JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Financial Intelligence Analysis and Threat Assessment Training Course

20 – 24 December 2026
Cairo

Financial Intelligence Analysis and Threat Assessment Training Course

Ref: 3148_119582 **Date:** 20 – 24 December 2026 **Location:** Cairo **Fees:** 3500 GBP

Financial Intelligence Analysis and Threat Assessment is a 1-week training course for financial intelligence analysts, compliance investigators and fraud analysts who must turn suspicious activity reports, transaction records and open information into a financial threat assessment brief. Criminal networks now move value through layered accounts, digital wallets and trade flows faster than case-by-case review can follow. Jupiter Prime Training shapes this course around analysis that leads to action.

Why Financial Intelligence Analysis and Threat Assessment Matters Now

Three forces shape this discipline today. Reporting volumes keep rising while analyst headcount stays flat, so triage and prioritisation decide what gets examined at all. Payment rails, digital assets and cross-border trade create new layering routes that older detection rules miss. Senior leaders, investigators and external partners also expect intelligence that tells them what to do next, not a pile of alerts. An organisation that reads these signals well disrupts schemes early and directs scarce investigative time to the highest harm; one that reads them poorly files reports nobody acts upon. The course rests on the intelligence cycle, the risk-based approach and structured analytic techniques that test competing explanations.

Who Gains Most from Financial Intelligence Analysis and Threat Assessment

- Analysts deciding which suspicious activity reports become cases
- Investigators tracing funds between accounts and companies
- Fraud specialists handling transaction alerts and repeated schemes
- Compliance staff briefing senior managers on illicit finance exposure
- Monitoring officers tuning detection scenarios from analytical findings

An intelligence unit gains most when analysts and investigators attend together and agree one shared method.

Financial Intelligence Analysis and Threat Assessment Capabilities

Participants move from reading single reports to judging networks, methods and likely future activity.

- Design a collection plan that matches intelligence requirements to data holdings — case prioritisation
- Build link charts and network maps from transaction and ownership records — investigators
- Test competing hypotheses about the purpose of a flow of funds — escalation decisions
- Assess a typology against observed indicators and grade its likelihood — monitoring owners
- Apply source and information grading to every piece of evidence — legal and review teams

- Communicate a threat assessment in a short briefing with clear judgements — senior leaders

Key Financial Intelligence Analysis and Threat Assessment Terms

- Intelligence Requirement — a question decision makers need answered that drives collection.
- Typology — a described pattern of methods criminals use to move or hide funds.
- Link Chart — a diagram showing people, accounts, companies and transactions as connected entities.
- Source Grading — a scale rating the reliability of a source and the credibility of the information it provides.
- Strategic Assessment — a forward-looking product describing threats, trends and vulnerabilities across many cases.
- Estimative Language — agreed words expressing likelihood so readers understand how confident an analytical judgement is.

Financial Intelligence Analysis and Threat Assessment Day by Day

Day 1: The Intelligence Cycle and Illicit Finance Landscape

- Intelligence Cycle Stages — Where Analysis Adds Value to Casework
- Illicit Finance Threat Landscape — Priority Crimes Generating Proceeds
- Tactical, Operational and Strategic Products — Matching Output to Audience
- Intelligence Requirements Register — Setting Questions Decision Makers Need Answered
- Suspicious Activity Report Anatomy — Judging Report Quality and Gaps

Day 2: Collection Planning and Data Sources

- Collection Plan Matrix — Linking Requirements to Internal and External Holdings
- Transaction Data Extraction — Choosing Fields, Periods and Counterparties
- Corporate Registry and Ownership Records — Identifying Beneficial Controllers
- Open Information Searching — Adverse Media and Public Record Leads
- Source and Information Grading — Weighing Reliability Before Use

Day 3: Network and Flow Analysis

- Entity Resolution — Merging Duplicate Names, Accounts and Addresses
- Link Chart Construction — Showing Control, Ownership and Fund Movement
- Flow of Funds Charting — Following Layering Across Accounts and Jurisdictions
- Network Centrality Measures — Finding Brokers, Hubs and Controllers
- Timeline and Event Charting — Sequencing Activity Around Trigger Events

Day 4: Typologies, Hypotheses and Judgements

- Typology Building — Turning Repeated Cases into Detectable Indicator Sets
- Trade-Based Value Transfer Indicators — Spotting Mispriced Goods and Invoices
- Hypothesis Matrix Testing — Weighing Rival Explanations Against Evidence
- Indicator Validation — Feeding Findings Back into Monitoring Scenarios
- Estimative Language Scale — Expressing Confidence and Likelihood Consistently

Day 5: Practising the Financial Threat Assessment Brief

- Case Study Collection Plan — Applying Requirements to a Banking Scenario
- Network Chart Review — Applying Link Analysis to a Trading Company Case
- Hypothesis Challenge Session — Peer Testing of Analytical Judgements
- Decision Maker Briefing — Presenting Findings in Ten Clear Minutes
- Financial Threat Assessment Brief — Completing Judgements, Gaps and Recommendations

Applying Financial Intelligence Analysis and Threat Assessment After the Course

- Rank open cases against an intelligence requirements register to choose which deserve link chart analysis first.
- Convert three recent cases into typology indicator sets with monitoring colleagues and test them against detection scenarios.

Financial Intelligence Analysis and Threat Assessment Questions FAQ

What is financial intelligence analysis and threat assessment, and why does it matter now?

It is the discipline of turning reports, transactions and open information into judgements about who is moving illicit funds, how and what is likely next. Rising report volumes and faster payment routes make prioritised, evidence-based judgements essential for directing scarce investigative effort.

Which roles gain most from financial intelligence analysis and threat assessment skills?

Analysts reviewing suspicious activity reports, investigators tracing funds, fraud specialists handling alerts and compliance staff briefing senior managers gain most.

How does financial intelligence analysis and threat assessment differ from a fraud investigation course?

It focuses on analysis before and around investigation rather than evidence handling and interviews. You learn to plan collection, chart networks, test hypotheses and write graded judgements.

What do you bring back from financial intelligence analysis and threat assessment training?

You bring back a completed threat assessment brief built on a realistic case, with a collection plan, link chart, tested hypotheses and graded judgements. Your unit can reuse it.

Financial Intelligence Analysis and Threat Assessment: The Way Forward

The financial threat assessment brief gives an intelligence unit one consistent product for its priority cases. Its first use is deciding which network to refer for investigation and which indicators to add to monitoring. Investigators, compliance heads and senior managers read it together. After the first cycle, revisit the collection plan to see which sources added most and which gaps still limit judgements.