Brochure of IS Audit and Control

The Vision:

CMAs are preferred finance professionals who provide the financial leadership in enterprises across the globe.

One of the objectives of the institute is “To develop the professional body of members and equip them fully to discharge their functions and fulfil the objectives of the Institute in the context of providing financial leadership of enterprises globally.”

The Institute constantly endeavours to enable its members upgrade their competencies and skills to provide management accountancy services to commercial and not-for-profit enterprises to enable them to adequately address new challenges in a dynamic environment in which they operate.

IS Audit and Control

The Program:

This is a Certification program of the Institute. The Program adopts the curriculum of ISACA and seeks their help in choosing the right faculty and examiners. ISACA (International Systems Audit and Control Association) - is an international professional association focused on IS Audit, IS Security, IT Governance and IT Risk Management.

Raison D’être of the Program:

Post liberalization, India has chosen the path of market-driven economy. The way of doing business has undergone a paradigm change, thanks to the technological changes, and constantly changing the customers’ aspirations, geographical boundaries, and regulatory environment.

The Revolution in the realm of computing has brought in its wake, speed, flexibility and mobility. Along with the Risk of losing, stealing, and manipulating the precious data has increased by many times.In the days of click and portal, the emphasis is on online transactions, divorcing in a large way, the pen and paper mode. These developments no doubt have susceptibilities and it is a constant challenge for an Auditor to overcome and ensure protection of the business interests of the Auditor and the client.

The above revolution has posed serious challenges to Accountants and Audit professionals. Today's business enterprises are totally automated with very few manual dependencies. Processes and controls are in-built in modern technologies and therefore need to be reviewed with a fresh perspective by using latest tools and techniques.

The Programme aims to build capabilities among the members of the Institute to take those challenges and to handle challenges in auditing in an IT environment using IT tools.

ISACA

ISACA is a non-profit global association that was formed, and continues to exist today, to meet the unique and diverse technology needs of the continually developing IT field. In an industry in which change is constant, ISACA has moved with agility and speed to bridge the needs of the international business community and the IT control community

The Curriculum

The Institute has adopted the ISACA Model curriculum for IS audit and control (3rd edition).

The topics covered by the model are grouped into five content domains. These domains are divided into major topic areas, and subtopics are provided within each topic area, along with the number of contact hours needed to adequately cover the topic, which **total 240 hours.** The Domains as under**:**

- The Process of auditing information systems
- Governance and management of IT
- Information systems acquisition, development and implementation
- Information systems operations, maintenance and support
- Protection of information assets

Benefits to Members:

The ISACA model curriculum entitles the program to be posted on the ISACA web site, and graduates of the program shall qualify for one year of work experience toward the CISA certification. ICAI members would be entitled to two years of further credit. Therefore, of the total requirement of five years of work experience in the IS Audit Domain, members successfully undergoing this course would need only two more years of relevant experience. The course curriculum would give them the required technical impetus and exposure to successfully complete the remaining two years of training requirement.

It is envisioned that the contact hours would typically be in some type of classroom, but the model is designed so that the contact could be accomplished through other education delivery methods, including distance learning programs.

Duration: One Year

Pedagogy:

Self learning mode in the form of periodical contact sessions and web based learning through webinars

Scheme of Evaluation:

Since the course requires a dedicated and disciplined approach, the evaluation is being carried on periodically.

Examination:

At the end of the duration there will be one examination of MCQ of 4 hrs duration. The examinations will be conducted twice in a year normally in the month of June and December. Examinations will be conducted by the Examination Department of the Institute.

The Pattern of Examination:

The Question Paper will be Objective with multiple choice questions.

The Eligibility Criteria:

Only members of the Institute are eligible for registration for the programme.

Registration Process:

Registration will be online and the link will be provided to applicants. For registrations please visit the Institute's web site www.icmai.in

Fee

Rs.20,000 (Twenty thousand rupees only). The fee does not include examination fee and the cost of course material, if any.

*Note: **Awarding of the CEP** Credit Hours to the members of the Institute is under active Consideration.*

Curriculum

Domain 1:

The Process of auditing information systems

Knowledge Objective
Developing the knowledge necessary to provide audit services in accordance with IT audit Standards to assist the enterprise with protecting and controlling information systems.

Learning Objectives

- Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
- Plan specific audits to determine whether information systems are protected, controlled and Provide value to the enterprise.
- Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
- Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
- Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner

Risk-Based IT Audit Strategy: Risk Assessment Concepts. Control Objectives and information systems control. Applicable laws and regulations affecting the audit scope. Quality assurance systems and framework. Technology and audit environment changes.

Specific Audit Planning: Audit Charter /engagement letters. ISACA IT Audit and assurance standards, guidelines, assurance guide, tools and techniques, code of professional ethics. Audit Planning Techniques and Project Management. Audit Planning Steps. Business Processes (e.g. Accounting, HR). Performing Risk assessments

IT Audit Standards: Evidence Collection techniques (e.g. observation, inquiry, interviews, inspection, data analysis). Sampling methodologies. Internal control and control types (preventive, detective etc.,). Steps to determine regulatory requirements. Procedures for testing and evaluating internal controls. Fraud detection techniques and tools. Use of self assessments

Audit reporting, communication and follow up: Reporting and communicating techniques. Exit Interviewing. Presentation and reporting techniques

Domain 2

Governance and Management of IT

Knowledge Objective

Understands and can provide assurance that the enterprise has the structure, policies, Accountability mechanisms and monitoring practices in place to achieve the requirements of Corporate Governance of IT.

Learning Objectives

- Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, Directions and performance support the enterprise's strategies and objectives.
- Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the enterprise's strategies and objectives.
- Evaluate the IT strategy, including the IT direction, and the processes for the strategy's Development, approval, implementation and maintenance for alignment with the enterprise's strategies and objectives.
- Evaluate the enterprise's IT policies, standards and procedures, and the processes for their development, approval, implementation, maintenance and monitoring to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- Evaluate the adequacy of the quality management system (QMS) to determine whether it supports the enterprise's strategies and objectives in a cost-effective manner.
- Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance) for compliance with the enterprise's policies, standards and procedures.
- Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the enterprise's strategies and objectives.

- Evaluate IT contracting strategies and policies, and contract management practices to Determine whether they support the enterprise’s strategies and objectives.
- Evaluate risk management practices to determine whether the enterprise’s IT-related risk is properly managed.
- Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
- Evaluate the enterprise’s business continuity plan (BCP) to determine the enterprise’s ability to continue essential business operations during the period of an IT disruption.

IT governance structures: IT strategy, policies, standards and procedures for an enterprise and the essential elements of each. IT governance, security and control frameworks, related standards, guidelines and practices. IT audit role in governance

IT organizational structure and HR: Committee structures with their roles and responsibilities. Organizational structure, roles and responsibilities related to IT HR policies such as hiring, performance and training. Segregation of duties and mapping to roles and responsibilities.

IT strategy and direction: Organizational technology direction. Organizational business strategic direction and how IT aligns with it

IT policies, standards and procedures: Processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures for an enterprise and the essential elements of each Regulatory and legal requirements impacting the enterprise

QMS and IT management of controls: Quality management systems. Investment and financial allocation techniques

Monitoring and assurance practices: Process optimization techniques. Sourcing practices. Global sourcing practices. Service and operating level agreements (OLAs)

IT contracting strategies and policies: Third-party and outsourcing practices and techniques. Change management techniques. Supplier/vendor selection, contract and relationship management

Risk management Practices: Business impact analysis (BIA) and risk management practices. Enterprise risk management (ERM) system

Business continuity planning (BCP) : Standards and procedures for the development and maintenance of the BCP and the testing methods.

Domain 3

Information Systems Acquisition, Development and Implementation

Knowledge Objective

Understands and can provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the enterprise's strategies and objectives

Learning Objectives

- Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
- Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risk to the enterprise.
- Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the enterprise's policies, standards, procedures and applicable external requirements.
- Evaluate the readiness of information systems for implementation and migration into Production to determine whether project deliverables, controls and the enterprises requirements are met.
- Conduct post implementation reviews of systems to determine whether project deliverables, controls and the enterprise's requirements are met.

Business case Development: Benefits realization techniques (total cost of ownership [TCO], return on investment [ROI]), Project and portfolio management techniques.

Project management practices: Project governance mechanisms, Project control frameworks, practices and tools, Project risk management practices.

Project reviews: Project success factors and risk, Risk management practices applied to projects

Develop project Controls: IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, n-tier applications), Acquisition practices, Requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis vulnerability management, security requirements), Control objectives and techniques that ensure completeness, validity, accuracy and authorization of transactions and data (e.g., COBIT), Systems development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques), Testing methodologies and practices related to information systems.

Information systems implementation and migration: Configuration and release management related to systems development, Systems migration and infrastructure deployment practices and data Conversion tools, techniques and procedures.

Post implementation reviews: Post implementation review objectives and practices (e.g., project closure, control implementation, benefits realization and performance measurement).

Domain 4

Information Systems Operations, Maintenance and Support

Knowledge Objective

Understands and can provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the enterprise's objectives.

Learning Objectives

- Conduct periodic reviews of information systems to determine whether they continue to meet the enterprise's objectives.
- Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
- Evaluate third-party management practices to determine whether the levels of controls expected by the enterprise are being adhered to by the provider.
- Evaluate operations and end-user procedures to determine whether scheduled and Non-scheduled processes are managed to completion.

- Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the enterprise's objectives.
- Evaluate data administration practices to determine the integrity and optimization of databases.
- Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the enterprise's objectives.
- Evaluate problem and incident management practices to determine whether incidents, Problems or errors are recorded, analyzed and resolved in a timely manner.
- Evaluate change, configuration and release management practices to determine whether scheduled and non-scheduled changes made to the enterprise's production environment are adequately controlled and documented

Information systems reviews: Technology concepts related to hardware and network components, System software and database management systems, Systems resiliency tools

Service level management practices: Service level management practices and components within a service level agreement (SLA),

Third-party management practices: Software licensing and inventory practices , Monitoring techniques for third-party compliance with enterprise internal controls (SSAE16 and SOC reporting, IAE 3402)

End-user procedures and operations: Operations and end-user procedures for managing scheduled and non-scheduled processes.

Maintenance of information systems: Control techniques that ensure the integrity of system interfaces Data administration practices: Database administration practices

Capacity and performance monitoring: Capacity planning and related monitoring tools and techniques, Systems performance monitoring processes and tools (e.g., network analyzers, system utilization reports, load balancing). Problem and incident management: Problem and incident management practices (e.g., help desk, escalation procedures, tracking and monitoring)

Change, configuration and release management: Processes for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices

Backup and restoration of systems: Data backup, storage, maintenance, retention and restoration practices.

Domain 5

Protection of Information Assets

Knowledge Objective

Understands and can provide assurance that the security architecture (policies, standards, Procedures and controls) ensures the confidentiality, integrity and availability of information Assets. Information security policies, standards and procedures and generally accepted practices : Approaches and techniques for the design, implementation and monitoring of security controls, including awareness programs, Incident management techniques, Risk and control associated with data leakage, Evidence preservation techniques for forensics investigations.

Learning Objectives

- Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
- Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
- Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.
- Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
- Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data and softcopy media) to determine whether information assets are adequately safeguarded

Design, implementation and monitoring of system: Logical access controls for the identification, authentication and restriction of users. and logical security controls to verify confidentiality, integrity, availability (CIA) : to authorize functions and data, Risk and controls associated with virtual systems , Network and Internet security devices, protocols, techniques, Detection tools and control techniques, Security testing techniques(intrusion testing, vulnerability scanning), Encryption tools and techniques, Public key infrastructure, Risk associated with peer-to-peer computing, Risk associated with peer-to-peer computing.

Data classification processes and procedures: Data classification standards and supporting procedures, Procedures for storing, retrieving, transporting and disposal of confidential information assets,

Physical access and environmental controls: Physical access controls for the identification, authentication and restriction of users to authorized facilities, Environmental protection devices and supporting practices. Processes for storing, retrieving, transporting and disposing of information assets: Procedures for storing, retrieving, transporting and disposal of confidential information assets, Encryption-related techniques

--End--