Audit in CIS Environment – Bird Eyeview

Basics of CIS Environment	Internal Controls in CIS Environment		Audit Techniques
	Management Perspective – Design & Exercise	**Auditor Perspective - Evaluation**	
1. Meaning 2. Types of Processing System 3. Types of File Systems 4. Characteristics of CIS Environment	1. Controls to be Exercised (a) General CIS Controls • Organisation Structure Controls • System Development Controls • System Software Controls • System Operation Controls • Data Entry and Program Controls (b) CIS Application Controls • Control Over Input • Control Over Processing • Control over Output 2. Problems Faced while exercising controls in CIS Environment	1. Controls to be evaluated 2. Clauses of Controls to be evaluated 3. Audit Plan to determine the reliability of controls evaluated	1. Audit Trail 2. Computer Assisted audit Techniques (CAAT) • Meaning of CAAT • Need of CAAT • Uses of CAAT • Types of CAAT – Audit Software & Test Data • Considerations in application of CAAT • CAAT in small Organisations • Controls procedures using CAAT • Characteristics of Audit Program 3. Collection and Evaluation of Audit Evidence 4. Tagging and Tracing

Audit in CIS Environment - Basics

Types of Processing System		Types of File System	Characteristics of CIS Environment
Batch Processing System	**Online Real Time Processing System**		
Meaning: Transactions are accumulated and processed in a group. **Steps**: 4 steps • Occurrence of transaction. • Recorded in transaction file • Updation of master file. • Generation of output. **Advantages**: Simple, existence of Audit Trail, processing volume of transactions. **Limitations**: Time gap in between occurrence and processing.	**Meaning**: Transactions are processed as they occurred. **Features**: • Validation Check. • Online access of system to users. • Non-existence of audit Trail. • Unrestricted access to programmers. **Advantages**: Immediate processing and continuous updation. **Limitations**: Non-existence of Audit Trail.	1. **Flat File System**: • Exclusive access to and use of individual data. • Wastage of memory space and data redundancy. 2. **Integrated Database System**: • Inter related master files to reduce data redundancy. • Work with OLRT System	1. Lack of Transaction Trail 2. Uniform Processing of Transaction 3. Lack of Segregation of Functions. 4. Potential for Errors and Irregularities 5. Automatic execution of transactions. 6. Dependence of other Controls over computer processing. 7. Potential for increased management supervision. 8. Potential for use of CAAT.

Audit in CIS Environment – Internal Controls – Management Perspective (Design and Exercise)

Controls to be designed and exercised			Problems in implementation of Internal Control in CIS
General CIS Controls	**CIS application Controls**	**Other Safeguards**	
Purpose: To establish framework of overall control over CIS Activities & provide reasonable assurance that overall objectives of I.C. are achieved. **Types**: 5 Types 1. Organisation Structure and Management Controls. 2. Application System Development and Maintenance Controls. 3. Computer Operations Controls. 4. System Software Controls 5. Data Entry and Program Controls	**Purpose**: To establish specific control procedures over the accounting applications and provide reasonable assurance that all transactions are authorized, recorded and processed on a timely basis. **Types**: 3 Types 1. Controls over Input 2. Controls over processing 3. Controls over Output.	1. Offsite back up of data and computer programmes 2. Recovery procedures in the event of loss of data. 3. Provision for offsite processing	1. Separation of Duties. 2. Delegation of authority and Responsibility. 3. Availability of competent and Trustworthy person. 4. System of Authorisation due to inbuilt controls. 5. Non-Existence of adequate Documents & Records. 6. Physical Control over assets and records due to risk of loss and unauthorised access. 7. Management Supervision over employees as work may have to be carried out remotely. 8. Difficult in detection of unauthorised modifications to programs or data files.

Audit in CIS Environment – Internal Controls – Auditor Perspective (Evaluation)

Controls to be Evaluated over Data	Clauses of Controls to be evaluated	Audit Plan to determine Reliability of Controls
1. **Organisation structure Control** – Authority and Responsibility 2. **Documentation Control** – Existence, Adequacy, Authorisation for Changes 3. **Access Control** – Unauthorised access 4. **Input Control** – Authorised and Validation Check 5. **Processing Control** – Integrity of data, validation check 6. **Recording Control** – records to be kept free of errors 7. **Storage Control** – Back up and recover facilities 8. **Output Control** – access to authorized person, audit trail	1. **Authenticity**: to verify the identity of individuals involved. 2. **Accuracy**: to ensure correctness of data 3. **Completeness**: to ensure that no data is missing. 4. **Privacy**: to ensure protection of data. 5. **Audit Trail**: to ensure traceability of all events. 6. **Redundancy**: to avoid data duplication. 7. **Existence**: to ensure ongoing availability of system resources. 8. **Asset Safeguarding**: protection of resources from destruction. 9. **Effectiveness**: to ensure that system achieves its goals. 10. **Efficiency**: use of minimum resources to achieve goals.	1. Existence and Effectiveness on Controls desired. 2. Generality versus specialty of control. 3. Focus on: • Preventive Controls • Detective Controls • Corrective Controls 4. Number of components used to execute the control.

Audit in CIS Environment – Audit Techniques

Audit Trail	CAAT – Computer Assisted Audit Techniques		
	Meaning, Need and Uses	**Commonly Used CAAT**	**Considerations in Use of CAAT**
Meaning: Facility to trace individual transactions from source to completion or vice versa. In CIS Environment, audit trail is often missing or sketchy. **Reason for non-existence of Audit Trail in CIS**: 1. Non-availability of source documents. 2. Replacement of ledger summaries by Master Files. 3. Generation of reports on exception only. **Remedies for audit trail**: • Use of Computer Programs. • Use of Test Packs (Test Data)	**Meaning**: Those auditing Techniques that take assistance of computer for being applied to audit. **Need for CAAT**: arises due to 1. Absence of Input Documents. 2. System generated Transactions; 3. the lack of a visible audit trail; and 4. the lack of visible output. **Uses of CAAT**: in performing various auditing procedures: 1. *Compliance Test of General CIS Controls*: through Test Data 2. *Compliance Test of CIS Application Controls*: through Test Data 3. *Test of details of transactions and balances*: by use of Audit Software 4. *Analytical Review*: by use of Audit Software	1. **Audit Software**: Computer programs used by auditor to process data of audit significance. 3 types • **Package Programs**: Generalized programs designed to perform data processing. • **Purpose Written Programs**: Programs designed to perform audit task in specific circumstances. • **Utility Programs**: Programs to perform common data processing functions. Not designed for audit purpose. 2. **Test Data**: A set of Hypothetical data entered into computer system of organisation and result obtained is compared with pre-determined results. It is used in an "**Integrated Test Facility (ITF)**" where a dummy unit is established and to which test transactions are posted during normal processing. Under these circumstances, auditor is required to ensure that test transactions are subsequently eliminated. 3. **Tagging and Tracing**: It involves tagging the client's input data in such a way that relevant information is displayed at key points. It uses the actual data and hence no need of reversal.	1. Availability of Sufficient IT knowledge and Expertise. 2. Incompatibility between CAAT and Computer Facilities. 3. Impracticability of manual test. 4. Impact of effectiveness and efficiency in extracting a data 5. Time Constraints.

Control Procedures while using CAAT	Essential features of Computer Audit Program	Collection and Evaluation of Audit Evidence – Reasons for Changes
Audit Software Application: 1. Participating in design and testing. 2. Checking the coding of the programme. 3. Ensure Compatibility of software with entity's operating system. 4. Running the audit software on small test files before running on main data files. 5. Ensuring that the correct files were used. 6. Obtaining evidence that the audit software functioned as planned. 7. Establishing security measures to safeguard against manipulations of the entity's data files. **Test Data Application**: 1. Controlling the sequence of submissions of test data. 2. Performing test runs containing small amounts of test data before submitting the main audit test data. 3. Comparing results of the test data with pre-determined results. 4. Ensure Test data is processed over the answered version of programmes. 5. Ensure that the programmes used to process the test data were applied throughout the applicable audit period.	1. Simplicity 2. Understandability 3. Adaptability 4. **Vendor Technical Support** – Installation, documentation, training, updations. 5. **Capability of statistical Sampling** – at different confidence levels. 6. **Acceptabilty** – to both auditor and computer centre in terms of compatibility, interference etc. 7. **Processing Capabilities** - Multiple applications, extended data selection, stratification etc. 8. Ability to prepare multiple reports.	**Reasons for Changes in Collection of Evidences**: 1. Existence of diverse and complex range of I.C. technology. 2. Rapid development in Hardware and Software technology. 3. Cryptographic Controls to protect the privacy of data. 4. Non-possibility of collection of audit evidence by manual means. **Reasons for Changes in Evaluation of Evidences**: 1. Increasing complexity of computer system and control technology. 2. Updation of Multiple data by a single input transaction. 3. Deterministic nature of errors. 4. Speed at which errors are generated and the high cost and effort to correct and rerun the program.

Examination Weightage (Nov. 08 – Nov. 11)

N-08	8	Clauses of control
M-09	0	
N-09	8	Collection and Evaluation of audit evidence
M-10	0	
N-10	8	Review of Controls by auditor
M-11	0	
N-11	5	Audit Plan for Evaluating the Reliability of I.C.

Important Questions

Q. No. 1: "Online Real time processing system and Batch Processing System have their inherent strengths and weeknesses". Comment.

Q. No. 2: Discuss the control procedures which the auditor should adopt in applying CAAT in an audit under CIS Environment.

Q. No. 3: State the important characteristics of an effective system of computer audit programme.

Q. No. 4: "The method of collecting and evaluating audit evidence in CIS environment changes drastically" Comment.

Q. No. 5: State the specific problems, which may arise in the implementation on internal control in CIS Environment.

Q. No. 6: The auditor must evaluate major clauses of control used in a CIS System to enhance its reliability. Comment.

Q. No. 6: Write Short Note on: (a) Uses of CAAT (b) Tagging and Tracing