IS audit process and control

Following **factors** should be considered in determining **whether to use CAATs in an audit**:

- IT knowledge, expertise, and experience of the IS auditor
- Availability of suitable CAATs and IS facilities
- Efficiency and effectiveness of using CAATs over manual techniques
- Level of audit risk
- time constraints
- integrity of information system and IT environment

An IS Auditor would consider the following important **matters** while **selecting** a Computer Assisted Audit Technique:

- Ease of use.
- Capacity to handle data.
- Efficiency of analysis.
- Level of training required.
- Effectiveness in preventing and/or detecting frauds.
- Cost and licensing structure.

Advantages: Greater productivity and improved quality of audits may be achieved through CAATs as:

- Automated repetitive tasks reduce the time required for audits.
- More time is available for critical functions.
- Project documentation is simplified.
- CAATs can analyze entire data for audit period, thereby reducing the audit risk.
- Integrity of analysis is assured.
- Audit methodologies are standardized.

An IS auditor should make the following **arrangements with the client** while using CAATs in an audit:

- Data owners or users have to spend sufficient time in interacting with the auditor to help him properly design the CAAT and interpret the data.
- The purpose, scope, timing and goals of the CAATs are to be explained to the client.
- Clear expectations should be communicated at the outset of the CAAT.
- Data files such as detailed transaction files are often only retained for a short period of time; therefore, arrangements should be made for the retention of the data as required by the auditor.
- Access to the organisation's IS facilities, programs/systems and data should, as far as possible, be arranged well in advance of the needed time period to minimise the effect on the organisation's production environment.

Following **steps** are required to be taken while **planning the use of CAATs**:

- Set the objective of the CAAT application.
- Determine the accessibility and availability of the entity's IS facilities, programs/systems and data.
- Determine resource requirements, i.e., personnel, CAATs, processing environment.
- Clearly understand composition of data to be processed including quantity, type, format and layout.
- Obtain access to the entity's IS facilities, programs/systems and data, including file definitions.
- Define the test and procedures to be undertaken.
- Define the output requirements.
- Document CAATS to be used, including high level flowcharts and run instructions.

Matters to be documented in respect of CAATs:

At planning stage:
Documentation should include:
- CAATs objectives
- CAATs to be used
- Controls to be exercised
- Staffing and timing

At the stage of execution including gathering audit evidence:
Documentation should include:
- CAATs preparation and testing procedures and controls
- Details of the tests performed by the CAATs
- Details of inputs, testing periods, and outputs
- Listing of relevant parameters or source code
- Output produced
- Description of how output was analysed
- Audit findings
- Audit conclusions
- Audit recommendations

Case Study: FMC Associates provides financial and management consultancy services. Its internal auditor has recently completed a review of its information systems and reported the following key findings:
(i) Security controls over personnel are lacking.
(ii) Information Security objectives related to personnel have not been developed.
(iii) Acceptable Usage Policy (AUP) is very brief as it does not cover all aspects of the technology usage.

Significance of the internal auditor's findings is as follows:
(i) Insufficient controls over personnel would weaken the organization's ability to mitigate information security risk inherent in human interactions.
(ii) Absence of Information Security objectives related to personnel may lead to improper/insufficient users awareness and training in the area of information security which in turn may lead to increased confidentiality breaches.
(iii) Insufficient Acceptable Usage Policy (AUP) could lead to misuse of organization's technology resources/organisation's resources.

Following **information security objectives** may become part of the **information security policy** of the company:

- Ensure that all employees understand their responsibilities and liabilities related to information security.
- Reduce the risk of human error by ensuring that all employees are aware of information security threats and concerns.
- Reduce the risk of theft, fraud or misuse of information technology facilities.
- Reduce the human dependency for availability of systems by imparting appropriate training and implementing delegations in a controlled manner.

Following points should be included in the **Acceptable Usage Policy (AUP)** of the company:

- The users must ensure that the Information Technology assets are used in accordance with the prescribed policies of the organisation.
- Users shall be responsible for activities performed with their personal User IDs/access cards. They must not permit any other user to perform any activity with their User IDs, and vice versa.
- Computers including desktops, portable computers/laptops, servers and communication devices must be locked when unattended or logged off at the end of an active session.
- Users shall exercise good judgment and take reasonable care to safeguard mobile and portable computing equipment like laptops etc., while taking such devices outside the office premises.
- Only authorised application programs shall be installed on the laptop and other mobile devices.
- All employees shall return all the company's technological assets in their possession upon termination of their employment, contract or agreement.
- Sending inappropriate email messages using company's email ID shall not be allowed.

Case Study: Your firm is conducting IT audit of Elegant (Private) Limited (EPL) which is a distributor of FMCG and has a network of branches across the country. Successful implementation of an ERP system in the company last year has led to widespread availability of information in all business areas.
Being the job in-charge on this assignment you have decided to adopt 'concurrent auditing techniques'. However, the audit manager has advised you that since concurrent auditing techniques have never been used previously, the change should be communicated to the client before implementing the same.

Following **factors** have necessitated the use of concurrent auditing techniques (CAATs):

- With the implementation of ERP, paper based audit trail is less likely to be found for various critical processes. Concurrent auditing techniques provide a way to capture the evidence that previously existed in documentary form.
- Errors or irregularities in ERP systems can propagate quickly to most of the integrated modules which may cause material losses. Through concurrent auditing techniques these systems can be monitored on timely basis.
- Performing transaction walkthroughs in ERP systems is more difficult because they often have a large number of complex execution paths. Concurrent auditing techniques provide means of tracing transactions through different execution paths.
- Majority of the controls to be tested during the audit exist inside the system. Concurrent auditing techniques provide ways to verify the accuracy of such controls.
- All systems have entropy, which is their tendency to move towards internal disorder and eventual collapse. In ERP systems entropy arises due to various reasons e.g., change in user requirements, significant increase in number of transactions resulting in workload which the software and hardware are unable to handle satisfactorily etc. Concurrent auditing techniques provide early warning of the presence of entropy in application systems.
- Since ERP has been implemented across the country wide branch network, it would be difficult for the auditors to be present at information system facilities to gather evidence. The embedded audit routines used with concurrent auditing techniques provide a way of collecting audit evidence when application system processing is being carried out at remote locations.

Three common concurrent auditing techniques are as follows:

Integrated test facility (ITF)
It involves establishing a dummy entity on an application system's files and processing audit test data against this dummy entity. By comparing the processed result of dummy entity with its independently calculated result, the auditor can verify authenticity, accuracy and completeness of application system processing.

Snapshots
In this technique embedded audit modules take pictures of transactions as they flow through various points in an application system. Auditor must decide place of snapshot points in an application system and which transactions will be subject to snapshot and how and when snapshot data will be presented for audit evaluation purposes.

The system control audit review file & Embedded Audit Modules (SCARF/EAM)
It involves embedding audit modules in an application system to provide continuous monitoring of a system's transactions. The data collected via these routines may include errors and irregularities, policy and procedural variances, system exceptions, statistical samples and snapshots and extended records etc. The collected data is written to a special SCARF file for immediate or subsequent audit evaluation.

Continuous and Intermittent Simulation (CIS)
During the processing of transactions, the computer system simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and, if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

Following **factors** should be considered while selecting an **appropriate continuous online auditing technique:**

- Complexity of the organization's computer systems and applications.
- Advantages and disadvantages or limitation of each type of online auditing techniques.

 IS auditor's ability to understand the system with and without the use of continuous online auditing techniques.

Case study: City Club (CC) is an established social and recreational centre having more than five thousand members. Besides cash/cheques, CC allows its members to pay their fee through CC's website using credit cards.

CC's management wishes to evaluate the process of collection of membership fees through its website and have appointed you as Information System Auditor. During the planning process, you have obtained the following information:

(i) The member is required to input his name (as on the credit card), type of credit card (Visa/Master), credit card number, expiry date of card and billing address, on a Secured Socket Layer protected page at CC's website.

(ii) The above data is stored on the CC's web server which is hosted by a third party.

(iii) An automated email containing member's particulars in text format is generated by the web server and sent to the official email ID of CC's Assistant Manager Finance (AMF).

(iv) The details of all emails received during the day are posted by the AMF in a single pre-formatted spread sheet. At the day end, these are sent to a designated employee of the commercial bank for the settlement of transactions.

(v) The bank processes the transactions and sends the success and failure status of each transaction to AMF on the next working day.

(vi) AMF sends the fee receipts to members whose transactions have been successfully processed and intimates the other members about the transaction failure.

(vii) All computers in CC are interconnected via LAN.

(viii) Backup of data on AMF's computer is stored on a backup file server automatically on daily basis. Only the Network Administrator is authorised to restore the data.

(ix) The online fee payment procedure has been functioning satisfactorily for the past five years without any complaints or problems.

Control Weaknesses	Suggested Controls
Members' credit card details are stored on web server hosted by a third party.	Members' credit card details should be stored on the club's server placed in its own premises. If keeping own web server is not possible, the club management should get nondisclosure agreement (NDA) signed by the third party. The data should be stored in encrypted form.
Emails containing members' data remain at that server at least for some time.	Create privilege users' accountability and auditability by logging users' activities at email server. Logs of email server should be reviewed periodically at appropriate level.
Data is transferred without encryption.	Emails from web server and emails sent by AMF should be encrypted.
Disclosure of information by bank's employees.	CC should get the NDA signed by the bank authorities. CC should ensure that the bank deploys appropriate controls for the security of the data. In this regard, preferred controls should be agreed and documented.
Risk of exposure of confidential information to unauthorized (unconcerned) employees.	Sharing of AMF's computer should be disabled. Establish rules for access to information on AMF's computer for normal as well as exceptional circumstances. If possible use a separate computer for storing such information.
AMF intentionally leaks the data.	Get the NDA signed by AMF and other concerned staff. Strict disciplinary policies should be made for confidentiality breaches.

Network Administrator can restore AMF's computer data from backup file server.	□ Members' credit card details stored on AMF's computer must be encrypted.
Lack of review.	□ All the controls mentioned above should be deployed in order to avoid this risk. □ Periodic compliance testing of the deployed controls should be performed.

If, however, CC opens a merchant account for online payments, then except risk (iv) all the risks identified above would be eliminated.

The **risks** associated with the given **situation** are listed hereunder: (observations are in bold and related risks are listed below)

(a) FFL did not have a formal Information Technology Strategy.
(i) The IT objectives may not be aligned with the business objectives.
(ii) Future IT investments in hardware and software may not be those that best meet the entity's medium to long term needs.
(iii) There may be no/limited succession planning.

(b) The security module in the financial application was not configured for:
(i) **Periodic password changes.**
• High probability of compromising users' passwords.
(ii) **Account lockout policy.**
• Unauthorized log on attempts may not be identified.
• The chance of password compromise increases.
(iii) **Logging of user access.**
• Attempts of unauthorized access to applications and data remain undetected.
• Failure to fix responsibilities for errors (intentional and unintentional).

(c) **FFL has formal backup and recovery procedures but has not yet documented a formal Business Continuity and Disaster Recovery Plan.**
(i) Backup and recovery procedures may not be enough to avoid extended disruptions of business in the event of a disaster.
(ii) Critical business processes and critical recovery time may not be known.
(iii) The management may not be able to determine the steps required to recover from a disaster or contingency.
(iv) Formal roles and responsibilities of disaster recovery teams may remain undefined.

(d) **A server based antivirus solution is being used but its maintenance period has expired and**
vendor has ceased to support that version.
(i) Failure to detect new types of viruses.
(ii) Absence of technical support.

(e) **Firewall is configured at default (vendor) settings and the network administrator is not trained to configure the firewall.**
(i) The firewall may allow unauthorized access.
(ii) It may restrict access to authorized users also.

Case Study: Superb Limited (SL) is a distributor of FMCG and is operating this business since the last fifteen years. SL's management is considering to automate the process of executing orders so that the time lag between receipt and supply of goods may be reduced. To achieve this objective, SL intends to provide smart phones with customized application to the sales force.
This may enable them to immediately communicate the customers' orders to the company's system. Moreover, Area Sales Managers (ASMs) will be provided laptops with pre-installed application software of the company. This would enable ASMs to monitor the progress of their sales team at all times from any location.

Following **controls** should be in place so that **risks associated with inter-connection of smart phones (SPs) and the laptops (LTs)** with the company's system can be **mitigated**.

- Installation and configuration of applications on SPs and LTs should comply with the existing company standards for security.
- Addition, deletion or modification of any application should not be allowed to their holders. For any such change, documented procedure should be followed.
- SP and LT information should be synchronized only with organization's resources contained in the company system.
- Employees should be instructed to exercise due care during travel as well as within office environments. Any loss or theft of a SP or LT should be treated as security breach and reported immediately.
- Identify all remote access points of entry through which access to company system is allowed and that no other remote access points can be used to access the company system.
- Appropriate authentication mechanisms should be available at company system to ensure that those accessing it are duly authorized.
- All the security controls over access to the company system remotely should be appropriately documented.
- Data flowing between SPs/LTs and the company should be encrypted.
- At the company, server access logs should be generated regularly and reviewed periodically.
- All SPs and LTs should be protected with updated antivirus software.
- Properly configured firewall should be installed in the company system.
- In addition to the firewall, an intrusion detection system should also be installed in the company system.

Generalized audit software is a computer assisted audit technique (CAAT) which is used to identify and select data and transactions of interest to the auditor for further analysis. These may be used to verify the adequacy of file integrity controls such as data editing and validation routines, non-continuous monitoring of transactions and for sampling of transactions.

Major functions performed by GAS are as follows:

- File access i.e. reading different types of file structures, record formats and data formats.
- File reorganization i.e. storage and merging of files.
- Selection i.e. extracting data that satisfies certain conditional tests.
- Arithmetic operations including addition, multiplication, subtraction, division etc.
- Stratification and frequency analysis i.e. categorization and summarization of data in different ways.
- File creation and updating
- Reporting i.e. formatting output in the required manner.

Functional capabilities provided by generalized audit software:

Stratification and frequency analysis:

It allows data to be categorized and summarized in different ways. Frequency analysis and aging analysis can be under taken. Frequency tables and bar charts can be produced.

Examples

(i) Accounts receivable balances can be stratified to determine whether the provision for doubtful debts is adequate.

(ii) The frequency with which various types of monetary transactions occur, can be determined to see whether in any period there is a marked deviation from the norm.

Arithmetic:

Arithmetic functions enable computations to be performed on data.

Examples

(i) The discounting calculations performed by an invoicing program can be recomputed to check their accuracy.

(ii) Monetary updates of an account can be performed to check that the application update program does not contain erroneous logic.

File reorganization:
File reorganization function allows the files to be sorted and merged.
Examples
(i) A file may be sorted to determine whether duplicate records exist on the file.
(ii) Files of various periods may be merged to identify a trend in financial position.

Statistical:
Statistical function allows sampling to be undertaken and the result of sampling to be evaluated.
Examples
(i) The sampling capabilities can be used to select records for confirmation.
(ii) A random selection of inventory records can be undertaken so a physical count can be made to verify the accuracy and completeness of the records.

Following are the **limitations** of generalized audit software:

- Timely evidence collection may not be possible because evidence on the state of an application system can only be gathered after the data has been processed.
- The program may not be able to perform all the tests which an auditor may require.
- Least likely to be used for inquiry of on-line data files.
- Cannot perform a physical count of inventory or cash.
- Cannot perform continuous monitoring and analysis of transactions.
- Cannot be customized easily for specific situations.

Key contents of audit charter:

An **audit charter** is used to clearly document the formal acceptance of IS auditor's mandate to perform the IS audit function.

An audit charter addresses the four aspects i.e., purpose, responsibility, authority and accountability.

Purpose: Following contents are covered under this aspect:
 Role
 Aims/goals
 Scope
 Objectives

Responsibility: Following contents are covered under this aspect:
 Operating principles
 Independence
 Relationship with external audit
 Auditee requirements
 Critical success factors
 Key performance indicators
 Risk assessment
 Other measures of performance

Authority: Following contents are covered under this aspect:
 Right of access to information, personnel, locations and systems relevant to the performance of audits
 Scope or any limitations of scope
 Functions to be audited
 Organisational structure, including reporting lines to board and senior management
 Grading of IS audit staff

Accountability: Following contents are covered under this aspect:
 Reporting lines to senior management.
 Assignment performance appraisals.
 Personnel performance appraisals.
 Auditee rights.
 Independent quality reviews.

- Assessment of compliance with standards.
- Benchmarking performance and functions.
- Comparison of budget to actual costs.
- Agreed actions, e.g., penalties when either party fails to carry out their responsibilities.

Case study: Marvi Hospital (MH) is a large sized hospital. It uses an integrated application for recording and maintaining the patients' medical history. As the IS auditor of the hospital, data privacy is one of the major concerns requiring your attention.

I would like to ask the following **questions to assess the privacy risks** being faced by MH:

- What type of personal information does MH collect?
- What are MH's privacy policies and procedures with respect to collection, use, retention, destruction, and disclosure of personal information?
- What privacy laws and regulations impact MH? Are the policies revised in line with the revision in such regulations?
- Are the privacy policies properly circulated and signed off by all the employees?
- Has MH assigned responsibility and accountability for managing a privacy program?
- What measures have been incorporated in the computer systems to ensure compliance with the privacy laws?
- In case any personal information collected by MH is disclosed to third parties, what safeguards and controls are applied?
- History of privacy breaches and action taken there off.
- Are employees properly trained in handling privacy issues and concerns?
- Is compliance with privacy policy being monitored at appropriate levels?
- Does MH conduct periodic assessment to ensure that privacy policies and procedures are being followed?
- Does MH have adequate resources to develop, implement, and maintain an effective privacy program?

The following are the **potential benefits** of **certification** for compliance with International Standard for Information Security Management System:

- **Assurance**: Management can be assured of the security and reliability of the system, if a recognized framework or approach is followed.
- **Competitive Advantage:** Following an international standard will help to gain competitive advantage.
- **Bench Marking:** It can be used as a benchmark for current position and progress within the peer community.
- Awareness Implementation of standard results in **greater awareness** about information security practices within an organization.
- **Alignment:** Implementation of standards tends to involve both business management and technical staff, therefore; greater IT and business alignment often results.
- **Interoperability:** Systems from diverse parties are more likely to fit together if they follow a common guideline.

I would take the following **steps** for getting my organization certified towards an **international security standard**:

- Obtain understanding of security issues addressed in the international security standards.
- Develop a business case.
- Get management support.
- Define scope and boundaries.
- Develop an implementation program.
- Develop policies, procedures, standards as required.
- Conduct risk assessment / gap analysis.
- Implement controls to fill the gaps.
- Conduct a pre-certification assessment and take corrective actions if any gaps still exist.
- Invite certification body for certification audit.

Case Study: The newly appointed CEO of Digital Corporation (DC) is of the view that the company's General Ledger (GL) application developed by a renowned software house suffers from many limitations. Some of its modules are of little use to the company. The CEO feels that cost incurred for development of software was very high besides he also has doubts on the accuracy of the data being produced. He has appointed RBC & Company to carry out an assessment of the effectiveness, efficiency and relevance of the system.

Required:

(a) Identify the documents which RBC's team would review to gain an understanding of the GL application. Also, explain briefly the importance of each of the identified document. (06)

(b) Identify and briefly explain the various types of controls which could satisfy RBC about the effectiveness of the system and the reliability of data. Explain how they would test their effectiveness. (10)

Following **documents** may be reviewed to gain an understanding of the GL application:

Documents describing user requirements: These documents help in identifying the essential system components.

Documents describing cost benefit analysis: These documents help in understanding the need and objective of each module and functionality of the application.

Functional design specifications: This document provides a detailed explanation of the application.

Documents describing modifications in program: Such documents will help in evaluating whether the application has been working satisfactorily, understanding the change in user requirements and change management controls.

User manuals: A review of the user manual will allow us to determine whether it contains appropriate guidance for the users.

Technical reference manual: Its review helps in understanding access rules and logic of the application.

Input Controls

Terminal/Client's workstation identification check: This check is used to limit input to specific terminals as well as to individuals. Client workstations in a network can be configured with a unique form of identification, such as serial number or computer name, that is authenticated by the system.

Effectiveness testing:

(i) Check if list of authorized terminals is in place and is updated.

(ii) Attempt accessing the system from unauthorized terminal.

(iii) Observe process of input and review source documents for evidence of authorization.

OR

Completeness check:

Fields like national identity card number accepts data of standard length. If incomplete card number is entered, an alert is generated to complete the entry. At record level, when we want to move on next record without entering mandatory fields' value, an alert will be generated to complete the record entries.

Effectiveness testing:

(i) Observing the data entry process.

(ii) Input some records on test basis and intentionally skipping mandatory fields blank while adding new records.

OR

Authorization on source document

Authorized person's signature in an appropriate area of the source document provides evidence of proper authorization.

Effectiveness testing

Review some source documents corresponding to records present in the system and verify the authorized signatures.

Processing Controls:

Exception reports

Such reports are generated when some transaction or data appear to be incorrect.

Effectiveness testing

Review exception reports and check if these were reviewed by the concerned user and the

evidence of actions taken thereof.
OR
Reconciliation of control totals
It involves checking of totals produced by the computer with those determined manually.
Effectiveness testing
(i) Assessing whether the reconciliations are being prepared as appropriate.
(ii) Checking calculations as appearing on the reconciliations.
OR
File Version Check
For correct processing, the system ensures that transaction should be applied to the most current database.
Effectiveness testing
Process some sample transactions and compare the results with current version of the database.

Output Controls:

Printing and storage of output reports
Critical output reports should be produced and maintained in a secure area in an authorized manner.
Effectiveness testing
(i) Review of the access rules
(ii) Reviewing and assessing the procedures adopted by the management for monitoring the output.
(iii) Reconciliation of total pages printed with the readings as shown on the counter installed in the printer.
OR
Distribution of reports
Authorized distribution parameters are set for output reports. All reports are logged prior to distribution. Recipient is required to sign the distribution log as evidence of receipt of output.
Effectiveness testing
(i) Observation and review of distribution output logs.
(ii) Verifying recipients'' signatures on distribution log.

How would you evaluate the information in italic?

System logs of all critical systems are available
I would check whether:
 these are reviewed periodically at an appropriate level.
 these logs are not editable.
I would also check the policy regarding retention and over writing of these logs and if this policy is in line with the overall security policy of CIC.

Firewall configuration and rules are documented
I would check whether:
 the default firewall configuration and passwords have been changed and when they were changed.
 passwords (to access firewall) meet the complexity requirement and forced password change policy is in place.
 the documented rules are in-line with the overall security policy of CIC.
 unnecessary ports and services are turned off.
 the firewall configuration and rules have been reviewed and approved by an appropriate authority.
 there are any users who could bypass firewall while connecting to internet. If yes, what are the reasons for such exception and whether these are documented.
 there have been any instances of breach in the past. If yes, what preventive measures were introduced in response to the event.

Security patches have been installed on operating systems and software, including anti-virus updates
I would check whether:
 there exists documented policy and procedure for installing security patches and antivirus updates.
 virus definitions are updated automatically or manually.
 security patches are tested before installation.

 evidence exists for past updates and is in line with the defined policy.

Access control lists are in place at routers, firewall and servers
I would check whether:
 these lists are current.
 these lists are complete.
 documentary evidence exists that these are updated and reviewed at regular intervals at an appropriate level.
 access to critical functions and resources is granted on need to know and need to do basis.

Employees and key business partners have remote access to CIC information system
I would check whether:
 remote access points are authenticated and encrypted.
 how remote access is authenticated.
 remote access is granted on 'need to have' basis or is available to all employees and key business partners at their convenience.
 such users have firewall installed at their systems.
 how such users connect to the corporate network; whether they connect through a VPN tunnel or through public internet.
 penetration testing has ever been performed.

An incident response plan is in place to address any debilitating cyber incident
I would check whether:
 the plan has ever been tested.
 it is current.
 anyone has been assigned the responsibility for execution of the plan and whether he knows his responsibility.
 the plan review and update process is in place.
 there have been any such incidence in the past. If yes, what preventive measures were introduced in response to the event.

All users of CIC's information system understand the importance of protecting the information resources
 I would conduct interviews of key users to assess their understanding about protection of information resources.
 I would check whether there exists any evidence of users awareness and training sessions.
 I would check whether an undertaking has been signed by each user with regard to the confidentiality of information.

Internet access is available to all users. Facebook and Twitter is blocked; however, users may access weather advisories, free email and some instant messaging services
 I would check whether an internet usage policy exists. If yes, are users made aware of that?
 I would conduct interviews of users to assess their understanding about internet related threats.
 I would check whether there exists a system that monitors and filters users' internet access.

Case Study: You are reviewing the Data Processing System of Outsourcers Limited (OL). OL has claimed that data entry into its system is free of errors since:
(i) completeness, format and range checks have been incorporated at field levels in its program.
(ii) reasonableness, logical relationship and sequence checks have been incorporated at the record level.
(iii) on completion of data entry of each batch, a list is printed which is compared with the original source. Observed errors, if any, are immediately corrected.
Besides above controls, a verifiable audit trail in the data entry system also exists.
Required:
(a) In respect of each of the above controls, discuss how and to what extent they are useful in ensuring that the data entry is free of error. (08)
(b) List any six types of information that should be available to ensure the existence of an effective audit trail in the data entry system. (03)

Completeness check: It is deployed on fields of pre-defined length and ensures that such fields are completely entered. For example, if length of a field is defined as 13 characters, the cursor will not forward to the next field until 13 characters are entered into that field e.g., CNIC number.

Format check: It is deployed over fields with custom format such as date, postal code, CNIC etc. For example in case of date, entered data would be automatically entered with separator between days, months and years.

Range check: It is deployed over numeric or date fields by setting upper and lower limits. It ensures that the user is prompted if entered data is outside the possible range. For example, overtime rate of employees may not exceed Rs. 100 per hour and may not be less than Rs. 50 per hour. The cursor will not move forward if out of range value is entered or it will give a message guiding user about the valid range values.

Reasonableness check: It matches the input data to predetermined limits or occurrence rates. For example, a gadget manufacturer usually receives orders for no more than 20 gadgets from a particular retailer. If an order for more than 20 gadgets is received from that retailer, a warning is immediately generated that the order appears unreasonable.

Logical relationship check: It checks logical relationship amongst two or more fields in a record to ensure data integrity rules of database. For example, date of manufacture cannot be earlier than date of expiry., amount of payment cannot be greater than amount of invoice etc.

Sequence check: This check is to ensure the sequence of documents. The sequencing is done either by the computer itself or where overriding of sequence may be extremely necessary, the user types the sequence number which is checked by the computer. For example, serial numbers of purchase orders of a company are normally allotted by the computer. If serial numbers are allotted manually, then any number which is entered twice as well as any out of sequence number is rejected.

On completion of data entry of each batch, a list is printed that is compared with the original source. Any error found in comparison is immediately corrected:

This check ensures data accuracy; however, this is incomplete. After correction of errors found in the first list, another list reflecting all changes made since the printing of first list should be printed. The 2nd list will be compared with the first list and any errors found are then corrected. This process is to be continued until removal of all errors. Afterwards, the data will be locked so that no modification could be made.

I would look for the following information in the **audit trail** to ensure its effectiveness:
(i) The identity of the data source.
(ii) The identity of data entry source. (person/process)
(iii) Time and date of data capturing process.
(iv) Identifier of the physical device used to enter data into the system. (computer mac address)
(v) The account or record to be updated by input data.
(vi) The number of physical or logical batch to which each transaction belongs to.

Case Study: You have been appointed by Peak Bank Limited to review various controls over its nationwide money transfer service which has been launched recently. To avail the service it is not necessary for the customers to open an account or even to visit the bank premises. PBL has authorized various merchants to execute the transactions. Customers are required to fill a form containing the following fields:
- Name of sender
- CNIC # of sender
- Mobile/Phone number of sender
- Name of receiver
- CNIC # of receiver
- Mobile/Phone number of receiver
- Amount to be sent

To initiate the transaction, the merchant logs on to the bank's website using his ID and password and enters the transaction details. The sender is then requested to enter a password which he has to communicate to the receiver. Transaction confirmation alerts are received by the sender as well as the receiver, on their mobile phones. The receiver is required to visit his nearest authorized merchant to

collect the money. He receives the money on showing his original CNIC, transaction confirmation SMS and the password set by the sender.

Input controls: We would evaluate whether the following types of controls are in place:
(i)The system ensures that all validated fields are entered.
(ii)The system highlights/reports amounts outside of the expected range.
(iii)There are appropriate controls to ensure that no values beyond the expected limits are accepted.
(iv)There are appropriate controls to ensure that the total value of messages is within an agreed (daily) limit.
(v)Transaction amount and receiver's CNIC are keyed-in twice at the time of transaction initiation.
(vi)The initiating merchant checks the transaction detail with the originating document before finally submitting it to the bank's website.
(vii)The system generates control totals for number and value of messages input, and checks them against input records.
(viii)Sequence of fields on the form at the bank's website should be same as in the printed form to be filled by the sender.
Transmission and system failures controls: We would evaluate whether the following types of controls are in place:
(i)In case of message interruption during transmission, whether the system provides a record / acknowledgement of accepted messages.
(ii)Whether there are written procedures for the retransmission of non-accepted messages.
(iii)Whether list of all messages is reconciled with list of accepted and list of rejected messages.
(iv)Whether an incident log is kept for all interruptions.
(v)Whether there are controls to prevent duplication of message processing following system recovery.
(vi)Are appropriate procedures in place to address an abrupt failure when the sender's message is being processed and the initiating merchant's system is not restored within reasonable time.
(vii)Is proper helpline service available?
(viii)Whether interruptions are reviewed.
(ix)Whether the communications protocol uses error-detection/correction techniques.
(x)Whether the system generates any check-sums, control totals etc.
(xi)Whether UPS, alternative hardware resources and other necessary backup equipment are in place?

Case study: Mr. Akhlaq is conducting the information systems audit of Varied Services Limited (VSL). Some of the policies regarding users' account listed by the IT Manager are as follows:
(i) Users' accounts are created by the system administrator only.
(ii) Initial passwords are communicated to the users confidentially.
(iii) Password must follow a complex syntax.
(iv) Users can not repeat their last seven passwords.
(v) Users' accounts can only be unlocked by the system administrator on written request from the user.
(vi) Logon IDs of employees who take more than one week's leave are made inactive on intimation from HR department.

To **verify** that these settings actually are working, Mr. Akhlaq can perform the following manual tests:
(i) He should logon to the domain server with various privileged/key user IDs, including the ID of system administrator, and try to create new users. The creation of user IDs should be allowed to the system administrator only.
(ii) He can interview a sample of users to determine how they were communicated their first passwords. If the passwords were communicated through phone or verbally, this shows a control weakness. The passwords should have been given to the user by-hand, in a sealed envelope.
(iii) He should attempt to create passwords in a format that is invalid, such as too short, too long, incorrect mix of alpha or numeric characters, or the use of inappropriate characters.
(iv) He should attempt to create passwords which are same as any of the previous seven passwords to ascertain whether these are accepted by the server or not.
(v) He can review system logs and try to identify the users' account lock out incidences of the past. Once such incidence is found, he should check whether a written request is present with the system administrator in respect thereof.
(vi) He should obtain a list of those employees from the HR department who are presently on leave. Then he should check whether a written intimation from HR department is present with the system administrator and check whether their accounts have been disabled/locked out by the system administrator.

Q. Karim Associates is a partnership firm of legal attorneys and has offices in Karachi, Lahore and Islamabad. Up to 30 June 2012, the firm maintained its accounting records manually. With effect from 1 July 2012, it switched over to a software-based computerised accounting system. However, the partners are not satisfied with the reports generated by the new software. The firm has asked you to review the accounting software.
Required:
List the tests of controls that should be performed in order to assess the weaknesses in the system/controls.

The following **test of controls** may be performed:
(i) Verify adherence to processing control procedures by observing computer operations.
(ii) Reconcile a sample of batch totals and observe how discrepancies (if any) are removed.
(iii) Trace disposition of a sample of errors flagged by data edit routines to ensure proper handling.
(iv) Verify processing accuracy for a sample of sensitive transactions.
(v) Verify processing accuracy for a selected computer generated transactions.
(vi) Search for erroneous or unauthorized code via analysis of program logic.
(vii) Monitor online processing using concurrent audit techniques**.**

Q. As part of an IS audit, you are documenting the IT general controls and mapping them with the best practices. You have noted that all the users have access to the entire printing options. The client is of the view that this practice makes the system user friendly and enhances its operating efficiency. The client also believes that it would not create any threat.
Required:
Comment on the arguments provided by the client and state what action would you take. (05 marks)

The arguments provided by the client do not seem appropriate on account of the following:

(i) Unrestricted access to the report option results in an exposure of information to undesired users. A careful analysis is to be done to determine the relevant user to access and print a report.
(ii) Efficiency and effectiveness are not relevant factors in this situation. They might exist but the cost / risk is higher.
(iii) User friendliness and flexibility for everybody is never the first choice for an IT system, particularly at the cost of information security. The system needs to be user friendly for the intended users only.
(iv) Information could be transmitted outside as electronic files i.e. without printing hard copies as print options allow for printing in an electronic form as well e.g. like print to file, or print to PDF.

Therefore, it can be concluded that a greater exposure exists since blanket permission is available to all users. Accordingly, this point should be reported to the management.

Q. Your firm is engaged in the audit of an information system processing facility. You have been assigned the task of evaluating the effectiveness of the logical and environmental controls related to the following areas:
(i) Data confidentiality, integrity and availability
(ii) Power and fire hazards
Required:
Specify the questions that you would ask and the matters that you would like to observe to assess the effectiveness of controls related to the above areas.

To evaluate the effectiveness of the logical and environmental controls related to the given areas I would ask the following questions:
(a) **Data confidentiality, integrity and availability**
(i) Is there a corporate policy requiring strong passwords?
(ii) Is there a corporate policy requiring periodic change of passwords? If so, what is its periodicity?
(iii) Are employees aware that passwords and accounts are not to be shared?
(iv) Whether users' passwords are communicated in a secure manner?
(v) How sensitive data is being stored? Password protected or encrypted?
(vi) Is there a user authorization matrix in place?
(vii) Is the use of external storage devices allowed? If so, what controls are in place to minimise the exposures due to use of such devices?

(viii) How the media containing confidential and sensitive information, which is no longer required, is disposed off?
(ix) Enquire and seek evidence if users' activity logs and audit trails are maintained and reviewed.
(x) Enquire and seek evidence if prior written authoristaion is required for modification in data.
(xi) Are all workstations running the latest version of antivirus software, scanning engine and service packs of operating/application software?
(xii) How does the data and application software backed up? (frequency /procedure)
(xiii) Are backup files periodically restored as a test to verify whether they are a viable alternative?
(xiv) Are backup files sent to a physically secure offsite location?

(b) **Power and Fire hazards**
(i) Enquire whether any fire fighting system is installed.
(ii) Observe whether smoke detectors, water sprinkles, fire extinguishers fire blankets are placed in strategic visible locations throughout the facility.
(iii) Enquire and seek evidence whether the fire extinguishers and other fire fighting components are inspected periodically.
(iv) Enquire and seek evidence whether the fire fighting drills are conducted periodically.
(v) Enquire if there is any emergency exit for staff to evacuate safely in case of fire.
(vi) Observe whether emergency exit is visibly marked and easily accessible.
(vii) Interview staff to ascertain their training and awareness level as regards to fire hazard and evacuation procedures.
(viii) Observe that electrical surge protectors are installed on sensitive and expensive computer equipment.
(ix) Visit the IT facility at regular intervals to determine if temperature and humidity are appropriate.
(x) Seek evidence whether fire fighting equipments, electrical fittings and UPS are inspected/tested frequently.

Q. Sunny Bank Limited (SBL) has recently entered into an arrangement with Glitter Inc. (GI), which provides facilities for world-wide transfer of funds. GI has installed a dedicated system application covering all branches of SBL, for electronic transfer of funds and interchange of data. The installed application will run over a Value Added Network.
Required:
As the SBL's Internal IS Auditor, identify and briefly explain any twelve controls which you would look for, in the GI's application.

I would look for the following controls while reviewing the GI's application:
(i) Internet encryption processes put in place to assure authenticity, integrity, confidentiality and non-repudiation of transactions.
(ii) Edit checks to identify erroneous, unusual or invalid transactions prior to updating the application.
(iii) Additional computerized checking to assess reasonableness and validity of the transactions.
(iv) Assess whether all inbound/outbound transaction are being logged.
(v) Check whether total number and value of transactions as reported by various branches are being reconciled with the totals communicated by GI.
(vi) Segment count totals built into the transactions set trailer by the sender.
(vii) The system has inbuilt controls whereby amounts remitted but not acknowledged by SBL within a specified time are investigated by GI.
(viii) Any change in GI's receiving centres details are duly approved and promptly documented.
(ix) Receiving centre's code is matched automatically by the system with the approved list, prior to each transaction.
(x) Approval limits have been assigned to the concerned users and are verified by the system before executing each transaction.
(xi) Initiation, approval and transmission responsibilities for high risk transactions are appropriately segregated.
(xii) Management sign-off on programmed procedures and subsequent changes are appropriately documented.
(xiii) Reporting of large value or unusual transactions for review, prior to or after transmission. (Exception reporting)

Q. Shakeel Enterprises Limited (SEL) is in the process of computerising its payment function. The system would consist of two modules, one pertaining to purchase of goods and the other for all remaining payments. The present system of payments against goods involves the following key processes:

 Purchase Order (PO) is raised by the Purchase Department.
 On receipt of goods a Goods Received Note (GRN) is prepared by the Store In-charge.
 The Accounts Officer processes the supplier's Invoice by matching the quantities purchased and price with GRN and PO and checking arithmetical accuracy of the Invoice.
 The payment voucher and cheque is prepared by Senior Accounts Officer and the cheque is finally signed jointly by the Finance Manager and a Director of the company.

Required:

List the significant controls that SEL should incorporate while computerising the payment of goods.

SEL should incorporate the following **controls** while computerizing its payment function:

(i) Data entry of Purchase Order (PO), Invoice, and Goods Received Note (GRN) should be made by different users using their own IDs and passwords.
(ii) The authority limits should be assigned to the authorized persons in line with company's policy.
(iii) The POs and GRNs should have computer generated numbers and date.
(iv) The computer system should match the details on the PO, Invoice and GRN.
(v) The system should check the accuracy of computations.
(vi) The system should prepare the cheque for manager to sign.
(vii) Reports of POs and GRNs issued should be electronically reviewed by a senior officer at regular intervals.
(viii) The system should prepare exception reports such as POs/Invoices outstanding for longer than a certain time period.