COURSE SYLLABUS

Data Analytics for Fraud Detection for Investigators Course

Develop data analysis skills to detect fraud patterns in grants, contracts, and financial systems using forensic tools and case-based methods.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://sdfm.graduateschool.edu/courses/data-analytics-for-fraud-detection-for-investigators



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

Course Outline

Module 1: Why Data Analytics in Investigations

- Explain why analytics is essential to fraud detection and investigative triage.
- Discuss real-world fraud examples and how data revealed the schemes.
- Frame the seminar's goals, outcomes, and hands-on approach with real data.
- Review the day agenda and expectations for participation.

Module 2: Data vs. Information & Structure

- Differentiate raw data from actionable information and why context matters.
- Compare structured (tables/databases) and unstructured (PDFs, email, images) data.
- Identify tools and effort needed to tag, normalize, and search unstructured sources.
- Practice enriching data to answer investigative questions.

Module 3: Internal & External Data Sources

- Inventory common internal sources (ERP, HR, POS, T&E, financial systems).
- Use public datasets (SAM/UEI, OFAC, CMS provider data, OIG exclusions, BLS, GSA rates).
- Explore state/city open data, SIC codes, and oversight.gov reports.
- Understand deep/surface web research considerations and data quality/privacy risks.

Module 4: Transactional vs. Analytical Systems

- Contrast systems optimized for entry/storage with those built for analysis.
- Join multiple sources (e.g., sales, vendor, HR) to answer cross-cutting questions.
- Introduce data marts/warehouses and denormalized models for analysis.
- Work through data quality issues that arise when combining systems.

Module 5: Governance, Privacy & Compliance

- Define metadata and the role of a data dictionary for consistent definitions.

- Review PII/PHI handling and investigative safeguards.
- Summarize GDPR, CCPA/CPRA, VCDPA obligations and breach/reporting expectations.
- Connect governance to reliable, defensible investigative analytics.

Module 6: Analytics Maturity & Methodology

- Use the Data Analytics Maturity Model to assess current capabilities.
- Plan a discovery-to-improvement pathway with risk, budget, and benefits in mind.
- Survey big data, IoT, and cloud impacts on investigative workflows.
- Outline a repeatable analysis process from scoping to results.

Module 7: Data Visualization Fundamentals

- Explain why visuals accelerate insight and learning.
- Start with high-level dashboards, then drill for anomalies and red flags.
- Evaluate static vs. dynamic visualizations and storytelling best practices.
- See example public-health/census maps and translate lessons to investigations.

Module 8: Tools Landscape

- Compare reporting and visualization platforms (Excel, Power BI, Tableau, InfoZoom).
- Review investigation-oriented tools (ACL/Arbutus/IDEA, TeamMate).
- Introduce statistics/programming tools (SPSS, SAS, R, SQL, Python) for advanced work.
- Note emerging trends: in-memory analytics, cloud services, continuous monitoring.

Module 9: Excel for Investigations

- Use AutoSum, descriptive functions, sorting, and filters for quick cuts.
- Build pivot tables/charts to summarize claims, vendors, offices, and dates.
- Format and troubleshoot formulas; manage large datasets efficiently.
- Create shareable charts that communicate investigative findings.

Module 10: InfoZoom Essentials

- Navigate Table, Compressed, and Overview views to profile data fast.
- Use Attributes, Mark Selection, and Sum to build “pivot-like” analyses.
- Create interactive charts/reports and link/join external sources.
- Practice with sample .fox datasets to answer investigative questions.

Module 11: Core Investigative Exercises

- Initial discovery & stratification to surface outliers and risk areas.
- Duplicates: single/multiple attributes; vendor/employee/address normalization.
- Cardholder/vendor limit testing; identify split transactions.
- MCC-code checks for restricted or personal transactions; Top-10 vendor analyses.

Module 12: Dates, Patterns, Benford & Automation

- Day-of-week and key date comparisons (post vs. transaction; invoice vs. PO).
- Apply Benford’s Law and interpret signals vs. noise in ledgers.
- Design sampling approaches for follow-up testing and fieldwork.
- Automate “yes/no” logic to scale repeatable fraud detection tests.

Module 13: Trends & Advanced Considerations

- Discuss cloud tiers, enterprise services, and security considerations.
- Set realistic KPI targets; build goal-oriented visuals (trendlines, YoY deltas).

- Plan for continuous monitoring with governance and change control.
- Summarize takeaways and additional software/data trends to watch.