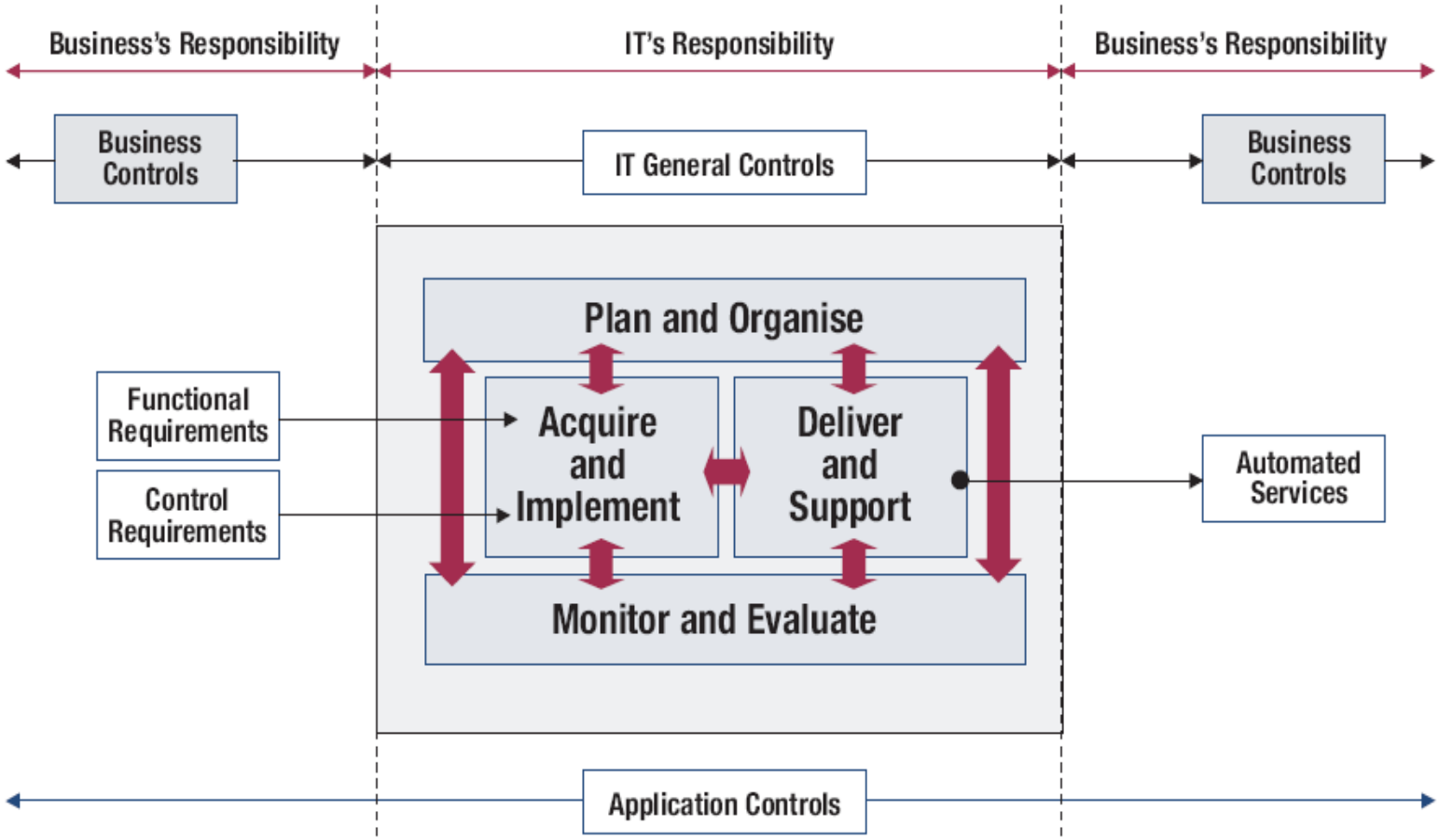
การควบคุมระดับ File

เพื่อให้มั่นใจว่าได้มีการนำ File ที่ถูกต้องมาทำการประมวลผล:

- การตรวจสอบฉลากภายใน (Internal label checks) ซึ่งต้องอ่านด้วยเครื่อง ว่า เป็นแฟ้มข้อมูลเวอร์ชั่นที่ถูกต้อง (Version checks) หรือ
- การตรวจสอบวันหมดอายุของแฟ้มข้อมูล (Expiration date check)

Output >>Detective control>>User should be able to determine when output is incomplete or not reasonable, particularly when user prepare the input (Quality Assurance)

Boundaries of Business, IT General and Application Controls



Source: COBIT 4.1 Research

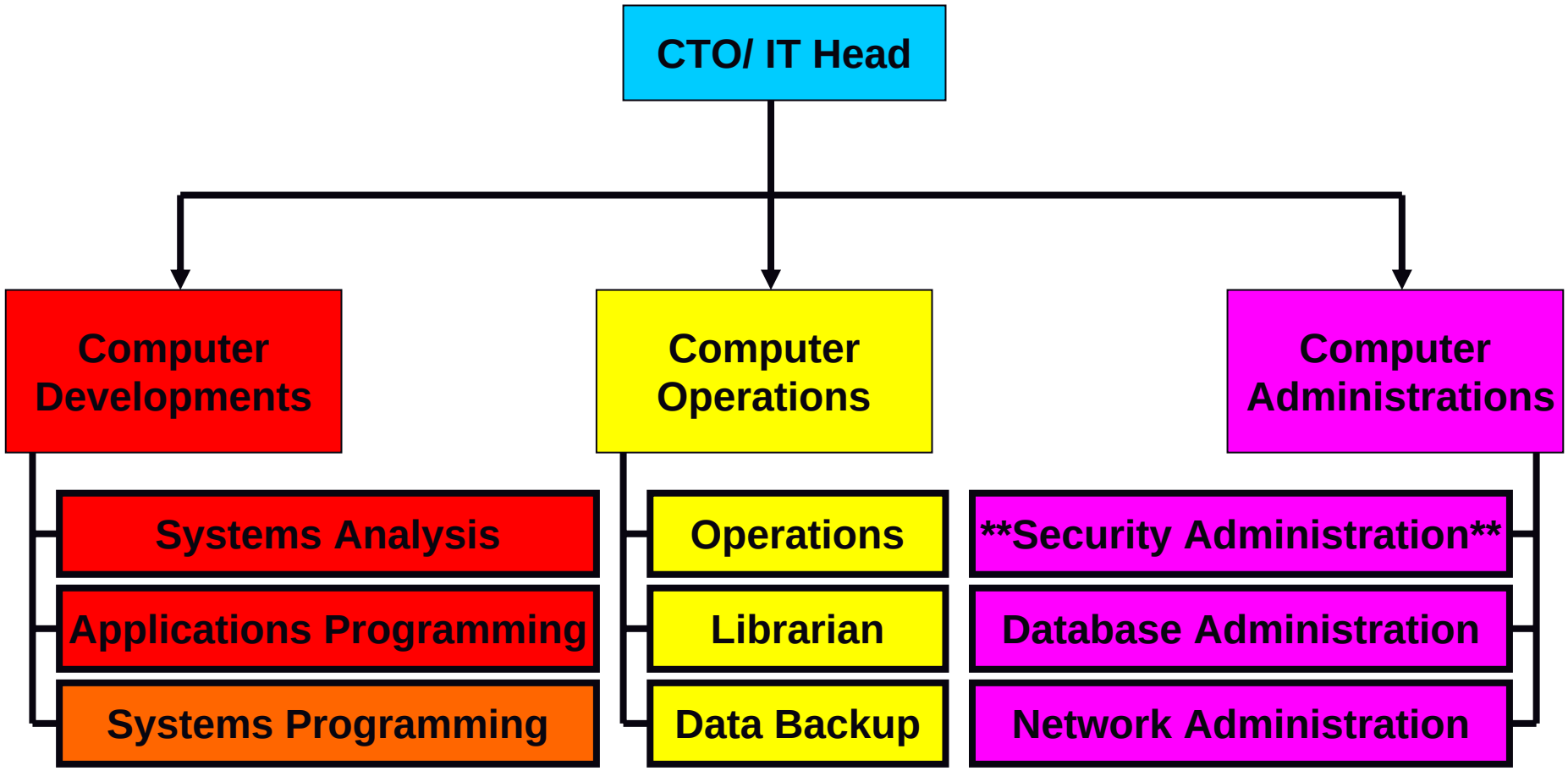
2. Aspects of Automated Information processing

Functional areas of IT operations:

- Transaction trails are depend on transaction modes.
- Uniform processing virtually eliminates clerical error >>constant output
- Proper segregation of duties (SOD) should be included within the IT environment.
- The responsibilities of systems analysts, programmers, operations, file librarians, the control group, and others should be assigned to different individuals, and proper supervision should be provided.
- Potential of errors and fraud>>access control, identification and authentication>>must decrease of human involve in handling transactions.

IT Organization Control

IT Steering Committee



>>>>End-Users/System owner

2. Aspects of Automated Information processing

Data center operations:

- Batch mode, Service bureaus for subscribers
- Online mode, real-time – direct communication with computers
  - OLTP-Online Transaction Processing
- Timesharing,many users can access through the remote terminals>CPU devotes a fixed time for each user program (time slice)
- Totally centralized systems, development and processing are done at one data center>economies of scale/strengthening of control
- Totally decentralized systems,each has own development and smaller computers>local needs
- Downsizing, moving to mid-range or networked computers (using less expensive system)>increased complexity>less reliable
- Distributed data processing. with fail-soft protection>processing needs are examined in their totality>some parts best for locally, some possibly centralized>increased interdependence/cooperative processing>two-phase commit disk-writing protocol

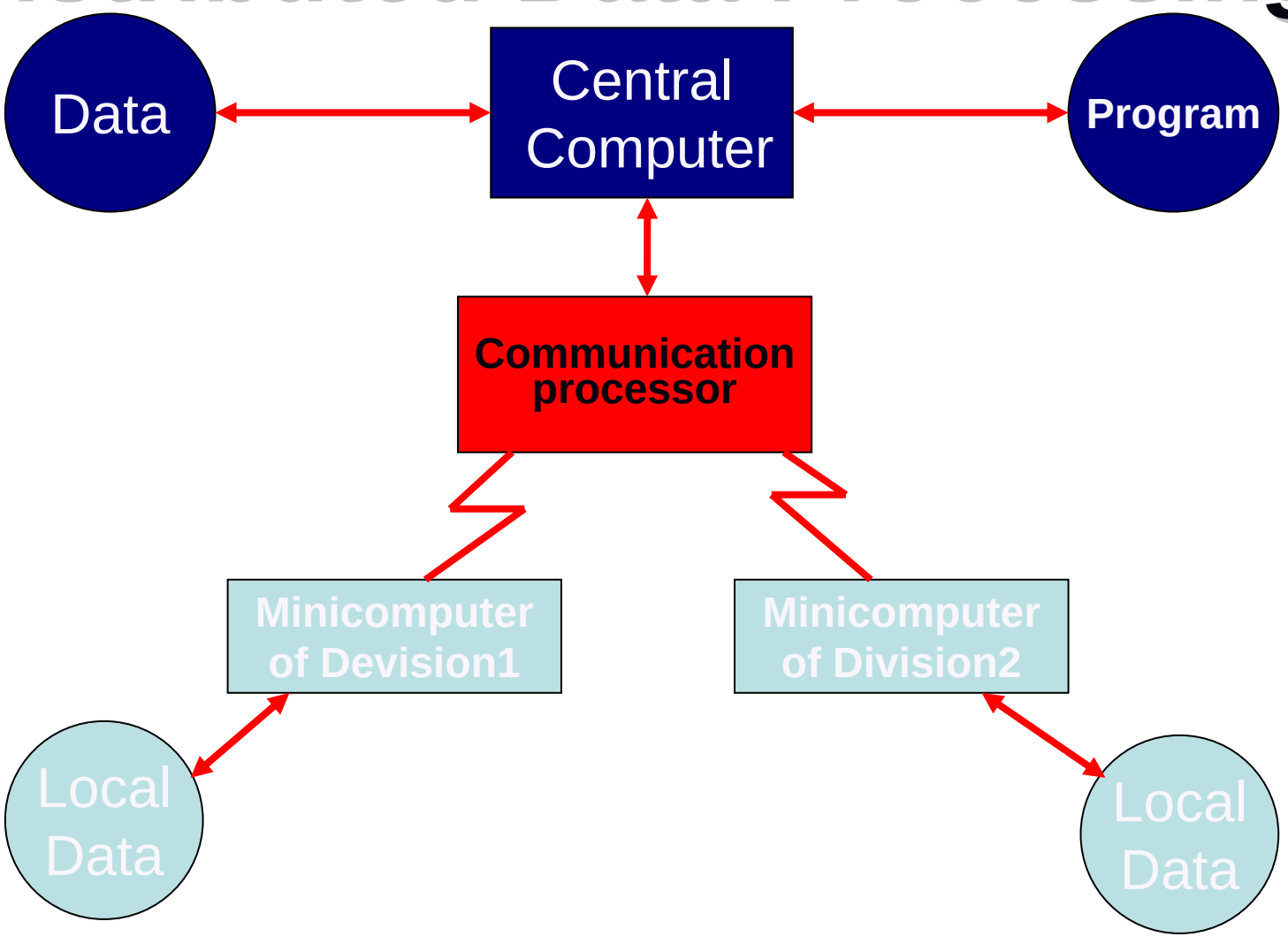
Distributed Data Processing

- Decentralizing Computer Functions & Power.
- Easier Access to Data/Program.
- Client/Server Architecture.
  - –Client : Desktop PC/Workstation.
  - –Server : Minicomputer/Mainframe.

➔ ***Audit Implications;***

- ***Limit access to system.***
- ***Transaction Completeness between Client&Server.***

Distributed Data Processing



3. Data Communications & Networks

Teleprocessing:

- Computer processing via remote terminals
- Require communication software that performs functions
  - Receives input, perform processing, passes the output to the user,
  - Identifies and corrects errors and provide security,
  - Maintains a log,
  - Manage buffer (special storage areas) that hold input before processing,
  - Manages the sequencing and proper routing of messages.

3. Data Communications & Networks

Teleprocessing: (cont.)

- Protocol
  - Set of rules for message transmission,
  - Each device should adhere to the same protocol.
- Snapshot
  - Copies of files are created at time intervals,
  - A risk → could be obsolete by the time they are downloaded.

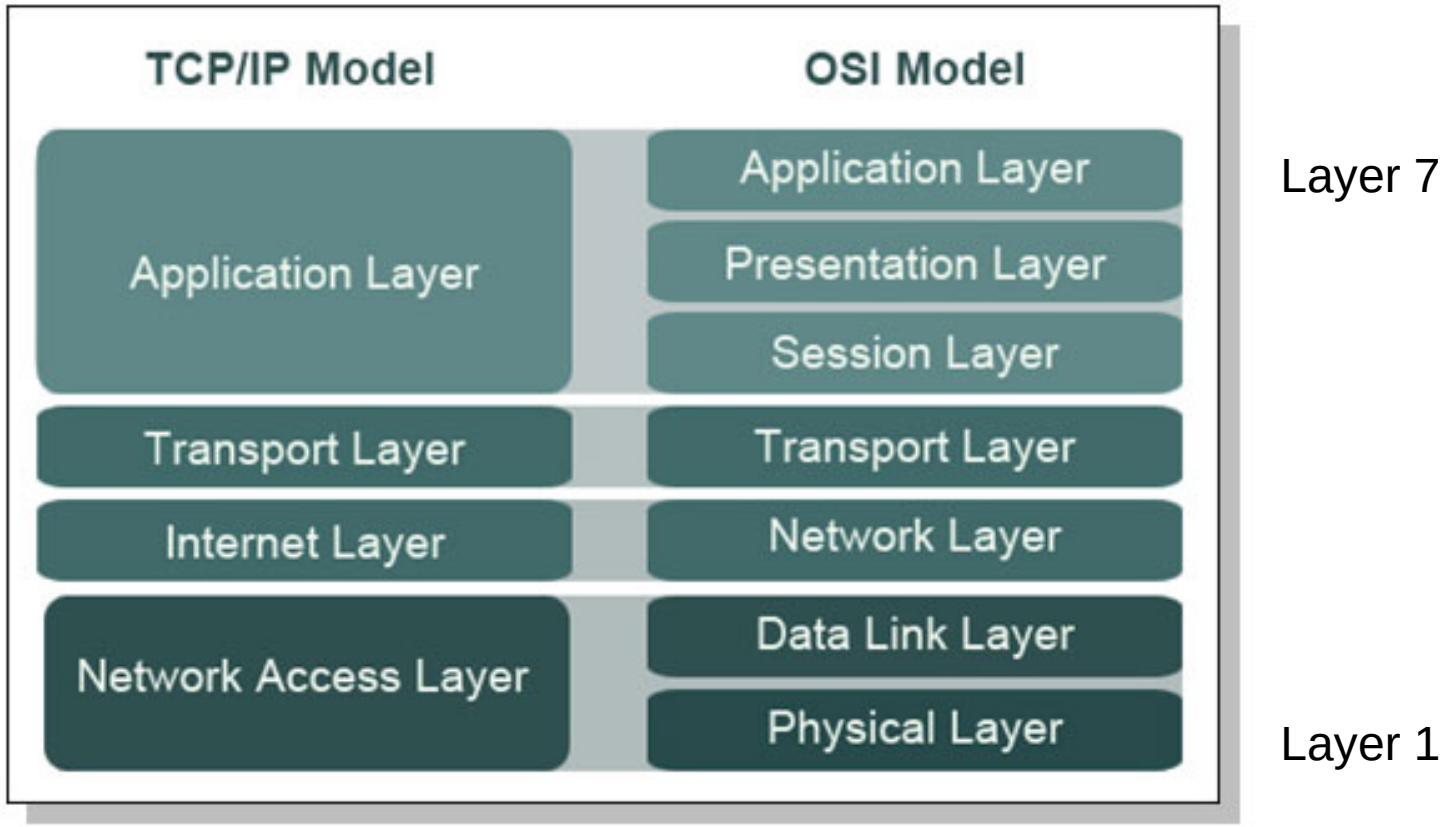
Real-Time Systems

- **Immediate responses to an inquiry.**
- **Benefits;**
  - **Reduction in paper works.**
  - **Faster turnaround times for transaction.**
- **Example.**
  - **Just in Time inventory system.**
  - **Automatically ordering the raw material.**
  - **Point of Sales (POS)**

➔ ***Audit Implications;***

- ***No batch-type control.***
- ***Control over access to the system.***
- ***Transactions Authorization control.***
- ***Entity's Controls.***
- ***More continuously audit.***

OSI Model
(Open Systems Interconnection)



Originated by International Org for Standardization (ISO): e.g., write a letter, fold, and place in the custody of postal service.

3. Data Communications & Networks

Open systems

- All operating system can be connected to each other,
- Interfaces are defined by public standard.

Open system interconnect (OSI)

- Has been developed by the International Organization for Standardization,
- 7-Layer Network Reference model that allows different types of computers and networks to communicate. From Lowest (Physical) to highest (Application) layer

Integrated Services Digital Network (ISDN)

- Provide international standards of voice, video, and data communications over the telephone lines.

3. Data Communications & Networks

- Communication devices → to connect computers and remote terminals devices may be used:
  - Front-end processors
  - Multiplexers
  - Modem (modulator-demodulator)
  - Communications channels
  - Network communication devices → hub, switch, bridges, routers

3. Data Communications & Networks

- Front-end processors
  - FEPs are responsible for linking client applications and their associated networks to host computer based applications. The need for these functions is especially important in mission critical transaction environments such as banking, government, point-of-sale, security, and health care applications.
- Multiplexers
  - Be switch devices,
  - Intermix the two-way flow of data so that data may flow over one line (interleaving),
  - Concentrator → programmable device that collects messages until it has enough to be transmitted in a burst of signals.

3. Data Communications & Networks

- Modem → modulator-demodulator
  - Is a hardware device,
  - For sending, convert digital signals → analog signals,
  - For receiving, convert analog signals → digital signals,
  - Bit rate (bits per second) → measurement of the transmission speed.
  - Baud rate → number of signal changes or cycles per period of time. Cannot exceed the bandwidth of the communication channel.

3. Data Communications & Networks

- Communication channels → classified according to their capacity:
  - Narrowband → telegraph lines
  - Voiceband → telegraph lines
  - Broadband
    - Provides multiple paths,
    - Permits simultaneous transmission of different kinds of data,
    - Example is fiber-optic cable, microware circuits, and satellite channels
  - Baseband network → type of LAN

3. Data Communications & Networks

- Network communication devices
  - Hub → is a central connecting device, joins communications lines in a star configuration.
    - Passive hubs → are connecting units,
    - Active hubs → multiport repeaters, regenerate the data bits to maintain a strong signal,
    - Intelligent hubs → provide added functionality e.g. network management, bridging, routing, and switching

3. Data Communications & Networks

- Network communication devices (cont.)
  - Switch
    - Is a connecting device,
    - Each port can give full bandwidth to a single server, client, or hub.
  - Bridges
    - Connect 2 or more LAN segments,
    - Improve network performance by keeping traffic contained within smaller segments

3. Data Communications & Networks

- Network communication devices (cont.)
  - Routers have more intelligence than hubs, bridges, or switches
    - Route data packets from one LAN or WAN to another,
    - Read network address in each transmitted frame and make a decision on how to send it (based on route cost),
    - Also perform the central switching function on the Internet,
    - Example of network address → 190.10.11.1 (IP address).
- Transmission Control Protocol/Internet Protocol (TCP/IP): a routing protocol suite operates on layer 4 and 3 of OSI reference model
- IP addressing: heart of internet routing (numeral 0 – 255)
- Dynamic Host Configuration Protocol (DHCP) allows tremendous flexibilities (enable the constant reuse of IP)

3. Data Communications & Networks

- Wireless
  - Use the electromagnetic spectrum,
  - Microware → use high-frequency radio signals transmitted thought the atmosphere,
  - Satellites → serve as relay points,
  - Mobile data networks → established for two-way data transmission between handheld computers.
  - Wi-Fi (usable area: hotspot) 300 feet around a wireless router.
  - Bluetooth>30 feet (PAN:Personal Area Network)
  - Wimax using microwaves for entire city (old MAN model – 10 miles)
  - RFID: Radio-Frequency Identification uses a combined microchip with antenna to store data for product, pet, vehicle common app> Inventory tracking, lost pet identification, Tollbooth collection

3. Data Communications & Networks

- Transmission modes
  - Asynchronous or start-stop transmission
  - Synchronous transmission
- Transmission circuits
  - Simplex
  - Half-duplex
  - Duplex
- Teleprocessing
  - Functions
  - Protocol
  - Snapshot

3. Data Communications & Networks

- Types of networks
  - Private networks
  - Public-switched networks
  - Value-added networks (VANs), private network with reliable, high-speed and secure transmission
  - Local area network (LAN)
  - Wide area networks (WAN), public or private
  - Internet → network of networks
  - Intranet, Extranet
  - Virtual private network (VPN), relatively inexpensive
  - Private branch exchange (PBX), voice and data traffic
  - Connectivity → Open systems, Open system interconnection (OSI), ISDN.

3. Data Communications & Networks

Private networks:

- Dedicated facilities → satellites, microwave, telephone lines, leased lines, PBX (private branch exchange),
- PBX uses telephone lines, so its data transmission capacity is limited,
- No dial-up access is required.

Public-switched networks:

- Use public telephone lines,
- Most economical, but lower quality, no connection may be available,
- Security measures may be ineffective.

3. Data Communications & Networks

Value-added network (VANs):

- Private network,
- Transmit the data of subscribing entities,
- Provide error detection and correction services, e-mail for EDI, and security for e-mail.
- Data transmission → Packet switching → divides a file into small packages that are sent independently by available communication channels:
  - Frame relay
  - Asynchronous transfer mode (ATM)
  - Internet protocol (IP)

3. Data Communications & Networks

LAN - Local area network:

- Local distributed computer system → single office,
- Computers are linked by cable,
- Require SW and HW (cable, server, gateway, Ethernet, network) to facilitate data communication,
- Channel technology may be:
  - Baseband → allows one path for transmission,
  - Broadband → provides multiple paths.
- Peer-to-peer network → operates without a mainframe or server,
- A LAN may use wireless spread spectrum broadcasting (Wireless LAN),

3. Data Communications & Networks

WAN - Wide area network:

- Provide data communication and file sharing among remote offices,
- Combine dedicated lines,

The Internet → a network of networks:

- Descended from the ARPANet (Advanced Research Projects Agency Network),
- Idea was to have a network that could not be brought down during an enemy attack by bombing a single central location,
- Facilitates inexpensive communication,
- Obtain connections through ISPs (Internet service providers),

3. Data Communications & Networks

The Internet → a network of networks: (cont.)

- Three main parts of the Internet are → servers, clients, TCP/IP protocol,
- Using HTML (hypertext markup language) and HTTP (hypertext transfer protocol) to display rich graphics and streaming audio and video in addition to text.

An Intranet

- Permits sharing of information throughout an organization (internal network),
- Outsiders can be access by providing identification,

3. Data Communications & Networks

An Extranet

- Consists of the linked intranets of 2 or more organizations,
- E.g. supplier and its customers.

Virtual private network (VPN)

- Can securely share information over the Internet,
- Develop secure encryption products that protect data while in transit across the Internet.

3. Data Communications & Networks

- Transmission media
  - Twisted copper wire
  - Coaxial cable
  - Fiber optic cable
  - Wireless ->
    - Pagers
    - Cell phone
    - Mobile data networks
    - Personal communication services (PCS)
    - Personal digital assistant (PDA)

3. Data Communications & Networks

- Transmission modes
  - Asynchronous or start-stop transmission
  - Synchronous transmission
- Transmission circuits
  - Simplex
  - Half-duplex
  - Duplex
- Teleprocessing
  - Functions
  - Protocol
  - Snapshot

3. Data Communications & Networks

- Fiber optic cable
  - Uses light impulses that travel through clear flexible tubing half the size of a human hair,
  - Not subject to electrical interference,
  - Highly reliable, extremely flexible, and fast data transmission,
  - Strong signal across long distances,
  - Cannot be wiretapped,
  - More expensive.
  - Does not tend to weaken (attenuate)

3. Data Communications & Networks

- Network configurations (Topologies)
  - Point-to-point
  - Multidrop (bus) → the most successful protocol, Ethernet (polite conversation- listen for free traffic and then send its message)
  - Ring networks (Ring)→ token ring network, higher speed→ IBM, attach the message to the free “Token”
  - Completely connected networks
  - Star networks

3. Data Communications & Networks

Point-to-point

- Provide a separate, direct link between each remote terminal and the CPU.

Multidrop (bus)

- Provide links for each terminal to a single communication line connect to the CPU,
- One terminal may send or receive messages at one time,
- Ethernet is an example.

3. Data Communications & Networks

Ring networks

- Have no central computer,
- Each computer can communicate with every other computers,
- Data pass from one device to another in one direct as a close loop.
- Example is token ring network (invented by IBM)

Completely connected networks

- Have direct link among all computer locations.

Star networks

- Permit each remote computer a direct link to the central location but not to other remote computers.

3. Data Communications & Networks

- Basic Architectures for Desktop Computing
  - Client-server model
    - User interaction
    - Server
    - Security
    - Secure Electronic Transaction (SET)
    - Digital certificates
  - Terminal
    - Dumb terminal → Text display
    - Smart terminal → GUI

4. EFT, E-Commerce and EDI

- Electronic funds transfer (EFT)
- Implications for IA
  - Elimination of paper documents
  - Existence of evidence
  - Evaluation of digital signatures
  - Consideration of other subsystems
- EFT for direct deposit and check collection to reduce enormous volume of paper, can computerised>transaction costs are lower than manual system

การชำระเงินทางอิเล็กทรอนิกส์

ลักษณะสำคัญ

- โอนสิทธิการถือครองเงิน หรือโอนสิทธิการถอนเงิน หรือหักเงินจากบัญชีของผู้ใช้บริการ
- ใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน
- ผู้ให้บริการเป็น "ตัวกลาง" ในกระบวนการชำระเงินระหว่าง ผู้ซื้อ (ผู้โอน) และผู้ขาย (ผู้รับโอน) หรือ ระหว่างสมาชิกผู้ให้บริการ

E-Commerce

- Using EDI technology
  - B2B,B2C,B2E from technology changes with pervasively impact to business. The dramatic growth of c-Commerce creates significant control and management challenges (audit competency and capacity concern). New Threat vs Opportunity Risk. Critical Risk and Control issues should be raised by Auditor i.e., data/network integrity, security threats and legal concerns.

Electronic Commerce (E-commerce)

- Risk&control issues:
  - Threat event to achieve its objectives and execute strategies
  - Single loss exposure values (make financial impacts)
  - Frequency/probability
  - Uncertainty
  - Safeguards and controls (including cost)
  - Cost/benefit or ROI analysis
  - Critical risk and control, e.g., security threat and technology changes

Electronic Commerce (E-commerce)

- Critical risk and control,
  - Security threat and technology changes
  - Fraud
  - Authentication: 2 factors or multi-factors authentication (knowledge, possession and biometric)

    >>>OTP-One Time Password
  - Corruption of data/business interruptions
  - Management issues, business model, economical review

EDI

- EDI terms and components
  - Standards
  - Conventions
  - Data dictionary
  - Transmission protocols
- Methods of communication among computers
  - Point-to-point
  - Value-added networks (VAN)
  - Internet

EDI

- EDI controls
  - Authorized users access
  - Message authentication
  - Message protection → Encryption, Numerical Sequencing, Nonrepudiation
- Secure Electronic Transaction (SET)
  - SET was intended to become the de facto standard of payment method on the Internet between the merchants, the buyers, and the credit-card companies. Despite heavy publicity, it failed to win market share. SET incorporates the following features:Confidentiality, Integrity, Cardholder account authentication and Merchant authentication
- Electronic Mail (E-mail)
  - Risks
  - Acceptable use policy
- Publicly available systems

1. Which of the following statements accurately describes the impact that Automation has on the controls normally present in a manual system

   a. Transaction trails are more extensive in a computer-based system that in a manual system because there is always a one-for-one correspondence between data entry and output.
   b. Responsibility for custody of information assets is more concentrated In user departments in a computer-based system that it is in a manual system.
   c. Controls must be more explicit in a computer-based system because many processing point that present opportunities for human judgment in a manual system are eliminated.
   d. The quality of documentation becomes less critical in a computer-based system that it is in a manual system because data records are stored in machine-readable files.

2. What type of information system uses communications capabilities to make needed data and computing capability available to end users at separate locations
    a. Distributed processing system.
    b. Time-sharing system.
    c. Online processing system.
    d. Personal computing system.

3. Even though an organization is committed to using its mainframe for its manufacturing plant operations, it has been looking ways to downsize other applications. The purpose of downsizing is to
    a. Improve reliability.
    b. Improve security.
    c. Reduce complexity.
    d. Decrease costs.

4. A benefit of using computer-aided software engineering (CASE) technology is that it can ensure that
    a. No obsolete data fields occur in files.
    b. Users become committed to new systems.
    c. All programs are optimized for efficiency.
    d. Data integrity rules are applied consistently.

5. A systems development approach used to quickly produce a model of user interfaces, user interactions with the system, and process logic is called
    a. Neural networking.
    b. Prototyping.
    c. Reengineering.
    d. Application generation.

6. An MIS manager has only enough resources to install either a new payroll system or a new data security system, but not both. Which of the following actions is most appropriate?
   a. Giving priority to the security system.
   b. Leaving the decision to the MIS manager.
   c. Increasing MIS staff output in order for both systems to be installed.
   d. Having the information systems steering committee set the priority.

7. A mail-order retailer of low-cost novelty items is receiving an increasing number of complaints from customers about the wrong merchandise being shipped. The order code for items has the format *wwxxyyzz*. The major category is *ww, xx* is the minor category, *yy* identifies the item, and *zz* identifies the catalog. In many cases, the wrong merchandise was sent because adjacent characters in the order code has been transposed. The best control for decreasing the number of orders with the wrong merchandise is to

   a. Require customers to specify the name for each item they order.
   b. Add check-digits to the order codes and verify them for each order.
   c. Separate the parts of the order codes with hyphens to make the characters easier to read.
   d. Use a master file reference for all order codes to verify the existence of items.

8. Which of the following computerized control procedures would be most effective in ensuring that data uploaded from personal computers to a mainframe are complete and that no additional data are added?

   a. Self-checking digits to ensure that only authorized part numbers are added to the database.

   b. Batch control totals, including control totals and hash totals.

   c. Passwords that effectively limit access to only those authorized to upload the data to the mainframe computer.

   d. Field-level edit controls that test each field for alphanumerical integrity.

9. Detecting errors in real memory is a function of

   a. Memory protection
   b. Parity checking.
   c. Validity checking.
   d. Rang checking.

10. After using the mainframe report writer for several months, the marketing analysts gained confidence in using it, but the marketing department manager became concerned. Whenever analysts revised reports they had written earlier, the coding errors kept reappearing in their command sequences. The manager was sure that all the analysts knew what the errors were and how to avoid them. The most likely cause of the reappearance of the same coding errors is inadequate
    a. Backups.
    b. Change control.
    c. Access control.
    d. Testing.

11. Traditional information systems development procedures that ensure proper consideration of controls may not be followed by users developing end-user computing (EUC) applications. Which of the following is a prevalent risk in the development of EUC applications?

    a. Management decision making may be impaired due to diminished responsiveness to management's requests for computerized information.

    b. Management may be less capable of reacting quickly to competitive pressures due to increased application development time.

    c. Management may place the same degree of reliance on reports produced by EUC applications as it does on reports produced under traditional systems development procedures.

    d. Management may incur increased application development and maintenance costs for EUC systems, compared with traditional (mainframe) systems.

12. The practice of maintaining a test program library separate from the production program library is an example of
    a. An organizational control
    b. Physical security
    c. An input control
    d. A concurrency control

13. Regardless of the language in which an application program is written, its execution by a computer requires that primary memory contain
    a. A utility program.
    b. An operating system.
    c. Compiler.
    d. Assembly.

14. Computers containing more than one central processing unit (CPU) are increasingly common. This feature enables a computer to execute multiple instruction from multiple programs simultaneously. This process is
    a. Time sharing.
    b. Multitasking.
    c. Multiprocessing
    d. Batch processing

15. In the accounting department of a large organization, the most likely use of a CD-ROM would be to
    a. Create permanent audit trails of EDI transaction.
    b. Store images of documents received in the department.
    c. Record the front and back of checks returned from the bank.
    d. Provide a way to look up accounting standards and guidelines

16. The process of monitoring, evaluating, and modifying a system as needed referred to as systems
    a. Analysis.
    b. Feasibility study.
    c. Maintenance.
    d. Implementation.

17. When assessing application controls, which one of the following input controls or edit checks is most customer account number field?
    a. Limit check.
    b. Validity check.
    c. Control total.
    d. Hash total.

18. The online data entry control called pre-formatting is
    a. A program initiated prior to regular input to discover errors in data before entry so that the errors can be corrected.
    b. A check to determine if all data items for a transaction have been entered by the terminal operator.
    c. A series of requests for required input data that requires an acceptable response to each request before a subsequent request is made.
    d. The display of a document with blanks for data items to be entered by the terminal operator.

19. Which one of the following input controls or edit checks would catch certain types of errors within the payment amount field of a transaction?

a. Record count.

b. Echo check.

c. Check digit.

d Limit check.

20. The key verification process associated with keying computer records for input to a computer system is

    a. Effectively used to detect the erroneous recording of data on source documents.

    b. Inexpensive and therefore widely used.

    c. Used to detect errors introduced by the keying process.

    d. Ordinarily used with a computer program written to check the data.

Manit Panichakul, BA (Stat.), MBA, CIA, CISA, CISM, CRISC

ผู้อำนวยการอาวุโส หัวหน้าสายงานตรวจสอบเทคโนโลยีสารสนเทศและปฏิบัติการ ธนาคารยูโอบี จก. (มหาชน)

ประธานชมรมผู้ตรวจสอบภายในธนาคารและสถาบันการเงิน

กรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการพัฒนาการตรวจสอบภายในภาคราชการ (ปี 2548 - ปัจจุบัน)
กรรมการวิชาการและวิจัย สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย

อดีตกรรมการสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย

(IIAT ปี 2548 **-** 2552)

อดีตนายกสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ ภาคพื้นกรุงเทพฯ (ISACA ปี 2537 – 2539)

E-mail : Manit.Pan@uob.co.th **Tel.:** 02-620-2170