Total Marks = 90

Q.2 (a) Components that one could expect to see in a typical E-commerce architecture would include:

1) Marketing, sales and customer service components (e.g., personalization, membership, product catalog, customer ordering, invoicing, shipping, inventory replacement, online training and problem notification).

2) Application servers will support a particular component model and provide services (such as data management, security and transaction management) either directly or through connection to another service or middleware product. Application servers in conjunction with other middleware products provide for multitier systems (i.e., a business transaction can span multiple platforms and software layers).

3) A web server will be used to manage web content and connections; business logic and other services will be provided by the application server; and one or more database(s) will be used for data storage.

4) Databases play a key role in most e-commerce systems, maintaining data for web site pages, accumulating customer information, and possibly storing click-stream data for analyzing web site usage.

b) Following are the typical types of computers, based on their processing power, size, and architecture.

Supercomputer: These are very large and expensive computers with the highest processing speed, designed to be used for specialized purposes or fields that require extensive processing power (e.g., complex mathematical or logical calculations). They are typically dedicated to a few specific specialized system or application programs.

Mainframes: Large, general-purpose computers that are made to share their processing power and facilities with thousands of internal or external users. Mainframes accomplish this by executing a large variety of tasks almost simultaneously. The range of capabilities of these computers is extensive. A mainframe computer often has its own proprietary operating system that can support background (batch) and real-time (online) programs operating parallel applications. Mainframes have traditionally been the main data processing and data warehousing resource of large concerns and, as such, have long been protected by a number of the early security and control tools.

High-end and midrange servers: Multiprocessing systems capable of supporting thousands of simultaneous users. In size and power, they can be comparable to a mainframe. High end/midrange sewers have many of the control features of mainframes such as online memory and CPU management, physical and logical partitioning, etc. Their capabilities are also comparable to small mainframes in terms of speed for processing data and execution of client programs, but they cost much less than mainframes. Their operating systems and system software base components are often commercial products. The higher-end devices generally utilize UNIX and, in many cases, are used as database sewers while smaller devices are more likely

to utilize the Windows operating system and be used as application servers and file/print sewers.

Personal computers (PC): Small computer systems referred to as PCs or workstations that are designed for individual users, inexpensively priced and based small database management, interaction with web-based applications and others such as personal graphics, voice ,imaging, design, web access and entertainment. Although designed as single-user systems, these computers are commonly linked together to form a network.

Thin client computers: These are personal computers that are generally configured with minimal hardware features (e.g., diskless workstation) with the intent being that most processing occurs at the sewer level using software, such as Microsoft Terminal Services or Citrix Presentation Server, to access a suite of applications.

Laptop computers: Lightweight (under 10 pounds/5 kilograms) personal computers that are easily transportable and are powered by a normal AC connection or by a rechargeable battery pack. Similar to the desktop variety of personal computers in capability, they have similar CPUs, memory capacity and disk storage capacity, but the battery pack makes them less vulnerable to power failures.

Smartphones, tablets and other handheld devices: Handheld devices that enable their users to use a small computing device as a substitute for a laptop computer. Some of its uses include a scheduler, a telephone and address book, creating and tracking to-do lists, an expense manager, eReader, web browser, and an assortment of other functions. Such devices can also combine computing, telephone/fax and networking features together so they can be used anytime and anywhere. Handheld devices are also capable of interfacing with PCs to back up or transfer important information. Likewise, information from a PC can be downloaded to a handheld device.

Q.3 (a) **Project Organizational Forms**

Three major forms of organizational alignment for project management within the business organization can be observed:

1. Influence project organization
2. Pure project organization
3. Matrix project organization

In influence project organization, the project manager has only a staff function without formal management authority. The project manager is only allowed to advise peers and team members as to which activities should be completed.

In a pure project organization, the project manager has formal authority over those taking part in the project. Often, this is bolstered by providing a special working area for the project team that is separated from their normal office space.

In a matrix project organization, management authority is shared between the project manager and the department heads.

For an auditor, it is important to understand these organizational forms and their implications on

controls in project management activities.

b) Following are three important duties of IS management w.r.t. problem management in information systems management.

1) IS management should ensure that the incident and problem management mechanisms are properly maintained and monitored and that outstanding errors are being adequately addressed and resolved in a timely manner.

2) IS management should develop operations documentation to ensure that procedures exist for the escalation of unresolved problems to a higher level of IS management. While there are many reasons why a problem may remain outstanding for a long period of time, it should not be acceptable for a problem to remain unresolved indefinitely. The primary risk resulting from lack of attention to unresolved problems is the interruption of business operations. An unresolved hardware or software problem could potentially corrupt production data. Problem escalation procedures should be well-documented. IS management should ensure that the problem escalation procedures are being adhered to properly.

3) IS management should ensure that departments and positions responsible for problem resolution should be part of problem management documentation. This documentation must be maintained properly to be useful.

Q.4 (a) The IS auditor should perform the following important duties while analyzing feasibility studies:

1. Review the documentation produced in this phase for reasonableness
2. Determine whether all cost justifications/benefits are verifiable and, showing the anticipated costs and benefits to be realized.
3. Identify and determine the criticality of the need.
4. Determine if a solution can be achieved with systems already in place. If not, review the evaluation of alternative solutions for reasonableness.
5. Determine the reasonableness of the chosen solution.

b) Following are the key features of network database model and relational database model.

Network database model

In the network model, the basic data modeling construct is called a set. A set is formed by an owner record type, a member record type and a name. A member record type can have that role in more than one set, so a multi-owner relationship is allowed. An owner record type can also be a member or owner in another set. Usually, a set defines a l:N relationship, although one-to-one (1: l) is permitted. A disadvantage of the network model is that such structures can be extremely

complex and difficult to comprehend, modify or reconstruct in case of failure. This model is rarely used in current environments. The network model does not support high-level queries. The user programs have to navigate the data structures.

Relational database model

The relational model is based on the set theory and relational calculations. A relational database allows the definition of data structures, storage/retrieval operations and integrity constraints. In such a database the data and relationships among these data are organized in tables. A table is a collection of rows, also known as tuples, and each tuple in a table contains the same columns. Columns, called domains or attributes, correspond to fields. Tuples are equal to records in a conventional file structure. Certain fields may be designated as keys , so searches for specific values of that field will be quicker because of the use of indexing. The relational model is independent from any physical implementation of the data structure. Another key feature of relational model is normalization rules that optimize the amount of information needed in the tables.

Q.5 (a) Following are the five stages of risk-based audit approach.

1) Gather Information and Plan

a. Knowledge of business and industry

b. Regulatory statutes

c. Prior year's audit results

d. Inherent risk assessments

e. Recent financial information

2) Obtain Understanding of Internal Control

a. Control environment

b. Control risk assessment

c. Control procedures

d. Equate total risk

e. Detection risk assessment

3) **Perform Compliance Tests**

a. Identity key controls to be tested

b. Perform tests on reliability, risk prevention and adherence to organization policies and procedures.

4) **Perform Substantive Tests**

   a. Analytical procedures

   b. Detailed tests of account balances

   c. Other substantive audit procedures

5) **Conclude the Audit**

   a. Create recommendations

   b. Write audit report

b) A Steering Committee performs following primary functions:

1) Review the long- and short-range plans of the IS department to ensure that they are in accordance with the corporate objectives.

2) Review and approve major acquisitions of hardware and software within the limits approved by the board of directors.

3) Approve and monitor major projects and the status of IS plans and budgets, establish priorities, approve standards and procedures, and monitor overall IS performance.

4) Review and approve sourcing strategies for select or all IS activities, including insourcing or outsourcing, and the globalization or offshoring of functions.

5) Review adequacy of resources and allocation of resources in terms of time, personnel and equipment.

6) Make decisions regarding centralization vs. decentralization and assignment of responsibility.

7) Support development and implementation of an enterprise wide information security management program.

8) Report to the board of directors on IS activities.

Q.6 (a) Key points to be taken into consideration in a data conversion project are to ensure:

1) Completeness of data conversion—i.e., the total number of records from the source database is transferred to the new database (assuming the number of fields is the same)

2) Integrity of data—-i.e., the data are not altered manually, mechanically or electronically by person, program, substitution or overwriting in the new system. Integrity problems also include errors due to transposition, transcription errors, and problems transferring particular records, fields, files and libraries.

3) Storage and security of data under conversion—i.e., data are backed up before

conversion for future reference or any emergency that might arise out of data conversion program management. Unauthorized copy or too many copies can lead to misuse, abuse or theft of data from the system.

4) Consistency of data—i.e., the field/record called for from the new application should be consistent with that of the original application. This should enable consistency in repeatability of the testing exercise.

5) Continuity—i.e., the new application should be able to continue with newer records as addition (append) and help in ensuring seamless business continuity.

6) The last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform should be maintained separately in the archive for any future reference.

b) The IS auditor should review the system development project to ensure:

1. The project meets cooperative goals and objectives
2. Project planning is performed, including effective estimates of resources, budget and time
3. Scope creep is controlled and there is a software baseline to prevent requirements from being added into the software design or having an uncontrolled development process
4. Management is tracking software design and development activities
5. Senior management support is provided to the software projects design and development efforts.
6. Periodic review and risk analysis is performed in each project phase

Q.7 (a) Following are the general features of firewall:

1. Block access to particular sites on the Internet
2. Limit traffic on an organization's public services segment to relevant addresses and ports
3. Prevent certain users from accessing certain servers or services
4. Monitor communications and record communications between an internal and an external network
5. Monitor and record all communications between an internal network and the outside world to investigate network penetrations or detect internal subversion
6. Encrypt packets that are sent between different physical locations within an organization by creating a VPN over the Internet (i.e., IP security [IPSec], VPN

tunnels)

Problems faced by organizations that have implemented firewalls include:

1. A false sense of security may exist where management feels that no further security checks and controls are needed on the internal network (i.e., the majority of incidents are caused by insiders, who ate not controlled by firewalls).
2. The circumvention of firewalls through the use of modems may connect users directly to ISPs. Management should provide assurance that the use of modems when a firewall exists IS strictly controlled or prohibited altogether.
3. Misconfigured firewalls may allow unknown and dangerous services to pass through freely.

b) Specific types of coverage available are:

1. IS equipment and facilities—Provides coverage about physical damage to the Internal Processing Facility (IPF) and owned equipment. (Insurance of leased equipment should be obtained when the lessee is responsible for hazard coverage.).
2. Media (software) reconstruction—Covers damage to IS media that is the property of the insured and for which the insured may be liable.
3. Extra expense—Designed to cover the extra costs of continuing operations following damage or destruction at the IPF. The amount of extra-expense insurance needed is based on the availability and cost of backup facilities and operations.
4. Business interruption—Covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IS organization
5. Valuable papers and records—Covers the actual cash value of papers and records (not defined as media) on the insured's premises against direct physical loss or damage.
6. Errors and omissions——Provides legal liability protection in the event that the professional practitioner commits an act, error or omission that results in financial loss to a client.
7. Fidelity coverage—Usually takes the form of bankers blanket bonds, excess fidelity insurance and commercial blanket bonds, and covers loss from dishonest or fraudulent acts by employees.
8. Media transportation—Provides coverage for potential loss or damage to media in transit to off-premises lPFs.

THE END