

CHAPTER 6-AUDIT IN AN AUTOMATED ENVIRONMENT

RELEVANCE OF 'IT' IN AN AUDIT

- Computation and Calculations are automatically carried out (for example, bank interest computation and inventory valuation).
- Accounting entries are posted automatically (for example, sub-ledger to GL postings are automatic).
- Business policies and procedures, including internal controls, are applied automatically (for example, delegation of authority for journal approvals, customer credit limit checks are performed automatically).
- Reports used in business are produced from systems. Management and other stakeholders rely on these reports and information produced (for example, debtors ageing report).
- User access and security are controlled by assigning system roles to users (for example, segregation of duties can be enforced effectively).

Given below are some situations in which IT will be relevant to an audit:

- Increased use of Systems and Application software in Business (for example, use of ERPs)
- Complexity of transactions has increased (multiple systems, network of systems)
- Hi-tech nature of business (Telecom, e-Commerce).
- Volume of transactions are high (Insurance, Banking, Railways ticketing).
- Company Policy (Compliance).
- Regulatory requirements - Companies Act 2013 IFC, IT Act 2008.
- Required by Indian and International Standards - ISO,SA 315,.
- Increases efficiency and effectiveness of audit.

Understanding Automated Environment

- Given below are some of the points that an auditor should consider to obtain an understanding of the company's automated environment:
- Information systems being used (one or more application systems and what they are).
 - Their purpose (financial and non-financial).
 - Location of IT systems - local vs global.
 - Architecture (desktop based, client-server, web application, cloud based).
 - Version (functions and risks could vary in different versions of same application).
 - Interfaces within systems (in case multiple systems exist).
 - In-house vs Packaged.
 - Outsourced activities (IT maintenance and support).
 - Key persons (CIO, CISO, Administrators).

Risks that arise from the use of IT systems

- Inaccurate processing of data, processing inaccurate data, or both.
- Unauthorized access to data
- Direct data changes (backend changes).
- Excessive access / Privileged access (super users).
- Lack of adequate segregation of duties.
- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Loss of data.

Impact of IT related risks i.e. on Substantive Audit, Controls and Reporting

- The above risks, if not mitigated, could have an impact on audit in different ways. Let us understand how:
- First, we may not be able to rely on the data obtained from systems where such risks exist. This means, all forms of data, information or reports that we obtain from systems for the purpose of audit has to be thoroughly tested and corroborated for completeness and accuracy.
 - Second, we will not be able to rely on automated controls, calculations, accounting procedures that are built into the applications. Additional audit work may be required in this case.
 - Third, due to the regulatory requirement of auditors to report on internal financial controls of a company, the audit report also may have to be modified in some instances.

Types of Controls in an Automated Environment

A.)General IT Controls

"General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, miniframe, and end-user environments.

General IT-controls that maintain the integrity of information and security of data commonly include controls over the following:" (SA 315)

1.Data Center and Network Operations

- Activities:
- Overall Management of Computer Operations Activities
 - Batch jobs - preparing, scheduling and executing
 - Backups - monitoring, storage & retention
 - Performance Monitoring - operating system, database and networks
 - Recovery from Failures - BCP, DRP
 - Help Desk Functions - recording, monitoring & tracking
 - Service Level Agreements - monitoring & compliance
 - Documentation - operations manuals, service reports

2.Program Change

- Activities:
- Change Management Process - definition, roles & responsibilities
 - Change Requests - record, manage, track
 - Making Changes - analyze, design, develop
 - Test Changes - test plan, test cases, UAT
 - Apply Changes in Production
 - Emergency & Minor Changes
 - Documentation - user/technical manuals
 - User Training

3.Access Security

- Activities:
- Security Organization & Management
 - Security Policies & Procedures
 - Application Security
 - Data Security
 - Operating System Security
 - Network Security - internal network, perimeter network
 - Physical Security - access controls, environment controls
 - System Administration & Privileged Accounts - Sysadmins, DBAs, Super users

4.Application system acquisition, development, and maintenance

- Activities:
- Overall Mgmt. of Development Activities
 - Project Initiation
 - Analysis & Design
 - Construction
 - Testing & Quality Assurance
 - Data Conversion
 - Go-Live Decision
 - Documentation & Training

These are IT controls generally implemented to mitigate the IT specific risks and applied commonly across multiple IT systems, applications and business processes. Hence, General IT controls are known as "pervasive" controls or "indirect" controls.

B)Application Controls

Application controls include both automated or manual controls that operate at a business process level. Automated Application controls are embedded into IT applications viz., ERPs and help in ensuring the completeness, accuracy and integrity of data in those systems.

Examples of automated applications include edit checks and validation of input data, sequence number checks, user limit checks, reasonableness checks, mandatory data fields.

C) IT dependent Controls

IT dependent controls are basically manual controls that make use of some form of data or information or report produced from IT systems and applications. In this case, even though the control is performed manually, the design and effectiveness of such controls depends on the reliability of source data.

Due to the inherent dependency on IT, the effectiveness and reliability of Automated application controls and IT dependent controls require the General IT Controls to be effective.

TESTING METHODS

When testing in an automated environment, some of the more common methods are as follows:

- Obtain an understanding of how an automated transaction is processed by doing a walkthrough of one end-to-end transaction using a combination of inquiry, observation and inspection.

- Observe how a user processes transactions under different scenarios.
- Inspect the configuration defined in an application.
- Inspect the system logs to determine any changes made since last audit testing.
- Inspect technical manual / user manual of systems and applications.
- Carry out a test check (negative testing) and observe the error message displayed by the application.
- Conduct reperformance using raw source data and independently applying formulae, business rules or validations on the source data using CAATs.

INTERNAL FINANCIAL CONTROLS

- The term Internal Financial Controls (IFC) basically refers to the policies and procedures put in place by companies for ensuring:
- reliability of financial reporting
 - effectiveness and efficiency of operations
 - compliance with applicable laws and regulations
 - safeguarding of assets
 - prevention and detection of frauds

DATA ANALYTICS FOR AUDIT

- Data analytics can be used in testing of electronic records and data residing in IT systems using spreadsheets and specialised audit tools viz., IDEA and ACL to perform the following:
- Check completeness of data and population that is used in either test of controls or substantive audit tests.
 - Selection of audit samples - random sampling, systematic sampling.
 - Re-computation of balances - reconstruction of trial balance from transaction data.
 - Reperformance of mathematical calculations - depreciation, bank interest calculation.
 - Analysis of journal entries as required by SA 240.
 - Fraud investigation.
 - Evaluating impact of control deficiencies.

ASSESS AND REPORT AUDIT FINDINGS

- Are there any weaknesses in IT controls?
- What is the impact of these weaknesses on overall audit?
- Report deficiencies to management - Internal Controls Memo or Management Letter.
- Communicate in writing any significant deficiencies to Those Charged With Governance.



VISIT NJ INFINITY CHANNEL ON YOUTUBE FOR MORE CHARTS / FAST TRACK NOTES AND MCQ'S