COURSE SYLLABUS

Fraud Detection and Prevention for Investigators Certificate Program (Self-Paced)

Prepare to detect and prevent fraud in government programs, grants, and contracts through targeted investigative training aligned with OIG standards.

Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/fraud-detection-and-prevention-for-investigators-certificate-program-self-paced



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

Course Outline

This package includes these courses

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

Attend the AI for Law Enforcement & Public Safety class for free as part of this certificate. Choose your date after you register for the program.

AI for Law Enforcement & Public Safety Course (Self-Paced)

Detection and Prevention of Fraud for Investigators (Self-Paced)

- Define fraud and explain its five elements.
- Describe the classic fraud schemes.
- Cite auditor responsibilities for the prevention and detection of fraud.
- Describe where and how fraud is committed and who commits it.
- Identify indicators/red flags and detection techniques associated with fraud.
- Describe the criminal statutes related to fraud.
- Describe the federal rules of evidence for prosecuting fraud. Identify factors of auditor cooperation with investigators; timing and content of investigative referrals.

Contract and Procurement Fraud for Investigators Course (Self-Paced)

Equip audit and investigative professionals with strategies to identify and document contract and procurement fraud. Training includes real-world case studies and methods to quantify fraud and evaluate evidence while supporting legal and administrative actions.

- Recognize common fraud schemes, such as false claims, product substitution, and misuse of minority-front firms.
- Interpret federal criminal and civil laws that govern procurement fraud responses.
- Analyze red flags and assess indicators to quantify exposure in contract and grant transactions.
- Collaborate effectively with investigators, prosecutors, contracting officials, and whistleblowers.
- Develop audit and investigative plans addressing independence, evidence sourcing, and stakeholder coordination.

Making Your Case to Prosecute Fraud for Investigators Course (Self-Paced)

Learn how to build and present a prosecutable fraud case through evidence gathering, investigation planning, and effective task force collaboration.

- Describe and apply the five elements of a prosecutable fraud scheme.
- Detail 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 investigating with 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.
- Describe the principles of the forensic investigation, and be able to apply them during a class project.
- State the basic rules of trial procedure, as well as the role of each participant.
- Describe the task force participant's responsibilities as a potential witness, and apply techniques to properly address defense attorney tactics.

Red Flags of Infrastructure Fraud for Investigators Course (Self-Paced)

Designed for auditors, investigators, special agents, and grant or contract managers working on IIJA-funded infrastructure projects, this intermediate-level self-paced training highlights how fast-moving funds and weak controls create fraud risks.

- Understand IIJA funding channels, key project types, and participating agencies.
- Recognize common infrastructure fraud schemes and red-flag indicators in federally funded projects.
- Assess environments for risk, control weaknesses, and fraud vulnerability.
- Review relevant federal civil and criminal statutes that apply to fraud violations.
- Reinforce learning with real-world infrastructure fraud case studies and control failure examples.

Data Analytics Tools for Investigations Course (Self-Paced)

This self-paced intermediate-level course equips investigators, auditors, and analysts with hands-on experience using data analytics to uncover fraud. Through real-world case studies and forensic tools, you will learn to spot anomalies, assess risk indicators, and present findings clearly and effectively in investigative contexts.

- Identify patterns, anomalies, and red flags in structured and unstructured data.
- Apply audit-specific analytics software and tools in case studies.
- Use the Data Analysis Maturity Model to assess organizational readiness.

- Practice data visualization and tabular reporting for clear evidence presentation.
- Understand emerging trends in data governance and analysis for investigations.

Counterintelligence for Information Security Assessment and Protection for Investigators Course (Self-Paced)

- Define the risks and threats associated with counterintelligence and information security.
- 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 countermeasures 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