CA Final – May 2012
Information System Control and Audit
Suggested Answers (for self evaluation)

1. (a) Refer RTP May 2012 Q25(a)

(b) Refer RTP May 2012 Q25(b)

(c) Refer RTP May 2012 Q25(c)

(d) A Good Information Security Policy should comprises following contents:-

1) Purpose and Scope,
2) Security Organizational Structure
3) Responsibility Allocation
4) Assets Classification and Security Classification
5) Access Control
6) Incident Handling
7) Physical and Environmental Security
8) Business Continuity Management and
9) System Development and Maintenance Control.

Framing of good security policy can be based upon some standards like ISO 27001-2005

2. (a) Unauthorized Intrusion refers to unauthorized access to a computer system or network to gain access thereupon with malafide intention. It is somehow mean Hacking, but hacking, generally, bear malafide intention.

The word "Hacking" is one of the most common words used in the field of Cyber Crimes. In fact it is more or less a generic term used to represent Cyber Crimes. Hacking refers to "Unauthorized Access to a Computer Network" which may otherwise be called an "**Unauthorized Intrusion**".

A difference between Intrusion and Hacking is that "Intrusion" is with a criminal intention of causing harm, while Hacking is made with an aim of entertainment.

In such cases the "Unauthorized Intrusion" may be called "Cracking". On the other hand, access undertaken to check the security vulnerability of a system though unauthorized, is also called "Hacking" and is considered a part of the IT security testing.

Damage by Hackers

As such Hacker has no intention of causing harm. Sometimes such hackers also act under the knowledge and permission (without access privileges being shared) of the Information Asset owners. Following damage a hacker can do:-

1) Copy or modification of data/information,
2) Theft of password,
3) Transmission of data over network
4) Supply of unwanted material

[Note:- Here, actions specified u/s 43 of the Information Technology (Amendment) Act, 2008 can also be specified]

(b) Guideline for implementation of an ERP Package

The general guidelines to be following before starting the implementation are:-

1) Define the needs and organization culture to adopt a suitable matching implementation technique,
2) Re-design the business processes prior to starting the implementation,
3) Establish a good communication network across the organization,
4) Provide a strong and effective leadership to motivate the people down the line,
5) Find an effective and efficient Project Manager,
6) Create a balanced team of Implementation Consultants and Users, who can work together,
7) Select a good implementation methodology with minimum customization,
8) Adopt the new system & make required changes in the working environment to use the system effectively.

(c) Power of Central Government to make rules in respect of Electronic Signature under section 10

For the purpose of this Act, the Central Government may, by rules, prescribe:-

1) The type of Electronic Signature,
2) The manner and format in which ES shall be affixed,
3) The manner or procedure which facilitate identification of the person affixing the ES,
4) The control processes and procedures and
5) Any other matter, which is necessary to give legal effects to ES.

3 (a) Benefits of Computerized System

1) (Handle) Large Volume of Data,
2) Speedy Processing,
3) Quick Data Retrieval,
4) Widened Scope of Analysis
5) (More) Comprehensive Information,
6) Increase Effectiveness of IS
7) Integrate Sub-systems
8) (More) Accuracy in Output,
9) Cost Effective (low Cost of processing),
10) Flexible and User Friendly,

[Note: Although, question is asking about **benefits** that can result **from development** of a computerized system, it can be answered that development of computerized system will provide all the benefits of Computerized System, as mentioned above.]

(b) Decision Support System

- DSS is software based IS which help management to take decisions at right time.
- It can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own way.
- DSS support the human decision-making process, rather than providing a means to replace it.

Characteristics of DSS

1) Deals with semi-structured or unstructured decision making,
2) Enough flexible to update itself to respond changing needs of manager/decision maker,
3) Easy to use

(c) Activities Involved in Design of a Database

The design of database involve the following four major activities

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) 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.

3) 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.

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, tacks, and sectors on a disk and the computers in a LAN or WAN.

4 (a) IT Infrastructure Library (ITIL)

- ITIL is an official publication of the Office of Government Commerce in the United Kingdom.
- It is a set of practices for **IT Service Management** (i.e. ITIL is an ITSM Framework).
- ITIL (the IT Infrastructure Library) is a series of documents that are used to aid the implementation of a lifecycle framework for IT Service Management.
- The 2011 edition of ITIL consists of 5 core publications – Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.

Configuration Management (CM) in ITIL

It is an **Information Technology Infrastructure Library** (ITIL) version 2 and an IT Service Management (ITSM) **process** that tracks all of the individual Configuration Items (CI) in an IT system which may be as simple as a single server, or as complex as the entire IT department.

Configuration Management is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department. Configuration Management includes:

1) Creating a parts list of every CI (hardware or software) in the system.
2) Defining the relationship of CIs in the system
3) Tracking of the status of each CI, both its current status and its history.
4) Tracking all Requests for Change to the system.
5) Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

1) Planning
2) Identification
3) Control
4) Status accounting and
5) Verification and Audit

(b) 1) **Mapics XA (Marcam Corporation) :** Mapics has been around for a long time, and many view it as a dated, legacy application. Mapics is a suite of 40 modules with 'good enough' functionality. Many users report that Mapics now offers more functionality than they need. It offers robustness, easy implementation and reasonable value for money.

2) **MFG/Pro (QAD) :** QAD's strength is in repetitive manufacturing. Originally designed to meet the MRP II criteria published by Oliver Wight, MFG/Pro's reputation includes reliable manufacturing functionality and straightforward implementations.

3) **Oracle Applications (Oracle) :** Oracle's Manufacturing Applications will tempt IT departments, with its vision of Internet-enabled, network-centric computing. As a one-stop shop, it offers the database, tools, implementation, applications and Unix operating systems running on a wide choice of hardware. Oracle has invested heavily to enhance functionality but production managers should still check that it delivers all the functionality they want.

4) **Prism (Marcam Corporation) :** Prism is a specialist process manufacturing solution for the AS/400. Its production model, which is akin to a flowchart, handles process industry problems elegantly. Although out dated, it does the job.

5) **R/3 (SAP):** In five years, R/3 is the market leader in new sales. Its philosophy of matching business processes to modules is excellent. It offers a wide range of functions and its major shortcomings are yet to be identified. However, it remains complex, because it offers much; few people know how to get the best from it. R/3 will be around for a long time; few people get fired for buying it.

6) **System 21 (JBA) :** JBA develops and implements System 21. Its software license revenues are small compared to those of other major ERP vendors. Nevertheless, it is a world player. It does not offer leading-edge technology, but does offer a rugged, reliable manufacturing solution.

(c) Parameters that would help in planning a documentation process of IS Audit

1) The importance of planning and understanding the planning process requires identifying three planning questions:
   a) Knowing your resources
   b) Defining the scope and audience
   c) Using a Scope Definition Report
2) The Documentation Writer: The qualities and skills that the documentation writer would need. The requirement may often be legal in nature
3) Rules to guide documentation writing: The four steps of writing documentation described in subsequent section

5 (a) Virus Meaning

According to Explanation to Section 43, Computer Virus means "any computer instruction, information, data or programme that destroys, damages, degrades adversely affects the performance of a computer resources or attaches itself to another itself to another computer resources and operates when a programme, date or instruction is executed or some other even takes place in that computer resource."

Policy and Procedure Control against Virus

The best policy for virus control is preventive control. Of course, detective and controls should be in place to ensure complete control over virus proliferation and damage control. Recommended policies and procedural controls are as below:-

1) The Security Policy should address the virus threats, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degrees of risks and suitable controls thereof.
2) Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning and quarantining should be given to all employees.
3) Hardware installations and associated computing devices should be periodically verified for parameter settings.
4) As part of SDLC Controls the develo0ment area should be free of viruses and sufficient safeguards must be in place to secure the area from viruses.
5) Provision of derives to read media should be restricted to certain controlled terminals and should be write-protected.
6) Network access to the Internet should be restricted preferably to stand-alone computers.
7) Networks should be protected by means of firewalls that can prevent entry of known viruses.
8) The servers and all terminals must have rated anti-virus software installed with sufficient number of user licenses.
9) Procedures should ensure that systematic updates are applied to all anti-virus installations at frequent intervals.
10) External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified b y the Department.
11) Vendors and consultants should not be allowed to run their demonstrations and presentations on organizational systems.

(b) Electronic Record Definition

According to Section 2(t) of the Information Technology (Amendment) Act, 2008, electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

Provision relating to **Retention of Electronic Records**
Section 7 of the Act provides the provision in respect of retention of Electronic Records, which is as below:-

Sec 7. Retention of electronic records.-
(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if-
   (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
   (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
   (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.
(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

(c) Constraints in Operating a MIS

1) **Non-availability of experts,** who can diagnose the objectives of the organization and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.

2) Experts usually face the **problem of selecting the sub-system** of MIS to be installed and operated upon. The criteria, which should guide the experts, depend upon the need and importance of a function for which MIS can be installed first.

3) Due to **varied objectives of business concerns**, the approach adopted by experts for designing and implementing MIS is a non-standardized one.

4) **Non-availability of cooperation from staff** is a crucial problem which should be handled tactfully. This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

6 (a) Review of LAN

An understanding of following information enables the auditor/ reviewer to make an assessment of the significant threats to the LAN:-
1) LAN topology and network design,,
2) Significant LAN components (such as modem and server)
3) LAN uses,
4) LAN Administrator,,
5) Significant groups of LAN users,

In addition to above, the reviewer should gain the understanding of following:-
1) Functions performed by LAN administrator,
2) The company's division or department procedure and standards relating to the network, and
3) LAN transmission media and techniques.

(b) Steps to be Following for conducting IT Audit

1) Scoping and Pre-audit Survey - Under this step, the auditor determined the main area of focus and such areas which are not material to review.
2) Planning and Preparation - Under this step, on the basis of outcome of 1st stage, the auditor prepares a plan for audit work to be executed.
3) Fieldwork - Under this step, the auditor collects evidences by application of various techniques.
4) Analysis - Under this step, the auditor analysis collected evidences using various analytical tools.
5) Reporting - Under this step, the auditor draft his opinion in standard format called report and submit it to management.
6) Closure - At this last step, the auditor maintained documentation of collected evidences and conclusions.

(c) Types of Service Auditor's Report under SAS 70

1) **Type I report** describes the description of controls of Service Organization at a specific point of time. This form of report is used by SAR to provide details of control activities of Service Organization to their users and users' auditors.
2) **Type II report**, not only includes description of Service Organization's Controls, but also includes opinion on whether the specific controls were operating effectively during the period under review (i.e. opinion upon results of detailed testing of such controls over a minimum six months period).

7 (a) Data Dictionary

Data dictionary is a computer file that contains descriptive information about the data items in the files of a business Information System. Thus Data Dictionary is a computer file about data in that computer.

Benefits of Data Dictionary to System Auditor

1) A data dictionary can help to establish an audit trail, because it can identify the input source of data items, the computer programs that modify it and the managerial reports on which the data items are output.
2) A data dictionary can also used to plan the flow of transaction data through the system.

(b) Risk Mitigation Measures

Most common Risk Mitigation Techniques/tools are:-

1) Insurance
2) Outsourcing and
3) Service Level Agreement

(c) Software Process Maturity

SPM is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. Maturity implies a potential for growth in capability and indicates both the richness and consistency.

As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone.

Five Levels of Software Process Maturity

1) Initial level
2) Repeatable level
3) Defined level
4) Managed level and
5) Optimized level

(d) Preventive and Restorative Information Protection

The security protection program can be classified into two types:-

1) **Preventive Protection** - This type of protection requires safeguarding IS resources from any damage. It requires use of **Information System Security Controls** and
2) **Restorative Protection** - This type of protection requires developing and maintaining backup and restore plans.

Types of IS Security **Preventive Protection** Controls

1) Physical Controls, such as Doors, locks, Entry Register, CCTV Guards etc., are intended to prevent unauthorized entry to IS location.
2) Logical Controls, such as Password, Firewall, Power Protection program etc., are intended to prevent unauthorized access to IS resources.
3) Administrative Controls, such as security policy, users' ethics etc., are those rules and regulation which are required to be followed by every internal parties to organization.

Key question to be asked under **Restorative Protection** Program

1) Has the recovery process been tested recently?
2) How long the recovery process takes time?
3) How much productivity was lost?
4) Did everything go according to plan?
5) How much extra time needed to restore last changed back-up?

(e) Objectives of Information Technology Act, 2000

1) Grant legal recognition to E-commerce,
2) Give legal recognition to Digital Signature,
3) Facilitate E-filling with Govt. agencies,
4) Facilitate electronic storage and maintenance of records
5) Give legal recognition to keeping books of accounts in e-form by banking companies,
6) Amend the Indian Penal Code, the Indian Evidence Act, the Banker's Book Evidence Act and the RBI Act [Although, provision relating to this amendment has been removed from the Information Technology (Amendment) Act, 2008.]

Compiled by
Arvind Sharma
1108.arvind@gmail.com
9582089920