COURSE SYLLABUS

Information Systems Auditing Course

Master the tools and techniques of information systems auditing with hands-on training in compliance, risk assessment, and fraud detection.

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-systems-auditing

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

Course Outline

Module 1: Performing Information System Controls Audits

- Plan, test, and report IS controls using a risk-based strategy that scopes work to objectives and resources.
- Review audit trail concepts, layers of control, and fundamentals of reliable, available, auditable systems.
- Plan the IS audit: define objectives and scope, understand operations and networks, identify key areas and risks, and document plans.
- Test controls at entity, system, and application levels; evaluate effectiveness; and report results with required documentation.

Module 2: Professional Guidance and Standards

- Survey GAO guidance (e.g., Green Book), NIST publications, and OMB circulars pertinent to IS control assessments.
- Review IIA frameworks (PPF, Practice Guides/GTAG, GAIT) and ISACA standards/objectives.
- Note PCAOB standards and their implications for reporting control deficiencies.

Module 3: Risk Considerations for an IT System

- Define scope and identify potential threat-sources, vulnerabilities, and existing controls.
- Assess likelihood and impact to determine risk levels (confidentiality, integrity, availability).
- Document results and develop control recommendations and audit procedures.

Module 4: Auditing in a Changing Environment

- Examine evolution and complexity of IT (ERP, cloud) and associated control classifications.
- Differentiate preventive, detective/corrective, and directive controls specific to IT.
- Apply audit strategies and CAATs (e.g., test data, parallel simulation) in an IT environment.

Module 5: Assessing the Effectiveness of General Controls

- Use a structured methodology to evaluate entity-wide and system-level general controls.
- Assess security management, access controls, configuration management, segregation of duties, and contingency planning.
- Link general-control effectiveness to reliability of application-level controls.

Module 6: Assessing the Effectiveness of Business Process Application Controls

- Coordinate testing of application-level controls with entity and system general controls.
- Evaluate application security (AS), business process controls (BP), interface controls (IN), and data management system controls (DA).

- Perform audit programs for input, processing, and output controls to ensure completeness, accuracy, validity, confidentiality, and availability.

Module 7: Case Study

- Apply the full IS controls audit lifecycle—planning, testing, evaluation, and reporting—to a practical scenario.
- Integrate risk analysis and control assessment findings to form conclusions and recommendations.