JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Financial Crime Risk Assessment and Controls Testing Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Financial Crime Risk Assessment and Controls Testing Training Course

Financial Crime Risk Assessment and Controls Testing is a 2-week advanced training course for financial crime and compliance officers, who build an enterprise financial crime risk assessment and controls testing plan. Fraud schemes, sanctions evasion and bribery routes now move faster than annual reviews, so boards want inherent exposure scored by typology and every key control tested on evidence. Jupiter Prime Training delivers this Financial Crime Risk Assessment and Controls Testing course.

Why Financial Crime Risk Assessment and Controls Testing Matters Now

Three forces shape this work: faster payment rails and digital onboarding that shorten the window for detection, sanctions lists that change with little notice, and supervisors and auditors who expect a documented, risk-based rationale for every control. Firms that score typologies and test controls against them direct investigation capacity where losses and penalties would fall; firms that rely on policy attestations discover gaps only after an incident. The course draws on Basel Committee on Banking Supervision BCBS guidance on operational and money laundering risk, ISO 31000 risk management guidelines, ISO 37301 compliance management systems and the IIA Three Lines Model.

Who Gains Most from Financial Crime Risk Assessment and Controls Testing

- Officers who own the enterprise-wide money laundering and fraud risk assessment
- Specialists who tune sanctions screening and transaction monitoring scenarios
- Anti-bribery leads who approve third parties, gifts and hospitality
- Second-line testers who design and run compliance monitoring reviews
- Investigation heads who turn case lessons into control changes

Financial crime units that send their risk assessment owner together with their testing lead gain most, because both sides of the assessment-to-testing link are present.

Financial Crime Risk Assessment and Controls Testing Capabilities

Participants connect typologies, inherent exposure and control evidence into one scored and testable view of financial crime.

- Assess inherent financial crime exposure by customer, product, channel and geography — the money laundering reporting officer
- Design control effectiveness ratings for fraud, bribery and sanctions controls — the risk committee
- Calculate residual exposure and compare it with stated appetite — the board
- Build test scripts with sampling rules and evidence standards — internal audit
- Test sanctions screening and monitoring scenarios for tuning gaps — the head of operations
-

Communicate testing findings with remediation owners and deadlines — senior management

Key Financial Crime Risk Assessment and Controls Testing Terms

- Typology — A described pattern of how a financial crime is committed, used to link exposure to specific detective and preventive controls.
- Inherent exposure — The level of financial crime risk before controls, driven by customers, products, channels and jurisdictions served.
- Control effectiveness rating — A graded judgement of how well a control is designed and operates, based on tested evidence.
- Residual exposure — The risk remaining after controls are applied, compared with appetite to decide whether action is needed.
- Sanctions screening — Checking customers, counterparties and payments against restricted-party lists before and during the relationship.
- Market abuse surveillance — Monitoring orders and trades for insider dealing and manipulation patterns that require escalation and reporting.

Financial Crime Risk Assessment and Controls Testing Day by Day

Day 1: The Financial Crime Exposure Landscape

- Typology Library — Fraud, Bribery, Sanctions, Tax and Market Abuse Patterns
- Risk-Based Approach Principles — Allocating Effort to Higher Exposure
- BCBS Guidance on Money Laundering Risk — Expectations for Banks
- IIA Three Lines Model — Roles in Assessment and Testing
- Exposure Drivers Map — Customers, Products, Channels and Jurisdictions

Day 2: Building the Enterprise Risk Assessment

- Inherent Exposure Scoring Model — Weighting Drivers by Typology
- Data Sourcing for Risk Factors — Customer and Transaction Volumes
- ISO 31000 Risk Criteria — Setting Likelihood and Impact Scales
- Business Line Self-Assessment Questionnaires — Consistent Inputs Across Units
- Appetite Statement for Financial Crime — Thresholds for Residual Ratings

Day 3: Fraud Risk and Controls

- Internal and External Fraud Scenarios — Payment, Procurement and Payroll Cases
- Fraud Red Flag Analytics — Rules That Trigger Investigation
- Segregation of Duties Matrix — Preventing Single-Person Payment Release
- Account Takeover Controls — Authentication and Behavioural Monitoring
- Fraud Loss Event Data — Feeding Results Back into Scoring

Day 4: Bribery and Corruption Controls

- Bribery Exposure Assessment — Intermediaries, Licences and Public Officials
- Third-Party Due Diligence Tiers — Depth Matched to Exposure
- Gifts, Hospitality and Donations Register — Approval and Review Rules
- ISO 37301 Compliance Controls — Linking Policy to Operating Evidence
- Payment Approval Red Flags — Unusual Commissions and Consultancy Fees

Day 5: Sanctions Screening Effectiveness

- List Management Process — Timely Updates and Version Control
- Fuzzy Matching Thresholds — Balancing Alerts Against Missed Matches
- Payment Message Screening — Fields, Formats and Stripping Risks
- Ownership and Control Analysis — Identifying Indirectly Sanctioned Entities
- Alert Disposition Quality Review — Consistency of Clearing Decisions

Day 6: Tax Evasion Facilitation and Market Abuse

- Tax Evasion Facilitation Scenarios — Staff and Associated Persons
- Reasonable Prevention Procedures — Assessing Tax Facilitation Controls
- Market Abuse Surveillance Scenarios — Insider Dealing and Manipulation Patterns
- Information Barriers and Insider Lists — Managing Price-Sensitive Information
- Suspicious Order Escalation — Reporting Paths and Documentation

Day 7: Rating Control Effectiveness

- Control Inventory by Typology — Preventive, Detective and Corrective Mapping
- Design Effectiveness Criteria — Coverage, Timing and Ownership
- Operating Effectiveness Evidence — What Proves a Control Ran
- Residual Exposure Calculation — Combining Inherent Scores and Control Ratings
- COSO ERM Alignment — Presenting Residual Exposure Against Appetite

Day 8: Designing the Testing Approach

- Risk-Based Testing Calendar — Frequency Driven by Residual Ratings
- Test Script Templates — Objective, Population, Steps and Evidence
- Sampling Methods — Statistical and Judgemental Sample Selection
- Scenario Tuning Tests for Transaction Monitoring — Below-Threshold Analysis
- Data Integrity Checks — Confirming Feeds Reach Screening and Monitoring Systems

Day 9: Findings, Remediation and Reporting

- Finding Severity Scale — Linking Gaps to Exposure and Appetite
- Root Cause Analysis — Distinguishing Design, Execution and Data Failures
- Remediation Tracker — Owners, Deadlines and Validation Retests
- Committee Reporting Pack — Trends Across Typologies and Business Lines
- Sector Case Studies — Retail Banks and Commodity Traders

Day 10: Practising the Controls Testing Plan

- Inherent Scoring Applied to a Case Firm — Peer Calibration
- Control Ratings and Residual Exposure for the Case — Appetite Check
- Test Scripts for Sanctions and Fraud Controls — Evidence Walkthrough
- Board Summary of Testing Priorities — Challenge Session
- Financial Crime Risk Assessment and Controls Testing Plan — Final Version

Applying Financial Crime Risk Assessment and Controls Testing After the Course

- Rescore inherent exposure for one business line using the typology-based model and present residual ratings to the risk committee
- Run one sanctions screening or fraud control test with the new script template and log findings in the remediation tracker

Financial Crime Risk Assessment and Controls Testing Questions FAQ

What is Financial Crime Risk Assessment and Controls Testing, and why does it matter now?

It is the practice of scoring exposure to fraud, bribery, sanctions breaches, tax evasion facilitation and market abuse, then testing the controls that reduce it. It matters now because faster payments and changing sanctions lists leave less time to catch failures.

Which roles gain most from Financial Crime Risk Assessment and Controls Testing skills?

Financial crime and compliance officers who own the enterprise risk assessment gain most, alongside second-line testers, sanctions specialists and anti-bribery leads. Investigation heads also benefit when they turn case lessons into control changes.

How does the Financial Crime Risk Assessment and Controls Testing course differ from an introductory anti-money laundering course?

It works at an advanced level across several crime types and focuses on scoring and testing. An introductory anti-money laundering course explains customer due diligence and reporting duties; this one builds scoring models, control ratings and test scripts.

What do you bring back from the Financial Crime Risk Assessment and Controls Testing course?

You bring back a scored assessment of inherent and residual exposure by typology, control effectiveness ratings, test scripts and a risk-based testing calendar, ready to present to your risk committee.

Financial Crime Risk Assessment and Controls Testing: The Way Forward

The financial crime risk assessment and controls testing plan first informs which controls are tested this cycle and how deeply. Compliance officers use it to set priorities, testers to schedule reviews and committees to track remediation. After the first full testing cycle, revisit the inherent scoring weights against actual incidents and alerts to confirm they still reflect real exposure.