PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

*Question No. **1** is compulsory.*

*Candidates are required to answer any **four** questions*

*from the remaining **five** questions.*

Question 1

ABC bank is a large bank with more than 4000 branches and 20000 ATMs in India. With an aim to grow further, it has acquired three smaller private banks with similar lines of business. This acquisition has brought a variety of products, applications and branches under its umbrella. Besides consumer banking through brick and mortar branches, ABC bank also wants to consolidate its position through internet banking.

The growth strategy of the Bank has resulted in fragmented business operations that operate in a regional structure as well as in distributed IT environment. Hence, ABC bank wishes to implement a new, cutting edge web-based core banking system to manage all its operations from a single window. ABC bank also recognizes that failure or malfunction of any critical system will cause significant operational disruptions and materially impact its ability to provide service to its customers, besides loss of reputation. To overcome this risk, ABC bank plans to implement Business Continuity Management (BCM). You have been appointed as an IT consultant by ABC bank to make a presentation to the Board of Directors to justify the need for the new system. Answer the following queries raised by the Management:

(a) What are the key management practices which are required for aligning the IT Strategy of ABC bank with its Enterprise Strategy? ***(6 Marks)***

(b) What are the IT tools you may consider critical for business growth? ***(5 Marks)***

(c) Explain the five stages or components of the BCM process which will help ABC bank to manage any future disruptions to the proposed new core banking system. ***(3 Marks)***

Answer

(a) The key management practices, which are required for aligning IT strategy with enterprise strategy are as follows:

- **Understand enterprise direction:** It involves the understanding of the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. It also considers the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** It assesses the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. It identifies issues currently being experienced and develop recommendations in areas that could benefit from improvement. It considers service provider differentiators and

options and the financial impact and potential costs and benefits of using external services.

- **Define the target IT capabilities:** It defines the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** It identifies the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base.
- **Define the strategic plan and road map:** It creates a strategic plan that defines in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. It includes how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** It creates awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

(b) Some IT tools that may be crucial for any business growth are as follows:

(i) **Business Website –** By having a website, enterprise/business becomes reachable to large number of customers. In addition, it can also be used in an advertisement, which is cost effective and in Customer Relationship Management. These websites can be designed by using HTML, XML, ASP.NET etc.

(ii) **Internet and Intranet –** It is the best source of communication. Time and space are no more obstacles for conducting meeting of people working in a team from multiple locations, or with different vendors and companies. Intranet is system that permits the electronic exchange of business data within an organization, mostly between managers and senior staff. E-commerce among partners (suppliers, wholesalers, retailers, distributors) using intranets, e-mail etc. provides new platform to the business world for conducting business in a faster and easier way. E-commerce provides business to business, business to customer, customer to customer and customer to business communication with a click of mouse.

(iii) **Software and Packages** - DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making and can boost the business in the competitive world. These can be used in

Supply chain logistics, including planning, purchasing, replenishment, logistics, and space management.

(iv) **Business Intelligence (BI) –** This refers to applications and technologies that are used to collect and provide access and analyze data and information about companies' operations. Some BI applications are used to analyze performance or internal operations e.g. EIS (Executive Information System), business planning, finance and budgeting tools. While others are used to store and analyze data e.g. Data mining, data warehouses, decision support system etc. Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools.

(v) **Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc.-** Webcam, microphone etc. are used in conducting long distance meeting. Use of computer systems, printer and scanner lead to increase in accuracy; reduced processing times, enable quick decision -making and speed up customer service.

(c) The components/stages of Business Continuity Management (BCM) Process are given below:

(i) **Stage 1 - BCM Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.

(ii) **Stage 2 - BCM Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services.

(iii) **Stage 3 - BCM Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.

(iv) **Stage 4 - BCM Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and identifies opportunities for improvement.

(v) **Stage 5 - BCM Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

Question 2

(a) You are appointed by a leading enterprise to assess and to evaluate its system of IT internal controls. What are the key management practices to be followed to carry out the assignment in compliance with COBIT5? ***(6 Marks)***

(b) 'There is a practical set of principles to guide the design of measures and indicators to be included in an EIS.' Explain those principles in brief. ***(5 Marks)***

(c) What are the common operating system access controls to protect IT resources from unauthorized access? List any six controls. ***(3 Marks)***

Answer

(a) The key management practices for assessing and evaluating the system of IT Internal Controls in an enterprise are as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.

- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

(b) A practical set of principles to guide the design of measures and indicators to be included in an Enterprise Information Systems (EIS) is as below:

- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.
- EIS measures must be based on a balanced view of an organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.
- Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.
- EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
- EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
- EIS measures must evolve to meet the changing needs of the organization.

(c) List of common Operating System Access Controls is as follows:

- Automated terminal identification;
- Terminal log-in procedures;
- Access Token;
- Access Control List;
- Discretionary Access Control;
- User identification and authentication;
- Password management system;
- Use of system utilities;
- Duress alarm to safeguard users;
- Terminal time out; and

- Limitation of connection time.

Question 3

(a) 'Crimes can be committed by using computers and can damage the stability, reputation, morale and even the existence of an organization.' What are the problems that an organization can face as a result of computer crimes? ***(6 Marks)***

(b) Risk assessment is an important part of the information systems auditor's planning and implementation. Enumerate the steps followed for a risk-based approach to prepare an audit plan and briefly describe how risks are categorized. ***(5 Marks)***

(c) The Spiral model is intended for large, expensive and complicated projects. What are the major strengths of this model? ***(3 Marks)***

Answer

(a) Computer crimes generally result in loss of customers, embarrassment to management and legal actions against the organizations. These are given as follows:

- **Financial Loss:** Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.
- **Legal Repercussions:** An organization has to adhere to many laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.
- **Loss of Credibility or Competitive Edge:** In order to maintain competitive edge, many companies especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
- **Blackmail/Industrial Espionage:** By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** These events can spoil the reputation of the organization. Legal or regulatory actions against the company may be also a result of disclosure.
- **Sabotage:** Some people though may not be interested in the financial gain may still want to spoil the credibility of the company or involve themselves in such activities because of their dislike towards the organization or for their intemperance.
- **Spoofing:** A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. It occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that he is interacting with the operating system. For example, a penetrator duplicates the

login procedure, capture the user's password, attempt for system crash and makes the user login again.

(b) The steps that can be followed for a risk-based approach to prepare an audit plan are as follows:

- Inventory the information systems in use in the organization and categorize them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- Assess what risks affect these systems and the severity of the impact on the business.
- Based on the above assessment; decide the audit priority, resources, schedule and frequency.

Risks are categorized as follows:

- **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls.
- **Control Risk:** Control risk is the risk that could occur in an audit area and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level will not be prevented or detected by the client's internal control system.
- **Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

(c) Major strengths that are identified by the experts and practitioners of the Spiral Model include the following:

- It enhances the risk avoidance.
- It is useful in helping for optimal development of a given software iteration based on project risk.
- It can incorporate Waterfall, Prototyping, and Incremental methodologies as special cases in the framework, and provide guidance as to which combination of these models best fit a given software iteration, based upon the type of project risk.

Question 4

(a) A company has decided to outsource its backup and recovery process to a third-party site. What are the issues that should be considered by the security administrators while drafting the contract? ***(6 Marks)***

(b) As an IS Auditor of a company, you want to use SCARF technique for collecting some information; which you want to utilize for discharging some of your functions. Briefly describe the type of information that can be collected using SCARF technique. ***(5 Marks)***

(c) Discuss the 'Use of Electronic Records in Government and its agencies' in the light of Section 6 of Information Technology Act, 2000. ***(3 Marks)***

Answer

(a) If a third-party site is to be used for backup and recovery purposes; security administrators must ensure that a contract is written to cover issues such as -

- how soon the site will be made available subsequent to a disaster;
- the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- the priority to be given to concurrent users of the site in the event of a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- the facilities and services the site provider agrees to make available; and
- what controls will be in place and working at the off-site facility.

(b) As an IS Auditor of a company, the type of information that can be collected using SCARF techniques are as follows:

- **Application System Errors:** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and Procedural Variances:** Organizations must adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception:** SCARF can be used to monitor different types of application system exceptions. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample:** Some embedded audit routines might be statistical sampling

routines; SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

- **Snapshots and Extended Records:** Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling Data:** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance Measurement:** Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(c) [Section 6] of Information Technology Act, 2000 is as follows:

[Section 6] Use of Electronic Records and Electronic Signatures in Government and its agencies

(1) Where any law provides for -

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe -

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

Explanation –

Section 6 lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.

Question 5

(a) Audit is vital, as information systems are vulnerable to destruction, error, abuse and system quality problems. Briefly describe the different types of audit tools. ***(6 Marks)***

(b) What is a Knowledge Management System? Discuss in brief. ***(5 Marks)***

(c) COBIT is a set of best practices for Information Technology management which provides a business framework for the governance and management of enterprise Information Technology. Briefly describe its components. ***(3 Marks)***

Answer

(a) Different types of Audit Tools are as follows:

(i) Snapshot: Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

(ii) Integrated Test Facility (ITF): The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases, the auditor decides the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

(iii) System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

(iv) Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique that provides an online auditing capability and can be used to trap exceptions whenever the application system uses a Database Management System (DBMS). The DBMS reads an application system transaction and passes it to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system. Exceptions identified by CIS are written to an exception log file.

(v) Audit Hooks: There are audit routines that flag/tag suspicious transactions. The internal audit department will investigate these tagged records for detecting fraud.

When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

(b) Knowledge Management System (KMS): Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organizational knowledge. It refers to a multi-disciplined approach to achieving organizational objectives by making the best use of knowledge**.** KMS refers to any kind of IT system that stores and retrieves knowledge, improves collaboration, locates knowledge sources, mines repositories for hidden knowledge, captures and uses knowledge, or in some other way enhances the KM process. KMS treats the knowledge component of any organization's activities as an explicit concern reflected in strategy, policy, and practice at all levels of an organization.

There are two broad types of knowledge - **Explicit** and **Tacit**. KMS makes a direct connection between an organization's intellectual assets – both Explicit and Tacit.

- **Explicit Knowledge:** Explicit knowledge is that which can be formalized easily and consequently is easily available across the organization. Explicit knowledge is articulated and represented as spoken words, written material and compiled data. This type of knowledge is codified, easy to document, transfer and reproduce. For example – Online tutorials, Policy and procedural manuals.
- **Tacit Knowledge:** Tacit knowledge, resides in a few often-in just one person and hasn't been captured by the organization or made available to others. Tacit knowledge is unarticulated and represented as intuition, perspective, beliefs and values that individuals form based on their experiences. It is personal, experimental and context specific. It is difficult to document and communicate the tacit knowledge. For example – hand-on skills, special know-how, employee experiences.

(c) Components in COBIT are as follows:

- **Framework:** This organizes IT governance objectives and good practices by IT domains and processes, and links them to business requirements.
- **Process Descriptions:** This provides a reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives:** These provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- **Management Guidelines:** These guidelines help to assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
- **Maturity Models:** These are used to assess maturity and capability per process and helps to address gaps.

Question 6

(a) What is an Information Security Policy? What are its different types? Explain in brief and write a note on the members comprising the security policy. ***(6 Marks)***

(b) Discuss any five characteristics of Platform as a Service (PaaS). ***(5 Marks)***

(c) Discuss the key components of Mobile Computing in brief. ***(3 Marks)***

OR

What is the concept of BYOD? Explain briefly.

Answer

(a) An **Information Security Policy** may be defined as any one of the following:

- In its basic form, an **Information Security Policy** is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business.
- An **Information Security Policy** should be in written form that provides a definition of Information Security, its overall objective and the importance that applies to all users. It provides instructions to employees about 'What kind of behavior or resource usage are required and acceptable', and about 'What is unacceptable'. An Information Security policy also provides direction to all employees about how to protect organization's information assets, and instructions regarding acceptable (and unacceptable) practices and behavior.
- An **Information Security Policy** may be defined as the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide.
- An **Information Security Policy** is defined as an essential foundation for an effective and comprehensive information security program. It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems.

Various types of Information Security Policies are as follows:

- **User Security Policies –** These include **User Security Policy** and **Acceptable Usage Policy**. The User Security Policy sets out the responsibilities and requirements for all IT system users and provides security terms of reference for Users, Line Managers and System Owners; whereas Acceptable Usage Policy sets out the policy for acceptable use of email, Internet services and other IT resources.

- **Organization Security Policies** – These include **Organizational Information Security Policy**, **Network & System Security Policy** and **Information Classification Policy**. An Organizational Information Security Policy is the main IT security policy document that sets out the Group policy for the security of its information assets and the IT systems processing this information. The Network & System Security Policy sets out detailed policy for system and network security and applies to IT department users whereas Information Classification Policy sets out the policy for the classification of information.
- **Conditions of Connection Policy-** This sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group and relates to the conditions that apply to different suppliers' systems.

Members of Security Policy

Information Security must encompass managerial, technological and legal aspects. The IS Policy broadly comprises the members from the three groups of management - **Management members** who have budget and policy authority; **Technical group** who know what can and cannot be supported, and **Legal experts** who know the legal ramifications of various policy charges.

(b) Characteristics of Platform as a Service (PaaS) are as follows:

- **All in One:** Most of the PaaS providers offer services like programming languages to develop, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).
- **Web access to the development platform:** PaaS provides web access to the development platform that helps the developers to create, modify, test and deploy different applications on the same platform.
- **Offline Access:** To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.
- **Built-in Scalability:** PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.
- **Collaborative Platform:** To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.
- **Diverse Client Tools:** PaaS providers offer a wide variety of client tools like Web User Interface (UI), Application Programming Interface (API) etc. to help the developers to choose the tool of their choice.

(c) The key components of Mobile Computing are as follows:

- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.
- **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network. The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.
- **Mobile Software:** Mobile Software is an actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is an essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

OR

BYOD (Bring Your Own Device): This refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours.

Advantages of BYOD are as follows:

- **Happy Employees**: Employees love to use their own devices when at work. This also reduces the number of devices an employee must carry; otherwise he would be carrying his personal as well as organization provided devices.
- **Lower IT budgets:** Could involve financial savings to the organization since employees would be using the devices they already possess; thus, reducing the outlay of the organization in providing devices to employees.
- **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.

- **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.
- **Increased employee efficiency**: The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.

BYOD Threats are as follows:

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network.
- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.
- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. Most employees' phones and smart devices connected to the corporate network are not protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding 'who is responsible for device security - the organization or the user'.
- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse.