Certified Internal Auditor Part II
Information Technology II

Phises Boonraksa

11 June 2011

CCSA ,CISA, CISM, CISSP, ITIL Foundation

Agenda:

- Data Communications and Networks
- Voice Communications
- System Security
- Contingency Planning
- Databases
- Functional Areas of IT Operations
- Web Infrastructure
- Software Licensing

1. Data Communications & Networks:

1.1 Types of Networks:

Definition:

- A network consists of multiple connected computers at multiple locations.
- Computer that are electronically linked permit an organization to assemble and share transaction and other information among different physical locations.

1. Data Communications & Networks:

1.1 Types of Networks:

3 types of networks:

- LAN → Local area network
- MAN → Metropolitan area network
- WAN → Wide area network

Local Area Network (LAN):

- LAN connects devices within a single office or home or among buildings in an office park.
- LAN is owned entirely by a single organization.
- LAN is the network familiar to office workers all over the world.
- In its simplest conception, it can consist of a few desktop computers and a printer.

1. Data Communications & Networks:

1.1 Types of Networks:

Metropolitan Area Network (MAN):

- MAN connects devices across an urban area, for instance, 2 or more office parks.
- This conception had limited success as a wire-based network but may make a comeback using microwaves.

Wide Area Network (WAN):

- WAN consists of a conglomerate of LANs over widely separated locations.
- The key aspect here is that a WAN can be either publicly or private owned.
- WANs come in many configurations. In its simplest conception, it can consist of a lone desktop computer.

1. Data Communications & Networks:

1.1 Types of Networks:

WAN – Publicly Owned:

- Such as public telephone system and the Internet are available to any user with a compatible device.
- These network are paid for by means other than individually imposed user fees.
  - Use public telephone lines to carry data.
  - This arrangement is economical.
  - The quality of data transmission cannot be guaranteed and security is highly questionable.

1. Data Communications & Networks:

1.1 Types of Networks:

WAN – Privately Owned:

- Value-added networks (VANs).
  - Private networks that provide their customers with reliable, high-speed secure transmission of data.
  - To compete with the Internet, these third-party networks add value by providing their customers with error detection and correction services, electronic mailbox facilities for EDI purposes, EDI translation, and security for email and data transmission.

1. Data Communications & Networks:

1.1 Types of Networks:

WAN – Privately Owned:

- Virtual private network (VPNs).
  - Emerged as a relatively inexpensive way to solve the problem of the high cost of leased lines.
  - A company connects each office or LAN to a local ISP and routes data through the shared, low-cost public Internet.
  - The success of VPNs depends on the development of secure encryption products that protect data while in transit.
- Private branch exchange (PBX).
  - A specialized computer used to handle both voice and data traffic.
  - Can switch digital data among computers and office equipment, e.g., printers, copiers, and fax machines.
  - Use telephone lines, so its data transmission capacity is limited.

1. Data Communications & Networks:

Question:

1. Large organizations often have their own telecommunications networks for transmitting and receiving voice, data, and images. Very small organizations, however, are unlikely to be able to make the investment required for their own networks and are more likely to use
   A. Public switched lines.
   B. Fast-packet switches.
   C. Standard electronic mail systems.
   D. A WAN.

1. Data Communications & Networks:

Question:

2. Which of the following represents the greatest exposure to the integrity of electronic funds transfer data transmitted from a remote terminal?
   A. Poor physical access controls over the data center.
   B. Network viruses.
   C. Poor system documentation.
   D. Leased telephone circuits.

1. Data Communications & Networks:

Question:

3. Which of the following is considered to be a server in a local area network (LAN)
   A. The cabling that physically interconnects the nodes of the LAN.
   B. A device that stores program and data files for users of the LAN.
   C. A device that connects the LAN to other networks.
   D. A workstation that is dedicated to a single user on the LAN.

2. Voice Communications:

Voice communications channels:

1. Internet telephony or Voice over IP (VOIP)
   - Transmission of two-way voice communication that uses the Internet for all or part of its path.
   - This can be performed with traditional telephone devices; desktop computers equipped with sound card, microphone, and speakers; or terminals dedicated to this function.
2. Voice recognition:
   - Another alternative to keyboard input (an input devices).
   - Functions by comparing voice patterns with prerecorded patterns.
3. Voice output device:
   - Converts digital data into speech using prerecorded sounds.
4. Pagers:
   - Used to alert the recipient of a message, but newer systems now permit transmission of brief text messages.

2. Voice Communications:

Voice communications channels: (cont.)

5. Cell phone
   - Uses radio waves to transmit voice and data through antennas in a succession of cells or defined geographic areas.
6. Personal communications services (PCS)
   - A cellular technology based on lower-power, higher-frequency radio waves.
   - Cells must be smaller and more numerous, but the phones should be smaller and less expensive and be able to operate where other such devices cannot.
7. Voice mail
   - Converts spoken message form analog to digital form, transmits them over a network, and stores them on a disk.
   - Messages are then converted back to analog form when the recipient desires to hear them. Afterward, they may be saved, forwarded, or deleted.
8. Teleconferencing →
   - Conducing an electronic meeting among several parties at remote sites by → telephone, electronic mail group communication software, videoconferencing.

2. Voice Communications:

Question:

1. An electronic meeting conducted between several parties at remote sites is referred to as
   A. Teleprocessing.
   B. Interactive processing.
   C. Telecommuting.
   D. Teleconferencing.

3. Systems Security:

Data integrity:

An organization-wide network security policy should promote the following objectives: →CIA

- Confidentiality (security, privacy) → The secrecy of information that could adversely affect the organization if revealed to the public or competitors should be assured.
- Integrity →Unauthorized or accidental modification of data should be prevented.
- Availability → The intended and authorized users should be able to access data to meet organizational goals.

3. Systems Security:

Data integrity: (cont.)

- The difficulty of maintaining the integrity of the data is the most significant limitation of computer-based audit tools.
- Electronic evidence is difficult to authenticate and easy to fabricate.
- IA must be careful not to treat computer printouts as traditional paper evidence.
- The degree of reliance on electronic evidence by the IA depends on the effectiveness of the controls over the system from which such evidence is taken.

3. Systems Security:

Access control

- 2 broad types of access control, physical controls (physical access controls & environmental controls), and logical controls.

Physical controls:

1. Physical access controls:
   - Keypad devices → enter a password or code to gain entry.
   - Card reader controls → read information from a magnetic strip on access card to gain access.
   - Biometric technologies → These are automated methods of establishing an individual's identity using physiological or behavioral traits, Including fingerprints, retina patterns, hand geometry, signature dynamics, speech, and keystroke dynamics.

3. Systems Security:

Physical controls: (cont.)

2. Environmental controls: → designed to protect the organization's physical information assets.
   - Temperature and humidity control.
   - Gaseous fire-suppression system (not water).
   - Data center not located on an outside wall.
   - Building housing data center not located in a flood plain.

Logical controls:

1. Access control software:
   - Protects files, programs, data dictionaries, processing, etc. from unauthorized access;
   - Restricts use of certain devices (e.g. terminals); and
   - May provide an audit trail for both successful and unsuccessful access attempts
   - For example, a firewall separates internal form external networks.

3. Systems Security:

Logical controls: (cont.)

2. Segregation of functions:

- An individual who has access to the computer may perform incompatible functions.
- Use of password controls to prevent incompatible functions from being performed by individuals with online access to assets and records.
- Access controls provide assurance that only authorized individuals use the system and that usage is for authorized purposes.

3. Passwords and ID numbers:

- Using passwords and identification numbers is an effective control in an online system to prevent unauthorized access to computer files.
- Password generating procedures is required to assure that valid.
- Password are known only by the proper individuals.
- Password should not be displayed when entered at a keyboard.
- Passwords should consist of random letters, symbols, and numbers, words, or phrases.

3. Systems Security:

Internet security:

Connection to the Internet presents security issues.

- Organization-wide network security policy should include:
  - A user account management system.
  - Installation of an Internet firewall.
  - Methods such as encryption to ensure that only the intended user receives that information and that the information is complete and accurate.
- User account management involves installing a system to ensure that:
  - New accounts are added correctly and assigned only to authorized user.
  - Old and unused accounts are removed promptly.
  - Password are changed periodically.
  - Employees are educated on how to choose a password that cannot be easily guessed.

3. Systems Security:

Internet security: (cont.)

- A firewall separates an internal network from an external network.
- It identifies names, Internet Protocol (IP) addresses, applications, etc., and compares them with programmed access rules.

Source	Destination	Allow/Reject
Any	10.15.0.9	Allow
10.0.0.10	192.10.15.2	Allow
192.0.0.1	192.10.0.1	Allow
Any	Any	Reject

- Firewall can produce reports on Internet use, unusual usage patterns, and system penetration attempts.
- These reports are very helpful to IA as a method of continuous monitoring, or logging of the system.
- Firewalls do not provide adequate protection against computer viruses.
- Antivirus measures then should be included in organization network security policy.

3. Systems Security:

Question:

1. Which of the following would not be appropriate to consider in the physical design of a data center?
   A. Evaluation of potential risks from railroad lines and highways.
   B. Use of biometric access systems.
   C. Design of authorization tables for operating system access.
   D. Inclusion of an uninterruptible power supply system and surge protection.

3. Systems Security:

Question:

2. Authentication is the process by which the

A. System verifies that the user is entitled to enter the transaction requested.

B. System verifies the identity of the user.

C. User identifies him/herself to the system.

D. User indicates to the system that the transaction was processed correctly.

3. Systems Security:

Question:

3. Passwords for personal computer software programs are designed to prevent

A. Inaccurate processing of data.

B. Unauthorized access to the computer.

C. Incomplete updating of data files.

D. Unauthorized use of the software.

3. Systems Security:

Question:

4. An auditor has just completed a physical security audit of a data center. Because the center engages in top-secret defense contract work, the auditor has chosen to recommend biometric authentication for workers entering the building. The recommendation might include devices that verify all of the following except
   A. Fingerprints.
   B. Retina patterns.
   C. Speech patterns.
   D. Password patterns.

3. Systems Security:

Question:

5. An Internet firewall is designed to provide adequate protection against which of the following?
   A. A computer virus.
   B. Unauthenticated logins from outside users.
   C. Insider leaking of confidential information.
   D. A Trojan horse application.

3. Systems Security:

Question:

6. Which of the following is the most effective user account management control in preventing the unauthorized use of a computer system?

   A. Management enforces an aggressive password policy that requires passwords to be 10 characters long, to be nonreusable, and to be changed weekly.

   B. An account manager is responsible for authorizing and issuing new accounts.

   C. The passwords and usernames of failed log-in attempts are logged and documented in order to cite attempted infiltration of the system.

   D. Employees are required to renew their accounts semiannually.

3. Systems Security:

Question:

7. The best source of evidence to determine if ex-employees continue to have access to a company's automated databases is

   A. Discussing the password removal process with the database administrator.

   B. Reviewing computer logs of access attempts.

   C. Reconciling current payroll lists with database access lists.

   D. Reviewing access control software to determine whether the most current version is implemented.

3. Systems Security:

Question:

8. Data access security related to applications may be enforced through all the following except

   A. User identification and authentication functions incorporated in the application.

   B. Utility software functions.

   C. User identification and authentication functions in access control software.

   D. Security functions provided by a database management system.

4. Contingency Planning:

Overview:

- Contingency planning is the name commonly given to this activity:
  - Disaster recovery is the process of resuming normal information processing operations after the occurrence of an major interruption.
  - Business continuity is the continuation of business by other means during the period in which computer processing is unavailable or less that normal.
- 2 types of contingencies must be planned for:
  - Power failure, random intrusions such as viruses, and deliberate intrusions such as hacking incidents.
  - Disaster (much more serious) such as floods, fires, hurricanes, earthquakes, etc.

4. Contingency Planning:

Backup and rotation:

- Data is more valuable that its hardware.
- If data is ever destroyed, it cannot be replaced. For this reason, periodic backup and rotation are essential.
- A typical backup routine involves duplicating all data files and application programs once a month.
- Incremental changes are the backed up and taken to the offsite location once a week.
- Application files must be backed up in addition to data since programs change too.
- The offsite location must be temperature- and humidity- controlled and guarded against physical intrusion.
- It must be geographically remote enough from the site of the organization's main operations that it would not be effected by the same natural disaster.

4. Contingency Planning:

Two categories of contingencies:

1. Data center available:
   - Power failures can be guarded against by the purchase of backup electrical generators.
   - Attacks such as viruses and denial-of-service call for a completely different response.
     - System must be brought down to halt the spread of the infection.
     - IT staff must be well trained in the nature of the latest virus threats.
2. Alternate processing facility:
   - A physical location maintained by an outside contractor for the express purpose of providing processing facilities for customers in case of disaster.

4. Contingency Planning:

Two categories of contingencies:

2. Alternate processing facility: (cont.)
   - The recovery center must be far enough away for the main data center to avoid same natural disaster.
   - Once the determination is made that processing is no longer possible at the principal site, the backup files are retrieved from the secure storage location and taken to the recovery center.

Recovery centers:

1. Hot site
   - Fully operational processing facility that is immediately available.
   - Usually, the organization enters into a contract with a service provider.
   - For a set fee, the service provider agrees to have a hardware platform and communications lines substantially identical to the organization's ready for use 24 hours a day, 365 days a year.
   - This is the least risky and most expensive solution.

4. Contingency Planning:

Recovery centers: (cont.)

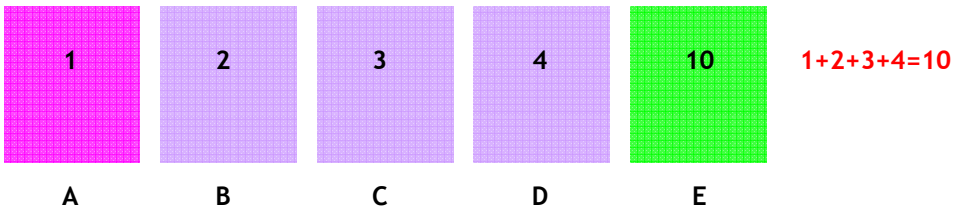
2. Cold site
   - Simply a shell facility with sufficient electrical power, environmental controls, and communications lines to permit the organization to install its own newly-acquired equipment.
   - On an ongoing basis, this is a much less expensive solution.
   - However, the time to procure replacement equipment can be weeks or months. Also, emergency procurements from equipment vendors can be very expensive.
3. Any contract for a hot site must include a provision for annual testing.
   - The service provider agrees to window of time in which the organization can declare a fake disaster, load its backup files onto the equipment at the hot site, and determine how long it takes to resume normal processing.

4. Contingency Planning:

Other technologies:

Fault-tolerant computer systems (formerly called fail-soft systems)

- Have additional hardware and software as well as backup power supply.
- A fault-tolerant computer has additional chips and disk storage. This technology is used for mission-critical applications that cannot afford to suffer downtime.
- RAID (Redundant array of inexpensive discs) is the enabling technology for fault-tolerance. It is a group of multiple hard drives with special software that allows for data delivery along multiple paths. If one drive fails, the other discs can compensate for the loss.



4. Contingency Planning:

Other technologies: (cont.)

High-availability computing

- Used for less-critical applications because it provides for a short recovery time rather than the elimination of recovery time.

4. Contingency Planning:

Question:

1. If High Tech Corporation's disaster recovery plan requires fast recovery with little or no downtime, which of the following backup sites should it choose?
   A. Hot site.
   B. Warm site.
   C. Cold site.
   D. Quick site.

4. Contingency Planning:

Question:

2. The system requiring the most extensive backup and recovery procedures is
   A. A batch system for payroll processing.
   B. A database system for online order entry.
   C. A file-oriented system for billing clients.
   D. An indexed sequential access method file system for fixed asset accounting.

4. Contingency Planning:

Question:

3. Which of the following procedures would an entity most likely include in its disaster recovery plan?

A. Convert all data from EDI format to an internal company format.

B. Maintain a Trojan horse program to prevent illicit activity.

C. Develop an auxiliary power supply to provide uninterrupted electricity.

D. Store duplicate copies of files in a location away from the computer center.

4. Contingency Planning:

Question:

4. Good planning will help an organization restore computer operations after a processing outage. Good recovery planning should ensure that

A. Backup/restart procedures have been built into job streams and programs.

B. Change control procedures cannot be bypassed by operating personnel.

C. Planned changes in equipment capacities are compatible with projected workloads.

D. Service level agreements with owners of applications are documented.

4. Contingency Planning:

Question:

5. A company updates its accounts receivable master file weekly and retains the master files and corresponding update transactions for the most recent 2-week period. The purpose of this practice is to

   A. Verify run-to-run control totals for receivables.

   B. Match internal labels to avoid writing on the wrong volume.

   C. Permit reconstruction of the master file if needed.

   D. Validate groups of update transactions for each version.

4. Contingency Planning:

Question:

6. Contingency plans for information systems should include appropriate backup agreements. Which of the following arrangements would be considered too vendor-dependent when vital operations require almost immediate availability of computer resources?

   A. A “hot site” arrangement.

   B. A “cold site” arrangement.

   C. A “cold and hot site” combination arrangement.

   D. Using excess capacity at another data center within the organization.

5. Databases:

Overview:

- A series of related files combined to eliminate redundancy of data items.
- A single integrated system allows for improved data accessibility.
- Data are stored physically on direct-access storage devices (e.g. disk).
- Logical data model is a user view without regard to how the data are physically stored.
- Flat files → Mainframe computer used flat files. All the records followed on behind the other.

Item no.	Cust Name	Address	Order No.	Part No.	Qty	Price
1	AAAA	123 aaa	001	P-1200	1,000	500
…..	……	Many intervening record			……..	……
7	AAAA	123 aaa	002	P-1010	5,000	10

5. Databases:

Relational structure:

- An individual data item is called a field, column or attribute,
- Multiple records make up a file, table or relation,
- Tables can be jointed or linked.
- Distributed database → Database is stored in two or more physical sites using either replication or petitioning,
- Deadlock → occurs when each of two transactions has a lock on a single data resource.

Emp_ID	Name	Surname
1001	AAAAA	XXXXX
1002	BBBBB	YYYYY
1003	CCCCC	ZZZZZ

Emp_ID	Salary	Allowance
1001	100,000	1,000
1002	200,000	2,000
1003	150,000	1,000

5. Databases:

Database Management System (DBMS):

- An integrated set of computer programs that create the database, maintain the elements, safeguard the data from loss or destruction, make the data available to applications programs and inquiries.
- Allows programmers and system designed to work independently of the physical and logical structure of the DB.
- Data-definition language → create schema (a description of the overall logical structure).
- Data manipulation language → add, delete, retrieve, modify data & relationship.
- E.g. → select * from employee

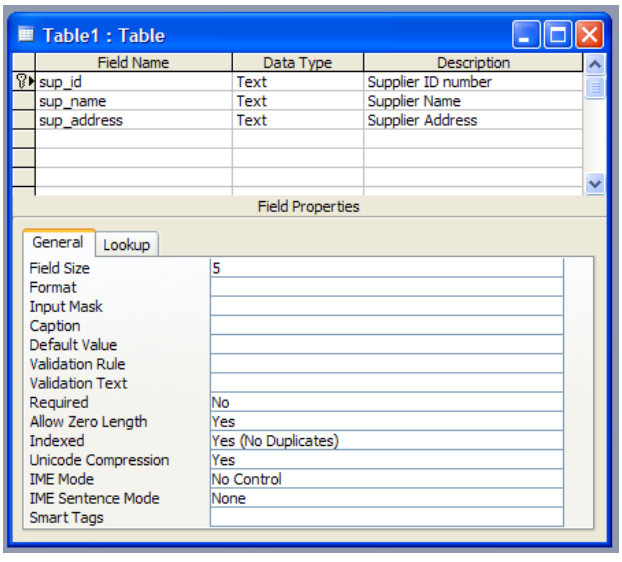
Emp_ID	Name	Surname
1001	AAAAA	XXXXX
1002	BBBBB	YYYYY
1003	CCCCC	ZZZZZ

1001, AAAAA, XXXXX
1002, BBBBB, YYYYY
1003, CCCCC, ZZZZZ

5. Databases:

Other Database Definitions:

- Database administrator (DBA) → developing and maintaining the DB, and establishing controls to protect data integrity.
- Data dictionary → a file describing characteristics of every data element in a DB.



5. Databases:

Question:

1. Of the following, the greatest advantage of a database (server) architecture is

   A. Data redundancy can be reduced.

   B. Conversion to a database system is inexpensive and can be accomplished quickly.

   C. Multiple occurrences of data items are useful for consistency checking.

   D. Backup and recovery procedures are minimized.

5. Databases:

Question:

2. An inventory clerk, using a computer terminal, views the following on screen: part number, part description, quantity on-hand, quantity on-order, order quantity and reorder point for a particular inventory item. Collectively, these data make up a

   A. Field.

   B. File.

   C. Database.

   D. Record.

5. Databases:

Question:

3. The responsibilities of a data administrator (DA) include monitoring
   A. The database industry.
   B. The performance of the database.
   C. Database security.
   D. Backup of the system.

5. Databases:

Question:

4. The To trace data through several application programs, an auditor needs to know what programs use the data, which files contain the data, and which printed reports display the data. If data exist only in a database system, the auditor could probably find all of this information in a
   A. Data dictionary.
   B. Database schema.
   C. Data encryptor.
   D. Decision table.

6. Functional Areas of IT Operations:

Responsibilities of IT Personnel:

1. System analysts:
   - Analyze and design computer information systems.
   - Survey existing system.
   - Analyze the organization's information requirement.
   - Design new systems to meet the requirement.
   - Design specification will be used to guide the preparation of programs.
2. Database administrator (DBA):
   - Responsible for developing and maintaining the database.
   - Establish controls to protect its integrity.
   - Only the DBA should be able to update data dictionaries.
   - (In larger applications) DBA uses a DBMS as a primary tool.

6. Functional Areas of IT Operations:

Responsibilities of IT Personnel: (cont.)

3. Programmers:
   - Design, write, test, and document programs according to specification.
   - Programmers (as well as analysts) may be able to modify programs , data files, and controls.
   - No access to computer equipment and files.
   - No access to copies of programs used in production.
4. Webmaster:
   - Responsible for the content of the organization's website.
   - Work closely with programmers and network technicians.
   - Ensure the appropriate content is displayed and the site is reliably available to users.

6. Functional Areas of IT Operations:

Responsibilities of IT Personnel: (cont.)

5. Operators:
   - Responsible for the day-to-day functioning of the computer center → load data, mount storage devices.
   - Should not be assigned programming duties or system design.
   - Ideally, operator should not have programming knowledge.
6. Help desks:
   - Usually a responsibility of computer operations.
   - Responsible for:
     - Logging reported problems,
     - Resolving minor problem,
     - Forward more difficult problems to the appropriate IS resources (e.g. technical support unit or vendor assistance).

6. Functional Areas of IT Operations:

Responsibilities of IT Personnel: (cont.)

7. Network technicians:
   - Maintain network devices.
   - Responsible for maintaining the organization's connection to other network → e.g. Internet.
8. End users:
   - Need access to applications data and functions only.

6. Functional Areas of IT Operations:

Question:

1. 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.

6. Functional Areas of IT Operations:

Question:

2. Which of the following terms best describes the type of control practice evidenced by a segregation of duties between computer programmers and computer operators?

   A. Systems development control.

   B. Hardware control.

   C. Applications control.

   D. Organizational control.

6. Functional Areas of IT Operations:

Question:

3. For control purposes, which of the following should be organizationally segregated from the computer operations function?

A. Data conversion.

B. Surveillance of screen display messages.

C. Systems development.

D. Minor maintenance according to a schedule.

6. Functional Areas of IT Operations:

Question:

4. In the organization of the information systems function, the most important separation of duties is

A. Not allowing the data librarian to assist in data processing operations.

B. Assuring that those responsible for programming the system do not have access to data processing operations.

C. Having a separate information officer at the top level of the organization outside of the accounting function.

D. Using different programming personnel to maintain utility programs from those who maintain the application programs.

7. Web Infrastructure:

Internet:

- The Internet is a network of networks.
- Descended from the ARPANet.
- 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).
- 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.

7. Web Infrastructure:

Intranet:

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

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.

URL:

- Stands for universal resource locator.
- E.g. www.yahoo.com.

Home page:

- The first screen encountered by users, and subsidiary web pages.

7. Web Infrastructure:

URL:

- Stands for universal resource locator.
- e.g “www.yahoo.com”.

Home page:

- The first screen encountered by users, and subsidiary web pages.

7. Web Infrastructure:

Question:

1. The Internet consists of a series of networks that include

A. Gateways to allow personal computers to connect to mainframe computers.

B. Bridges to direct messages through the optimum data path.

C. Repeaters to physically connect separate local area networks (LANs).

D. Routers to strengthen data signals between distant computers.

7. Web Infrastructure:

Question:

2. Which of the following is true concerning HTML

A. The acronym stands for Hyper Text Material Listing.

B. The language is among the most difficult to learn.

C. The language is independent of hardware and software.

D. HTML is the only language that can be used for Internet documents.

8. Software Licensing:

Overview:

- Software is copyrightable, but a substantial amount is in the public domain. Networks of computer users may share such software.

Shareware:

- Is a software made available for a fee (usually with an initial free trial period) by the owners to users through a distributor (or websites or electronic bulletin board services).

Software piracy:

- Use of unlicensed software increases the risk of introducing computer viruses into organization. Such software is less likely to have been carefully tested.
- A software licensing agreement permits a user to employ either a specified or an unlimited number of copies of a software product at given locations, at particular machines, or throughout the organization. These agreement may restrict reproduction or resale, and it may provide subsequent customer support and product improvements.

8. Software Licensing:

Diskless workstations:

- Increase security by preventing the copying of software to a floppy disk from a workstation.
- This control not only protects the company's interests in its data and proprietary programs but also guards against theft of licensed third party software.

Electronic software distribution (ESD):

- ESD helps to shorten the installation time for revised software in a network, which is the computer-to-computer installation of software on workstations.
- Instead of weeks, software distribution can be accomplished in hours or days and can be controlled centrally.
- Another advantage of ESD is that it permits the tracking of PC program licenses.

8. Software Licensing:

Question:

1. Which of the following would be the most appropriate starting point for a compliance evaluation of software licensing requirements for an organization with more than 15,000 computer workstations?

   A. Determine if software installation is controlled centrally or distributed throughout the organization.

   B. Determine what software packages have been installed on the organization's computers and the number of each package installed.

   C. Determine how many copies of each software package have been purchased by the organization.

   D. Determine what mechanisms have been installed for monitoring software usage.

8. Software Licensing:

Question:

2. Use of unlicensed software in an organization

I. Increases the risk of introducing viruses into the organization

II. Is not a serious exposure if only low-cost software is involved

III. Can be detected by software checking routines that run from a network server

A. I only.

B. I and II only.

C. I, II, and III.

D. I and III only.