Degree Level: Undergraduate/baccalaureate or (post) graduate

Course Description:
This course introduces students to information technology (IT) auditing. It covers management's role in controlling IT and addressing the major risks related to technology. Topics include information security, contingency planning, key IT risks, general and application controls, systems development controls, and assurance of information related to on-line, client-server, web-based, internet, and other computer systems. Students will learn approaches to evaluating and addressing IT risks throughout the organization from the perspective of assurance and advisory providers in addition to the view of every end user.

Sample Overall Learning Objectives:
1. Understand and identify key IT risks and how to mitigate those risks.
2. Understand and develop a control checklist and key audit steps related to technology risks.
3. Understand and apply the applicable professional standards, including those of The IIA's GTAGs.
4. Understand the process for auditing general and application controls.
5. Identify risks in an e-business environment.
6. Understand how to adapt audit coverage to areas of emerging technologies.

General Topic	Content Recommendations
Introduction to the Course	- Definition of IT auditing - Overview of IT audit frameworks (e.g., COSO, COBIT, ISO, etc.) - Types of IT audits - Audit IT controls (general vs. application controls) - Definitions of commonly used terms
IT Strategies, Plans, and Budgets	- IT governance and frameworks (roles, responsibilities, execution, etc.) - Alignment between IT and business strategy - Understand organization IT infrastructure, applications, and tools - Understand IT department knowledge, skills, experience, and the value of continuing education - Collaboration/relationships between IT department and internal providers of assurance
IT Design, Development, Change, and Maintenance	- System development life cycle (SDLC) methodology and other program/system change policies and procedures - Formal change management procedures: - Program changes - System changes - Maintenance (including patches or changes to system software)

General Topic	Content Recommendations
Information Security and Data Management	• Introduction to cyber risks and security management process • Overview of vulnerability assessment process • Data access policy development and maintenance of that access, extraction, usage, maintenance, and transmission, including personal information • System and application authentication and access mechanisms • Access rights on financial reporting (and other) systems • Application software and data storage systems configurations • Segregation of duties in network, operating, and application systems • Identifying and handling significant IT events or failures (e.g., security breaches, major system failures, or regulatory failures) • Physical access controls and authentication • Firewalls and intrusion detection
IT Infrastructure (Computer Operations) Provides Reliable Support to Key Business Processes Note: For a better logical sequence, this part could follow the third general topic (now IT design, development, etc.)	• Data and program ownership responsibilities • Monitoring performance and capacity levels of the systems and network • Problem management tracking and resolution systems • Backup of data and programs • Determining the effectiveness of the restoration process and the quality of backup media • Understanding the importance and need for standard procedures for IT operations, including scheduling, managing, monitoring, and responding to events
Auditing Skills	• Recognizing legislation, rules, and regulations related to IT auditing • Analyzing the unique risks of IT and related data • Practicing decision-making skills in a small group setting • Acquiring experience with audit software (e.g., ACL, CaseWare IDEA, MindBridge), test application controls in accounting software (e.g., Sage Pastel, Peachtree), flow charting (e.g., Visio, AllClear, SmartDraw, Pacestar), and software to manage the internal audit engagement (e.g., TeamMate, GRC Paisley, AutoAudit) – *These examples do not constitute an endorsement of any products by The IIA* • Preparing audit reports for IT engagements • Learning about the foundations of data analytics in the internal audit function