Chapter 4 "Audit in an Automated Environment (New Syllabus)"

4.1 – Meaning and Components of Automated Environment

Meaning	Automated Environment may be defined as a system within an overall business environment which comprise of people, processes and technology.
Components	1. Business Applications like Tally, Tally ERP, SAR R/3, Business Suite. 2. Database like Oracle 12g, MS-SQL Server. 3. Operating Systems like Windows, UNIX. 4. Storage Devices like disks, tapes, NAS (Network attached Storage). 5. Network devices like switches, routers. 6. Networks like LAN, WAN, VPN etc. 7. Physical and Environmental Components like CCTVs, temperature controls, firefighting equipment etc.
Real Time environment	• Real Time Environment is a type of automated environment in which business operations and transactions are initiated, processed and recorded on a real-time basis, i.e. immediately on their occurrence. • Examples of Such environments are Airlines and Railway Reservations, CORE Banking, E-Commerce, ERP etc. • Real Time Environment facilitates anytime, anywhere transactions to take place. For this purpose, it is essential to have the systems, networks and applications available during all times.
	IT Components required in Real Time Environment
	1. Applications like ERP, Core Banking Etc. 2. Middleware like web servers 3. Networks like WAN, Internet hosting. 4. Hardware like Data centers, storage devices, power supply etc.

4.2 – Auditing in an Automated Environment

1	**Understanding of Automated Environment**	
	As required by SA 315, auditor is required to obtain an understanding of the entity and its environment as a part of Risk Assessment procedure to identify and assess RMM. In an automated environment, auditor is required to obtain an understating of the following: 1. Applications being used by the entity; 2. IT infrastructure components for each of the application; 3. Organisation structure and governance; 4. Policies, procedures and processes followed; 5. IT risks and controls.	
2	**Considerations of automated environment in different stages of Audit**	
	Planning	**Risk Assessment Process**
		• Consider risk arising from use of IT systems. • Identify significant accounts and disclosures. • Identify likely sources of misstatement.
		Understanding of the Business
		• Document understanding of business processes using Flowcharts / Narratives. • Prepare Risk and Control Matrices. • Understand design of controls by performing walkthrough of end-to-end process. • Process wide considerations for Entity Level Controls, Segregation of Duties.
	Execution	**Assessing Entity Level Controls**
		Consider aspects related to • understanding and review of IT Governance. • Segregation of duties, • Review of General IT Controls and Application Controls.
		Assessing Process Level Controls
		Consider aspects relating to Risks and Controls with each process, sub-process and activity.
	Reporting	**Testing of Reports & Information produced by the entity at completion stage**
		Consider the evaluation of control deficiencies using Data Analytics.

Chapter 4 "Audit in an Automated Environment (New Syllabus)"

4.3 – Enterprise Risk Management (ERM)

Enterprise Risk management	• ERM is a formal program that is implemented across an enterprise for enabling risk management. • In many countries, companies are required to have a formal ERM Program as a statutory requirement. • In India, Sec. 134(3) of Companies Act, 2013 requires the Board of Directors to include in their report a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company.	
Risk Assessment Process	**Steps involved in Risk Assessment Process**	Step 1 - Define Business Objectives and Goals. Step 2 - Identify events that affect achievement of business objectives. Step 3 - Assess likelihood and impact. Step 4 - Respond and mitigate risks. Step 5 - Assess Residual Risks.
	Considerations of Risk Assessment Process	1. Qualitative and Quantitative Factors; 2. Definition of Key Performance and Risk Indicators; 3. Risk Appetite; 4. Risk Scores, Scales and Maps; 5. Use of Data & Metrics; 6. Benchmarking.
Commonly used framework for ERM	The most common framework that is suitable for implementing an effective ERM is the COSO Enterprise Risk Management – Integrated Framework developed by the Committee of Sponsoring Organisations (COSO) in 2004 and subsequently updated in 2016 to address the changes in business environment. Besides COSO framework, another widely available framework is the ISO 31000 Risk Management standard published by the International Organization for Standardization.	

4.4 – Assessing IT Related Risks and Controls

Considerations in assessing IT Risks

Entity Level Risks	Entity Level Risks (Pervasive Risks) are related to Governance, Organization and Management of IT and requires examination of following aspects: (a) Whether management established an IT Security Policy; (b) Whether policy is being communicated to all employees; (c) Whether relevant training has been provided to employees; and (d) Whether management monitor the adherence of the established policies.
Process Level Risks	Process Level Risks are related to Risks in the IT Processes and Procedures being followed and requires examination of following aspects: (a) Whether unauthorized changes to IT Systems application being prevented and detected in a timely manner; and (b) Whether user access to systems commensurate with roles and responsibilities of the user.
Transaction Level Risks	Transaction Level Risks are related to IT Risks at each layer of the automated environment and requires examination of following aspects: (a) Whether direct data changes to databases prevented; and (b) Whether strong passwords used in the operating system.

Controls required to mitigate IT Risks

General IT Controls	Policies & procedures that relate to many applications & support the effective functioning of application controls. General IT-Controls that maintain integrity of information & security of data commonly include controls over the following: 1. Data center and network operations. 2. System software acquisition, change & maintenance. 3. Program change. 4. Access security. 5. Application system acquisition, development, and maintenance.
Application Controls	• Manual or automated procedures that typically operate at a business process level & apply to processing of individual applications. • They can be preventive or detective in nature. • They relate to procedures used to initiate, record, process and report transactions or other financial data. • Examples of Application controls are: 1. Edit checks and Validation of input data, 2. Sequence Number checks. 3. Limit Checks. 4. Reasonable Checks. 5. Mandatory Data Fields.
IT Dependent Controls	• Manual controls that make use of some form of data or information or report produced from IT systems and applications. • Though the control is performed manually, the design and effectiveness of such controls depend on the reliability of source data.

4.5 – Evaluating Controls at Entity Level and Process Level

Entity Level Controls (ELCs)

Characteristics		• Entity Level controls also known as pervasive controls operate across an entity at all levels of management, i.e. from top management to lower management. • Entity Level Controls are considered to a part of a company's internal control framework and related to components of Internal Control other than control activities. It means that Entity Level Controls are related to (a) Control Environment (b) Entity's Risk Assessment Process. (c) Information Systems and Communication. (d) Monitoring. • Entity level controls are subjective by nature and therefore require application of more professional judgment in their evaluation and testing.
Types	**Direct ELCs**	Direct ELCs operate at a level of business process to prevent, detect or correct a misstatement in a timely manner. Examples of Direct ELCs are: • Business performance reviews; • Monitoring of effectiveness of control by Internal Audit function.
	Indirect ELCs	Indirect ELCs do not relate to any specific business process, transaction or account balance and therefore, cannot prevent, detect or correct misstatements. Indirect ELCs contribute indirectly to the effective operation of direct ELCs. Examples of Indirect ELCs are: • Company code of conduct; • Human resource policies; • Job roles & responsibilities.
Testing of ELCs		• As a part of audit engagement, auditors are required to understand, evaluate and validate the entity level controls. Result of testing entity level controls could have an impact on the NTE of other audit procedures including testing of controls. • When the ELCs at a company are effective, the auditor may consider reducing the number of samples in the TOCs and vice versa. • In small organisations, the ELCs may not be formally documented and hence, auditor should design audit procedures accordingly to obtain evidence of the existence and effectiveness of entity level controls.

Process Level Controls

- Process Level Controls primarily focus on control activities and the monitoring of those activities at the process level.
- Examples of Process Level Controls are: approvals, authorizations, verifications and reconciliations, etc.

Testing of Process Level Controls	• SA 315 require the auditor to understand the business process that makes up an account balance or financial statement line item. • Understanding the business process helps the auditor in identification of risks and controls within each process, sub-process and activity. • The auditor should document this understanding of the company's business process and flow of transactions in the audit file in accordance with SA 230.

4.6 – Data Analytics

Concept of Data Analytics	• Data analytics is an analytical process by which meaning information is generated and prepared from raw system data using processes, tools, and techniques. • In an automated environment, various insights can be extracted from operational, financial, and other forms of electronic data internal or external to the organization. • The data so extracted is useful for preparation of management information system (MIS) reports and electronic dashboards that give a high-level snapshot of business performance. • The data analytics methods used in an audit are known as Computer Assisted Auditing Techniques or CAATs.
Application of Data Analytics	In an automated environment, auditors can apply the concept of data analytics for several aspects of an audit including the following: 1. Preliminary Analytics; 2. Risk Assessment; 3. Control Testing; 4. Non-Standard Journal Analysis; 5. Evaluation of Deficiencies; 6. Fraud Risk assessment.
Steps involved in using Data Analytics	Step-1: Understand Business Environment including IT. Step-2: Defines the Objectives and Criteria against which subject matter will be evaluated. Step-3: Identify Source and Format of Data. Step-4: Extract Data. Step-5: Verify, Completeness, accuracy and Validity of extracted Data. Step-6: Apply Criteria on data extracted. Step-7: Validate and Confirm results. Step-8: Document the results and Report the conclusions

4.7 – Standards, Guidelines and Procedures

Standards on Auditing	AASB of ICAI issues various standards which are required to be followed while auditing the financial statements of an entity.
Sec. 143(3)(i) of Companies Act, 2013	Section 143(3)(i) of Companies Act, 2013 requires statutory auditors to provide an Independent Opinion on the Design and Operating Effectiveness of Internal Financial Controls Over Financial Reporting (IFC-FR) of the company as at Balance Sheet date.
Section 404 of SOX Act, 2002	Section 404 of SOX Act 2002 requires public listed companies to implement, assess and ensure effectiveness of internal controls over financial reporting. Auditors of such companies are required to express an independent opinion on the design and operating effectiveness of internal controls over financial reporting (ICFR).
ISO 27001:2013	ISO 27001:2013 is the Information Security Management System (ISMS) standard issued by the International Organization for Standardization (ISO). This standard provides the framework, guidelines and procedures for implementing information security and related controls in a company.
ITIL and ISO 20000	ITIL (Information Technology Infrastructure Library) and ISO 20000 provide a set of best practice processes and procedures for IT service management in a company. Some of the areas that could be relevant to audit includes change management, incident management, problem management, IT operations, IT asset management etc.
PCI-DSS	• The Payment Card Industry – Data Security Standard, is the most widely adopted information security standard for the payment cards industry. • Any entity that is involved in the storage, retrieval, transmission or handling of credit card/debit card information are required to implement the security controls in accordance with this standard.
SSAE 18	Statements on Standards for Attest Engagements (SSAE) 18 is issued by AICPA and effective from 01.05.2017 (Supersedes SSAE 16) requires the organizations to issue their System and Organization Controls (SOC) Report under the SSAE-18 standard in SOC 1, SOC 2 and SOC 3 reports. • SOC 1 for reporting on controls at a service organization relevant to user entities' internal control over financial reporting (ICFR). • SOC 2 and SOC 3 for reporting on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy i.e., controls other than ICFR.
CoBIT	CoBIT is best practice IT Governance and Management framework published by Information Systems Audit and Control Association. It provides the required tools, resources and guidelines that are relevant to IT governance, risk, compliance and information security.
Cyber security Framework	CSF published by the National Institute of Standards & Technology is one of the most popular framework for improving critical infrastructure cyber security, which provides a set of standards and best practices for companies to manage cyber security risks.