Total Marks = 90

Q.2 (a) **Data integrity testing:**

Data Integrity testing is a set of substantive tests that examines accuracy, completeness, consistency and authorization of data presently held in a system. It employs testing similar to that used for input control. Data Integrity tests will indicate failures in input or processing controls.

ACID Principle:

In multi-user transaction systems, it is necessary to manage parallel user access to stored data typically controlled by a DBMS and delver fault tolerance. Of particular importance are four online data integrity requirements known collectively as the **ACID** principle.

Atomicity:-

Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes.

Consistency:-

All integrity conditions in the data base are maintained with each transitions ,taking the database from one consistent stage into another consistent stage. It ensures that ensures that any transaction will bring the database from one valid state to another.

Isolation:-

Each transaction is isolated from other transactions and hence each transaction only accesses data that are part of a consistent database state.

Durability:-

If a transaction has been reported back to a user as complete, the resulting changes to the database survive subsequent hardware or software failures. It ensure that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

Q.2 (b) (C) **CRM:**

It is the emerging customer-driven business trend is to be focused on the wants and need of the customers. This emphasizes the importance of focusing on information relating to transaction data, preferences, purchase pattern, status, contact history, demographic information and service trends of customers rather than on products.

The customer expectations are increasing tremendously which, in turn, raises the expectations of service levels. Therefore, the customer-centered applications focus on CRM processes emphasizing the customer, rather then marketing, sales or any other function. Customer relationship management describes a company-wide business strategy including customer-interface departments as well as other departments.

Operational vs Analytical CRM:

Operational CRM is concerned with maximizing the utility of the customer‟s service experience while also capturing useful data about the customer interaction.

Analytical CRM seeks to analyze information captured by the organization about its customers and their interactions with the organization into the information that allows greater value to be obtained from the customer base. Among uses of analytical CRM are increasing "share of customer wallet", moving customer into higher margin products, moving customer to lower-cost service channels, increasing marketing success rates and making pricing decisions.

Operational CRM relates to the operational factors of implementing a CRM system while analytical CRM refers to customer data analysis to determine behavioral responses.

Q.3 (a) <u>**Virtualization:-**</u>

virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources.

Advantages and Disadvantages of virtualization:-

Advantages	Disadvantages
Server hardware costs may decrease for both server builds server maintenance	Inadequate configuration of the host could create vulnerabilities that affect not only the host, but also the guests.
Multiple Oss can share processing capacity and storage space.	Exploits of vulnerabilities within the host's configuration ,or DDOS attacks against the host ,could affect all of the host's guests.
The physical footprint of servers may decrease within the data center.	A compromise of the management console could grant unapproved administrative access to the hosts guests.
A single host can have multiple version s of same or different Operating system.	Performance issues of the host's own OS could impact each of the host's guest.
Creation of duplication copies in alternate locations can support business continuity efforts.	Data could leak between guests.
A single machine can house a multitier network. Provide cloud computing facility.	Insecure protocol for remote access to the management console and guest's could result in exposure of administrative credentials.
If set up correctly ,a well-built, single access control on the host can provide tighter control for the host's multiple guests.	May cause single point of failure with in a system.

Q.3 (b) (A) **EDI:**

EDI process generally involves three functions within each trading partner's computer system.

i. Communication handler: Process for transmitting and receiving electronic documents between trading partners via dial-up-lines, public-switched network, multiple dedicated lines or a value-added networks.

ii. EDI Interface: It manipulates and routes data between the application system and the communications handler. Their interface consists of two components:

-EDI Translator: This device translates the data between the standard format and a trading partner's proprietary format.

-Application Interface: This interface moves electronic transactions to or from the application system and performs data mapping. Data mapping is the process by which

DISCLAIMER: The suggested answers provided on and made available through the Institute's website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.

data are extracted from the EDI translation process and integrated with the data or processes of the receiving company.

iii. Application System: The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the controls for existing applications, if left unchanged, are usually unaffected.

Application-initiated transactions are passed to a common application interface for storage and interpretation. All outbound transactions are formatted according to an externally defined standard and batched by destination and transaction type by the translator. The batches of transactions are routed to the communication processor for transmission. The entire process is reversed for inbound transactions.

Q.4 (a) **Software development methodologies:-**

A **software development process**, also known as a **software development life-cycle (SDLC)**, is a structure imposed on the development of a software product.

Software development models

Several models exist to streamline the development process. Each one has its pros and cons, and it's up to the development team to adopt the most appropriate one for the project. Sometimes a combination of the models may be more suitable.

Waterfall model

The waterfall model shows a process, where developers are to follow these phases in order:

1. Requirements specification (Requirements analysis)
2. Software design
3. Implementation and Integration
4. Testing (or Validation)
5. Deployment (or Installation)
6. Maintenance

In a strict Waterfall model, after each phase is finished, it proceeds to the next one. Reviews may occur before moving to the next phase which allows for the possibility of changes (which may involve a formal change control process). Reviews may also be employed to ensure that the phase is indeed complete; the phase completion criteria are often referred to as a "gate" that the project must pass through to move to the next phase. Waterfall discourages revisiting and revising any prior phase once it's complete. This "inflexibility" in a pure Waterfall model has been a source of criticism by supporters of other more "flexible" models.

Spiral model

The key characteristic of a Spiral model is risk management at regular stages in the development cycle. In 1988, Barry Boehm published a formal software system development "spiral model," which combines some key aspect of the waterfall model and rapid prototyping methodologies, but provided emphasis in a key area many felt had been neglected by other methodologies: deliberate iterative risk analysis, particularly suited to large-scale complex systems.

The key is continual development; it is intended to help manage risks. You should not define the entire system in detail at first. The developers should only define the highest-priority features. This type of development relies on developing prototypes and then giving them back to the user for trial. With this feedback the next prototype is created.

Risk-driven spiral model, emphasizing the conditions of options and constraints in order to support software reuse, software quality can help as a special goal of integration into the product development. However, the spiral model has some restrictive conditions, as follows:

1. The spiral model emphasizes risk analysis, and thus requires customers to accept this analysis and act on it. This requires both trust in the developer as well as the willingness to spend more to fix the issues, which is the reason why this model is often used for large-scale internal software development.
2. If the implementation of risk analysis will greatly affect the profits of the project, the spiral model should not be used.
3. Software developers have to actively look for possible risks, and analyze it accurately for the spiral model to work.

The first stage is to formulate a plan to achieve the objectives with these constraints, and then strive to find and remove all potential risks through careful analysis and, if necessary, by constructing a prototype. If some risks can not be ruled out, the customer has to decide whether to terminate the project or to ignore the risks and continue anyway. Finally, the results are evaluated and the design of the next phase begins.

Q.4 (b) **WAN Technologies:**

Some common types of WAN technologies used to manage and provide point to point connectivity among different sites of bank to its central head office are as follows.

Point-to-Point Links

A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network, such as a telephone company, to a remote network. A point-to-point link is also known as a leased line because its established path is permanent and fixed for each remote network reached through the carrier facilities.

Packet Switching

Packet switching is a WAN switching method in which network devices share a single point-to-point link to transport packets from a source to a destination across a carrier network. Statistical multiplexing is used to enable devices to share these circuits. Asynchronous Transfer Mode (ATM), Frame Relay, MPLS and X.25 are examples of packet-switched WAN technologies.

Frame Relay

Frame Relay is a Date Link and Physical Layer specification that provides high performance. . Frame Relay is more cost-effective than point-to-point links and can run at speeds of 64Kbps to 45Mbps. Frame Relay provides features for dynamic-bandwidth allocation and congestion control.

ISDN

Integrated Services Digital Network is a set of digital services that transmit voice and data over existing phone lines. ISDN can offer a cost-effective solution for remote users who need a higher-speed connection than an analog dial-up link offers. ISDN is also a good choice as a backup link for other types of links.

ATM:-

Asynchronous Transfer Mode (ATM) is a technology that has the potential of revolutionizing data communications and telecommunications. ATM is a cell-relay technology that divides upper-level data units into 53-byte cells for transmission over the physical medium. It operates independently of the type of transmission being generated

DISCLAIMER: The suggested answers provided on and made available through the Institute's website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.

at the upper layers AND of the type and speed of the physical-layer medium below it.

This allows the ATM technology to transport all kinds of transmissions (e.g, data, voice, video, etc.) in a single integrated data stream over any medium, ranging from existing T1/E1 lines, to SONET OC-3 at speeds of 155 Mbps, and beyond.

MPLS:-

Multiprotocol label switching provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels t network packets that describe how to forward them through the network. By configuring MPLS on router we can provide secure connectivity of banks different remote sites to its central head office. MPLS is the today ‟solution that ensure QOS.

DSL:-

Digital subscriber line (DSL, originally digital subscriber loop) is a family of technologies that provide internet access by transmitting digital data over the wires of a local telephone network. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology.

The data bit rate of consumer DSL services typically ranges from 256 Kbit/s to 40 Mbit/s in the direction to the customer (downstream), depending on DSL technology. DSL is cheaper solution and more feasible for backup connectivity between different bank sites to central office.

VPN:-

A virtual private network (VPN) extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

DXX Links:

A **digital cross-connect system** (DCS or DXC) is a piece of circuit-switched network equipment, used in telecommunications networks to connect different remote sites of banks. DCS devices can be used for "grooming" telecommunications traffic, switching traffic from one circuit to another in the event of a network failure, supporting automated provisioning, and other applications. DXX links can be used as primary or backup connectivity between banks remote sites.

Q.5 (a) Why Symmetric Encryption used for data Encryption and Asymmetric Encryption used in Key exchange:

Encryption methods can be *SYMMETRIC* in which encryption and decryption keys are the same. Symmetric key size is normally smaller so CPU utilization is relatively very low and results in less processing time. Symmetric key cryptosystems such as DES or AES are less complicated and, therefore, use up less processing power than asymmetric techniques. This makes symmetric key cryptosystems ideally suited for bulk data encryption.

ASYMMETRIC in which encryption and decryption keys differ. 'Public Key' methods must be asymmetric, to the extent that the decryption key CANNOT be easily derived from the encryption key. In key exchange methods usually deploy Asymmetric key mechanism. It is more secure due to larger key size. Size of data is also limited in key exchange mechanism so Asymmetric key is preferable in key exchange mechanism.

-If a symmetric keys were used to encrypt bulk data, the processes would be very slow;

DISCLAIMER: The suggested answers provided on and made available through the Institute’s website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.

this is the reason they are used to encrypt short messages such as signatures etc.

How public-key cryptography works:-

The distinguishing technique used in public-key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys - a **public encryption key** and a **private decryption key**. The publicly available encrypting-key is widely distributed, while the private decrypting-key is known only to the recipient. Messages are encrypted with the recipient's public key, and can be decrypted *only* with the corresponding private key. The keys are related mathematically, but the parameters are chosen so that determining the private key from the public key is either impossible or prohibitively expensive.

Q.5 (b) **Hardware review:**

When auditing infrastructure and operations, hardware reviews should include the following points:

i) Hardware acquisition plan review:

- Is the plan aligned with business requirements?
- Is the plan synchronized with business plans?
- Is the plan synchronized with IS plans?
- Have criteria for the acquisition of hardware been developed?
- Is the environment adequate to accommodate existing and new hardware?
- Are the hardware, software specification etc adequately documented?

ii) Capacity management and monitoring review:

- Are criteria used in hardware performance monitoring plan based on historical data and analysis obtained from the IS logs, processing schedules, job accounting system reports, preventive maintenance schedules and reports?
- Is continue review performed of hardware and system software performance and capacity?
- Is monitoring adequate for equipments that has been programmed to contact its manufacturer in case of any equipment failure?

iii) Preventative maintenance schedule review:

- Is the prescribed maintenance frequency recommended by the respective hardware vendors being observed?
- Is maintenance done during off-peak workload periods?
- Is preventative maintenance performed at times other than when the system is processing critical or sensitive applications?

iv) Hardware availability and utilization reports review:

- Is scheduling adequate to meet workload schedules and user requirements?
- Is scheduling sufficiently flexible to accommodate required hardware preventive maintenance?
- Are IS resources readily available for critical application programs?

v) Problem logs & Job accounting system reports review:

- Have IS management staff reviewed hardware malfunctions abnormal system terminations and operator actions?

vi) Acquisition of Hardware review:

- ¤ Is the acquisition in line with the hardware acquisition plan?
- ¤ Are requests accompanied by cost-benefit analysis?
- ¤ Have procedures and forms been established to facilitate the acquisition approval access?
- ¤ Are purchase routed via purchasing department to streamline the process?

Q.6 (a) **<u>Information security policy document:</u>**

The information security policy document should state management's commitment and set out the organization's approach to managing information security. The ISO 27002 standard may be considered a benchmark for the content covered by the Information Security Policy Document.

The policy document should contain:

¤ A definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.

¤ A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives.

¤ A framework for setting control objectives and controls, including the structure of risk assessment and risk management.

¤ A brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization including:

-Compliance with legislative, regulatory and contractual requirements.

-Security education, training and awareness requirements.

-Business continuity management.

-Consequences of information security policy violations.

¤ A definition of general and specific responsibilities for information security management, including reporting information security incidents.

¤ References to documentation which may support the policy; e.g. more detailed security policies, standards, and procedures for specific information systems or security rules with which users should comply.

The information security policy should be communicated throughout the organization to users in a form that is accessible and understandable to the intended reader. The information security policy may be part of general policy document and may be suitable for distribution to third parties and vendors as long as care is taken not to disclose sensitive organizational information.

Acceptable Internet usage policy:-

The AUP is a set of guidelines or rules that are put into effect by an enterprise to control how its information system resources will be used. The most common form of AUP is Acceptable Internet usage policy, which prescribes the code of conduct that governs the behavior of a user while connected to the network/internet. The code of conduct may be include "netiquette"__ a description of language that is considered appropriate to use while online. The code of conduct also should outline what is considered illegal or an excessive personal activity. Adherence to a code of conduct helps IS auditor to ensure that activities embarked on by a user will not expose the enterprise to information security risks. IS auditor should ensure that Acceptable internet usage policy implement with its true sprits in organization.

DISCLAIMER: The suggested answers provided on and made available through the Institute's website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.

Q.6 (b) **CAAT:-**

Today’s information processing environments pose a significant challenge to the IS auditor to collect sufficient, relevant and useful evidence since the evidence exists on magnetic media.

Computer Assisted Audit Techniques are important tools for the IS auditor in gathering information from these environments. When systems have different hardware and software environments, data structure, record formats or processing functions, it is almost impossible for the auditors to collect evidence without a software tool to collect and analyze the records. CAAT also enables IS auditors to gather information independently. CAAT’s provide means to gain access and analyze data for a predetermined audit objectives, and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system.

GAS:-

Generalized audit software is important tool for CAAT. GAS refers to standard software that has the capability to directly read and access data from various database platforms, flat-file systems and ASCII formats. The following functions supported by GAS:

-**File access:-**

Enables the reading the reading of different record formats and file structures.

-File reorganization:

Enables indexing, sorting, merging and linking with another file.

-**Data Selection:**

Enables global filtration conditions and selection criteria.

-**Statistical functions:**

Enables sampling and frequency analysis.

-**Arithmetical functions:**

Enables arithmetic operators and functions.

Q.7 (a) **Reasons for ACLs**

There are many reasons to create ACLs. For example, ACLs can be used to:

- Limit network traffic and increase network performance.
- Provide traffic flow control. For example, ACLs can restrict or reduce the contents of routing updates. These restrictions are used to limit information about specific networks from propagating through the network.
- Provide a basic level of security for network access. For example, ACLs can allow one host to access a part of your network and prevent another host from accessing the same area.
- Decide which types of traffic are forwarded or blocked at the router interfaces. For example, you can permit e-mail traffic to be routed, but at the same time block all TELNET traffic.

Extended ACL:

ACLs are lists of instructions you apply to a router's interface. These lists tell the router what kinds of packets to accept and what kinds of packets to deny. Acceptance and denial can be based on certain specifications, such as source address, destination address, and port number. ACLs enable you to manage traffic and scan specific packets by applying the ACL to a router interface. Any traffic going through the interface is tested against certain conditions that are part of the ACL.

DISCLAIMER: The suggested answers provided on and made available through the Institute’s website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.

Extended IP access-lists have the ability to look at source and destination IP addresses, layer 4 protocols, layer 4 specific information such as source and destination ports, and various protocol flags at layer 3 and layer 4.

Q.7 (b) **(A)<u>Business Continuity Plan</u>:**

To ensure continuous service , a BCP should be written to minimize the impact of disruptions. Therefore the process of developing and maintaining an appropriate BCP would be:

- Conduct risk assessment- Identify and prioritize the systems and other resources required to support critical business processes in the event of a disruption. Identify and prioritize threads and vulnerabilities.
- Prepare business impact analysis of the effect of the loss of critical business processes and their supporting components.
- Choose appropriate controls and measures for recovery IT.
- Developed detailed DRP plan.
- Developed a detailed plan for critical business functions to continue to operate at an acceptable level .
- Maintain the plans as the business changes and systems develop.

Auditor Tasks:

While auditing business plan IS auditor tasks include:

- Understanding and evaluating business continuity strategy and its connection to business objectives.
- Evaluating the BCPs and comparing them to appropriate standard.
- Verifying that BCPs are effective, by reviewing the results from previous tests performed by IS and end-user personnel.
- Evaluating offsite storage.
- Verifying the arrangements for transporting backup media and ensure their security requirements.
- Evaluating the ability of personnel in emergency situations, by reviewing emergency procedures and employee trainings.
- Ensuring that the process of maintaining plans is in place and effective and covers both periodic and unscheduled revisions.

Evaluating whether business continuity manuals and procedures are written in simple and easy to understand manner.

THE END

DISCLAIMER: The suggested answers provided on and made available through the Institute's website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.