

# Certified Information Systems Auditor (CISA)

16<sup>th</sup> - 20<sup>th</sup> October 2011 Abu Dhabi UAE

Price: USD 2,695 /Per Delegate

Registration is available online log in to [www.invention-i.com](http://www.invention-i.com)

## 5 Days Course outline

### Day 1 – CISA Boot Camp The Process of Auditing Information Systems

(Corresponds to Domain 1 of the CISA exam – 14%)

#### Description:

The rapid and dramatic advances in information technology (IT) in recent years have without question generated tremendous benefits. At the same time, however, they have created significant, unprecedented risks to enterprises public, private, and governmental.

Computer security has, in turn, become much more important as organizations of all sizes utilize information systems security measures to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information. Such use of computer security is essential in minimizing the risk of malicious attacks from individuals and groups.

To be effective in ensuring accountability, auditors must be able to evaluate information systems security and offer recommendations for reducing security risks to an acceptable level.

Information System Auditing is primarily an examination of the system controls within an IT architecture -- which is the process of evaluating the suitability and validity of an organization's IT configurations, practices and operations. Information System Auditing has been developed to allow an enterprise to achieve goals effectively and efficiently through assessing whether computer systems safeguard assets and maintain data integrity.

Auditors are concerned with four objectives: asset safeguards, data integrity, system effectiveness, system efficiency. One of the key issues of auditing is to identify whether errors and irregularities will cause material losses. Auditing might also assess whether the processes followed have contributed or are contributing to any ongoing losses. To assess these auditors need to collect evidence.

#### Objectives: After completing this session, participants will be able to:

- Understand the IS Audit Process
- Identify ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards
- Comprehend risk assessment concepts, tools and techniques in an audit context
- Identify control objectives and controls related to information systems
- Distinguish applicable laws and regulations which affect evidence collection
- Determine appropriate evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis) used to gather, protect and preserve audit evidence
- Explain different sampling methodologies related to audit processes.
- Address the examination requirements for Domain 1 of the CISA exam.

#### Session Outline:

Introduction  
 The Major Elements of an IS Audit  
 Management of the IS Audit Function  
 Steps to perform in planning an audit  
 Policies and Procedures  
 Organization and Management  
 IT Infrastructure  
 Operating Software  
 Application Systems Development  
 Application Systems Reviews  
 ISACA IS Auditing Standards, Guidelines and Procedures

- S1, S2, S4, S9, and S14
- G5, G10, G18, and G28
- P1, P5, P7, and P8

Defining Risk  
 Information Risk Management  
 What is risk analysis?  
 The Components of Risk

#### Calculating Risk

- Quantitative Risk
- Qualitative Risk Analysis

#### Analyzing Risk

- Business Threat Modeling

#### Assessing Risk

- What Is A Risk Assessment?
- Threat Assessment Process

#### Evaluation of risks

What Is 'Information Risk' Exactly?

Asset Valuation

Other Risk Analysis Methods

Risk Mitigation Options

Compliance testing and Substantive testing

Evidence collection techniques

- Interview
- Data analysis

#### Summary

- Audience Participation Activities  
Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)  
Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

# Day 2 – CISA Boot Camp Governance and Management of IT

(Corresponds to Domain 2 of the CISA exam – 14%)

## Description:

The combination of business changes (market demands), enterprise responses (in terms of IT-intensive organizational changes), and technologies dispersed into business units, creates a need to explore how IT is most effectively and efficiently governed.

IT Governance may be defined as a framework for the ongoing leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that IT supports and enables the achievement of both IT and organizational strategies and objectives.

IT portfolio management is a restricted collection of IT assets, plotted against investment strategies, which are tied to acceptable risk levels designed to meet business objectives. This is achieved through a calculated, favorable mix (the proportion or variety of investments made in each enterprise area), based on a postulation about future performance, (planned and deliberate development expectations of the enterprise).

The result is in taking advantage of the reward versus risk tradeoffs (guaranteeing that the identified IT investments provide the required level of usefulness for the cost and risk involved) in maximizing the enterprise's returns on its IT spend.

This session addresses the critical linkage between proactive IT governance and practical IT portfolio management.

## Objectives :After completing this session, attendees will be able to:

- 1.Map business and IT assets into a portfolio representation.
- 2.Use portfolio representations as a communication tool among various parts of the business, the IT group, and the executive office.
- 3.Recognize the inter-relationships between governance, risk and compliance as a means to effectively govern IT
- 4.Identify and categorize IT investments according to their levels of necessity and risk.
- 5.Evaluate the “line items” in an IT portfolio. The line-items constitute the applications, or the infrastructure elements, or the IT services, or the development projects.
- 6.Detect elements of continuing “disconnects” between the business leadership and their IT assets and resources, and assess whether these disconnects get in the way of successful exploitation of IT by businesses.
- 7.Determine the responsiveness of IT to the needs of users and the enterprise.
- 8.Identify practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators, and key goal indicators).
- 9.Better understand business impact analysis (BIA) as it relates to business continuity planning.
- 10.Address the examination requirements for Domain 2 of the CISA exam.

## Session Outline:

### **Introduction**

- Governance, Risk, Compliance (GRC)

### **Governance**

- Governance Framework
- GRC Objectives
- Why is GRC Needed?
- What Does GRC Include?
- The GRC Challenge
- Why Does GRC Matter?

### **IT Governance vs. Data Governance**

- Why IT Governance?
- What is IT Governance?
- IT Governance Objectives
- Benefits of IT Governance

### **Risk and Compliance**

- Asset Based Risk Assessment
- Threat Modeling
- Technical Audit
- Dependency Modeling
- Gap Analysis

### **IT Governance vs. Data Governance**

- Why IT Governance?
- What is IT Governance?
- IT Governance Objectives
- Benefits of IT Governance

### **Risk and Compliance**

- Asset Based Risk Assessment
- Threat Modeling
- Technical Audit
- Dependency Modeling
- Gap Analysis

### **IT Governance Frameworks**

- COBIT
- ITIL
- COSO
- CMMI

### **Open Compliance & Ethics Group (OCEG)**

- What is OCEG?
- OCEG Framework

### **IT Portfolio Management**

- IT Portfolio Assessment
- Governing IT Activities

### **Summary**

- GRC Key Challenges
- GRC Success Factors
- Effective Governance Enablers
- IT Governance Maturity Benchmark

### **Reporting of IT performance**

- Balanced scorecards
- Key performance indicators [KPI]
- Key Goal Indicators [KGI]

### **Business Impact Analysis Related to Business Continuity Planning**

## Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

## Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

# Day 3 – CISA Boot Camp Information Systems Acquisition, Development and Implementation

(Corresponds to Domain 3 of the CISA exam – 19%)

## Description:

Managing software projects is difficult under the best circumstances. Organizations can improve chances of success by applying known industry smart practices for software project management.

The system development life cycle (SDLC) is a common methodology for systems development in many organizations. This methodology features distinctive phases, each of which records the progress of the systems analysis and design project. The potential for abuse, inefficiencies, and the potential to deliver application systems, which do not meet the needs of the end-user, warrants the involvement of IT and user management as well as the audit function in most all software development efforts.

This session will examine the basic elements of the SDLC process, and how the process of designing new systems has (and continues to) evolve. Attendees will also discuss strategic system design methodologies, and how the auditor can be an effective change agent within this process.

The session focuses on providing assurance that the practices for the acquisition, development, testing and implementation of information systems meet the organization's strategies and objectives.

## Objectives: After completing this session, participants will be able to:

- Interpret the requirements for PDLC application development from a base of confidence and understanding.
- Confidently advise management on specific controls necessary for successful application development.
- Find managing application development projects easier.
- Discuss with both end users and management, how successful systems are developed and maintained.
- Lay the foundation for successful application development projects, which includes planning the project, estimating the work, and tracking progress.
- Discuss the Capability Maturity Model (CMM) as a model of management practices for improving the quality of software.
- Recognize that one of the goals of the PDLC approach is total quality assurance through process-related improvements throughout an entire organization.
- Address the examination requirements for Domain 3 of the CISA exam.

## Session Outline:

Introduction to Systems design and Development

System Design Horror Stories

- Why Projects Fail or Go Wrong

Critical Issues Facing Applications Development

Traditional Systems Development Process

- Advantages
- Limitations

Logical Design Concepts

- Entity-relationship diagram (ERD)
- Data flow diagram
- Prototyping tools

Phases for Successful Project Implementation

What Existing Standards Does Your Organization Utilize?

Make – Buy Decision for Application Acquisition

Guidelines for Application Development

Formal Development Methodology

- Examining the Capability Maturity Model

Alternative Approaches to Systems Development

- RAD
- JAD
- Prototyping
- SWAT
- OO
- Spiral Model
- Extreme Programming
- Unified Modeling Language
- Agile Modeling
- Scrum

Risk Analysis: Systems Development Projects

- Strategy for Application Development

Quality Assurance and the Systems Development Life Cycle

Software Independent Verification & Validation

SDLC Sign-offs

Steps to Improving Applications Development

A Systems View of Project Management

Auditor's Role in Systems Development

- Auditors as Change Agents

## Summary

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

# Day 4 – CISA Boot Camp Information Systems Operations, Maintenance and Support

(Corresponds to Domain 4 of the CISA exam – 23%)

## Description:

While maintaining the operational status of information systems is a major function of all IT departments, information security is of just as great a concern. The steps organizations take to protect information assets from compromise or danger is the core and purpose of the CIA (Confidentiality, Integrity, and Availability) security model, and the basis for any organization's information security program.

All information systems are ultimately judged by their ability to provide continuous operations for the network services they support.

Installed technology needs ongoing maintenance and support, or it will not remain functional for long.

IT support services cover a range of services providing assistance with computer hardware, software, network or other. IT support services attempt to help the user solve specific problems with a product or a service, whereas IT maintenance services help your company prevent problems with your hardware, software, network and security.

Business applications require ongoing maintenance and support for their underlying infrastructure, which makes managing support contracts a crucial part of the overall IT and business management functions. Support and maintenance contract information must be readily available for planning and budgeting purposes— and especially in cases of emergencies. This helps reduce business risks associated with application support, capacity provisioning, and any other ongoing infrastructure issues.

This session focuses on those activities directly related to the operation, maintenance and support of information systems.

## **Objectives: After completing this session, participants will be able to:**

- Identify service level management practices and the components within a service level agreement
- Recognize appropriate software licensing and inventory practices
- Document sound database administration practices
- Identify proper change, configuration, release and patch management practices
- Address the development, maintenance and testing of disaster recovery plans
- Assess Business Impact Analysis (BIA) related to disaster recovery planning
- Evaluate capacity planning and related monitoring tools and techniques
- Recognize key business recovery objectives and metrics
- Address the examination requirements for Domain 4 of the CISA exam.

## **Session Outline:**

- Service level management practices and the components within a service level agreement
- Types of IT Maintenance Support Solutions
- Technology concepts related to hardware and network components, system software and database management systems
- Software licensing and inventory practices
- System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)
- Database administration practices
- Capacity planning and related monitoring tools and techniques
- Systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)
- Change, configuration, release and patch management practices
- Data backup, storage, maintenance, retention and restoration practices
- Development, maintenance and testing of disaster recovery plans
- Business Impact Analysis (BIA)
- The Purpose of the BIA
- What is Business Continuity Management?
- Objective of Business Continuity Management
- Business Impact Assessment (BIA)

## Key Business Recovery Objectives

- RTO
- RPO
- RTG
- ROG
- REG
- RCC
- RLS
- RSS
- MPO
- MTO
- MAD

## Recovery Gaps

Total Cost of Recover

## **Summary**

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

# Day 5 – CISA Boot Camp Protection of Information Assets

(Corresponds to Domain 5 of the CISA exam – 30%)

## Description:

Ensuring the integrity and confidentiality of information and the associated timely availability of systems to authorized users is the cornerstone of an effective system of internal controls to protect an organization's information assets.

Information is among an organization's more valuable assets and management relies upon information to support its business activities. The quality of preservation and retention of such information is key to an organization's ability to provide services to its customers and stakeholders.

Therefore, the security of an organization's information and of the technology that facilitates its use is a responsibility shared by all personnel. Any user who has been authorized to access the organization's information has an obligation to preserve and protect these information assets in a consistent and reliable manner.

Controls provide the necessary physical and procedural safeguards to accomplish such obligations. The establishment and management of such controls enable information to be shared while ensuring protection of that information and its associated systems.

Management, together with internal workforce and external third parties, is responsible for ensuring that appropriate controls are in place to maintain the objectives of confidentiality, integrity, and availability for the organization's information.

Compliance with applicable legislative and regulatory mandates is key elements of an organization's information asset protection program. Thus, compliance that all information is processed, maintained and disposed of in accordance with all relevant federal and state laws, rules, and regulations, is paramount.

The focus of this session will be to examine, in depth, the process, procedures, and methods used to protect an organization's information assets.

## Objectives: After completing this session, participants will be able to:

- Evaluate the techniques for the design, implementation, and monitoring of security controls, including security awareness programs
- Assess logical access controls for the identification, authentication and restriction of users to authorized functions and data
- Determine the configuration, implementation, operation and maintenance of network security controls
- Identify network and Internet security devices, protocols, and techniques
- Examine information system attack methods and techniques, including detection tools and control techniques (e.g., malware, virus detection, spyware)
- Apprise security testing techniques (e.g., intrusion testing, vulnerability scanning)
- Evaluate risks and controls associated with data leakage
- Assess encryption-related methodologies including, public key infrastructure (PKI) components and digital signature techniques
- Determine risks and controls for voice communications security (e.g., PBX, VoIP) along with mobile & wireless devices
- Examine the evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody)
- Recognize the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
- Address the examination requirements for Domain 5 of the CISA exam.

### Session Outline:

#### **Data Classification Processes and Procedures System and Logical Security Controls**

##### **What is Incident Management?**

- The Objectives of Incident Management
- What is Incident Response?
- The Objectives of Incident Response
- Risk in Incident Response
- Incident Response Organization Services
- Incident Response Planning
- Achieving the Objectives of Incident Response
- Components of an Effective, a Good Incident Management System
- Metrics for Incident Response
- Performance Measurements for Incident Response
- Six Steps to Handling an Incident Most Effectively
- Incident Management Deployment Phases

##### **Responding to security incidents**

- Escalation procedures
- Emergency incident response team

##### Network Security Controls

##### **Detection Tools**

- IPS
- IDS

##### **Security Testing Techniques**

- Intrusion testing
- Vulnerability scanning

##### **Encryption Concepts**

- Public Key Infrastructure
- Digital Signature Techniques

##### **Voice Communications Security**

- PBX
- VoIP

##### **What is Electronic Evidence?**

- How Evidence Is Destroyed?
- Rules of Evidence
- Chain of Custody, Chain of Evidence
- Evidence Documentation Methodologies

##### Summary

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

# Your Trainer

Albert J. Marcella Jr., Ph.D., CISA, CISM

Albert J. Marcella Jr. is an internationally recognized public speaker, researcher, workshop and seminar leader with over 30 years of experience in IT audit, security and assessing internal controls, and an author of numerous articles and 32 books on various IT, audit and security related subjects.

Dr. Marcella's book *Cyber Forensics: Collecting, Examining, and Preserving Electronic Evidence An Auditor's Field Manual*, second edition, focuses on issues, tools, and control techniques designed to assist audit, law enforcement, and info security professionals in the successful investigation of illegal activities perpetrated through the use of information technology.

Professor Marcella is a tenured, full-professor at Webster University in Saint Louis, MO, where he is responsible for teaching information technology management courses in the University's graduate and doctoral programs.

Dr. Marcella is the Institute of Internal Auditors Leon R. Radde Educator of the Year, 2000, Award recipient. Dr. Marcella has taught IT audit seminar courses for the Institute of Internal Auditors (IIA), continues to teach for the Information Systems Audit and Control Association (ISACA), and has been recognized by the IIA as a Distinguished Adjunct Faculty Member.

## DR. MARCELLA BELONGS TO THE FOLLOWING PROFESSIONAL ORGANISATIONS:

1. Information Systems Audit and Control Association (ISACA)
2. Institute of Internal Auditors (IIA)

## DR. MARCELLA HAS EARNED THE FOLLOWING U.S. UNIVERSITY ACADEMIC CREDENTIALS:

- Ph.D. (Information Management)
- MBA (Finance)
- B.S. (Information Technology)
- B.S. (Management)

ORGANIZED BY INVENSION INTERNATIONAL

Registration for CISA is available online:

log in to [www.inversion-i.com](http://www.inversion-i.com)

Price : USD 2,695 / Per Delegate

OR you may wish to contact the person in-charge:

Abdul Qadeer

Tel: +603 2162 8485

Fax: +603 2162 7485

Email. [qadeer.h@inversion-i.com](mailto:qadeer.h@inversion-i.com)