Auditing E-Commerce for Non-IT Auditors

E-Commerce refers to the use of electronic medium to carry out commercial activities performed through various electronic sources such as Internet, IT networks, ATM Machines, ET and EDI.

This training provides theoretical knowledge and practical skills in understanding basic IT Controls, E-Commerce infrastructure, critical security aspects, insight into countermeasures for addressing gaps and enabling Business auditors to interpret IT Audit outputs.

Objectives:

After attending this program participants will be able to:

- IT General Controls & its impact on Business Audits
- Cyber-threats / Risk in E-Commerce parlance
- Goals & Objectives of Business Auditors in E-Commerce Audits
- Basic skills to interpret IT Audit results
- Planning & Execution of Business Audits based on IT Audit results

Contents:

Domain 1 – Introduction to Information systems / IT Audit

- IT – audit: definition, basic concepts, goals and objectives
- Overview of standards, tools and approaches used in IT audit
- Risk assessment within audit process
- Techniques of planning and management of the audit process
- Collection of the information and audit evidence

Domain 2 – IT infrastructure Elements, IT Risks and IT General Controls Review

- Basic understanding of the IT infrastructural elements and their purpose
- Insight into IT Risks, Assessment and Framework
- Introduction to IT General Controls Review and interpretation of IT General Controls Assessment

Domain 3 – Information Security

- CIA Triad – Confidentiality, Integrity and Availability
- Information Security Controls
- Logical Access Controls and Access Management
- IT infrastructure Security

Domain 4 – Introduction to E-Commerce and Evolution of E-Business

- E-Commerce – Basic and the Growth of E-Business
- Understanding B2B, B2C and C2C
- E-Commerce – Related Parties, Components and IT landscape
Domain 5 – E-Commerce – Security Concepts

- IT Risks in E-Commerce Parlance and Overlying threats
- Data Integrity, Confidentiality and availability
- Online Banking and Mobile Banking – Risks and Controls
- Basic of Website Security and Secure transaction

Domain 6 – E-Commerce – Non IT Auditors’ Role

- Understanding IT Security concerns in E-Commerce
- Knowledge on Website vulnerabilities, Attack vectors and Tools
- Interpretation to OWASP, NIST and SANS
- Top 10 to Application Security Risks – OWASP

Domain 7 – Latest on Cyber Attacks and Cyber Warfare

- Hacktivism and Cyber Attacks
- Online Banking and ATM-related Attacks / Fraud
- Need for constant updating of security measures to mitigate and awareness campaign
- Social Engineering attacks – Phishing, Vishing, Tailgating, Pre-texting, Quid Pro Quo

**Method:**

Lecture – discussions and case studies

**Target Audience:**

New Business Auditors, Operational Risk personnel, Non-IT Business professional and New IT-Audit personnel who do not have exposure to E-Commerce

**Language:**

The program will be conducted in English

**Duration:**

24 training hours, four days, morning and afternoon sessions