MOCK TEST PAPER – 1

FINAL COURSE: GROUP – II

PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT

SUGGESTED ANSWERS/HINTS

1. (a) The main problem faced by ABC Ltd. is relating to the company's data management on real time basis though having various stand-alone computerized systems.

Major suggestions given by the Technical Consultant are given as follows:

- The key recommendation of the Technical Consultant was to implement a real time ERP package. The package should have all the necessary capabilities to integrate and synchronize the isolated functions into streamlined business processes.
- Second major recommendation was to consider information security related issues on top priority during the implementation of ERP package.
- In addition, the Consultant also suggested that the best practices of information security should be implemented right from the inception of the system, which will in turn provide a more secure system.

(b) Major benefits by implementing the ERP package are given as follows:

- Reducing paper documents by providing on-line formats for quickly entering and retrieving information.
- Improving timeliness of information by permitting posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
- Improved cost control.
- Faster response and follow-.up on customers.
- More efficient cash collection, say, material reduction in delay in payments by customers.
- Better monitoring and quicker resolution of queries.
- Enabling quick response to change in business operations and market conditions.
- Helping to achieve competitive advantage by improving its business process.
- Improving supply-demand linkage with remote locations and branches in different countries.

- Providing a unified customer database usable by all applications.
- Improving International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improving information access and management throughout the enterprise.

(Note: Candidates may explain any five benefits.)

(c) **'Big Bang' Implementation**: A 'Big Bang' implementation involves having all modules at all locations implemented at the same time. Characteristics of this approach include no need for temporary interfaces, limited requirement to maintain legacy software, cross-module functionality and overall cost if no contingencies arise.

Phased Implementation: In such technique, implementation takes place in various phases e.g. one or a group at a time, often a single location at a time. Benefits of this approach include: a smoothing of resource requirements, an ability to focus on a particular module, avail-ability of existing legacy systems as a fall-back, reduced risk, the knowledge gained with each phase and the usefulness of demonstrable working system.

(d) **[Section 3] Authentication of Electronic Records:**

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

2. (a) Major weaknesses of Prototyping approach are given as follows:

- Approval process and control are not strict.
- Incomplete or inadequate problem analysis may occur whereby only the most obvious and superficial needs will be addressed, resulting in current inefficient practices being easily built into the new system.
- Requirements may frequently change significantly.
- Identification of non-functional elements us difficult to document.
- Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design with narrow focus that limits future system potential.
- Prototype may not have sufficient checks and balances incorporated.
- Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system developers with change suggestions. The users may not be able or willing to spend the amount of time required under the prototyping approach.
- The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
- Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by users when they have to go through too many interactions of the prototype.

(b) The role of IS Auditors in Software Acquisition/Selection Process is given as follows:

- To highlight risks before a vendor contract or a software agreement contract is signed.
- Ensure that the decision to acquire software should flow from the thorough feasibility study, vendor evaluation and RFP (Request for proposal) adequacy checked for.
- A RFP would include transaction volume, data base size, turnaround time and response time requirements and vendor responsibilities.
- The auditor needs to also check the criteria for pre-qualification of vendors and

sufficient documentation available to justify the selection of the final vendor / product.

- The auditor may also collect information through his own sources on vendor viability, support infrastructure, service record and the like.
- Thorough review of the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures such as, source code availability and third party maintenance support.
- To ensure that the contract went through legal scrutiny before it was signed.

(c) [Section 68] Power of Controller to give directions:

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

3. (a) Major limitations of MIS are given as follows:

- The quality of the outputs of MIS is basically governed by the quantity of input and processes.
- MIS is not a substitute for effective management which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives.
- MIS is less useful for making non-programmed decisions. Such type of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in organizations, where the culture of

hoarding information and not sharing with other holds.

- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

(b) **Preventative Information Protection:** It is based on the usage of security controls, which are generally grouped into three types of controls: Physical, Logical, and Administrative. Organizations require all these three types of controls. The organization's Information Security Policy mandates the use of these controls through the associated Information Security Standards documentation. Some examples of each type of control are given as follows:

- **Physical Controls:** Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
- **Logical (Technical) Controls:** Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems; and
- **Administrative Controls:** Security Awareness, User Account Revocation, Policy.

(c) Various fact-finding techniques, which are used by the System Analysts for determining the needs/ requirements of their clients, are given as follows:

- **Documents:** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
- **Questionnaires:** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.
- **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide systems developer with a complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.
- **Observation:** In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed.

4. (a) Major tasks to be undertaken in the 'Vulnerability Assessment and definition of Requirement' phase while developing a Business Continuity Plan are given as follows:

- A thorough Security Assessment of the system and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
- The Security Assessment will enable the business continuity team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Define the scope of the planning effort.
- Analyse, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
- Develop a Plan Framework.
- Assemble business continuity team and conduct awareness sessions.

(b) Major points, which are required to be taken into consideration for Physical and Environmental Security with reference to Information Security Policy, are given as follows:

- Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- The IT infrastructure must be physically protected.
- Access to secure areas must remain limited to authorized staff only.
- Confidential and sensitive information and valuable assets must always be securely locked away when not in use.
- Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
- Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities
- Equipment, information or software must not be taken off-site without proper authorization.

- Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- The location of the equipment room(s) must not be obvious. It will also where practical be located away from, and protected against threats of, unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

(c) **Preventive Controls:** Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. Other examples of preventive controls are given as follows:

- Employ qualified personnel,
- Segregation of duties,
- Access control,
- Vaccination against diseases,
- Documentation,
- Prescribing appropriate books for a course,
- Training and retraining of staff,
- Authorization of transaction,
- Validation, edit checks in the application,
- Firewalls,
- Anti-virus software (sometimes this acts like a corrective control also), etc, and
- Passwords.

The broad characteristics of preventive controls are given as follows:

- A clear-cut understanding about the vulnerabilities of the asset;
- Understanding probable threats; and
- Provision of necessary controls for probable threats from materializing.

5. (a) **Decision Support System (DSS):** Decision Support Systems (DSS) are a specific class of computerized information systems that supports business and organizational decision-making activities. A properly-designed DSS is an interactive software-based system intended to help decision makers to compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions. A decision support system (DSS) can be defined as a system that provides tools to managers to assist

them in solving semi structured and unstructured problems in their own, somewhat personalized, way.

DSS is considered as more flexible and adaptable to changing decision making requirements than traditional Management reporting system. This system emerged from the developments of interactive display technology, micro computing and easy-to-use software tools. It handles unstructured and partially structured problems giving rise to unpredictable and unstructured information needs. A DSS does not require any high technology.

Three major characteristics of a Decision Support System are given as follows:

- They Support semi-structured or unstructured decision-making.
- They are adaptable to the changing needs of decision makers, and
- They are easy of learning and use.

Each of these characteristics is briefly discussed below:

- *Semi-structured and Unstructured Decisions*: Unstructured decisions and semi-structured decisions are made when information obtained from a computer system is only a portion of the total knowledge needed to make the decision. DSS is well adapted to help with semi-structured and unstructured decisions. A well-designed DSS helps in decision making process with the depth to which the available data can be tapped for useful information.
- *Ability to adapt the changing needs*: Semi-structured and unstructured decisions often do not conform to a predefined set of decision-making rules. DSS provides flexibility to enable users to model their own information needs. Rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.
- *Ease of Learning and Use*: DSS software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth – generation languages (4GL), natural English, and easily read documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.

(b) The detailed control objectives of Communications and Operations Management with reference to Information Security Management System (ISMS) are given as follows:

- *Operational procedures and responsibilities :* To ensure correct and secure operation of information processing facility;
- *System planning and acceptance :* To minimize risks of system failure;
- *Protection against malicious software :* To protect the integrity of software and information;

- *Housekeeping :* To maintain the integrity and availability of information processing and communication services;
- *Network Management :* To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- *Media handling and security :* Prevent damage to assets and interruptions to business activity; and
- *Exchanges of information and software:* To prevent loss, modification or misuse of information exchanged between organizations.

(c) Major advantages of continuous audit techniques are given as under:

- *Timely, comprehensive and detailed auditing* – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- *Surprise test capability* – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- *Information to system staff on meeting of objectives – Continuous audit techniques provides* information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- *Training for new users* – Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

6. (a) COBIT 5 Enablers: Enablers are factors that, individually and collectively, influence whether something will work— in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve. The COBIT 5 framework describes seven categories of enablers (shown in Fig. 1):

1. Principles, policies and frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
2. Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
3. Organizational structures are the key decision-making entities in an enterprise.
4. Culture, ethics and behavior of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.

5. Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

6. Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

7. People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

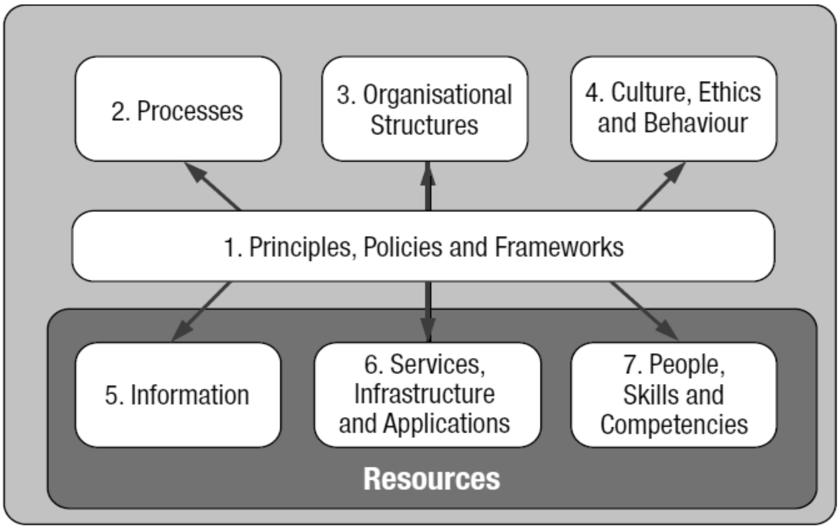
2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Fig. 1: Seven Enablers of COBIT 5

(b) Following are the major threats due to cyber crimes:

- 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.
- 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.

- Denial of Service (DoS): An action or series of actions that prevents access to a software system by its intended/authorized users or causes the delay of its time-critical operations or prevents any part of the system from functioning is termed as DoS. There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service those results in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
- Vandalism or sabotage*:* It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- Computer virus: A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.
- Others: Threat includes several other cases such as intrusions, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

(Note: Candidates may explain any four benefits.)

(c) 'Do Phase' of ISMS consists of the following major activities:

- *Writing a risk treatment plan* – describes who, how, when and with what budget applicable controls should be implemented;
- 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;
- Management of the normal operation of the ISMS;
- Management of ISMS resources; and
- Implementation of procedures for detecting and managing security incidents.

7. (a) Application-Level Firewalls : Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level

firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

(b) Adaptive Maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

(c) Delphi Approach for Risk Assessment: Delphi approach is defined as: 'a method for structuring a group communication process so that the process is effective in allowing a group of individuals as a whole to deal with a complex problem'. It was originally developed as a technique for the US Department of Defence. The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

(d) 'Service Design' under ITIL V3*:* Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings.

The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets. Service Design is not limited to new services and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services, taking into account the continuity of services, conformance to standards and regulations and achievement of service levels. It also provides guidance on the development of design capabilities for service management.

(e) [Section 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, -

(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:

However,

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. Publication of rules, regulation, etc. in Electronic Gazette.