Volume

1

ADVANCED AUDITING AND PROFESSIONAL ETHICS

PAPER 3 : CA Final

AUTHORED BY CA AKHIL MITTAL

DISHAAN COMMERCE ACADEMY

Self-Study guide for Audit

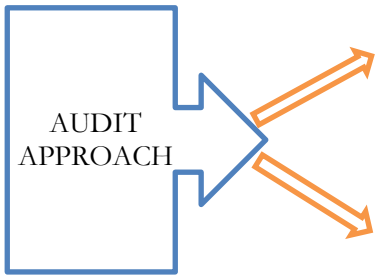
Faridabad
Phone 8826400873 • www.dcacademy.co.in

Chapter 1

AUDIT UNDER COMPUTERISED INFIRMATION SYSTEM (CIS) ENVIRONMENT

(A) Impact of computerization on audit approach:

Impact of Computerization on audit	Following are the factors to be kept in mind: 🗁 High speed of generating information without much loss of time. 🗁 Clerical error is minimized. 🗁 Computer program perform more than 1 function at a time resulting in non-deployment of personnel for every work in traditional approach. 🗁 System software controls are designed to provide reasonable assurance in a manner that they are designed and implemented in authorized manner. 🗁 Shifting of manual work to CIS has resulted in reporting of transactions with exceptional nature. It means that reporting of instances which occur by getting deviated from standard process 🗁 Wrong/incorrect system development may result in more harm
Audit approaches	**Following are the audit approaches in CIS environment:** 🗁 A black Box approach (Audit around the computer) 🗁 A White Box approach (Audit through the computer)



BLACK BOX TESTING:

-- Auditor concentrates on input and output & ignores processing of data.
-- If input matches output, then auditor assumes processing is correct
-- Output derives manually may be tested with output from computer.
-- Ease in audit trail but auditor not having directly tested the controls.

WHITE BOX TESTING:

-- Auditor controls input, processing part and output also.
-- In order to help the auditor to gain access to these processes, audit software may be used.
-- Auditor needs to have sufficient knowledge of computers to plan or direct.
-- Output derives manually may be tested with output from computer

Areas covered under Audit	**The areas covered in an auditor concentrate on these below controls:** ■ Input controls ■ Processing Controls ■ Storage Controls ■ Output Control, and ■ Distribution control	
	Auditor Role	■ Need to satisfy that there exist adequate controls. ■ Need to segregate transactions which are done manually and through computerized system. ■ Need to ensure that adequate supervision of personnel is administrated.
	Audit Process	Audit involves risks, exposures and need experiences and application of knowledge and expertise to handle different circumstances.
	Requisite for CIS	Auditor need not to have adequate knowledge and expertise of the system, but also must get exposed to system analysis and design so as to facilitate post implementation audit.
Effect of computers on Internal controls	Internal controls include separation of duties, delegation of authority and responsibility. So after computerization of business activities, auditor needs to know the effects of computers on the internal controls. These effect are:	
	Segregation of Duties	• Different persons are responsible for carrying various functions. • E.g. in computer system a program may carryout reconciliation of vendor invoices against a receipt document and also prepare a cheque payable to trade payable.
	Control overs assets & records	• Physical access to assets and records is critical in any type of system. • In computerized system, all records are concentrated at a single place hence the probability of losses of data to un-wanted events is high.
	Adequate Records & Documents	• Safeguard of assets and records are imperative in any system. • In manual system, documents and records are required to provide an audit trail. In computerized system, audit trail is not visible but auditor must assure that systems are designed to maintain all records of transaction.
	Authority & Responsibility delegation	• Structured authority is essential for any type of system. • In computerized system, no clear line of authority can be established since single resource is used by multiple users e.g. data Base Mgmt. System. • Some entity may have a single user as owner of the data.

Code to Remember

S.C. – RAMPS (Supreme Court RAMPS)

	Management Supervision to be adequate	• Under computerized system, supervisory control must be built in the system to compensate for the controls that usually can be exercised through observation. • Managers must periodically access the audit trail of employee activities and examine it for unauthorized actions.
	Performance check	• In computerized system, if a program code is authorized accurate and complete system will always follow the laid down procedure. • Independent checks on performance of programs have little value. Instead the control emphasis shifts to ensuring the veracity of program code.
	System Authorization	• Management authorization of transaction may be either: (a) **General authorization to establish policies for the entity.** (b) **Specific authorization applying to individual transactions.**
Effect of computers on Auditing	Auditors must provide competent opinion on financial statement so as to give true and fair view of affairs of the company. Computer has significant influence on how auditor collect the evidences:	
	Change to Evidence Collection	Collecting evidence in a computerized environment is far more complex as compared to manual system. Auditor has to face different type of technological controls which involves **system development controls and also requires set of hardware controls.** The effect of computers are: • Auditor must keep himself updated due to continuous advancement in field of technology. • The top most priority is to protect the data by obtaining reliance on the cryptographic controls. • Auditor faces difficulty in collecting evidences on reliability of controls due to rapid development. • Hence auditors have to run through computer system themselves if they have to collect the evidences.
	Change to Evidence Evaluation	Due to almost 100% automation in business operations, it is difficult for auditors to evaluate weakness and strengths of controls mechanism for placing reliability over whole system. Auditor need to ensure that: (a) Whether control is functioning reliably or multi-functioning. (b) Traceability of control strengths and weakness through the system. • An erroneous program results in incorrect data processing. • Error in computer program can involve extensive redesigning and reprogramming. • Controls warranting high quality computer system must be implemented and tested upon. • These controls must be strong enough to ensure safeguarding if assets, data integrity, system effectiveness & system efficiency.

Internal Controls in CIS environment

Internal control is pre-requisite for efficient and effective of evert type of management. In nut shell they are policies and procedures to be followed by the organization to achieve the objectives.

Due to computerized environment in entity, some of the internal controls **are CIS specific. However,** to set up internal control in CIS environment, overall CIS operations need to be broken in-to sub-systems. Basic component in a CIS environment"

- Hardware - CPU, monitor, printer etc.
- Software- Operating System, Data base management system etc.
- People – Data Entry operator, End user.
- Transmission Data.

Controls that are used to enhance component reliability

Major classes of controls that auditor must evaluate are:

Effectiveness Control	This control attempts to ensure that system achieve the required i.e. monitoring of user satisfaction.
Efficiency Control	This control attempts to ensure that system uses minimum resources to achieve desired results.
Audit Trail Controls	This control ensures traceability of all events occurred in a system. This is needed to answer queries, questions, detecting errors etc.
Authenticity Controls	This control exercised to verify the identity of the individuals or process involved in a system.
Safeguard Asset Control	This control attempts to ensure that all resources within a system are protected from any kind of destruction or damage.
Completeness Control	This control attempts to ensure that no data is missing and processing of such data is carried through proper channel.
Redundancy Control	This control attempts to ensure that a data is processed only once. (Meaning – फालतूपन)
Accuracy Control	This control attempts to ensure correctness of data and processes in a system.
Privacy Control	This control attempts to ensure that data is protected from unauthorized disclosures or access.

Internal control requirement under CIS environment	The requirement of internal control under CIS environment may cover the following aspects:	
General control in CIS	**Organizational & Management control**	• Designed to establish organizational framework for CIS. • Segregation of incompatible functions.
	Application system development & Mgmt. Control	• Systems are designed & maintained in authorized manner. • Control over changes made to application system. • Control over access to system documentations.
	Computer Operations Control	• Designed to control operations of the system. • Ensures systems are used for authorized purposes only. • Assures that errors are detected and corrected.
	System Software control	• This control ensures that system software is acquired/ developed in authorized manner. • Includes testing, implementation & documenting new system.
	Data Entry & Program Control	• Designed to provide assurance of access to data & program by authorized personnel only. • Authorization structure is established.
	Control Over Input	Control designed to provide reasonable assurance that-. • Transactions are properly authorized. • Transactions converted into machine readable form. • Transactions are not lost, added or duplicated or changed. • Incorrect transactions are rejected.
Pre-requisite while conducting audit under CIS	**Skill and Competency**	Auditor should have sufficient knowledge of computer information system to plan, direct, supervise and control the work performed.
	Planning	To plan audit, understanding of entity is must. Also significance of computer process, complexity, availability of data source documents, files etc.
	Assessing Risk	When CIS are significant, the auditor should assess whether it may influence the assessment of control and inherent risk.
	▪ There exists application system software, where there may not be complete audit trail. ▪ Computer program processing transactions virtually eliminating the clerical errors. ▪ Many controls become concentrated in CIS environment allowing data processing of incompatible functions. ▪ The auditor may apply computer audit techniques in execution of audit tests. ▪ Certain manual controls are dependent on computer generated controls for their effectiveness. ▪ Some process may be initiated internally which cannot be monitored manually.	

(B) REVIEWS OF CHECKS AND CONTROLS IN CIS ENVIRONMENT:

Erroneous data processing by a computer system is likely to be the result of incorrect data input. They operate over data moving into, through and out of the computer to ensure correct, complete and reliable processing and storage.

Organizational Structure/Control	CIS need to be organized in a manner that different groups are formed to perform different duties in a large CIS environment. Some of the typical function that must be performed by select groups includes:	
	Data Administrator	• Generates data requirement of users of information system. • Formulates plan, policies, and evaluation of data bases.
	Database Administrator	• Responsible for operational efficiency of corporate database.
	System Analyst	• Manage information requirement for new/existing applications. • Writes procedures, facilitates information system architecture.
	System Programmer	• Maintains and enhances operating system software. • Network, library software when unusual system failure occurs.
	Application Programmer	• Design programs to meet information requirements. codes; • Test, debugs program documents programs.
	Operational Specialist	• Maintains and enhances operating system software. • Network, library software when unusual system failure occurs
	Librarian	• Maintain library of magnetic media and documentation. Auditor must be concerned about below 2 things: Responsibilities of each job position must be clear. The job performed within information system function should maintain separation of duties.
Documentation Control	System and program must be adequately documented and properly approved before being used. (a) A system Flowchart (b) A program Flowchart. (c) Program Change (d) Operator Instructions (e) Program Description Adequate documentation evidencing approval of changes minimizes the probability of unauthorized system and program changes that may result in loss.	
Access Controls	This control aims to prevent unauthorized access to the system. This indeed ensures that unauthorized person don't have access to vital information of the organization.	

	Visitor Entry Log	• Log to be used to determine and documents those who have had access to the area.
	Segregation Log	• Access to perform documentation should be limited to those persons who require it. • Access to data and programs should be limited to those individual authorized to process data. • Access to computer hardware should be limited.
Code to Remember **V. – S.C.A.L.E.**	Call Back	• Specialized form of user identification in which user dials the systems identifies him and is disconnected from the system. • Either individual finds manually telephone number or system automatically finds authorized telephone number of individual.
	Application Controls	• Programmed application controls apply to specific application rather than multiple applications.
	Limited Physical Access to computer Facility	• Physical facility (Hold computer equipment, files) should have controls to limited access to authorized person. • These controls are- Using guard, automatic key cards, palm prints etc.
	Encryption	• Data is encoded when stored in computer files. • This coding protects data to use unauthorized data users must not only obtain access, but also decrypt data.
Input Controls	Input controls should be properly authorized and approved. It should verify all the relevant data filed used to record information.	
	Pre Printed Form	• All information to be printed on a source document.
	Check Digit	• There may be error while keying data leading to serious results. • One control used to guard against these types of error is "Check Digit" • A check digit can act a prefix. When the code is entered, a program recalculates the check digits to determine accuracy of data.
	Completeness Total	• To input data erroneously is one type error. To leave complete data is another type of error. • Batch Control, Batch Hash Control, Batch record Total, Sequence checks are the controls used to find out errors in inputs
	Reasonable Checks	• Sophisticated form of limit checks. • The check consists of subtracting last reading recording from the current reading and comparing with average usage for the period.
	Field Checks	The following types of field checks may be applied-

	Code to Remember M.A.R.S	**M**ater Reference	■ If master file can be referenced at same time input data is read, is there a master file match for key field.
		Alphabetic / Numeric	■ Doe a field that should contain only alphabetic or numeric contain alphanumeric characters.
		Range	■ Does that data for a field fall within allowable value range.
		Size	■ If variable-length fields are used and a set of permissible size is defined, does the field delimiter show the field to be one of these valid sizes?
	Record Checks	Following types of record checks can be applied:	
	Code to Remember M.A.R.S	**V**alid-sign Numeric	■ The content of one field might determine which sign is valid for a numeric field.
		Reason-ablensess	■ Even though a field value might pass a range check, the content of another field might determine reasonable value for the field.
		Size	■ The permissible sixe of fixed and variable length records also might depend on a field indicating record type.
Processing Controls	These controls are used when the inputs are done by the user. Processing controls ae essential to ensure the integrity of data. Following are the validation checks:		
	Cross – Footing	■ Separate Control totals can be developed for related fields and cross footed at the end of a run.	
	Run to Run Control	■ In tape based processing, processing involves several runs.	
	Range	■ An allowable value range can apply to a field.	
	Overflow	■ It can occur if a field used for computation is not initiated to zero at start.	
	Sign Test	■ The content of one record type field might determine which sign is valid for a numeric field.	
Recording Controls	This control enables records to be kept free of errors and transactions details that are input into system.		
	Error Log	■ Accuracy checks can only be carried to during run time processing. ■ It is important that a detected error can doesn't bring the run to halt.	
	Transaction Log	■ This log provides a record of all transactions entered in the system. ■ The transaction will be "stamped" with details of input. This includes input date, time, day, terminal number and user number.	

Storage Controls	This control ensures accurate and continuing and reliable storage of data. Special care must be taken to ensure integrity of the data which is vital resource of any organization. Following checks may be considered:	
	Physical Protection	■ Magnetic tapes carry rings to modify, re-write or erase the data. ■ Once these rings are removed, the files in the disks can be for read-only purpose.
	Label	■ These are attached to tapes to identify the content.
	Back-up Routine	■ Copies are taken for the information which is vital and confidential. ■ Backup process involves computer operation in which one file is used to produce same file.
	Cryptographic Storage	■ Data in computer files are written with the use of coding like ASCII, EBCDIC etc. ■ It can be interpreted by unauthorized reader gaining access to file.
	Data-Base Back-up Routine	■ Content of Data base is periodically dumped on to back up files; ■ Which is a tape which is then stored together with transaction log tape of all transactions occurring between last & current dump.
Output Controls	Output controls ensure that results of data processing are accurate, complete & are directed to authorize recipients. Auditor must check audit trail related to output.	

Code to Remember

P.L.B. – C - DBB
Pyare Lal Bhawan (PLB) Mein See(C) Database ka Backup (DBB)

(C) COMPUTER ASSISTED AUDIT TECHNIQUES:

Under CAAT, auditor uses computer as an audit tool for enhancing the effectiveness and efficiency of audit procedures. CAATs are computer programs and data that auditor uses as part of audit procedure to process

Use of CAATs	CAATs can be used for conducting various audit procedures. These are: ■ Test of details of transactions & Balance. **(E.g. recalculating interest etc.)** ■ Analytical procedures **(E.g. Identifying inconsistencies or fluctuations etc.)** ■ Test of general controls **(E.g. Testing set-up, configurations etc.)** ■ Sampling programs to extract data for audit testing. ■ Test of application control **(E.g. Testing functionality of programmed control)** ■ Re-performing calculations performed by entity's accounting systems.	
Audit Software	CAATs allows auditor to give access to data without depending on the client system. CAATs may consist of packages programs, purpose-written programs, utility programs etc. Following is the brief discussion on these programs:	
	Package Program	■ Generalized computer program designed to perform processing function. ■ E.g. reading data, selecting data, analyzing information etc.

	Purpose-Written Program	■ Performs audit tasks in specific circumstances. ■ These programs may be developed by auditor, auditee or outside agency hired by the auditor.
	Utility Program	■ Used by the entity to perform common data processing functions. ■ These programs are not specifically designed for audit purpose.
	System Management Program	■ These are tools that are party of sophisticated operating system environment. ■ Not specifically designed for audit purpose but required additional care while using the controls.
Consideration while Using CAATs	Auditor must consider appropriated combination of manual and CAAT. The factors to be considered:	
	Impracticability of manual Test	■ Many computer information systems perform tasks for which no hard copy evidence is available.
	Computer knowledge, Expertise & Experience	■ For conducting audit in CIS environment, auditor need to be expert and should possess necessary skills. ■ Audit team should execute, plan the CAATs techniques for conducting audit in efficient manner.
	Effectiveness & Efficiency	■ Through CAAT, auditing procedures can be improved in order to attain desired results. CAATs are regarded as **efficient way** used to test a large number of transactions by: 🌐 Analyzing and selecting samples from voluminous data. 🌐 Applying analytical procedures. 🌐 Performing substantive procedures (मूल प्रक्रिया) ■ In respect of **efficiency** that an auditor might consider: 🌐 Time taken to plan, design, execute & evaluate CAAT. 🌐 Technical review. 🌐 Designing and printing of forms. 🌐 Availability of computer resources.
	Availability of CAATs & computer Resources	■ Auditor may plan to use computer facilities when CAAT usage is impractical or uneconomical. ■ Auditor may use its own devices. Cooperation from entity's personnel may be required to provide processing facility at convenient time.
	Time Constraint	■ Transaction details records are kept for short period hence auditor should make necessary adjustments for retention of data required.
Steps for Using CAATs	Auditor must follow the following steps to undertake while applying CAAT. To have clear understanding/learning of the steps, please read the below diagram.	

Ovbjective setting ↓ **Data & Content** ↓ **CAAT designing, cost & Control** ↓ **Output** ↓ **Execution and Evaluation**	**Set the objective of CAAT Application** ↓ **Determining the content & accessibility of Entity's file** ↓ **Identify the specific files or database to be examined.** / **Understand relationship between data tables where database to be examined.** / **Arrnage with user & IT, for copies of relevant files.** ↓ **Identify person who may participate in CAAT design.** / **Refine the estimate of costs and benefits** / **Ensure use of CAAT is properly controlled.** ↓ **Reconcile Data to be used for CAAT with accounting & Other records** ↓ **Execute CAAT application and evaluate the results.** **Document CAATs o be used including objectives, flowcharts & run instruction**
Testing CAATs	Auditor should obtain assurance of the integrity, reliability, usefulness through appropriate planning, designing, testing and review of documentation. This is a pre-requisite before relying on CAAT.
Controlling CAATs	**Procedures to be carried out by auditor to control CAATs application:** ■ Participating in design and testing of CAAT. ■ Checking the coding of the program to ensure whether they are in line with the specifications. ■ Asking entity's personnel to review operating system instruction to ensure smooth functioning of software. ■ Running audit software on small files before running it on larger files/population. ■ Checking files by applying control total type of checks. ■ Obtaining evidence that **audit software** functioned as **planned.** ■ Establishing appropriate security measures to safeguard integrity & confidentiality of data.