Marks

Question No.2

(a) SLA: **06**

Definition:

A Service level agreement is an agreement between the IT organization and the customer. It describes the services in nontechnical terms, from the viewpoint of the customer.

– **Tools to measure SLA effectiveness**

Many tools are available to monitor the efficiency and effectiveness of services provided by IS personnel.

– **Exception reports:**

These automated reports identify all applications that did not successfully complete or otherwise malfunctioned.

– **System and application logs:**

Logs generated from various systems and applications should be considered to identify all application problems.

– **Operator problem reports:**

These manual reports are used by operators to log computer operations problems and their resolution.

– **Operator work schedules:**

These schedules are generally maintained manually by IS management to assist in human resource planning. These schedules should be flexible enough to allow for proper cross-training and emergency staffing requirements.

(b) (i) B2B: **06**

B2B is an acronym for Business to Business, as the name signifies, it is a type of commercial transaction where the purchasing and selling of merchandise are performed between two business houses, such as entity supplying material to another for production, or entity providing services to another.

The relationship among the selling services of two or more business opens up the possibility of reengineering business processes across the boundaries that have traditionally separated external entities from each other.

(ii) B2C:

B2C, where the business sells its goods and services to the final consumer. Those companies whose products and services are consumed directly by the end user are known as B2C companies.
The greatest potential power of e-commerce comes from its ability to redefine the relationship with customers in creating a new convenient, low-cost channel to transact business. Companies can tailor their marketing strategies to an individual's customer's needs and wants.

(iii) B2B2C:

Business to business to consumer (B2B2C) is an e-commerce model that combines business to business (B2B) and business to consumer (B2C) for a complete product or service transaction. B2B2C is a business model where online, or e-commerce, businesses and portals reach new markets and customers by partnering with consumer-oriented product and service businesses. A business developing a product, service or solution partners with another business to use a particular service, such as an e-commerce website, portal or blog. The two business combine forces and promote mutually beneficial products, services and/or solutions.

Marks

(c) Database controls: **06**

It is critical that database integrity and availability be maintained. This is ensured through the following controls:

- Establish and enforce definition standards.
- Establish and implement data backup and recovery procedures to ensure availability
- Establish the necessary levels of access controls, including privileged access.
- Establish controls to ensure that only authorized personnel can update the database.
- Establish controls to handle concurrent access problems.
- Establish controls to ensure accuracy, completeness and consistency of data elements and relationships in the database.
- Perform database reorganization to reduce unused disk space.
- Follow database restructuring procedures when making logical, physical and procedural changes.
- Use database performance reporting tools to monitor and maintain database efficiency.
- Minimize the ability to use non system tools, i.e., those outside security control, to access the database.

(d) Backup Scheme: **06**

(i) Full Backup:

This type of backup scheme copies all files and folders to the backup media, creating one backup set (with one or more media, depending on media capacity). The main advantage is having a unique repository in case of restoration, but it requires more time and media capacity.

(ii) Incremental Backup

It copies the files and folders that changed or are new since the last incremental or full backup. If you have a full back up on day 1, your incremental backup on day 2 will copy only the changes from day 1 to day 2. On day 3, it will copy only the changes from day 2 to day 3 and so on. Incremental backup is a faster method of backup and requires less media capacity.

(iii) Differential Backup

It copy all files and folders that have been added or changed since a full backup was performed. This type of backup is faster and requires less media capacity than a full backup and requires only the last full and differential backup sets to make a full restoration. I also require less time to restore than incremental backups, but it is slower and requires more media capacity than incremental backups because data are backed up are cumulative.

(e) Advantages of application firewall: **06**

- It employ the concept pf bastion hosting in that they handle all incoming requests from internet to the corporate network.
- Application-based firewall system are set up as proxy servers to act on the behalf of someone inside a company intranet.
- Application-level firewall implementation of proxy server function is based on providing a separate proxy for each application service. (e.g., FTP, Telnet, HTTP).
- It provide security for commonly used protocols and generally hide the internal network from outside untrusted network.

Marks

- Perform network address translation (NAT) function.
- Application firewalls specific to a particular kind of network traffic may be titled with the service name, such as a web application firewall. They may be implemented through software running on a host or a stand-alone piece of network hardware.
- Protection for third party modules used in web applications.

Question No.3

(a) Cloud computing essential characteristics: **06**

Characteristics	Description
On-demand self-service	The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service's provider.
Broad network access	Cloud network should be accessible anywhere, by almost any device
Resource pooling	The providers computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand .Example of resources include storage, processing, memory, network, bandwidth and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability. Resource usage can be monitored, controlled and reported, providing transparency for both he provider and customer of the utilized service.

(b) Risk-based audit approach: **08**

Gather Information and Plan	
• Knowledge of business and industry	• Regulatory statutes
• Prior years' audit results	• Inherent risk assessments
• Recent financial information	

Obtain Understanding of Internal Control	
• Control environment	• Control risk assessment
• Control procedures	• Equate total risk
• Detection risk assessment	

Marks

Perform Compliance Tests	
• Identify key controls	• Perform tests on reliability risk prevention and adherence to organization policies and procedures.

Perform Substantive Tests	
• Analytical procedures	• Other substantive audit procedures
• Detailed tests of account balances	

Conclude the Audit	
• Create recommendations	• Write audit report

Question No.4

(a) (i) Centralized computing **03**

Centralized computing is computing done at a central location, using terminals (dump terminals) that are attached to a central computer that performs all the computations and controls all the peripherals, such as printers.

Advantages

- Greater security because all processing is controlled at a central location.
- Various forms of redundancy have been built in to improve overall system reliability.
- More feasible for centralized function needed for business.
- Provide online access to central database by geographically dispersed users.

Disadvantages:

- Central computer must perform computing and must do work to control the remote terminals.
- Total reliance on the central computer; if it goes down, so does the entire system.
- The operating system consumes more CPU's processing power
- Tight schedule and controls required to balance the computer's work load to avoid peak-load problems.

(ii) Distributed computing **03**

In distributed systems, many computers connected to each other and share their resources with each other.

Advantages of distributed operating systems:

- Give more performance than single system
- If one pc in distributed system malfunction or corrupts then other node or pc will take care of it.
- More resources can be added easily
- Resources like printers can be shared on multiple pc's

Marks

- Greater ability to share work, information and resources.
- Ability to continue doing some useful work even if part of the network is down.

Disadvantages of distributed operating systems:-

- Security problem due to sharing
- Complex to administration.
- Some messages can be lost in the network system
- Bandwidth is another problem if there is large data then all network wires to be replaced which tends to become expensive
- Overloading is another problem in distributed operating systems
- If there is a database connected on local system and many users accessing that database through remote or distributed way then performance become slow
- The databases in network operating is difficult to administrate then single user system

(iii) Networking computing: **03**

Multiple network computers are linked to a central server that control their operation and that provides links to other servers.

Advantages:

- Greater ability to share work, information and resources.
- Easier to administer than distributed computing.
- It combine the traditional benefits of centralization with the flexibility and responsiveness of distributed computing.
- This approach is based on networks of stripped-down personal computer sometime called network computers (NCs) or thin clients. The NCs do not contain hard disks, and therefore cannot store programs or data.

Disadvantages:

- It reliance on centralized control and relative immaturity of software designed to support this approach.
- Limited processing ability at user's computer.

(b) Different methods for accessing data in a computer system from database: **06**

(i) Sequential access:

In this technique individual records within a single file are processed in sequence until all record have been processed or until the processing is terminated for some other reason.

Sequential access is the only method for data stored in tape, but it can also be used for data on a direct on a direct access device such as a disk. Sequential processing makes it unnecessary to know the exact location of each data item because data are processed according to the order in which they are sorted.

(ii) Direct access:

Processing events as they occur requires direct access, the ability to find an individual item in a file immediately. A direct access storage device has the electrical or electromechanical means to be immediately positioned for reading and writing at any addressable location on the device.

Marks

(iii) Indexed access:

An index is a table used to find the location of data. The index indicates where alphabetical groups of names are stored. Using indexes makes it possible to perform both sequential processing and direct access efficiently. Therefore, access to data using such indexes is often called the indexed Sequential access method (ISAM). To perform a sequential processing task, such as listing the phone directory in alphabetical order, a program read each index entry in turn and then reads all of the data pointed to by that index entry. If the index entries and the data pointed to by the index Entries are in alphabetical order, the listing will also be in alphabetical order. Although using indexes also causes complications. Database performance degrades as more data goes into the overflow areas. As a result, it is occasionally necessary to unload the data, store it again, and revise the indexes.

Question No.5 (Any 7@1 mark each=7 marks)

(a) Auditing system development, acquisition and maintenance project: **07**

Technique	Description
Snapshot	Records flow of designated transactions through logic paths within programs.
Mapping	Identifies specific program logic that has not been tested, and analyzes programs during execution to indicate whether program statements have been executed.
Tracing and tagging	Tracing shows the trail of instructions executed during an application. Tagging involves placing an indicator on selected transactions at input and using tracing to track them.
Test data/deck	Simulates transactions through real programs
Base-case system evaluation	• Uses test data sets developed as part of a comprehensive testing of program. • Verifies correct system operations before acceptance, as well as periodic revalidation.
Parallel operation	• Processes actual production data through existing and newly developed programs at the same time and compares results, and is used to verify changed production prior to replacing existing procedures.
Integrated testing facility	• Creates a fictitious file in the database with test transactions processed simultaneously with live data.
Parallel simulation	• Processes production data using computer programs that simulate application program logic.
Transaction selection programs	• Use audit software to screen and select transactions input to the regular production cycle.
Embedded audit data collection	• Software embedded in host computer applications screens. It selects input transactions and generated transactions during production. • System control audit review file auditors determines reasonableness of tests incorporated into normal processing .It provides information for further review. • Sample audit review file randomly selects transactions to provide representative file for analysis.
Extended records	• Gathers all data that have been affected by a particular program.

(b) Symmetric vs Asymmetric Encryption **06**

Symmetric encryption is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetrical encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters.

Marks

Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

Key elements of encryption systems:

(i) Encryption algorithm:

A mathematically based function or calculation that encrypts/decrypts data

(ii) Encryption key:

A piece of information that is used within an encryption algorithm to make the encryption or decryption process unique.

(iii) Key length:

A predetermined length for the key. The longer the key, the more difficult it is to compromise in brute-force attack where all possible key combinations are tried.

(c) E-commerce audit and control issues (Best practices): (any eight 08) **08**

When reviewing the adequacy of contracts in e-commerce applications, audit and control professionals should assess applicable use of the following items:

- Security mechanisms and procedures that, taken together , constitute a security architecture for e-commerce (e.g firewalls, PKI, encryption, certificates and password management)
- Firewall mechanism between internal and external network.
- A process whereby participants in e-commerce transaction can be identified uniquely and positively.
- Digital signatures so the initiator can be uniquely associated with it.
- Infrastructure to manage and control public key pairs and their corresponding certificates with include Certificate authority (CA), Registration authority (RA), certification revocation list and certification practice statement (CPS).
- Procedures in place to control changes to an e-commerce presence.
- E-commerce application logs which are monitored by responsible personnel.
- Methods and procedures for intrusion detection system (IDS).
- Features in e-commerce applications to reconstruct the activity performed by the application.
- Protection in place to ensure that data collected about individual are not disclosed without their consent.
- Ensure confidentiality of data between customer and vendors.
- Mechanism to protect the presence of e-commerce and supporting private network s from virus and to prevent them from propagation viruses.
- Means to ensure confidentiality of data communicated between customer and vendor.
- Mechanisms to protect the ecommerce application, infrastructure, network from viruses etc and to prevent them from propagating.
- Features within e-commerce architecture to keep all components from failing and allow them to repair themselves, if they should fail.
- Plan and procedure to continue e-commerce activities in the event of any outage.

Marks

- Commonly understood set of practices and procedures to define management's intention for the security of e-commerce.
- Shared responsibilities within an organization for e-commerce security
- Communication from vendors to customers about the level of security in an e-commerce architecture.
- Regular program of audit and assessment of the security of e-commerce environments and applications to provide assurance that controls are present and effective.

THE END