SUGGESTED SOLUTION

FINAL MAY 2014 EXAM

INFORMATION SYSTEMS CONTROL AND AUDIT

Prelims (Test Code - F M J 4 0 4 8)

(Date : 10 April, 2014)

Head Office : Shraddha, 3rd Floor, Near Chinai College, Andheri (E), Mumbai – 69.
Tel : (022) 26836666

Ans. 1

(a) Conversion from existing information system to a new system involves the following activities:

- **i.** Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';
- **ii.** Performing data cleansing before data conversion;
- **iii.** Identifying the methods to assess the accuracy of conversion like record counts and control totals;
- **iv.** Designing exception reports showing the data which could not be converted through software; and
- **v.** Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) Types of Operations:

The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

- **i.** Document capture: Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- **ii.** Document Creation: This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- **iii.** Receipts and Distribution: This basically includes distribution of correspondence to designated recipients.
- **iv.** Filling, Search, Retrieval and Follow-up: This is related to filling, indexing, searching of documents, which takes up significant time.
- **v.** Calculations: These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- **vi.** Recording Utilization of Resources: This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

(c) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

- **i.** Business resumption planning – The Operation's piece of business continuity planning;
- **ii.** Disaster recovery planning – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.
- **iii.** Crisis Management – The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

(d) Procedure to apply for a license to issue electronic signature under Section 22, IT (Amendment) Act, 2008 is given follows:

1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

2. Every application for issue of a license shall be accompanied by

- **i.** a certification practice statement;
- **ii.** a statement including the procedure with respect to identification of the applicant;
- **iii.** payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; and
- **iv.** Such other documents, as may be prescribed by the Central Government.

Ans. 2

(a) Constraints in Operating a Computer Based MIS

Followings are the major constraints in operating computer based MIS.

1. **Non availability of experts:** It is always difficult to find/hire experts who can identify the information needs of organization for decision making process then design and implement an effective MIS as per this information need.
2. **Problem of selecting the sub-systems of MIS to be installed and operated upon:** Sometime it becomes a major constraint to select first sub-systems (i.e. marketing or finance or production) for which MIS can be installed and operated upon because failure in acceptance of first sub-system affects the acceptance for total system.
3. **No standardization of MIS:** Due to varied business objectives normally MIS is a non-standardized product i.e. each organization requires MIS as per its own needs. This causes a problem in designing, implementing and maintaining the MIS.
4. **Lack of co-operation from staff:** Change is a major problem i.e. normally staff resists for acceptance of computerized system. But this is not a big problem now-a-days and this can be handled by educating staff.
5. **High turnover of experts:** Information technology is an evaluating field and there is a high-turnover (job switching) of experts for better pay-packets, promotion, etc. which causes a problem in operating MIS effectively.
6. **Difficulty in quantifying the benefits of MIS:** MIS is an expense nature of application. And it is very difficult to quantify the benefits of information system because of intangible nature of information benefits.

(b) Incremental Approach Model

- This approach is a further extension of Traditional or Waterfall approach
- It is also known as combination of traditional and prototype approach
- In this approach, entire sequence of steps used in traditional approach is repeated again and again until the entire system development is completed.
- Prototype development uses an iterative process only for requirement analysis step whereas in this approach iterative process is used for entire sequence of steps.

Strengths:

- Potential exist for use of knowledge gained in the initial increment (iteration) as the later increments are developed
- More flexible and less costly
- Problems are resolved earlier in the project, in the initial iterations
- Better involvements of users for giving feedback etc.

Weakness:

- Includes series of mini waterfalls for development, which lack to look at system as whole or with completeness.
- Each phase of iteration should be well defined which is a difficult task.
- Integration of system developed during each iterative process may be difficult.
- May includes overlapping and redundancy in activities in different iterations

(c) System Testing

In a System Testing, the entire system including software, hardware and other system components are tested as a whole. System testing begins just before the implementation of either the entire system or certain subsets of system are ready for implementation. The purpose of system testing is to ensure that the new or modified system functions properly.

The system testing may include the following tests:

Recovery Testing:

This is to check that system developed is able to recover from any crashes, hardware failure and other problems. Recovery of system is supported by backup of data and components required for recovery.

Security Testing:

This testing is done to check whether implemented security features/controls are able to protects data and information. In this testing basic security features - confidentiality, integrity, authorization, authentication, availability and non-repudiation - are reviewed and tested.

Stress or Volume Testing:

Stress test checks the capacity of system to support data volume and numbers of users etc without decreasing the system performance. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.

Performance Testing:

In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

Ans. 3

(a) Data Privacy

We all know that personal data is collected and stored by organization such as banks, hospital and telecom companies, etc. and this data should not be disclosed and shared with others without prior permission of user whom this data belongs. Overall, data privacy is an important aspect and technically it refers to the relationship between technology and the legal rights to public expectation of data privacy. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form. The most common sources of data that are affected by data privacy issues are:

- Health information.
- Financial information.
- Genetic information.
- Location information.

The challenge in data privacy is to share data while protecting the personally identifiable information. Consider the example of health data which is collected in hospitals; it is standard practice to share this only in aggregate. The idea of sharing the data in aggregate is to ensure that only non-identifiable data are shared.

The legal protection of rights to privacy in general, and of data privacy in particular, varies greatly around the world.

Protecting data privacy in information systems: We all know increasingly the different information systems are interconnected; like connection of banking system with mobile companies system, etc. Therefore, data privacy is gaining importance to protect individual rights of information privacy. There are several technologies that address to privacy protection in enterprise IT systems. These falls into two categories: communication and enforcement.

1. **Policy Communication:** P3P is a protocol for privacy preferences known as Platform for Privacy Preferences. P3P is a standard which define what all information about individual can be disclosed or shared while communication between two information system.
2. **Policy Enforcement:** The policy enforcement of data privacy is performed with the help of various access control services such as XACML (extensible Access Control Markup Language), EPAL (Enterprise Privacy Authorization Language) and WS- Privacy, etc

(b) The Auditor shall document a preliminary understanding of the Entity's IS controls, including the organization, staffing, responsibilities, authorities, and resources of the Entity's security management function. He shall include the following matters to the extent relevant to the audit objectives –

1. Identification of entity-wide level controls (and appropriate system level controls) designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and implemented (placed in operation), including identification of control objectives of control activities for which there are no or ineffective controls at the entity-wide level and the related risks,
2. Identification of business process level controls for key applications identified as key areas of audit interest, determination of where those controls are implemented (placed in operation) within the Entity's systems, and the Auditor's conclusion about whether the controls are designed effectively, including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data,
3. Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g. Penetration Tests, Disaster Recovery Tests, and Application-Specific Tests) performed during the last year,
4. Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS weaknesses and IS control weaknesses,
5. Status of the prior years' audit findings,

6. Documentation for any significant computer security related incidents identified and reported for the last year,
7. Documented Security Plans,
8. Documented risk assessments for relevant systems (e.g. general support systems and major applications),
9. System Certification and Accreditation documentation or equivalent for relevant systems,
10. Documented Business Continuity Plans and Disaster Recovery Plans,
11. A description of the Entity's use of third-party IT services,
12. Relevant Laws and Regulations and their relation to the audit objectives,
13. Description of the Auditor's procedures to consider the risk of fraud risk factors that the Auditor believes could affect the audit objectives, and planned audit procedures to detect any fraud significant to the audit objectives.
14. Audit resources planned.
15. Current multiyear testing plans.
16. Documentation of communications with entity management.
17. If IS controls are performed by Service Organizations, conclusions whether such controls are significant to the audit Objectives and any audit procedures performed with respect to such controls (e.g. review of Service Auditor Reports)
18. If the Auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
19. Audit plan that adequately describes the objectives, scope, and methodology of the audit.
20. Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

(c)

1. **Inherent Risk:** Every business has its inherent risk, i.e. the cost of running the business. In case of a technology driven business, the risks induced by technology failure is a part of the Operating Risk.

2. **Risk Acceptance:** Risk Acceptance Level refers to the issue of how much of the risk is acceptable, and what should be the price that the Firm would pay to reduce a certain part of the risk.

3. **Risk Appetite:** Risk Appetite of the organisation refers to the Management policy as to whether it wants to be **risk aggressive or risk averter.** Such comparison should be made within the framework of the industry, for ensuring usage of a consistent and relevant yardstick. For example, the risk appetite of a risk-aggressive Bank may be lower than that of a risk-averse Foreign Exchange Dealer.

4. **Risk Measurement:** For proper and effective risk management, the organisation should develop a process of risk and exposure measurement, preferably in numerical terms.

Ans. 4

(a) The **methodology** of developing a BCP, emphasises on the following aspects –

1. Providing Management with a comprehensive understanding of the **total efforts required** to develop and maintain an effective recovery plan,
2. Obtaining commitment from appropriate management to **support and participate** in the effort,
3. Defining recovery requirements from the perspective of **business functions,**
4. **Documenting** the impact of an extended loss to operations and also to key business functions, i.e. by way of Business Impact Analysis,
5. Focussing appropriately on **disaster prevention and impact minimisation,** as well as orderly recovery,
6. Selecting **Business Continuity Teams,** that ensure the proper balance required for plan development,
7. Involvement of Operations Managers and Key Employees in the development of the Plan,
8. Developing a Business Continuity Plan that is **understandable, easy to use and maintain,**
9. Listing of **assumptions** that are realistic and reasonable,
10. **Identification of Resources** that will be needed for recovery, and the location of their availability, and

11. Defining how business continuity considerations must be **integrated** into ongoing business planning and system development processes, to ensure that the plan remains viable over time.

(b) Risk and Governance Issues in ERP:

Migration to real-time and integrated ERP system, from old system, is not an easy process. It also involves many risks and governance issues; such as:

1. **Single Point Failure:** ERP provides an integrated system in the organization which is managed by a single ERP application (software). Failure of ERP application/main-server may bring down the working of entire organization's information system.
2. **Change Management:** ERP implementation is not only an implementation of a computer based integrated system; it require changes in existing processes, culture and working methods of organizations' staff/stakeholders. And adapting to new processes, culture and working method for staff is always a big challenge.
3. **Structural Changes:** Not only the implementation of ERP requires change in processes and working methods; it also requires the structural changes (re-arrangement of departments) in the organization through BPR to achieve the best practices.
4. **Job Profile Changes:** The change management and structural changes may need the change in job profiles of the staff from existing job profiles. This is also a very big risk and governance issue, as staff normally resist for change in their job profiles.
5. **On-line and Real-time System:** ERP provides an on-line and real-time data processing system which requires a continuous maintenance capability, and also requires a quick response to any system problems and new requirements. Maintaining such capabilities is always a big challenge for the organizations.
6. **Distributed Computing:** ERP provides a distributed data processing system, which helps to process data from anywhere. Inexperience with distributed computing implementation and management also put forward a big challenge.
7. **Dependence on External Assistance:** Previously, organizations used to manage information system through internal support only. But ERP management requires the support of external assistance and that may expose for security and resource management risks to organizations data and resources.
8. **Program Interfaces and Data Conversions:** ERP requires extensive interfaces with other systems (like banks, tax authorities, customers and suppliers' systems), and it also requires extensive data conversion from old (legacy) system. These tasks always pose a big challenge to organizations.
9. **Audit expertise:** ERP environment require expertise to implement the controls and audit those controls.
10. **Single sign on:** A single sign-in to ERP system provides access to multiple modules and applications which create a security problem to the organizations.
11. **Data Content Quality:** ERP system requires the data inputs from multiple external data sources like customers, suppliers and banks. This may affect the data quality in the system.
12. **Privacy and Confidentiality:** There is risk of disclosure of personnel information to greater extent as ERP systems are connected with multiple external data sources.

(c)

1. **Meaning:** Single Point of Failure refers to a single/ particular aspect of IT environment, that causes a disaster / disruption to the entire system. The objective is to identify any single point of failure within the Firm's infrastructure, in particular, the information technology infrastructure.

2. **Example:** The Telecommunication Infrastructure is an example of single point of failure. While the resiliency of network and the mean average failures Of communication devices, e.g. routers, have improved, it is still a single point of failure in a Firm that may lead to disaster being declared.

3. **Causes:** Single point of failure have increased significantly due to - (a) the continued growth and complexity in the Firm's IS environment, (b) changes in technology, and (c) customer's demands for new channels in the delivery of service and/or products, e,g. e-Commerce.

4. **Action Points:**
   i. To identify single point of failures within the Firm's IS architecture at the earliest possible stage, **a technology risk assessment** should be performed in every project.
   ii. Firms can respond to increase in the exposure from single point of failure, by implementing appropriate **risk mitigation strategies.**

Ans. 5

(a) BPR (Business Process Reengineering) is redesign (Reinvention) of business process to achieve dramatic improvements in business processes in terms of cost, quality, service and speed. BPR can be used for any function of organization like marketing, finance, personnel and production etc. It helps to achieve high performance processes (here processes mean methods of doing tasks).

An efficient or high performance Finance and Accounting department includes various tasks like data preparation, data entry, report generation etc for managing finance and accounts at enterprise level and in an integrated manner.

BPR can undertake the following important steps to improve the functioning of finance and accounting department

Analyze and Design Existing Finance and Accounts Department Functioning:

- Analyze the existing processes i.e. how data is prepared, how data is entered into the system, who all are responsible for data authorization and entry, and how data is maintained etc.
- Draw a process diagram or design of existing finance and accounting department functioning
- Includes locations and types of data models (databases) maintained in the design of existing finance department working.

Redesign the Finance and Accounts Department functioning by using Principles of BPR:

- Redesign the processes of existing department to avoid duplicity in data preparation and entry etc, i.e. any data will be prepared and entered once only. For example, in the cash withdrawal process of banks all the related books are updated automatically once a transaction is entered in the system.
- Develop a perfect coordination between multiple processes to achieve high performance processes. This can be scheduling for data preparation, data checking, data authorization and data entry to avoid delay.
- Develop an integrated database or common database which is the key step to achieve high performance functioning
- Use high performance data entry, processing and report generation devices such as high speed printers, high performance CPUs or servers etc to achieve speedy data processing
- Use data communication and networks (client / server system) to marinating finance and accounts in an integrated manner at consolidated level or at enterprise level.

(b) The features of Level 2, i.e. **Repeatable Level** are as under –

1. **Policies and Procedures:**
   i. At the Repeatable Level, policies for managing a software project and procedures to implement those policies are established.
   ii. Planning and managing new projects is based on experience with similar projects.
   iii. The organizational requirement for achieving Level 2 is that there are policies that guide the projects in establishing the appropriate management processes.
2. **Repeatable Processes:** In Level 2, the process is at least documented sufficiently such that repeating the same steps may be attempted, possibly with consistent results.
3. **Process Discipline:** Process Discipline is less rigorous, but where it exists, it may help to ensure that existing processes are maintained during times of stress.
4. **Software Process Capability:**
   i. Process Capability is enhanced by establishing basic process management discipline on a project-by-project basis.
   ii. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. Processes may differ between projects in a Level 2 organization.
   iii. The Software Process Capability of Level 2 Firms can be considered as **disciplined,** because planning and tracking of the software project is stable and earlier successes can be repeated.

5. **Controls:**
   - **i.** Projects in Level 2 organizations have installed basic software management controls.
   - **ii.** The project's process is under the effective control of a Project Management System, following realistic plans based on the performance of previous projects.
   - **iii.** The Software Project Team works with its sub-contractors, if any, to establish a Customer-Supplier relationship.

6. **Time Schedule:**
   - **i.** Realistic project commitments are based on the results observed on previous projects and on the requirements of the current project.
   - **ii.** Software Managers for a project track software costs, schedules, and functionality. So, any problems in meeting commitments are identified when they arise.
   - **iii.** Software requirements and the work products developed to satisfy them are baselined, and their integrity is controlled. Software Project Standards are defined, and the organization ensures they are faithfully followed.

(c)

1. **Controls are pervasive:** Every Firm that uses IT, uses a set of controls, sometimes even unconsciously, even if the "controls" are to let everyone have full access.
2. **Firm Specific Controls:** An ideal set of controls for any given Firm should depend on the business objectives, budget, personality, and context of that Firm.
3. **Control Objectives are common:** The set of control objectives, (as opposed to the set of controls) can and should be constant across Firms.
4. **Same Control Framework:** Each Firm could use the **same** control framework to manage their particular controls, in order to meet those constant control objectives.

Ans. 6

(a) The following points should be considered before implementing or deciding upon the measures of protection –

1. **Value of Data:** All data does not have the same value. Also, all information is not sensitive. Hence, information may be handled and protected differently. The value of the different types of information in the entire system must be determined before planning for the appropriate levels of protection.
2. **Area of Criticality / Sensitiveness:** The Firm should know where the critical data resides. The Firm's Information Systems Infrastructure is one area where all information are sensitive. In a network environment, sensitive information can be accessed by many people located at different areas. Each piece of information require different levels of protection, hence their area(s) must be located, so that an integrated security solution is established.
3. **Worthiness:** The worthiness of the information must be known before implementation. The cost of the information should not exceed the cost of the solutions. Protection solutions must be based on the most valuable information assets.
4. **Choice of Integrated Solutions:** Integrated Solutions are cost effective, since spending does not exceed the costs of individual information.
5. **Access control:** When information is inadvertently damaged, or disclosed or copied without the owner's knowledge, it may lead to damage and financial loss. Firms must establish access control methodology extending from the host to the network. Access of important data and the associated auditing should extend to the file level. Access should be restricted and also authorised.
6. **Storage of information:** The place of storage of information should be considered, particularly if information is stored in electronic media like floppy disks, CD-ROMS, magnetic media, etc. Also, when migrating information from one platform to another, care should be taken to control the status of hard drives and the associated data.
7. **Employee review:** Employees must be asked to keep a record of their daily work which should be reviewed daily. All initial and final drafts, working papers, other important details, etc. should be safeguarded and not allowed to be put in trash or recycle. There should be adequate facilities to monitor generation of important information by employees and its safety.
8. **Documentation on paper:** Some information requires to be documented even if it exists in an electronic form. Also some information can exist only in the paper documents. It is easier to defraud information held on papers. Measures to properly protect such information on paper must also be considered. If need be, they may be converted to electronic form for accessing, while the paper is put under tight security.

(b)

1. **Electronic Form [Sec. 2(1)(r)]:** Electronic form, with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device.

2. **Electronic Record [Sec. 2(1)(t)]:** Electronic Record means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.

3. **Retention of Electronic Records [Sec. 7]:** Sec.7 provides that the documents, records or information, which has to be retained under any statute for any specified period, shall be deemed to have been retained, if the same is retained in the electronic form. Electronic records are acceptable if the following conditions are satisfied –
   - **i.** Accessibility: The information therein remains accessible so as to be usable subsequently,
   - **ii.** Originality: The electronic record is retained in its original format or in a format which accurately represents the information contained,
   - **iii.** Identity: The details which will facilitate the identification of the origin, destination, dates and time of despatch or receipt of such electronic record are available therein.

4. **Exclusions:** However, this section does not apply to –
   - **i.** Any information, which is automatically generated solely for the purpose of enabling all electronic record to be despatched or received.
   - **ii.** Any law that expressly provides for the retention of documents, records or information in the form of electronic records.

5. **Facility only, not a right [Sec. 9]:** No person can insist that - (a) any Ministry or Department of the Central or State Government, or (b) any statutory Authority or Body or any Authority, or (c) Body controlled or funded by the Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

6. **Audit of e-records:** Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.

(c) Computers have made it possible to carry out processing which would have been either too difficult or too much time- consuming or even impossible to do manually. The reasons for using computers in business data processing are –

1. Handling **huge volume of data**, that is not manageable by human efforts.
2. **Storing** enormous volume of data for indefinite period without any decay.
3. **Quick and accurate** processing of data to match the competitive environment.
4. **Easy retrieval** of information on query.
5. Quick and efficient **transportation of data / information** to distant places almost at no cost.
6. Availability of software **tools** for quick decision making in a complex situation.
7. Generating **simple output** from complex Input, and multiple output with simple input.
8. **Better cost-performance ratio** with use of IT in business function, rather than the labour intensive manual system.

Ans. 7

(a) Difference between TPS and EIS

Traditional Information System (or TPS)	**Executive Information System (or EIS)**
Used by lower level of management	Used by top level of management
Provide routine information or status information	Provide information about problems and opportunities
Normally provide offline information	Provide online tools and information
Provide information based on internal sources only	Provide information based on based both internal and external sources
Drill down reporting is not available	Drill down reporting is available
Simple interface for computer operators	Highly user-friendly graphical interface

(b) Advantages of using SDLC:

The SDLC can also be viewed as systematic process oriented system development framework. The advantages of using systematic steps or SDLC are as follows:

- Better planning and control by project managers.
- Compliance to prescribed standards ensuring better quality.
- Documentation that SDLC stresses on is an important measure of communication and Control.
- The phases are important milestones and help project manager and users for review and signoff.

Advantages of using SDLC from Audit Perspective:

An IS Auditor can gain the following possible advantages, if SDLC framework is used for system development.

- The IS auditor can have clear understanding of the various phases/steps of system development if the SDLC is used
- The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
- If IS Auditor has technical knowledge and capability in the area of SDLC, auditor can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used for various development phases of the SDLC

(c) The Report Controls are –

1. **Standing Data / Internal Tables:**
   - **i.** Application Programs use many internal tables to perform various functions, e.g. Gross Pay Calculation, Billing Calculation based on a Price Table, Bank Int. Calculation, etc.
   - **ii.** Maintaining integrity of these Internal Tables, i.e. Pay Rate Table, Price Table and Interest Table, etc. is important, since any changes or errors in these tables would have an adverse effect on the organizations basic functions.
   - **iii.** Periodic monitoring of these Internal Tables by manual check or by calculating a control total is mandatory
2. **Print Run-to-Run Control Totals:** Run-to-Run Control Totals help in identifying errors or irregularities like record dropped erroneously from a Transaction File, working sequence of updating or the application software processing errors.
3. **Print Suspense Account Entries:** Similar to the Update Controls, the Suspense Account entries are to be periodically monitored with the respective Error File, and action should be taken on time.
4. **Existence / Recovery Controls:**
   - **i.** Backup and Recovery Strategies together encompass the controls required to restore failure in a Database.
   - **ii.** Backup Strategies are implemented using prior version and log of transactions or changes to the Database.
   - **iii.** Recovery Strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

(d) Operating System Review

In this auditor review the procurement, implementation, execution and maintenance of system Software such as operating system in terms of;

- Review the approval process of software selection
- Review cost/benefit analysis of system software procurement
- Review controls over the installation of system software
- Review systems documentation specifically in the areas of:
  - Operating documents
  - Maintenance documents
  - Users instructions, etc

- Review and test systems software implementation to determine adequacy of controls in:
  - Authorization procedures
  - Access security features
  - Documentation requirements

- Documentation of system testing
- Audit trails
- Review system software security procedures, etc

(e)

Point	Threat	Vulnerability
Meaning	Threat is any entity, circumstance or event, with the potential to harm the software system or components thereof, through its unauthorized access, destruction, modification, and/or denial of service	Vulnerability is the weakness in the system security that exposes the system to threats, and can be exploited by the Attackers.
Source / Types	Threats may be classified into - (a) physical / environmental, or (b) man-made, either internally or externally.	Vulnerabilities originate / arise from - (i) flaws on the software's design, (ii) defects in its implementation, or (iii) problems in its operation. .
Relation-ship	Threats occur because of vulnerabilities associated with use of information resources.	Vulnerabilities provide open doors to threats, leading to harm.
Examples	(a) Errors, (b) Malicious Damage/Attack, (c) Fraud, (d) Theft, and (e) Equipment / Software Failure.	(a) Lack of User Knowledge, (b) Lack of Security Functionality, (c) Poor Choice of Passwords, (d) Untested Technology, and (e) Transmission over unprotected communication medium.

MARKS ALLOCATION SHEET

Que. No.	*Sub point No.(if any)*	*Name of Chapter*	*Description of Concept*	*Mark Allocation*	*Total Marks*
1	(a)	Case study (IT Act & BCP)	Each point have 1 mark	5	5
1	(b)	Case study (IT Act & BCP)	Each point have 1 mark (any five point)	5	5
1	(c)	Case study (IT Act & BCP)	Meaning of BCP	2	
1	(c)	Case study (IT Act & BCP)	Areas covers in BCP	3	5
1	(d)	Case study (IT Act & BCP)	Point (1)	1	
1	(d)	Case study (IT Act & BCP)	Point (2)	4	5
2(a)	-	Is concepts	Each point have 1 mark	6	6
2(b)	-	SDLC	Explanation of incremental approach model	2	
2(b)	-	SDLC	Strengths	2	
2(b)	-	SDLC	Weakness	2	6
2(c)	-	SDLC	Each point have 1 mark	4	4
3(a)	-	Control objectives	Explanation	6	6
3(b)	-	Testing – general & automated controls	Each point have 0.5 marks (any 12 points)	6	6
3(c)	-	Risk Management methodologies	Each point have 1 mark	4	5
4(a)	-	BCP & DRP	Each point have 1 mark (any six point)	6	6
4(b)	-	Overview of ERP	Each point have 1 mark (any six point)	6	6
4(c)	-	BCP & DRP	Each point have 1 mark	4	4
5(a)	-	Overview of ERP	Explain BPR analyse & design excising & A/cs department functioning	1.5	
5(a)	-	Overview of ERP	Redesign finance & A/cs department functioning by using BPR	2.5	6
5(b)	-	IS guidelines	Each point have 1 mark	6	6
5(c)	-	IS guidelines	Each point have 1 mark	4	4
6(a)	-	IS security & Audit	Each point have 1 mark (any six point)	6	6
6(b)	-	IT Act	Each point have 1 mark	6	6
6(c)	-	IS Concepts	Each point have 1 mark (any four point)	4	4
7(a)	-	IS Concepts	Each difference have 1 mark (any four)	4	4
7(b)	-	SDLC	Advantages of using SDLC (each have 0.5 mark)	2	
7(b)	-	SDLC	Advantages of using SDLC from Audit perspective (each have 0.5 mark)	2	4
7(c)	-	IS control	Each point have 1 mark	4	4
7(d)	-	Testing – general & automated controls	Each point have 1 mark (any four point)	4	4
7(e)	-	Risk Management methodologies	Each difference have 1 mark	4	4