COURSE SYLLABUS

Information Technology for Auditors Course

Learn about the components of IT systems, their development and management, and understand your responsibilities under federal auditing standards, including FISCAM, NIST, and peer guidance.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://sdfm.graduateschool.edu/courses/information-technology-for-auditors

CustomerRelations@graduateschool.edu • (888) 744-4723

Course Outline

Module 1: Basic Computer Concepts, Components, and Terms

- Understand core computer hardware, software, data, and systems terminology.
- Explore the structure of information systems and their components.
- Examine storage media, input/output devices, and networking architecture.
- Identify roles of IT personnel, management, and system users.
- Recognize how actual practices can diverge from formal IT policies.

Module 2: Impact of Information Technology on the Auditor

- Understand how IT has changed audit evidence and methodology.
- Learn how audit trails and documentation are affected in automated environments.
- Evaluate segregation of duties and system access in IT systems.
- Identify electronic controls and how to assess their effectiveness.

Module 3: Protection of Information Assets

- Identify physical and logical security mechanisms for IT systems.
- Understand access control software functions and user authentication methods.
- Examine layered security: network, host, application, and data level.
- Explore encryption technologies and their role in data protection.

Module 4: Contingency Planning

- Define contingency planning, disaster recovery, and business continuity.
- Understand federal guidelines (e.g., NIST SP 800-34, SP 800-53) for recovery plans.
- Learn components of IT contingency plans, including testing and maintenance.
- Differentiate among hot, warm, cold, and mobile recovery sites.

Module 5: Systems Development, Acquisition, Implementation, Maintenance, and Review

- Explore the systems development life cycle (SDLC) and auditor's role in each phase.
- Evaluate acquisition of commercial software (COTS) and vendor management.
- Understand quality assurance, system testing, and change control procedures.
- Review post-implementation auditing and application service provider (ASP) risks.

Module 6: Internal Controls

- Classify controls as preventive, detective, corrective, or directive.
- Differentiate general vs. application controls across input, processing, and output.
- Study control frameworks such as COSO, COBIT, and GAGAS.
- Understand control objectives, implementation practices, and effectiveness assessments.

Module 7: Auditing Standards and Guidelines

- Review GAO, IIA, ISACA, and NIST publications relevant to IT audits.
- Understand how to apply GAGAS, FISCAM, and Green Book standards to IT auditing.
- Examine the COSO internal control model and its application in government audits.
- Identify key publications and guidelines for federal information systems audit processes.