COURSE SYLLABUS

Fraud Auditing and Awareness Certificate Program

Satisfy your CPE requirements with comprehensive training in fraud auditing, detection, and prevention designed for auditors and investigators.

> Group classes in Washington, DC and onsite training is available for this course.
> For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/certificate-of-accomplishment-in-fraud-auditing-and-awareness

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

Course Outline

This package includes these courses

- Contract and Procurement Fraud (12 Hours)
- Detection and Prevention of Fraud (12 Hours)
- Red Flags of Infrastructure Fraud (6 Hours)
- Data Analytics for Fraud Detection (6 Hours)
- Making Your Case to Prosecute Fraud (12 Hours)
- Counterintelligence for Information Security Assessment and Protection (12 Hours)

Contract and Procurement Fraud

Learn to identify and address procurement fraud in government contracts through comprehensive training and practical tools. This course equips auditors with the skills to detect fraud schemes, understand legal frameworks, and implement effective audit strategies.

- Recognize indicators of procurement fraud in contracts and grants.
- Develop audit strategies to identify and quantify fraud.
- Explore traditional fraud schemes like false claims, product substitution, and accounting fraud.
- Understand federal laws and regulations governing the contracting process.
- Learn about remedies for contract fraud, including criminal, civil, and administrative actions.
- Address challenges to auditor independence in fraud investigations.
- Gain insights into fraud issues related to e-commerce and government involvement.

Detection and Prevention of Fraud

Gain a comprehensive understanding of fraud detection and prevention, including legal frameworks, audit responsibilities, and

effective techniques. This course equips participants with the skills to identify fraud indicators, design audit procedures, and collaborate with investigators.

- Define fraud and understand its five elements.
- Explore classic fraud schemes and their indicators.
- Learn auditor responsibilities in fraud prevention and detection.
- Understand criminal statutes and federal rules of evidence for prosecuting fraud.
- Design audit procedures to detect fraud effectively.
- Collaborate with investigators and manage investigative referrals.
- Practice fraud detection methods through case exercises.

Red Flags of Infrastructure Fraud

This one-day workshop focuses on fraud awareness for auditors in infrastructure funding contexts. You will learn to identify control weaknesses, understand project risks, and review prosecuted cases to reinforce detection strategies.

- Understand the basics of IIJA, the agencies, the projects, and the spending.
- Understand Auditors' responsibilities for fraud awareness and detection.
- Assessing the risks, controls, and environment for fraud.
- Be aware of fraud schemes and indicators that are common to federally funded projects.
- Understand the federal civil and criminal statutes that fraud schemes violate.
- Reinforce knowledge of schemes through sampling of prosecuted infrastructure cases.

Data Analytics for Fraud Detection

This one-day intermediate seminar introduces investigators, auditors, and analysts to the principles and tools of data analytics applied to fraud detection. Using real-world cases, you will practice identifying patterns, outliers, and red flags in structured and unstructured data, and learn to visualize findings effectively for investigative reporting.

- Explain the importance of data analytics in support of investigations and fraud detection.
- Identify patterns and outliers quickly to assess possible improper activities.
- Describe the difference between structured and unstructured data.
- Use the Data Analysis Maturity Model to identify or search for specific red flags of fraud.
- Practice on multiple case studies doing analysis with specific forensic data analysis tools.
- List common data analysis tools that can be used in support of investigations.
- Explain various trends in data analysis, data architecture, and data governance and their implications on investigations.

Making Your Case to Prosecute Fraud

Participants gain essential skills for forensic auditing in collaboration with auditors, investigators, and prosecutors. Through case-based learning they explore the legal environment, evidence standards, and task force dynamics necessary to structure decisions and support criminal, civil, or administrative fraud actions.

- Describe and apply the five elements of a prosecutable fraud scheme.
- Be conversant with the criteria used by prosecutors in making litigation decisions.
- Describe the current situation that mandates joint task force efforts in combating fraud, and the participant's role on such a task force.
- Contrast the standards of evidence that apply in auditing from those that apply in prosecuting fraud Differentiate the various ways that a

government agency may obtain evidence for use in administrative, civil and criminal cases.

- Describe the restrictions that a government agency must observe in obtaining evidence for use in prosecuting a criminal fraud case.
- Understand the principles of the forensic audit; and be able to apply them during a class project.
- Be familiar with the basic rules of trial procedure, as well as the role of each participant Understand the task force participant's responsibilities as a potential witness; and be familiar with defense attorn.

Counterintelligence for Information Security Assessment and Protection

This advanced session trains professionals to identify, analyze, and mitigate risks related to foreign intelligence operations within IT and information systems. Topics include threat modeling, protective measures, and coordination with CI stakeholders.

- Define the risks and threats associated with counterintelligence and information security.
- Describe the roles and responsibilities of counterintelligence security personnel, and those charged with assessing and preventing risks associated with information.
- Identify the potential sources of domestic and foreign threats to information security.
- Explain the levels of information classification and required security.
- Recognize indicators and conditions of internal threats as well as methods used for information theft and exploitation.
- Apply counter measures and controls to increase awareness, prevention, detection and mitigation of threats.
- Develop and apply procedures for reacting to, recording and reporting threats, suspicious activity and actual breaches.