

Expanded Syllabus

Current Version December 2003

Expanded Syllabus

Syllabus Updating

Students need to check regularly the Institute's magazine and website for any update details.

The syllabus is reviewed in two ways:

Annual Review

For substantive changes the syllabus is reviewed annually. Where there are any changes they will be advised in the autumn prior to any new items becoming examinable – for the first time – in June the following year.

On-going Updating

Items that represent new developments that are relevant to the examinations can be examined after six months. For example, newly published reports and legislation could be the subject of examination questions six months after their publication or enactment. So, for example, something published on January 1st (or before) could be examined in the June examination. The minimum period of time (six months) will enable students, and tuition providers, to research the item and ensure that they have sufficient information and guidance on it to tackle the examination, should the item come up.

Module 4 – Business Information Systems Auditing

Aims and Objectives

This module is designed to enable the internal auditor to understand business information systems and the purposes and techniques of information systems auditing. In particular, the module focuses on:

- Developing an understanding of the value of information systems and their contribution to meeting corporate objectives and managing risk
- Explaining how to critically evaluate the effectiveness of an organisation's controls relating to its information and processes
- Developing an understanding of the main infrastructure components within the information systems environment
- Identifying risks to the confidentiality, integrity and availability of information and processes, and the control measures to effectively manage those risks
- Explaining how to critically evaluate the effectiveness of an organisation's information system developments and project management
- Explaining how information systems and technology can be used to deliver audit objectives.

Competencies to be demonstrated

The module develops competencies that are essential for the delivery of effective business information systems auditing. Those who have successfully completed the module will be able to demonstrate the following competencies:

- The provision of assurance on the effectiveness of an organisation's information and processes, and the effective use of resources
- The ability to carry out reviews covering areas where technical terminology is common and to effectively communicate any findings to senior management
- The provision of assurance on the effectiveness of information security and the ability to recommend actions to manage risks to acceptable levels
- An understanding of standards for information security and the ability to measure the degree of compliance with best practice
- The provision of advice to management on how to deliver successful information system projects
- The timely completion of audit reports at each stage of a systems development project to assist project stakeholders in making effective decisions
- The ability to formulate an effective audit plan, covering information systems topics and produce audit programmes for each topic
- An understanding of the use of information systems and technology to help the audit department successfully deliver its objectives.

Syllabus

The syllabus comprises five subject areas; business information processes, information systems infrastructure, security and control of information systems, information systems development and project management, and information systems auditing role and techniques. The details of the content of each subject area are given below.

1. Business Information and Processes

- 1.1 Explains the value of information systems to organisations in providing requisite information and effective business processes, and in the delivery of customer service requirements and competitive advantage
- 1.2 Explains how to assess the risks to the organisation of not having effective information systems and business processes
- 1.3 Explains the need for requisite information for decision making, such as the importance of providing the right information, pertinent to agreed policies and objectives, to the right person at the right time in the right medium in a clear and unambiguous form
- 1.4 Explains how to assesses the risks to business of not using requisite information
- 1.5 Describes the range of information from manual, basic accounting to advanced operational information for decision making
- 1.6 Explains how information can help to exploit opportunities and manage business risk
- 1.7 Describes and evaluates the use of the Internet and intranets as information sources
- 1.8 Explains what is understood by knowledge management and differentiates between knowledge, information and data
- 1.9 Defines data quality and explains how it underpins effective information
- 1.10 Outlines an effective information strategy and explains how it links with corporate objectives.

2. Information Systems Infrastructure

- 2.1 Identifies and appraises information delivery methods and types of user interfaces
- 2.2 Summarises the main software components, including operating software, network software and databases, and the risks associated with each
- 2.3 Summarises Internet and e-commerce software and the associated risks
- 2.4 Summarises the main types of corporate application software, including business applications, enterprise resource planning systems and customer relationship management systems, and the risks associated with each

- 2.5 Summarises the enabling software components, including email, workflow, document management and data warehousing
- 2.6 Summarises office and end-user applications and the associated risks
- 2.7 Summarises the main hardware components, including mainframes, servers, PCs, networks and network equipment, and the risks associated with each
- 2.8 Explains the different roles and responsibilities within an information systems department and the risks associated with each.

3. Security and Control of Information Systems

- 3.1 Explains the requirement for information security and data protection, including the protection of key corporate data, personal data and intellectual property
- 3.2 Outlines the main statutory and regulatory powers giving access to and governing the disclosure of information
- 3.3 Identifies the internal and external threats to information systems, including computer fraud and abuse, malicious software and viruses
- 3.4 Summarises standards for information security and how to measure the degree of compliance with best practice
- 3.5 Describes how to appraise an information security policy and summarise its coverage, including the categorisation of data, levels of access, passwords, data retention, Internet and email use
- 3.6 Describes the main information security controls and explains how each mitigates risk, including:
 - physical and environmental controls
 - business continuity planning and disaster recovery
 - network controls
 - system software controls
 - database controls
 - application controls
 - Internet and e-commerce controls
 - installation and operational controls
 - change controls
 - access controls
 - encryption, authentication and non-repudiation
 - personnel controls
 - end-user controls
 - software licensing controls.

4. Information Systems Development and Project Management

- 4.1 Explains why an organisation benefits from effective project management and how it realises the benefits of business process change

- 4.2 Summarises the risks associated with information systems projects and identifies mitigating controls
- 4.3 Explains what is meant by project methodologies, milestones and decision points
- 4.4 Identifies the requisite information required by project stakeholders at each decision point
- 4.5 Summarises the process for procuring and developing systems, the development controls and explains how the latter mitigate risk
- 4.6 Compares different types of development, including incremental, prototyping and rapid application development
- 4.7 Identifies the main types of systems documentation and explains what they evidence
- 4.8 Describes how to assess the effectiveness of system design and explains the role of quality assurance
- 4.9 Explains why an organisation would outsource facilities and identifies the risks and mitigating controls
- 4.10 Identifies the main types of outsourcing, including bureau, application service provision, facilities management, maintenance
- 4.11 Identifies the use of service level agreements and methods of service measurement
- 4.12 Identifies the main stages of systems implementation, including system configuration, data migration and interfaces to legacy systems, and identify the risks and mitigating controls
- 4.13 Compares different types of post project and development process reviews, including post-implementation reviews and learning from experience.

5. Information Systems Auditing Role and Techniques

- 5.1 Describes the information systems audit role and objectives
- 5.2 Summarises the audit process, based on a general risk assessment of the organisation's information and computing use, the formulation of an effective audit plan covering information systems topics and the production of audit programmes for each topic
- 5.3 Explains the role of internal audit in relation to systems development, including the review of the development process and participation in systems under development
- 5.4 Describes and evaluates the main audit uses of information systems and technology, explaining how each contributes to successfully delivering objectives:
 - risk and control assessment
 - data interrogation and extraction
 - systems testing
 - audit automation
- 5.5 Summarises data forensics and how to secure and preserve evidence

Module 11 Specialist Information Systems Auditing

Aim	Development of the knowledge and skills of specialist computer auditors to undertake technical audits.
Syllabus	<ol style="list-style-type: none">1. IT Management<ol style="list-style-type: none">1.1 Organisation and management of information systems1.2 IT strategies and their link to business objectives; decision making and systems selection1.3 IT project management1.4 Systems development approaches, including CASE, principles of object oriented development, rapid application developments and end user computing developments1.5 Performance planning and management1.6 Audit automation1.7 Outsourcing IT – the control and audit implications; auditing service level agreements. 2. Systems Software<ol style="list-style-type: none">2.1 Operating systems software and the role of systems programmers<ul style="list-style-type: none">• concepts, components, functions and operating systems software• role of systems programmers and other technical staff in configuration of systems software and change/version control• installation/modification/maintenance of systems software• audit of operating software and related activities, including controls over the usage of significant facilities• knowledge of a mainframe/mid range operating system2.2 Database management system software and the role of the database administration function on large database systems<ul style="list-style-type: none">• database concepts, types, file organisation structures• principle functions of database management software• data dictionary and its use by database specialists, users and auditors• control functions of database management software• database design, testing and implementation• controlling the database administrator and database administration function• query languages and their use by users and auditors, use of other audit software for database interrogation• audit of database systems and software

- knowledge of a specific database management system to be demonstrated
- 2.3 Other mainframe systems software and facilities
 - types and functions
 - audit implications and software.
- 2.4 Access control software packages and products
 - functions of specialist access control software
 - auditing access control software packages
 - knowledge of a specific access control software package to be demonstrated
- 2.5 Microcomputer operating systems and other software
 - functions of microcomputer operating systems
 - functions of other microcomputer software, including security packages, spreadsheets, accounting, database, word-processing, recovery software and utilities
 - audit approaches to microcomputer software, including demonstrating knowledge of specific software.

3. Security and Contingency Planning

- 3.1 Security and control of IT facilities in the mainframe/mid range environment
 - developing and enforcing an IT security policy
 - physical security, locations, buildings, services, fire, flood, electronic radiations and access control to computer facilities
 - personnel security
 - file security
 - terminal security
 - communications security
 - systems development and application change control security
 - computer operations security
- 3.2 Disaster recovery and contingency planning
 - business resumption planning
 - various disaster recovery methods
 - developing and testing the disaster recovery plan
 - managing total and partial disasters
- 3.3 Microcomputer security and contingency planning – relating the above to the micro-computer environment
- 3.4 Audit reviews of the above.

4. Network and On-line Systems

- 4.1 Hardware and software components, basic hardware components of on-line and real-time systems

- 4.2 Networks and telecommunications – technical descriptions, control and security issues, audit of networks and telecommunications
- 4.3 LAN's and WAN's – technical descriptions, control and security implications, audits of WAN's and LAN's
- 4.4 Client server architecture and PC's – technical descriptions, control and security implications and audit approaches to client/server systems

5. Auditing Applications and Advanced Systems

- 5.1 Auditing application systems – types and classification of controls, general approaches to system audits in IT
- 5.2 Advanced technology trends
- 5.3 Expert systems
 - business and audit uses of expert systems
 - technical descriptions of expert systems
 - impact on control
 - audit approaches to expert systems.
- 5.4 Document image processing
 - business considerations, advantages, disadvantages
 - technical descriptions, controls/security considerations and legal implications
 - audit approaches to document image processing.
- 5.5 Electronic mail
 - technical description
 - business considerations, advantages, disadvantages
 - control and security issues
 - audit approaches to electronic mail
- 5.6 Electronic Data Interchange (EDI)
 - technical description
 - business considerations, advantages, disadvantages
 - control, security and legal issues
 - audit approaches to EDI
- 5.7 Electronic Funds Transfer Systems (EFT)
 - technical description
 - business considerations, advantages, disadvantages
 - control, security and legal issues
 - audit approaches to EFT
- 5.8 Data Warehousing
 - technical description
 - business considerations, advantages, disadvantages
 - control and security issues
 - audit approaches to data warehousing

- 5.9 The Internet and E-commerce
- technical descriptions
 - business considerations, advantages, disadvantages
 - performance, control, security, and legal issues
 - audit approaches

