Day 1 – Process of Auditing Information Systems

Students will understand the audit and assurance standards, guidelines, and framework and be able perform an Information Systems Audit.

- Define the audit process
- Understand the audit and assurance standards, guidelines, and framework
- Implement policies, procedures, and organizational structures (internal controls) in order to reduce risk
- Understand how COBIT supports IT Assurance practices
- Plan and perform an IS audit
- Plan and perform a risk based audit
- Understand compliance and substantive testing
- Use different tools and techniques when performing an audit

Day 2 – Governance and Management of IT

Students will be able to govern and manage Information Technology within an enterprise.

- Understand IT Governance and audit’s role in the evaluation of IT Governance
- Define the seven steps of the risk management program
- Develop and analyze a risk management program
- Understand how to manage personnel and develop a sourcing strategy
- Identify Information Security roles and responsibilities
- Identify and develop a business continuity plan

Day 3 – Information Systems Acquisition, Development and Implementation

Students will be able to acquire, develop, and implement Information Systems.

- Identify and determine controls around a project management plan
- Follow a traditional SDLC approach to business application development
- Develop and acquire physical infrastructure
- Validate Information System processes to see that they meet control objectives
- Understand application controls objectives

Day 4 – Information Systems Operation, Maintenance and Support and Protection of Information Assets

Students will be able to run, maintain, and support Information Systems, and protect information assets.

- Manage Information System operations
• Define common Information System hardware and apply a maintenance program
• Understand Information Systems architecture, software, and network infrastructure
• Develop and implement a Disaster Recovery Planning (DRP)
• Classify and protect information assets
• Address privacy, HR, and cybercrime issues
• Understand logical access exposures and manage control software
• Define internet threats and apply network infrastructure security

*Topics covered per day may vary per instructor.*