JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Fraud Pattern Mining for Audit and Risk Analysts Training Course

10 – 14 January 2027
Cairo

Fraud Pattern Mining for Audit and Risk Analysts Training Course

Ref: 3105_117856 **Date:** 10 – 14 January 2027 **Location:** Cairo **Fees:** 4000 GBP

Fraud Pattern Mining for Audit and Risk Analysts is a 1-week training course for fraud, audit and risk analysts who leave with a fraud detection rule and scoring design. Payment volumes, supplier networks and digital channels now move faster than manual sampling can follow, so hidden schemes surface late and cost more to unwind. Jupiter Prime Training runs this course on fraud pattern mining for audit and risk analysts.

Why Fraud Pattern Mining Matters Now

Three pressures shape the subject. Instant payments and self-service portals shorten the window between a fraudulent act and an irreversible loss. Audit committees and boards ask for testing across whole populations of ledger entries rather than small samples. Investigators are swamped by false alerts and need sharper triage. An organisation that mines its transaction history well finds collusion, duplicate vendors and split purchases early; one that relies on static thresholds chases noise and misses organised rings. The course follows a cycle of profiling normal behaviour, scoring departures, tracing links between parties, tuning rules and ranking cases for review.

Who Gains Most from Fraud Pattern Mining

- Fraud analysts who design and maintain detection rules for payments, claims or accounts
- Internal auditors who test expense, procurement and payroll ledgers in full
- Risk analysts who track loss events and the controls meant to prevent them
- Investigation support staff who assemble evidence trails and relationship charts
- Compliance testers who check screening and approval controls against transaction records

A second-line or third-line assurance unit gains most when its rule designers, auditors and investigators attend together and share one scoring vocabulary.

Fraud Pattern Mining Capabilities

Participants turn raw ledger, payment and claims records into ranked suspicious cases backed by a clear rule and score.

- Build behavioural profiles of customers, employees and vendors — baselines for spotting departures
- Calculate anomaly scores from peer-group and time-based comparisons — alert thresholds
- Apply link analysis to shared addresses, accounts and devices — collusion and ring detection
- Test detection rules against known cases and false alerts — rule retention or retirement
- Design case ranking that weighs exposure and confidence — investigator workload

- Communicate rule logic and limits to audit committees — oversight and challenge

Key Fraud Pattern Mining Terms

- Behavioural profile — the normal range of amounts, timing and counterparties for one customer, employee or vendor.
- Anomaly score — a number showing how far a transaction departs from its profile or peer group.
- Peer group — entities with similar roles or activity used as a comparison base.
- Link analysis — mapping shared attributes between parties to reveal hidden relationships.
- False positive rate — the share of alerts that turn out to be legitimate activity.
- Case prioritisation — ordering alerts for review by likely loss and evidence strength.

Fraud Pattern Mining Day by Day

Day 1: Fraud Schemes and Detection Context

- Fraud Scheme Typology — Mapping Internal, External and Collusive Threats
- Red Flag Catalogue by Process — Linking Symptoms to Ledger Fields
- Full-Population Testing Versus Sampling — Choosing Coverage for Each Process
- Source Record Inventory — Deciding Which Ledgers and Logs to Join
- Detection Objective Statement — Agreeing Loss Types and Tolerance Levels

Day 2: Transaction Profiling

- Entity Resolution and Key Matching — Merging Duplicate Vendors and Customers
- Behavioural Baselines by Entity — Setting Normal Amount and Timing Ranges
- Peer Group Construction — Comparing Like with Like Across Units
- Digit and Round Amount Tests — Flagging Fabricated or Split Values
- Time Pattern Checks — Spotting Weekend, Late and Burst Activity

Day 3: Anomaly Scoring and Link Analysis

- Distance-from-Profile Scores — Ranking Departures from Expected Behaviour
- Outlier Clustering — Isolating Small Groups of Unusual Transactions
- Shared Attribute Graphs — Tracing Common Addresses, Accounts and Devices
- Network Centrality Measures — Identifying Hubs in Suspected Rings
- Combined Risk Score Weighting — Blending Rule Hits with Anomaly Signals

Day 4: Rule Tuning and Case Prioritisation

- Known-Case Back-Testing — Measuring Detection Against Confirmed Frauds
- Threshold Tuning Curves — Trading Missed Frauds Against Alert Volume
- Rule Retirement Log — Removing Rules That Add Noise Only
- Case Ranking Matrix — Ordering Alerts by Exposure and Confidence
- Investigator Feedback Loop — Feeding Case Outcomes Back into Rules

Day 5: Practising the Fraud Detection Rule and Scoring Design

- Procurement and Claims Case Exercise — Applying Profiles and Peer Groups
- Scoring and Link Chart for the Exercise — Reusing Anomaly and Graph Methods
- Tuned Thresholds for the Exercise — Applying Back-Testing Results
- Rule Documentation for Audit Committees — Recording Logic, Limits and Owners
- Fraud Detection Rule and Scoring Design — Completed Design for One Process

Applying Fraud Pattern Mining After the Course

- Run a duplicate vendor and shared bank account test across the full supplier master.
- Back-test one existing detection rule against recent confirmed cases and propose a tuned threshold.

Fraud Pattern Mining Questions FAQ

What is fraud pattern mining for audit and risk analysts, and why does it matter now?

It is the use of profiling, scoring and link methods to find suspicious transactions in full records. It matters now because faster payments and larger ledgers make sample-based checks too slow to stop losses.

Which roles gain most from fraud pattern mining for audit and risk analysts?

Fraud analysts, internal auditors and risk analysts gain most. Investigation support staff and compliance testers also benefit, since they rely on the same rules, scores and relationship charts.

How does fraud pattern mining for audit and risk analysts differ from a forensic accounting course?

It concentrates on detecting patterns across large volumes of records before a case opens. A forensic accounting course focuses on investigating a known case, tracing funds and preparing evidence after suspicion arises.

What do you bring back from fraud pattern mining for audit and risk analysts?

You bring back a completed rule and scoring design for one process in your organisation. It sets out the profiles, anomaly scores, link checks, tuned thresholds and case ranking needed to run it.

Fraud Pattern Mining: The Way Forward

The fraud detection rule and scoring design gives an assurance unit a documented way to find suspicious activity in one process. Its first use usually decides which alerts investigators open each week. Fraud analysts own it, auditors test it and committees challenge it. After a quarter of use, revisit the peer groups, since fraudsters adapt once a rule starts catching them.