COURSE OVERVIEW

* Are you dabbling in audits of Information Technology (IT)?
* Do you hear words like encryption, firewalls, security access, and application controls and cringe?
* Do you want to understand more about Information Technology risks and controls?
* Are you looking for something to alleviate the fear of auditing Information Technology?
* Are you preparing to sit for the Certified Internal Auditor exam?

If you answered yes to any of these questions, this course for you. This course was designed for business auditors who are not IT experts who realize the importance of integrating IT risk and control evaluation into their business audits and who are preparing to sit for the CIA Exam. This 1 day session starts with understanding how your business uses technology and which transactions / process are most risky from a technological standpoint and why it is important for all auditors to understand technology. Then we learn the basics of IT General and Application controls. Finally, we will explore how to integrate IT risk and control evaluation into each audit.

ATTENDEES WILL (NASBA Learning Objectives)

Understand and review the basics of IT

Develop skills to identify risks and controls of IT and its impact on business processes

Learn tests of IT controls that any auditor can perform

Gain practical audit knowledge and skills

WHO SHOULD ATTEND

* Auditors at all stages of their career
  + Staff
  + Seniors
  + Leads
  + Managers
  + Directors
  + Chief Audit Executives
* Risk Management staff
* Business, finance, and accounting students and professionals

COURSE OUTLINE (8 CPE)

Introduction (30 min)

* CIA Exam Content Review
* Test Taking Tips, Tricks, Strategies, and Practice
  + Changing your thinking
  + Secrets to the learning process
  + The facts of life
  + Testing techniques
  + Strategies for using your chosen review materials effectively

Introduction to Information Technology Auditing (1.5 hours)

* Functional areas of IT operations (e.g., data center operations)
* Concepts and definitions
* Control frameworks (eSAC, COSO, COBIT, Netcentric, FISCAM, NIST Special Publication 800-series on Security Controls for Federal Information Systems, GAIT, GTAG, FFEIC, ISO 27002)
* Role of Internal Auditors for IT and IIA standards and practice advisories
  + System Infrastructure and Networks
    - * Operating systems
      * Mainframe
      * Workstations
      * Data, voice, and network communications / connections (e.g., LAN, VAN, and WAN)
      * Server
      * Software licensing
      * Web infrastructure

General and Application Risk Assessments (1 hour)

* Understand the IT risks and continue to build on identified control frameworks
* Explore General and Application controls and their importance in core business processes, including the initiation, authorization, processing, summarization and reporting of critical business functions and data
* Explore the relationship between general and application controls
* Integration of systems and related risks (e.g. ERP, stand-alone)
* Outsourcing Business Processes

Define General Controls and Controls Objectives (2 hours)

* + Authoritative Guidance for Internal Auditors
    1. IIA Standards
    2. Global Technology Audit Guide (GTAG)
    3. Guide to the Assessment of IT General Controls (GAIT)
* Audits of General Controls

A. Security

* + - Physical/environmental / operational management system security (e.g., firewalls, access control)
    - Network security
    - Information protection (e.g., viruses, privacy)
    - Application authentication
    - Encryption

B. Application Development

* + - End-user computing
    - Change control / change management
    - Systems development methodology
    - Application development
    - Information systems development

C.  Business Continuity

* + - IT contingency planning
    - Disaster recovery

D. Databases / Database management

E. IT governance

F. IT infrastructure

G. IT control environment

Application Risk Assessments (1 hour)

* Identifying systems involved in the initiation, authorization, processing, summarization and reporting of critical business functions and data
  + Electronic Funds Transfer (EFT)/Electronic Data Interchange (EDI)/E-commerce
* Reliance on general controls
* Complexity of the application and transactions
* Application risk profile
* Integration of systems (e.g. ERP, stand-alone)
  + Enterprise-wide resource planning (ERP) software (e.g., SAP R/3)

Defining Application Controls and Application Control Objectives (30 min)

* Input Controls
* Processing Controls
* Output Controls

Types of Application Controls (1 hour)

* Embedded and configurable controls
* Input, processing, and output controls
* Integrity controls
* Preventive and detective controls
* Balancing and file version controls
* Application recoverability controls

Application Control Tests (30 min)

* Validating parameter and configuration settings changes
* Review and verification of application code changes
* Logical access tests