The Institute of Chartered Accountants of India

(Setup by an Act of Parliament)

Committee on Information Technology

Updated Syllabus

of

Information Systems Audit Course 2.0

Last updated on 20th June 2014

UPDATED SYLLABUS OF ISA COURSE 2.0

TABLE OF CONTENTS

ISA: INFORMATION SYSTEMS AUDIT COURSE 2.0

1. INTRODUCTION

The objective of the updated ISA course 2.0 is to equip CAs with unique body of knowledge and skill-sets so that they can become Information Systems Auditors (ISAs) who are technologically adept and are able to utilize and leverage technology to become more effective in their work and learn new ways that will add value to clients, customers and employers. This will also meet the increasing need of CAs with solid IT skills who can provide IT enabled services through consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements. This document containing details of the updated syllabus of the ISA Course 2.0 has been prepared based on inputs from senior faculty of the ISA course and also feedback received from other experts. It has also undergone numerous reviews over a period of more than two years. The updated syllabus has taken into consideration the latest curriculum of similar professional courses and the recent/emerging developments in the field of Information Technology and IS Auditing.

2. USE OF STRUCTURED APPROACH

The updated syllabus has been developed by using process oriented structured approach with a ten step methodology. This approach is based on the bloom taxonomy of learning and other global best practices. The approach covers the entire life cycle of the ISA Exam right from designing of the course objectives to the final testing methodology and also includes process/guidelines to be adapted in development of updated study material. This approach was shared with the authors, reviewers and SMEs who were involved in developing and reviewing the study material.

3. NEED FOR DISA 2.0 COURSE AND UPDATION PROCESS

The need for ISA course updation has been extensively discussed considering the objectives and utility of the course. It was decided to update the contents based on suggestions received considering the latest developments in the field of IT and IS Auditing. The updated course has revised modules with key areas of learning as practically relevant for CAs which will enable them to more effective in their practice for regular compliance audits and also enable to provide IT assurance or consulting services. The updated syllabus has also considered the IT knowledge acquired by the latest batch of CA students who have studied IT in IPCC and Final and have also gone through practical IT trainings. A bridge ISA course is expected to be developed to help existing ISAs to update their knowledge and skills as per the latest course.

Please note that ISA and DISA are used inter-changeably in the document and study material.

4. OVERALL OBJECTIVES

The ISA course combines technology, information assurance and information management expertise that enable a DISA to become trusted Information Technology advisor and provider of IS Assurance services. The DISA with the unique blend of knowledge would serve as the "bridge" between business and technology leveraging the CA's strategic and general business skills. DISA Certification through judicious blend of theoretical and practical training provides CAs with better understanding of technology deployment in enterprises enabling them to be more effective not only in their current area of work but also in offering innovative IT enabled services.

The IT knowledge and skills acquired in the ISA course would also enable DISAs to be more effective in using IT for auditing in a computerised environment in existing domains of compliance, consulting and assurance services. The objective of the updated DISA course 2.0 is: **"To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices**."

The ISA exam is designed to assess and certify Chartered Accountants for conducting Information Systems Audit. After successfully completing the course, the DISA candidates are expected to have required knowledge and skills to perform various assurance and consulting assignments relating to Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems, Information Technology and related areas. Further, this will enhance skills to be more effective in auditing in a computerised environment covering traditional areas of financial/compliance audits.

The DISA Course will provide basic understanding of how information technology is used and deployed. It facilitates understanding of how an IS Auditor is expected to analyse, review, evaluate and provide recommendations on identified control weaknesses in different areas of technology deployment. It is important to remember that the ISA course is not oriented towards teaching fundamentals of technology. However, the Primer on IT in module 1 covers basic IT concepts in self-study mode. The ISA course is conducted through a good blend of e-learning (online and facilitated), class room training, hands-on training with practical case studies and project work to ensure practical application of knowledge.

5. ISA COURSE – BASIC COMPETENCY REQUIREMENTS

The competency requirements are mapped with the detailed body of knowledge encompassing all the key tasks an IS Auditor has to perform in specific areas and the related knowledge required for performing these tasks. The skill requirements are represented as task statements and knowledge is represented by the knowledge statements. After successful completion of the course, the DISA candidates will have conceptual clarity and will demonstrate basic competency in the following key areas:

- Overall understanding of information system and technology: concepts and practice
- Risks of deployment of information system and technology
- Features and functionalities of security and controls of IT components and IT environment.
- Controls which could be implemented using the security features and functionalities so as to mitigate the risks in the relevant IT components and environments.
- Recommend IT risk management strategy as appropriate.
- Use global best practices and adapt them as required for the assignments.
- Apply appropriate strategy, approach, methodology and techniques for auditing technology using relevant IS Audit standards, guidelines and procedures and perform IS Assurance and consulting assignments as per requirements.

6. LEARNING OBJECTIVES

1. Demonstrate understanding of functioning of key components of existing and emerging information technology and their practical deployment.
2. Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.
3. Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.
4. Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.
5. Provide assurance or consulting services that the management practices relating to systems development:, acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.
6. Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.
7. Provide assurance or consulting services to confirm whether the Business continuity management strategy, processes and practices meet enterprise requirements to ensure timely resumption of IT enabled business operations and minimize the business impact of a disaster.
8. Plan and perform IS assurance or consulting assignments by applying knowledge learnt by presenting project assignment relating to allotted case study to confirm understanding.

The overall learning objective with detailed listing of tasks statements and knowledge statement, module-wise with the weightage (% of coverage) are given in Annexure-1.

7. MODULES OF THE ISA COURSE

The updated ISA certification is granted exclusively to CAs who demonstrate considerable expertise in domain areas of IT Governance, Security, Control and assurance through their knowledge, skills and experience The primary purpose of the ISA exam is to test whether the candidate has the requisite knowledge and skills to apply IS assurance principles and practices in the following modules:

No.	Name of Module	Weightage (%)
1	Primer on Information Technology, IS Infrastructure and Emerging Technologies	18
2	Information Systems Assurance Services	12
3	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	12
4	Protection of Information Systems Infrastructure and Information Assets	18
5	Systems Development: Acquisition, Maintenance and Implementation.	12
6	Business Continuity Management	12
7	Business Applications Software Audit	6
	Project report	10

It may be noted that the ISA course is not expected to be an in-depth comprehensive coverage of different aspects of information technology as computer hardware, operating system, network, databases, application software, etc. but is focussed on training on how to review IT risks, security and controls and provide assurance on secure technology deployment.

8. MAPPING OF CURRENT SYLLABUS WITH EXISTING SYLLABUS

The modules have been revised based on discussions in the faculty meet and suggestions received from ISA faculty and study of the similar courses offered globally by other professional institutes. The weightage of technology concepts has been drastically reduced and there is more emphasis on practical aspects of technology implementation. The weightage has been planned so that each day's session would be of 6 hours with four sessions of 90 minutes each.

The revised list of modules with weightage, mode of learning and mapping with old modules is given below:

	EL: E-Learning, Class: Class Room Training and HOT: Hands on Training						
Mod.	**Modules for Revised ISA Course**	**Weightage (%)**	**Coverage In Hours**			**Old Modules**	**Weightage (%)**
No.			**EL**	**Class**	**HOT**		
1	Primer on Information Technology, IS Infrastructure and Emerging Technologies:	18	12	6		Covered partly in Module 1: IT infrastructure & communication/Networking Technologies.	
2	Information Systems Assurance Services	12	6	6		Module 6: Information Systems Audit Process	10
3	Governance and Management of Enterprise IT, Risk Management and Compliance Reviews	12		12		Module 5: Information Systems Organization & Management	8
4	Protection of Information Systems Infrastructure and Information Assets	18		12	12	Module 1: IT infrastructure and communication /Networking technologies. Module 2: Protection of Information Assets	30 22
5	Systems Development: Acquisition, Maintenance and Implementation.	12		12		Module 3: Systems Development Life Cycle & Application Systems	20
6	Business Applications Software Audit	12		6		Covered partly in Module 4	
7	Business Continuity Management	6			12	Module 4: Business Continuity Planning	10
	Project report on IS Audit (training on case studies)	10					
	Total	**100**	**18**	**48**	**24**	**Total**	**100**

9. SKILL LEVELS

The updated syllabus provides specific skills in each of the three categories of skill areas. The suggested skill levels ensure that the updated syllabus through all the modules has right blend of concepts and practice. The skill levels will be considered by the authors of study material and also in testing methodology through the eligibility tests and assessment test.

The weightage and category of skills proposed are given below:

Skills Category	Weights
1. Knowledge and Understanding	30% - 40%
2. Application of the Body of Knowledge	55% - 60%
3. Written communication	5% - 10%

10. KEY HIGHLIGHTS OF ISA TRAINING

DISA Training includes eLearning, hands on training, project work in addition to class room lectures.

- Candidates will have to successfully complete e-learning mode before joining class room training.
- The training in classroom and hands-on training will follow the order in sequential order of the modules. This includes an inter-mix of classroom lectures and hands-on training. The hands-on training pre-supposes and builds on understanding of concepts of the classroom lectures.
- E-Learning of 12 hours for Module-1 and 6 hours for Module-2 is part of the DISA course and passing in the online test is mandatory and part of the eligibility score.
- Module-4 will have class room lectures and hands on training of 2 days each. Module-6 will have hands on training of 2 days. **Supplementary e-Learning Lectures of 30 hours covering Modules 4 and 6 is also proposed to be included in due course of time.**
- **Hands on training will be conducted by the experienced faculty at same venue as class rooms with all participants performing exercises on their own laptops with pre-loaded software as specified in advance.**

11. TESTING METHODOLOGY

The testing methodology includes online exam, module tests and evaluation of project work. There is no change in final exam except new pool of questions are to be developed. After the completion of the professional training classes, an eligibility test will be conducted in the month of May and November as per present practice. A member will be declared pass in case he/she secures 60% in aggregate.

A. ELIGIBILITY TEST DETAILS

Structure of Examination	Weightage (%)	Marks
1. Online Exam (Eligibility Test)	60	120
2. Module Tests	30	60
3. Project Work	10	20
Passing marks	**60**	**120**

NOTE: **It is mandatory to obtain minimum passing marks in online test and project work apart from overall minimum marks in total.**

B. PROJECT WORK

The Project will be allocated to the Group comprising of multiple members (group of 3 to 4). The group has to submit the project within 10 days of the allocation of the project. Marks awarded for the Project would be credited to the account of all Group members. In case Group members secure less than 50% marks in the Project Work, the Group has to re-submit the project based on feedback of the project evaluation. This is to ensure that all the participants submit project work which is based on their practical application of knowledge. The marks for the project work will be 20 marks. Obtaining minimum marks in project work is mandatory for passing the eligibility test.

Note:

The learning objectives, task statement and knowledge statements for each of the modules is given in Annexure-1.

Please refer to the Body of Knowledge for detailed mapping of task and knowledge statements and knowledge reference guide.

ANNEXURE-1

MODULE 1: PRIMER ON INFORMATION TECHNOLOGY, IS INFRASTRUCTURE AND EMERGING TECHNOLOGIES (18%)

(Covered in 12 hours of self- study through e-Learning and 1 day of Classroom Training)

OBJECTIVE:

Demonstrate understanding of functioning of key components of existing and emerging information Technologies and their practical deployment.

TASK STATEMENTS

1.1 Identify deployment of different components of IT and their functions: Computer Hardware, Operating system software, database management software, application software, middleware, Client Server Model, Communications technologies and networks, internet, peripherals, devices, accessories, etc.
1.2 Recognise the configuration of hardware, operating system software, database management software and application software.
1.3 Recognise function of Telecommunications and Network security including wireless, encryption, firewalls, Cryptography etc.
1.4 Analyze baseline security procedures, firewall configurations, user administration and user management.
1.5 Distinguish the technology architecture of a typical data centre in a centralised environment identifying different layers/components of technology and their functions.
1.6 Consider the impact of deployment of key existing and emerging technologies such as: XML, BURL, Cloud computing, Geo Location, Mobile computing, Social media, Bring Your Own Device (BYOD), Business Intelligence (BI), Big Data, Network Technologies – Web Services, Web 2.0, Data warehouse, Data Mining, Data Mart, Decision Support Systems (DSS), Executive Support Systems (ESS), Artificial Intelligence (AI), Electronic Funds Transfer (EFT), Electronic Transactions and Green IT.

KNOWLEDGE STATEMENTS (KNOWLEDGE OF)

1.1 Information Technology components of Information Systems Infrastructure and related processes in the context of practical deployment in enterprises.
1.2 Fundamental concepts of different components of IT and their functions: Computer Hardware, Operating system software, database management software, application software, middleware, Client Server Model, Communications technologies and networks, internet, peripherals, devices, accessories, etc.
1.3 Configuration management of hardware, system software, database management software and application software.
1.4 Telecommunications and Network security including wireless, encryption, firewalls, Cryptography etc.
1.5 Concepts related to applied cryptography, including plain-text, cipher-text, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
1.6 Baseline security procedures, firewall configurations, user administration and user management.
1.7 Information Technology components of a Data Centre in centralised environment
1.8 Functioning and impact of key emerging technologies such as: XML, XBRL, Cloud computing, Geo Location, Mobile computing, Social media, BYOD, BI, Big Data, Network Technologies – web services, Web 2.0, Data warehouse, Data Mining, Data Mart, DSS, ESS, AI, EFT, Electronic Transactions and Green IT

MODULE 2: INFORMATION SYSTEMS ASSURANCE SERVICES (12%)

(Covered in 1 day of class room training and 1 Day of self-study through e-learning)

Objective

Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.

Learning Objectives

Provide assurance or consulting services in the areas of Governance, Risk Management, Security, Controls and compliance by using relevant standards, guidelines, frameworks and best practices services.

TASK STATEMENTS

2.1. Develop and implement appropriate risk-based approach as per scope and objective of the assignment.
2.2. Adapt and use relevant IT assurance standards, guidelines, frameworks and best practices.
2.3. Plan assurance or consulting assignments covering specific steps such as: responding to request for proposal from client, submitting proposal, scoping of audit objectives, performing audit, evaluate findings and reporting, covering the complete life cycle of the assignment.
2.4. Document understanding of the enterprise technology deployment, IT organisation structure, technology environment including control architecture so as to analyse and assess IT risks.
2.5. Perform assurance or consulting services covering the complete assurance life cycle including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, performing audit as per audit objectives, obtaining and evaluating audit evidence identifying key areas of weaknesses, reporting findings, obtaining management response and follow up of implementation.
2.6. Use Computer Assisted Audit Techniques, tools and risk assessment techniques including sampling, data analysis, Business Intelligence and Business Analytics.
2.7. Distinguish between IS Assurance assignments and auditing in a computerised environment and use the relevant frameworks and best practices for compliance and assurance assignments.
2.8. Communicate/Report findings in specific format using standards/best practices as required.
2.9. Conduct follow-up reviews or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.
2.10. Distinguish key steps and processes of Cyber Frauds investigation and Cyber Forensics.
2.11. Create IS Assurance or consulting function in an enterprise/within CA office by identifying key enablers and resources including identifying required personnel with required competencies and skill sets.

KNOWLEDGE STATEMENTS

2.1. Relevant IT assurance standards, guidelines, frameworks and best practices as per scope and objective of the assignment.
2.2. Statements of auditing relating to auditing in a computerised environment.
2.3. Different aspects of IS Audit process - audit charter, audit planning, audit universe, risk-based audit approach, IS Audit standards, guidelines, regulations, procedures and audit reporting.
2.4. Role and responsibilities of IS Audit function/department and key enablers.
2.5. Documenting enterprise, technology deployment, organisation structure, technology environment including control architecture so as to analyse and assess Risks.
2.6. Audit Risk management strategy and approach

2.7. Assurance or consulting services including scoping, risk assessment, audit planning, audit program, audit procedures, using audit tools, analysis and reporting.
2.8. IS Audit process cycle from scoping to reporting
2.9. Defining Audit scope and objectives
2.10. Preparing request for proposal from client, submitting proposal
2.11. Audit documentation, obtaining and evaluating audit evidence
2.12. Analysis of evidence, Risk Rating of findings/Control weaknesses, reporting findings, obtaining management response and follow up of implementation.
2.13. Types of Internal control and related risks
2.14. Analytical procedures, compliance testing and substantive testing
2.15. Types of IT enabled services, IS Assurance assignments and auditing in a computerised environment and using the relevant processes and best practices for compliance and assurance assignments.
2.16. Cyber Frauds investigation and cybercrimes, specific process relating to Cyber Forensics.
2.17. Audit tools and techniques including CAAT, tools and risk assessment techniques including data analysis, Business Intelligence, sampling, Automation of IS Assurance, etc.
2.18. Using best practices frameworks such as COBIT, ISO etc.
2.19. Key provisions of Information Technology Act and Rules and impact on IS Assurance.
2.20. Follow up review

MODULE 3: GOVERNANCE AND MANAGEMENT OF ENTERPRISE INFORMATION TECHNOLOGY, RISK MANAGEMENT AND COMPLIANCE REVIEWS (12%)

(Covered in 2 days of class room training)

OBJECTIVE

Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.

TASK STATEMENTS

3.1 Review governance mechanisms and structures in place to assess whether these are adequate to meet internal/ external stakeholder needs and facilitate value delivery and benefit optimisation.
3.2 Distinguish between appropriate and inappropriate governance structures in an enterprise (e.g. tone at the top, policies, steering committees, strategies, oversight, etc.)
3.3 Assess framework for IT governance and evaluate whether the governance and management processes are meeting stakeholder needs and governance objectives.
3.4 Distinguish Governance and management processes and their objectives.
3.5 Evaluate key enablers as relevant: principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies) in the areas of Governance and Management of Enterprise IT.
3.6 Review information architecture and processes to determine compliance with specified standards or criteria.
3.7 Review alignment of IT strategy with the enterprise strategy so as to achieve enterprise objectives.
3.8 Review risk optimisation processes and practices in place to assess whether these are appropriate to mitigate risks as per risk management strategy.
3.9 Evaluate resource management practices to assess whether they ensure optimum utilisation

3.10 Review usage of IT resources considering value proposition of IT investments using Capex and Opex Models.
3.11 Determine the current status of the entity's use of Information Technology to support its business processes
3.12 Evaluate monitoring and assurance practices and the ways to measure and manage IT performance and costs through use of Key Goal Indicators, Key Goal Indicators including balance score cards, strategic score cards etc. to ensure timely reporting and monitoring
3.13 Review the process of IT Infrastructure management, IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, problem including incidence Management, Problem Management, Change Management, Configuration Management, Capacity Management and Performance Management.
3.14 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures
3.15 Review enterprise controls to ensure compliance with internal and external regulatory requirements and external service providers such as SOX, Clause 49 Listing requirements, Information Technology Act, etc.

KNOWLEDGE STATEMENTS

3.1 Enterprise Governance, Corporate Governance, Governance of Enterprise IT and their relationship,
3.2 Using standards, Frameworks and best practices such as COBIT, COSO, ISO 27001, ISO38500, ISO 31000 etc. for Governance and Management of IT in enterprises.
3.3 Implementing best practices of Enterprise Goals, IT enabled goals, process and activity goals, Key Goal indicators and Key performance indicators.
3.4 Aligning IT strategy with business strategy and the business processes for long-term and short-term
3.5 IT management and monitoring of controls (e.g., continuous monitoring, QA) for compliance with the organization's policies, standards and procedures
3.6 Value proposition of IT investments including Capex and Opex models.
3.7 Key enablers of Governance and Management of IT such as relevant: principles, policies and framework, processes, organisation structure, culture, ethics and behaviours and resources (information, services, infrastructure and applications, people, skills and competencies).
3.8 Enterprise Risk Management, Risk management practices, Risk mitigation strategy
3.9 IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives by using Capex and Opex models.
3.10 IT operational procedures and practices, service management practices, outsourcing, end-user procedures, IT service help desk, escalation matrix, etc.
3.11 Performance management systems including performance measures, KGI, KPI, Balanced score cards, strategic score cards etc.
3.12 Internal compliance/external national and international regulatory requirements and external service providers such as SOX, Clause 49 Listing requirements, Information Technology Act, etc.

MODULE 4: PROTECTION OF INFORMATION SYSTEMS INFRASTRUCTURE AND INFORMATION ASSETS (18%)

(Covered in 2 days of lecture, 2 days of hands on training and 20 hours of supplementary e-Learning)

OBJECTIVE

Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.

LEARNING OBJECTIVES

This module focuses on different methods for protecting information assets. This primarily covers following:

- Risk response and definition of controls for protection of information assets
- Essentials of information security management like objectives, processes, policies and procedures and compliance.
- Information asset protection based on information classification
- Essentials of Physical and environmental security
- Logical access controls
- Network and related security processes.
- Audit guidelines for information protection controls

TASK STATEMENTS

By completing the module, DISAs will be able to perform the following tasks:

4.1. Review Risk Management strategy of the enterprise so as to ensure Information security (Confidentiality, Integrity and Availability) and mapping of related risks and controls

4.2. Assess IT security management with reference to IT policies, procedures and methodologies that support the entity's strategic plan, IT organization related to system components, IT human resource policies and changes to IT organization and policies with focus on Corporate Security Policy.

4.3. Review information security policies of the organization and ensure they are communicated to all relevant stakeholders. Ensure that policies are reviewed, updated and maintained current.

4.4. Assess the procedures the entity utilizes to achieve and maintain its objectives in accordance with its established policies and standards and to protect the IT architecture and system assets including information assets against potential risks

4.5. Review the asset protection mechanism with reference to risk management and ensure that information and other assets are classified and protected in line with security policies and procedures.

4.6. Review environmental controls, protection devices and supporting practices

4.7. Review the physical access controls for the identification, authentication and restriction of users to authorized facilities

4.8. Review logical access controls for the identification, authentication and restriction of users to authorized functions and data.

4.9. Evaluate system software configuration and user management such as user rights and administration as per enterprise policies relating to segregation of duties by reviewing user rights granted to specific roles and responsibilities.

4.10. Review network security controls with respect to threats and vulnerabilities associated with network and network based infrastructure.
4.11. Review the processes and procedures used to encrypt, communicate, store, retrieve, transport and dispose of confidential information assets
4.12. Review intrusion detection tools and control techniques (e.g., firewalls, virus detection, spyware)

KNOWLEDGE STATEMENTS

By completing this module, DISAs will be able to gain knowledge of the following topics:

4.1. Best practices of Risk response and control definition strategy and practices.
4.2. Principles/Concepts of Information security (threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection,
4.3. IT Security Policies, procedures, standards, guidelines and best practices
4.4. Human resource policies and changes to IT organization and policies.
4.5. IT infrastructure and its relationship to other IT assets like applications, data and information
4.6. IT assets and Data classification policy and protection methods including Regulatory requirements of information security, Privacy, etc.
4.7. Physical access controls
4.8. Environmental controls
4.9. Logical access controls at different layers of technology such as Operating System Software and Database Management Software including setting of parameters and user administration and management by using baseline security procedures as relevant.
4.10. Security issues in a networked environment. Types of attacks on Information Technology such as cyber-attacks, mobile technology attacks, etc.
4.11. Communication controls and encryption (Cryptography, PKI Controls in the Telecommunication sub system including Firewall/IDS, VPN)
4.12. Intrusion detection tools and intrusion prevention tools.

Note: Module 4 will be covered as follows:

1. Supplementary self-study E-Learning covering concepts to be completed by participants: 20 hours (optional)
2. Class room lectures covering all the topics: 12 hours
3. Hands-on training covering Task statements 4.9 to 4.11 through practical case studies: 12 hours

Hands on training will cover logical access controls with **demo and exercise covering various features of security in identified software.**

MODULE 5: SYSTEMS DEVELOPMENT: ACQUISITION, MAINTENANCE AND IMPLEMENTATION (12%)

(Covered in 2 days of class Room training)

OBJECTIVE:

Provide assurance or consulting services that the management practices relating to systems development: acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.

LEARNING OBJECTIVES

Most IT departments or software development companies, irrespective of their size, have a formal set of procedures for initiating and developing new business information systems. This is often termed as System Development Life Cycle (SDLC) or the System Development Methodology (SDM). SDLC is an essential process of developing software solutions within organisations. This module covers all aspects of SDLC such as development or acquisition of application software as well as implementing IT using project management practices. This module covers the following topics:

1. Phases in SDLC and changes in these phases due to changes in environment and security requirements.
2. Initial phases of SLDC covering feasibility study, requirement definition, expected benefits to organisation and developing business case for SDLC project.
3. Project management practices for executing SDLC project.
4. Various models and methods that can be adopted based on requirements for development of application software.
5. Process for acquisition and/or outsourcing development, in case an organisation has decided to acquire software or outsourced development.
6. Implementation methods for application acquired/developed.
7. Impact on SDLC due to changes in technology.
8. Guidelines for auditing SDLC project.

TASK STATEMENTS

The task statements are what the ISA candidate is expected to know "how to perform". The knowledge statements delineate the areas in which ISA candidate must have a good understanding in order to perform the tasks.

5.1 Review SDLC objectives and organisation objectives, practices, requirement analysis and initiating SDLC.

5.2 Review need for SDLC projects, project management practices, milestones and framework are appropriate to meet organisation requirements, governance mechanism including benefits realization practices, (e.g., steering committee, business cases, total cost of ownership [TCO], ROI).

5.3 Review Systems Development Life Cycle (SDLC) methods and associated tools and techniques and alternate SDLC models used are appropriately deployed.

5.4 Review software and other acquisition processes, vendor selection process, SLA, etc. are in line with organisation objectives.

5.5 Assess risks associated with project are addressed in system design specification based on organisation and security requirements.

5.6 Assess systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, project benefits, resources used (financial and people), adequacy of acquisition, development and deployment, and the opportunities for improvement.
5.7 Assess controls for information systems during the requirements, acquisition or design, development and testing phases for compliance with the organisation's policies, standards, procedures and external requirements.
5.8 Review required software quality attributes, testing process against predefined performance metrics and use of software benchmarks as appropriate.
5.9 Review relevant use of industry trends when developing a solution strategy.
5.10 Perform post-implementation review of systems to determine whether project deliverables, controls and organisation requirements are met.

KNOWLEDGE STATEMENTS

5.1 Systems Development Life Cycle (SDLC) concepts, importance, and phases.
5.2 Roles and responsibilities in SDLC, implementation and functional segregation of duties within SDLC.
5.3 Need for initiating SDLC, triggers and pain points, defining business requirements including security requirements, business case development and benefits from output of SDLC (i.e. new application system) including risk management and definition of controls.
5.4 Project governance mechanisms (steering committee, project oversight board, organisational standards for program and project management practices, program and project management office, benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], Return on Investment (ROI) and resource management.
5.5 Software development methods such as: Waterfall, Spiral, Rapid Application Development, Agile Development, Prototypes, Object Oriented Analysis, baseline procedures in SDLC.
5.6 Use of CASE and other tools, software Re- engineering/Reverse Engineering, development effort estimates and software sizing techniques (e.g. LOC, FPA, etc.)
5.7 Project resource management, coding and testing practices, QAT and UAT, quality attributes and performance measurements of quality, testing methodologies and practices related to information systems development and software accreditation.
5.8 Systems implementation processes and techniques: system implementation plan, acceptance testing approach, data conversion approach, communication and training, hardware/software facilities, installation, cut-over plan, configuration and release management relating to the development of information systems.
5.9 Software support and maintenance practices, change management framework and practices, emergency changes, help desk, communication and training.
5.10 Sourcing and contracting strategies, policies and management practices, hardware/software acquisition and support policies.
5.11 Requirements mapping, software selection and evaluation practices and process.
5.12 Industry trends – cloud computing, mobile computing, BYOD, Big data and data analytics.
5.13 Post-implementation reviews of application systems.
5.14 Auditing SDLC processes.

MODULE 6: BUSINESS APPLICATIONS SOFTWARE AUDIT (12%)

(Covered in 2 days of Hands on training and 12 hours of supplementary e-learning)

OBJECTIVE:

Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.

LEARNING OBJECTIVES

- To understand business processes and business application software.
- To understand the business application implemented controls by organisations.
- To provide assurance on business application software and the implemented controls through business application audit.

TASK STATEMENTS

6.1 Assess the enterprise business models by performing preliminary review of effectiveness of the entity's business processes and embedded controls
6.2 Assess business processes - risks assessment and control evaluation in the context of business strategy, impact of business application software on Business processes/controls
6.3 Assess Business processes by performing preliminary review of adequacy of controls
6.4 Identify and document information technology environment and platforms, technology architecture, network, system software and application environment to assess control architecture.
6.5 Identify application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, etc.
6.6 Identify various types of Business Applications like ERP, Banking, and Accounting
6.7 Prepare audit program for planning and perform review of application software
6.8 Identify information systems that are used to process and accumulate transactional data, as well as provide monitoring and financial reporting information and assess the controls.
6.9 Review enterprise security policy relating to the identification, authentication and restriction of users to authorized functions and data.
6.10 Assess procedures to manage changes to business processes and impact on controls
6.11 Review database structure and tables, user creation, access levels and user management.
6.12 Evaluate application software configuration and user management features such as user rights and administration and map them with enterprise policies relating to segregation of duties by reviewing user rights granted to specific roles and responsibilities.
6.13 Evaluate internal control systems in application software relating to system design, data creation/input, data processing, data flow, data transmission and data storage.
6.14 Use reporting, query and SQL features as required for reviewing controls.
6.15 Audit specific application software users; assess business system functionality, user rights and segregation of duties levels of authorization, and data security by performing analytical procedures review, compliance testing and substantive testing.
6.16 Assess application software controls and identify areas of weaknesses in controls and advise remedial measures
6.17 Communicate/Report findings in specific format using standards/best practices as required.
6.18 Performing review of application controls as relevant for assurance or compliance assignments.

KNOWLEDGE STATEMENTS

6.1 Enterprise business models
6.2 Key features and functionalities of application software
6.3 Business processes controls, Analytical procedures, compliance testing and substantive testing
6.4 Risk assessment and control evaluation in the context of business strategy
6.5 Impact of Business application software on Business processes/controls
6.6 Information systems and financial reporting and regulatory requirements for controls.
6.7 structure, roles and responsibilities
6.8 Application controls in Data warehouse, Data Mart, DSS, ESS, AI, EFT, EDI, etc.
6.9 Various types of Business Applications like ERP, Banking, Accounting, etc.
6.10 Procedures to manage changes to business processes and impact on controls
6.11 Audit program for planning and perform review of application software
6.12 Application system software environment at different levels
6.13 Database architecture: database structure and tables, user creation and administration, reporting, query and SQL Features
6.14 Key business system users, key functionality, user rights and segregation of duties levels of authorization, and data security
6.15 Controls at different levels, areas of control weaknesses, risk rating and remedial measures
6.16 Report findings in specific format using standards/best practices as required.
6.17 Application controls review as relevant for assurance or compliance assignments.

Note: Module 6 will be covered as hands on training module. The concepts will be covered first and then specific aspects of Application controls will be covered. The training will be covered as follows:

1. Supplementary E-Learning module covering the concepts to be completed by participants: 12 hours (optional)
2. Hands-on training covering Task statements 6.1 to 6.10 through practical case studies: 4 hours
3. Hands-on training covering Tasks statements 6.11 to 6.18 through exercises using specific software: 8 hours.

The detailed coverage of the hands-on training will include demo and exercises covering various features of application controls in identified application software.

MODULE 7: BUSINESS CONTINUITY MANAGEMENT (6%)

(Covered in 1 day of class Room training)

OBJECTIVE:

Provide assurance or consulting services to confirm whether the Business continuity management (BCM) strategy, processes and practices meet organisation requirements to ensure timely resumption of IT enabled business operations and minimize the business impact of a disaster.

TASK STATEMENTS

7.1 Distinguish between Disaster recovery plan, Business Continuity Plan and BCM.
7.2 Evaluate the organisation business continuity plan to assess the adequacy and capability to continue essential business operations during the period of an IT or non-IT disruptions.
7.3 Applying industry best practices and regulatory requirements as relevant for BCM such as COBIT/ISO, etc.

7.4 Map business continuity management practices to organisation requirements, objectives and budgets.
7.5 Review the organisation processes of business resilience in the context of BCM.
7.6 Identify the business and operational risks inherent in an entity's disaster recovery/business continuity plan.
7.7 Assess the process of business Impact analysis.
7.8 Identifying recovery strategies and their adequacy to meet business needs.
7.9 Assess impact of RPO/RTO on Computer setup and IT Service Design.
7.10 Assess adequacy of operations and end-user procedures for managing disruptions and incident management.
7.11 Perform various types of tests for different aspects of Business continuity.
7.12 Assess adequacy of documentation and maintenance process of BCM.
7.13 Assess service level management practices and the components within a service level agreement.
7.14 Review monitoring of third party compliance with the organisation controls as relevant to BCM.
7.15 Evaluate adequacy of BCP processes and practices to confirm it meets business continuity requirements.
7.16 Evaluate organisation BCM practices to determine whether it meets organisation requirements

KNOWLEDGE STATEMENTS

7.1 DRP, BCP and BCM processes and practices and related documentation.
7.2 Industry best practices as relevant such as COBIT, ISO standard for BCP/DRP.
7.3 IT deployment in organisations and business continuity requirements at various levels of IT such as hardware, network, system software, database software, application software, data, facilities, human resources, etc.
7.4 System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, etc.).
7.5 Business impact analysis (BIA) related to disaster recovery planning.
7.6 Development and maintenance of BCM, BCP and DRP.
7.7 Problem and incident management practices (e.g., help desk, escalation procedures, tracking).
7.8 Analyzing SLA reports and relevant provisions.
7.9 Backup & Recovery strategies, Recovery Window, RPO and RTO.
7.10 Data backup, storage, maintenance, retention and restoration practices.
7.11 Regulatory, legal, contractual and insurance issues related to BCM.
7.12 Types of alternate processing sites and methods (e.g. hot sites, warm sites, cold sites).
7.13 Processes used to invoke the disaster recovery plans and BCP as relevant.
7.14 Testing methods for DRP/BCP and BCM.
7.15 Auditing the BCP-DRP plans.

PROJECT REPORT ON IS ASSURANCE (10%)

(Includes One Day of training on IS Audit case Studies as guidance for Project Work)

The objective of Project work is to ensure application of knowledge learnt by the participants of the ISA work so as to develop relevant skills. This will be done in group of 2-3 as selected by faculty. The Project work is to be completed and submitted covering live IS Audit or consulting assignment (based on case study) as assigned by the faculty. The project work has to be submitted within 4 weeks of completion of module 7 to CIT and marks awarded will be included in the eligibility test.

Note:

- **Obtaining minimum passing marks in project work is compulsory for passing the eligibility test.**
- **Each of the participants will be given same marks as this is a group exercise.**