COURSE DESCRIPTION:

Information technology, long considered as only an enabler of an organization's strategy, is now regarded as an integral part of this business strategy. Strategic alignment between Information Technology and enterprise objectives is one of the critical success factors. With the changing landscape concerning security, corporate governance, IT service delivery and systems reliability as well as regulatory requirements, the CISA course becomes vital for information technology line and senior managers. The course moduls information technology professionals into complete and competent individuals. The course covers the following five new CISA domain areas:

1. The Process of Auditing Information Systems
2. Governance and Management of IT
3. Information Systems Acquisition, Development and Implementation
4. Information Systems Operations, Maintenance and Support
5. Protection of Information Assets

TARGET AUDIENCE AND PRE-REQUISITES:

Information systems management, audit, control and security professionals including the following:

1. Aspiring IS auditors
2. IT/IS Professionals
3. Auditors
3. Security managers / analysts
4. Software Managers
5. Infrastructure/Network Managers

The course is meant for IS and Business professionals specified in the target group as well as college graduates aspiring to become CISA certified.

TRAINING METHODOLOGY:

The course is delivered using a blended learning model of lectures, discussions, case studies, assessment and practical exercises using a highly-structured, learner-centered teaching methodology that ensures maximum learning. Helpful learning resources will be provided.

COURSE OBJECTIVE:

The main objective of this course workshop is to provide a comprehensive understanding of Information Systems auditing. This course will equip participants with the knowledge and practical skills necessary to successfully perform an audit process.

COURSE OUTLINE

The following topics are presented and discussed to increase your understanding and abilities. CISA candidates are expected to have detailed understanding in each of these areas.

1. **The Process of Auditing Information Systems** Provide audit services in accordance with IT audit standards to assist the organization with protecting and controlling information systems. The auditing process covers IS auditing standards; Risk-based approach; Controls; Audit objectives, planning & scope; Cobit; Field Work; Identifying conditions & defining reportable findings; Review of work; Audit Results Communication.

2. **Governance and Management of IT** Provide assurance that the necessary leadership and organizational structures and processes are in place to achieve objectives and to support the organization's strategy. IT governance structure, IT organizational structure and HR management; Evaluating IT Strategies; Evaluating IT policies, standards & procedures; IT Resource Investment; Evaluating Risk-management, monitoring and assurance practices.

3. **Information Systems Acquisition, Development and Implementation** Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives. Evaluation approach, Project Management; Functional Requirements, Feasibility Analysis; System Design; System Development; System; Acquisition, Implementation, Post-Implementation;

4. **Information Systems Operations, Maintenance and Support** Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives. Service Level Management; Evaluating Systems Software; Evaluating Hardware Acquisition & Installation; Evaluating network infrastructure (voice & data); Evaluating change, configuration and release management; Capacity and Performance monitoring tools & techniques; Data Administration practices; Problem & Incident management practices.

5. Protection of Information Assets Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.