Solved

Scanner

Appendix

CA Final Gr. II

(Solution of November - 2014)

Paper - 6: **Information Systems Control and Audit**

Chapter - 1 : Concepts of Governance and Management of Information Systems

2014 - Nov [3] (c)

IT Governance:

It is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs.

- IT Governance focuses specifically on information technology systems.
- IT focuses on IT system performance and risk management.
- The primary goals of IT Governance are to assure that the investments in IT generate business value and it helps to mitigate the risks associated with IT.

Benefits of IT Governance:

⇒ Enhanced value for enterprise from use of IT.
⇒ Better user satisfaction with IT services.
⇒ Increased performance of IT or better returns on IT investment.
⇒ Improved management and mitigation of IT related risks.
⇒ More optimal utilization of IT resources.
⇒ IT contributes for improved business transperancy.

2014 - Nov [4] (b)

Key Management Practices of Risk Management:

1 **Collect data:** Identify and collect relevant related to the risks.
2. **Analyze Risk:** From the collected data, analyze risks taking into account impact on business for identified risks.

3. **Maintain a Risk Profile:** Maintain information for known risks and risk attributes. This includes expected frequency, potential impact and responses, and other related capabilities and controls activities for risks.
4. **Articulate Risks:** This requires providing information on the existing state of IT- related risks and existing state of controls to stakeholders.
5. **Define a Risk Management Action Portfolio:** This requires risk management policy or action statements from management on management risks to acceptable level considering opportunities and impacts for business .
6. **Respond to Risk:** This requires controls and actions for responding to risks in a timely and effective manner to limit the magnitude of loss from IT related risks.

2014 - Nov [7] (b), (c)

(b) Internal Controls as per COSO :

1. **Control Environment :**For each business process such as purchase, sale, new investment, making payment etc. organization should develop and maintain a control environment. This includes specifying criticalness and material importance of each business process plus specifying the owners of the business processes.
2. **Risk Assessment :**Each business process comes with various risks. A control environment must include on assessment of the risks associated with each business process.
3. **Control Activities :** Control activities must be developed to manage, mitigate and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.
4. Information and Communication :The control activities should be properly communicated to people managing processes.
5. **Monitoring :** The internal control processes must be continuously monitored with modifications made as warranted by changing conditions.

(c) Risk:

- Risk is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks.
- These risks lead to a gap between the need to protect system and the degree of protection applied.

- Some of the factors that cause gaps are widespread use of technology, interconnectivity of systems and devolution of management and control etc.

Vulnerability:

- It is the weakness in the system safeguards that exposes the system to threats.
- It may be weakness in an information system cryptographic system, internal controls etc., that could be exploited by a threat.
- Vulnerabilities potentially "allow" a threat to harm or exploit the system.

Threat:

- A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organisation.
- Threat is any circumstances or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services.

Chapter - 2 : Information Systems Concepts

2014 - Nov [3] (a)

Following are the IT tools crucial for carrying out day to day functions like sales, advertisement, purchase, management reports etc.:

Operation Support Systems:

1. **Transaction Processing System (TPS):** This system processes the transactions and provides the routine and regular reports/information. This system primarily automates those routine processes, which are used to support day to day business operations. TPS acts as a base to almost all other types of information systems. TPS accepts data as inputs and provides information (processed data) as outputs. For example, accepts transactions (i.e. sale, purchase, receipt, payment etc.) as inputs and provides routine and regular reports (i.e. balance sheet, trail balance etc.) as outputs. The components of TPS are:
   — Inputs
   — Processing
   — Storage
   — Outputs
2. **Process Control System (PCS):** In this type of system, computer is used to control ongoing physical processes. The computers are designed to automatically make decisions. Which adjust the physical production process. For example - automation of assembly lines of factories with robotics and computer controlled machines.

3. **Enterprise Collaboration Systems (ECSs):** These systems use a variety of technologies to help people work together in an integrated manner. ERP is a kind of ECS system.

2014 - Nov [5] (b)

Expert System (ES) : An expert system, also called a knowledge-based system, is an artificial intelligence system that applies reasoning capabilities to reach a conclusion. Expert systems are excellent for diagnostic and prescriptive problems. Diagnostic problems are those requiring an answer to the question, "What's wrong?" and correspond to the intelligence phase of decision making. Prescriptive problems are those that require an answer to the question, "What to do?" and correspond to the choice phase of decision making.

The properties that potential application should possess to quality for an expert system is as under:

1. **Expertise:** Solutions to the problem require the efforts of experts i.e. people who possess the knowledge, techniques and intution needed for problem-solving.
2. **Availability:** One or more experts who are capable of communicating how they approach a problem and solve it should be available.
3. **Domain:** The Domain or subject area of the problem should be relatively small and limited to a relatively well-defined problem area.
4. **Complexity:** Solution of the problems for which the expert system will be used is complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
5. **Structure:** The solution process must be able to cope with ill-structured, uncertain, missing and conflicting data and a dynamic problem-solving situation.

Chapter - 3 : Protection of Information Systems

2014 - Nov [5] (c)

Threats Due to Cyber Crime

- Cyber crime is general nomenclature for 'Electronic Offences' and it becoming more and more visible due to increasing use of computer network and internet and frauds thereof.
- Generally computerized environmental is dependent on people. Though they play a critical role in success of an enterprise computing, it is a fact that threats always exist due to cyber crimes committed by people.

- The special skill sets of IT operational team, programmers; data administrator, etc are key links in ensuring that the IT infrastructure delivers output as per user requirements.
- At the same time, social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise.
- Threats also arise on account of dependence on external agencies. IT computing services are significantly dependant on various vendors and service providers for equipment supply and support, consumables, systems and program maintenance air-conditioning, hot-site providers, utilities, etc.

Some of the common cyber crimes are:

1. **Embezzlement:** It is unlawful misappropriation of money or other things of value by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.

   Fraud : It occurs on account of intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.
2. **Denial of Service:** Not allowing organization to provide services to authorized users. This may either be due to external infrastructure organization on which organization services depends e.g. Reliance not allowing Tata Indicom to transfer their call on their network or it be may due to attacks such as IP Spoofing, ping attacks, port scanning problems etc from cyber criminals.
3. **Theft of proprietary information:** It is the illegal obtaining of designs, plans blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
4. **Vandalism or sabotage:** It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
5. **Computer Virus:** Viruses are destructive programs which can affect other programs in computer and some time result in big losses to organization in terms of loss of productivity and continuity of business etc.
6. **Other:** Threat includes several other cases such as intrusions, breaches and compromises of the respondent's computer networks (such as hacking of sniffing) regardless of whether damage or loss were sustained as a result.

Chapter - 4 : Business Continuity Planning and Disaster Recovery Planning

2014 - Nov [5] (a) **The matters to be verified in an audit or self assessment of the BCM Program of an enterprise is as under:**

- → Find out whether a disaster recovery/ business resumption plan exist or not, if it exists then was this developed using a reliable/ sound methodology.
- → Determine whether the recommendations made in the study were implemented or not.
- → Determine the sufficiency of backup procedures of DRP.
- → Review the resources availability under back up procedures.
- → Review and observe a telecommunication network working and appropriateness of other components.
- → Review about the resources being available are latest/updated or not.
- → Determine that BCP/DRP reflects the current IT setup.
- → Determine plan includes listing of IT assets with priority /importance.
- → Review the test plan and also verify the extent to which DRP has been tested.
- → Obtain and review the actual test results.
- → Check DRP. Consider the disruption of transport facilities such that the employees cannot reach to work due to this disruption and what plans are there to tackle this.
- → Review who all participated in BIA study and DRP preparation in terms of their experience, qualification etc.
- → Determine DRP. Include name of personnel and others responsible with their telephone numbers.
- → Determine that BCP/DRP covers the administrative procedures for handling disasters.
- → Determine that BCP/DRP covers procedures for declaration of disaster and general shutdown and other related events which can affect operation.

2014 - Nov [6] (c)

Key Objective of BCP

The key objectives of the BCP should be to :

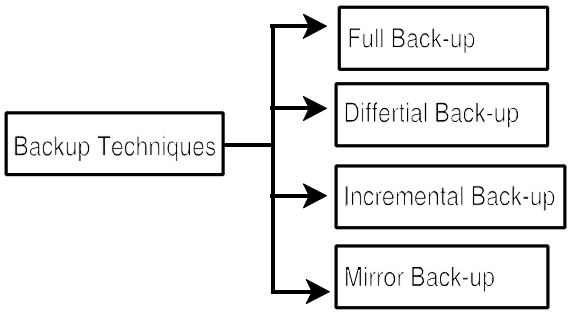
(i) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources).
(ii) Minimise immediate damage and losses.
(iii) Continue critical business operations.

(iv) Provide for the safety and well-being of people on the premises at the time of disaster.
(v) Establish management succession and emergency powers.
(vi) Facilitate effective co-ordination of recovery tasks.
(vii) Reduce the complexity of the recovery effort.
(viii) Identify critical lines of business and supporting functions.

2014 - Nov [7] [d]

Various Types of Systems Back-up

- Back-up of software and data is an important feature to avoid potential of service disruption and economic losses from various disasters.
- When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.
- There are various types of back-up:



Types of backups	Descriptions
1. Full Back-up	• This is the simplest but time and space consuming back-up technique. • In this type of back-up, all the files are entirely backed-up during each backup process • Every back-up generation contains every file in the back-up set. However, the amount of time and space such a back-up takes prevents it from being a realistic proposition for backing up a large amount of data. • This is the simplest form of back-up with a single restoring session for restoring all backed-up files.

2. Differential Back-up

- In this back-up, those files are backed up which have changed since last full back-up.
- This is in contrast to incremental back-up generation, which holds all the files that were modified since the last full or incremental back-up.
- It is faster and more economical in using the back-up space, as only the flies that have changed since the last full back-up are saved.
- Restoring files from this type of backup is a two step process :
  1. Restore from last full back-up.
  2. Restore from appropriate differential back-up.

3. Incremental Back-up

- This back-up is considered the most efficient and economical back-up technique in this the files which changed from last back-up whether as full or differential back or incremental back-up.
- This is the most economical method, as only the files that changed since the last back-up are backed up. This saves a lot of back-up time and space.
- Restoring from this type of back-up is difficult, first last back-up files are restored and then incrementally all other files are restored.

4. Mirror Back-up

- A mirror back-up is exact copy of files.
- This type of back-up is identical to full back-up, but difference is that the files are not stored in zip format and can not be protected with password.
- A mirror back-up is most frequently used to create an exact copy of the back-up data.

Chapter - 5 : Acquisition, Development and Implementation of Information Systems

2014 - Nov [1] {C} (a), (b), (c), (d)

(a) Data Integrity Policies:

The major data integrity policies I would suggest is as under:

1. **Virus-Signature Updating:** Virus signatures must be updated immediately when they are made available from vendor.
2. **Software Testing:** All software must be tested in a suitable test environment before installation on production system.

3. **Environment:** The division of environments into development, test and production is required for critical systems.
4. **Version Zero Software:** Version Zero Software must be avoided whenever possible, to avoid undiscovered bugs.
5. **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
6. **Period-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes.
7. **Disaster Recovery:** A Comprehensive Disaster Recovery Plan must be used to ensure continuity of the corporate business in the event of an outage.

(b) Aspects of Unit Testing:

The categories of tests that a programmer typically performs on a program unit are as under:

1. **Functional tests:** Functional tests check whether programs do what they are supposed to do or not. The test plan specifies operating conditions, input values and expected results, and as per this plan, the programmer checks by inputing the values to see whether the actual result and expected result match.
2. **Performance tests:** Performance tests are designed to verify (a) the response time (b) the execution time (c) the throughput, primary and secondary memory utilisation (d) traffic rates on data channels and communication lines.
3. **Stress tests:** Stress testing is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program.
4. **Structural tests:** Structural tests are concerned with examining the internal processing logic of a software system. For example if a function is responsible for tax calculation, the verification of the logic is a structural test.
5. **Parallel tests:** In parallel tests, the same test data is used in the new and old system and the output results are then compared.

(c) Critical Controls in Computerized Environment:

Critical control considerations in a computerized environment are:

- ⇒ Lack of management understanding of IS Risks and lack of necessary IS and related controls.
- ⇒ Absence or inadequate IS control framework.
- ⇒ Absence of or weak general controls and IS controls.
- ⇒ Lack of awareness and knowledge of IS Risks and controls amongst the Business Users and even IT staff.
- ⇒ Complexity of implementation of controls in distributed computing environments and extended enterprises.
- ⇒ Lack of control features of their implementation in highly technology driven environments.
- ⇒ Inappropriate technology implementations or inadequate security functionality in technologies implemented.

(d) Green Computing is related to responsible use of computers and related resources. The recommendations for efficient use of computer and IT resources to achieve the objectives of Green Computing are as follows:

- — Power down the CPU and all peripherals during extended periods of inactivity.
- — Use notebook computers rather than desktop computers whenever possible.
- — Power-up and power-down energy-intensive peripherals such as laser printers according to need.
- — Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- — Use auto power management features to turn off hard drives and displays after several minutes of inactivity.
- — Try to do computer-related tasks during continuous or contiguous and intensive blocks of time leaving hardware off at other times.
- — Minimize the use of paper and properly recycle waste paper.
- — Dispose of e-waste according to central, state & local regulations.
- — Employ alternative energy sources for computing workstations, servers, networks and data centers. Google buys mostly renewable power for it's data center working.

2014 - Nov [6] (b)

Agile Model: Agile software movement provides a conceptual framework for undertaking software engineering projects. Agile methods attempt to minimize risk by developing software in short time boxes called Iterations.

Each Iteration is like a miniature software project of its own and includes all the tasks necessary to release the mini-increment of new functionality i.e. planning, requirements analysis, design, coding testing and documentation. Agile Methodologies advocate the principle "Build short, Build often"so the given project is broken upto into sub-projects and each sub-project is developed and integrated into the already delivered system. Hence, the customer gets continuous delivery of useful and usable systems.

⇒ **Strengths of Agile Model:**

1. Software Development being essentially a human activity, will always have variations in processes and inputs. The Agile Model is flexible enough to handle these variations.
2. When the entire set of software requirements are not known at the beginning of the project or they keep on changing, Agile Methods can handle this dynamism by avoiding wastage of effort or ensuring that the final product meets the customer's needs.

2014 - Nov [7] (e)

Activities involved in the design of a database:

1. **Conceptual Modeling**: These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.
2. **Storage Structure Design**: Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example-tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.
3. **Data Modeling**: Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages.
4. **Physical Layout Design**: Decisions must be made on how to distribute the storage structure across specific storage media and locations for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

Chapter - 6 : Auditing of Information Systems

2014 - Nov [2] (c)

Risks to be reviewed relating to IT systems and processes as part of audit functions are as follows:

— It is required to check whether information security is adequate?
— Auditor review and check whether IT resources are efficiently utilized?
— Review and check IT related frauds.
— Review and check whether organizations have adequate IT related policies.
— Review and check whether system development and maintenance process is controlled processes or not?

2014 - Nov [3] (b)

General risks related to the use of PC's in the business of Mr. X are:

— PC can be easily shifted from one place to another, because they are smaller in size.
— User can easily log-in into PC, normally provides low level of security controls.
— Data in PC can be easily copied on pen drive.
— PC applications are easy to use and provide low access control.
— PC is prone to virus.

Following are the security measures to overcome them:

— Proper logging of equipments shifting must be done.
— Physical locking can be done for PC.
— Data in hard disk should be protected by using some specialized software.
— There should be proper virus protection software.
— There should be control that PC can be booted from hard disk only.
— There should be proper back up of data maintained in PC.

2014 - Nov [4] (a) **The output controls required to be reviewed with respect to application controls are as under:**

→ Maintaining log of output programs execution to know the details of communicated outputs.

→ **Spooling/Queue medication control:** Controls should be there on spooling / queue section to avoid unauthorized access of these sections. You might have experienced that many jobs to a single printer from multiple users get arranged in a queue and that queue is known as spooling section.

- **Controls over printing:** Selection of printer should be such that disclosure of confidential information should be avoided.
- Report Distribution to authorized users should be in a secured form.
- Secured information maintenance of sensitive printed output forms/ records.

2014 - Nov [6] (a) **Issues which affect financial control audit:**

Authorization: This involves obtaining the authority to perform some act, e.g. access to assets, passing accounting or application entries.

Cancellation of Documents : This makes a document in such a way to prevent its re-use. Example: Control over invoice marking them with a 'paid' or 'processed' stamp or punching a hole in the document.

Documentation : This includes written or typed explanations of action taken on specific transactions. It also refers to written or typed instructions, which explain the performance of risks.

Input/output verification: This involves comparing information provided by a computer system with input documents.

Safe keeping: This involves physically securing assets like computer disks, under lock and key in a desk drawer etc.

Segregation of duties: This involves assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check of the other persons work.

Sequentially numbered documents : These are working documents with pre-printed sequential numbers, which enables the detection of missing documents.

2014 - Nov [7] (a)

Operating System Security : The following security features are part of operating systems for a controlled operation of computer system:

1. **Login procedure :** This is the key security features provided by operating system which helps to prevent unauthorized access. It allows any authorized users to access the computer system by validating user's ID and password.
2. **Access Token :** If user's login is successful then operating system creates access token that contain key information about users such as ID, Password, user group and access rights granted to user.
3. **Access Control List :** Access to resources like printers, files, directories etc. are controlled by access control list. This list is attached to these resources and when a user wants to access any of these resources then operating system matches user ID and rights to user as per user's access token information and allows access of resources accordingly.

4. **Discretionary Access Control :** System administrator generally prepares access control list for each resource and is responsible for granting access rights to each user is the organization as per the users roles and responsibilities. However, in distributed data processing system where resources are distributed across the geography the system administrator cannot prepare access rights for each user in the Organization.

Chapter - 7 : Information Technology Regulatory Issues

2014 - Nov [2] (a)

The relevant requirements with respect to annual systems audit mandated by SEBI are as under:

⇒ SEBI has mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

⇒ The Audit shall be conducted according to the norms and terms of References and Guidelines issued by SEBI.

⇒ Stock Exchange/Depository may negotiate and the Board of the Stock Exchange/Depository shall appoint the Auditors based on prescribed Auditor selection norms and TOR.

⇒ The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.

⇒ Audit schedule shall be submitted to SEBI at least 2 months in advance, along with scope of current audit & previous audit.

⇒ The management provides their comment about the Non-Conformities and observations.

⇒ For each NC, specific time-bound corrective action must be taken and reported to SEBI. The Auditor should indicate if a follow-on audit is required to review the status of NCs.

⇒ Comments shall be submitted to SEBI with in 1 month of completion of the audit sample areas of review covered by IS Audit assignments.

2014 - Nov [4] (c)

Four Phases of ISMS.

The four phases of ISMS are:

→ Plan phase

→ Do phase

→ Check phase

→ Act Phase

1. **Plan Phase:** It provides 133 possible controls for selection to plan an appropriate information security. It helps to set objectives for information security, identify and assess risks and select the appropriate controls. This phase consist of the following key steps:
   - Determining scope of ISMS and writing an ISMS Policy.
   - Identifying methodology for risk assessment.
   - Identification of assets, vulnerabilities and threats.
   - Evaluating risks and risks treatment options.
   - Selection of controls.
2. **Do Phase:** This phase includes the following key activities:
   - Documenting the risk treatment plan.
   - Implementing the risk treatment plan.
   - Implementing applicable security controls.
   - Determining how to measure the effectiveness of controls.
   - Carrying out awareness programs and training of employees.
3. **Check Phase:** This phase consists of the following activities:
   - Implementation of procedures for monitoring and reviewing of controls for establishing any violation, incorrect data processing.
   - Finding whether the security activities are carried out as expected.
   - Regular reviews of the effectiveness of the ISMS .
   - Measuring effectiveness of controls.
   - Reviewing risks assessment at regular intervals.
   - Internal audits at planned intervals.
   - Identify opportunities for improvement.
4. **Act Phase:**
   - Implementation of identified improvements in the check phase.
   - Taking corrective and preventive actions applying security experiences.
   - Communicating activities and improvements to all stakeholders.
   - Ensuring that improvements achieve desired objectives.

Chapter - 8 : Emerging Technologies

2014 - Nov [2] (b)

The pertinent objectives in order to achieve the goals of cloud computing is as under:

1. **Threshold Policy:** This is a policy which defines cyclical use of any application e.g. use of credit card will rise sharply during the festival seasons and use will decrease significantly after the festival or buying season is over. The program processing the credit card should be having

the capability to provide more instances or processing capabilities during buying seasons and de-allocate these instances for other work when buying season is over. The threshold policy helps to detect sudden increase in the demand and results in the creation of additional instances to fill in the demand.

2. **Interoperability Issues:** These are no industry wide standards for interoperability of applications and data between different cloud computing vendors. If a company has outsourced the cloud computing to a vendor X the company will find it difficult to change to vendor Y who has proprietary API and different format for data import/export than X. This will require to change the data format and/or application logics.
3. **Hidden Costs:** Cloud computing service providers do not reveal hidden costs such as higher changes for data storage and use of applications during peak time and companies could experience slow services or latency in services particularly during heavy traffic.
4. **Un-Expected Behaviors:** Companies may get un-expected results or outputs while using cloud services. Therefore, it is necessary that before migrating to cloud the companies should test the cloud services for correct outputs particularly during heavy traffic or peak period.
5. **Security Issues:** Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or customer IT services over the internet. However, cloud computing presents an added level of risk because essential services are often outsourced to a third party, outsourcing makes it harder to maintain:
   - data security and privacy.
   - support data and service availability.
   - demonstrate compliance.

Shuchita Prakashan (P) Ltd.
25/19, L.I.C. Colony, Tagore Town,
Allahabad - 211002
Visit us: www.shuchita.com