JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Bank Incident Reporting and Investigation Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Bank Incident Reporting and Investigation Course

Advanced Bank Incident Reporting and Investigation is a 2-week training course for operational risk officers, compliance investigators and internal auditors in banks who must capture, examine and explain loss events, and each participant leaves with a drafted Incident Investigation Report. Payment fraud, system outages and failed manual processes now surface faster and cost more, while supervisors and boards expect timely, evidenced accounts of what happened. Jupiter Prime Training offers this course to financial institution control specialists.

Why Bank Incident Reporting and Investigation Matters Now

Three pressures sharpen bank incident reporting and investigation. Digital channels and instant payments let fraud and outages spread across thousands of customers within minutes. Supervisors and boards expect prompt notification, consistent loss data and proof that root causes, not symptoms, were fixed. Capital and insurance decisions increasingly rely on internal loss histories, so poor capture distorts risk measurement. A bank that investigates well closes control gaps, recovers funds and protects trust; one that does not sees the same failure recur and faces criticism for incomplete reporting. The course rests on standard operational risk event categories, root cause analysis methods and chain-of-custody evidence practice.

Who Gains Most from Bank Incident Reporting and Investigation

- Specialists who record operational loss events, near misses and recoveries in the loss database
- Investigators who examine fraud, misconduct and sanctions breaches across branches and digital channels
- Auditors who test whether incident remediation actually closed the control weakness
- Officers who coordinate technology outage post-mortems with IT and business continuity teams
- Analysts who prepare incident dashboards and narratives for risk committees

A second line risk function gains most when its operational risk, compliance and internal audit specialists attend together, because a single incident usually needs all three perspectives to be classified, investigated and closed.

Bank Incident Reporting and Investigation Capabilities

These outcomes follow an incident from the first alert to the closing entry in the loss database and the board paper that explains it.

- Apply an incident taxonomy that separates event type, cause and impact — the operational risk committee
- Specify escalation thresholds and notification timelines for material events — senior management and supervisors
- Build an investigation plan with interviews, document requests and data extracts — legal counsel and compliance
- Test root causes using structured techniques such as the five whys and fishbone diagrams — process owners
- Calculate gross loss, recoveries and net loss for consistent loss data entries — capital and insurance teams
- Communicate findings and remediation actions in board-ready language — the board risk committee

Key Bank Incident Reporting and Investigation Terms

- Operational loss event — an incident from inadequate processes, people, systems or external events that causes, or could cause, financial loss to the bank.
- Near miss — an incident that could have caused loss but was stopped in time, recorded to reveal weak controls.
- Root cause analysis — a structured search for the underlying failure that allowed an incident, beyond its immediate trigger.
- Chain of custody — the documented record of who collected, held and transferred evidence, preserving its integrity for later use.
- Boundary event — a loss that sits between operational and credit or market risk, requiring clear classification rules.
- Remediation action — a dated, owned control change agreed to stop an incident's root cause from recurring.

Bank Incident Reporting and Investigation Day by Day

Day 1: The Incident Landscape in Banking

- Operational Risk Event Categories — Fraud, Execution, Systems and External Events
- Three Lines Model Roles — Who Reports, Investigates and Assures
- Supervisory Expectations — Timely Notification and Evidenced Closure
- Incident Trend Signals — Instant Payments and Digital Channel Exposure
- Loss Culture Diagnostic — Barriers to Honest Incident Reporting

Day 2: Incident Capture and Taxonomy

- Incident Intake Forms — Minimum Data at First Notification
- Event Type, Cause and Impact Coding — Consistent Classification Rules
- Near Miss and Boundary Event Rules — What Enters the Loss Database
- Materiality Thresholds — Capture Limits Versus Data Completeness
- Data Quality Checks — Duplicates, Late Entries and Grouped Losses

Day 3: Escalation and Notification

- Severity Matrices — Financial, Customer and Reputational Impact Scales
- Escalation Routes — Business, Risk, Compliance and Executive Paths
- Notification Timelines — Internal Deadlines and External Reporting Duties
- Crisis Linkage — When an Incident Triggers Business Continuity
- Communication Holding Statements — Customers, Staff and Media

Day 4: Planning an Investigation

- Investigation Terms of Reference — Scope, Independence and Authority
- Hypothesis Mapping — What Could Explain the Event
- Data Extract Requests — Transaction Logs, Access Records and Emails
- Investigation Team Selection — Conflicts and Required Expertise
- Legal Privilege Considerations — Protecting Sensitive Working Papers

Day 5: Evidence Handling and Interviews

- Chain of Custody Procedures — Preserving Digital and Paper Evidence
- Forensic Imaging Basics — Working With IT Security Specialists
- Investigative Interview Techniques — Open Questions and Rapport
- Witness Statement Drafting — Accuracy and Signed Records
- Whistleblower Protection — Confidential Sources and Retaliation Risk

Day 6: Root Cause Analysis Methods

- Five Whys Technique — Moving Beyond the Immediate Trigger
- Fishbone Diagrams — People, Process, System and External Causes
- Timeline Reconstruction — Sequencing Events and Control Points
- Barrier Analysis — Which Controls Failed or Were Bypassed
- Control Design Versus Operating Failure — Choosing the Right Fix

Day 7: Fraud and Misconduct Incidents

- Internal Fraud Red Flags — Override, Collusion and Concealment
- Payment Fraud Patterns — Account Takeover and Authorised Push Scams
- Card and Digital Channel Fraud — Mule Accounts and Velocity Signals
- Fund Tracing and Recovery Steps — Recall Requests and Freezes
- Disciplinary Interface — Coordinating With Human Resources and Legal

Day 8: Technology Outages and Process Failures

- Outage Post-Mortems — Blameless Review of System Incidents
- Change Management Failures — Faulty Releases and Rollback Gaps
- Third-Party Incidents — Outsourced Provider and Cloud Failures
- Manual Process Errors — Payment Duplication and Settlement Breaks
- Customer Impact Quantification — Redress, Fees and Compensation

Day 9: Loss Data and Board Reporting

- Gross, Recovery and Net Loss Calculation — Consistent Loss Entries
- Loss Data Reconciliation — Matching the General Ledger
- Key Risk Indicator Links — Incidents That Signal Rising Risk
- Board Incident Dashboards — Trends, Themes and Overdue Actions
- Remediation Tracking — Owners, Deadlines and Validation Testing

Day 10: Practising the Incident Investigation Report

- Fraud Case Walk-Through — Applying Evidence Rules to a Retail Bank Scam
- Outage Case Walk-Through — Applying Root Cause Methods to a Payments Failure
- Loss Entry Exercise — Applying Classification to Both Cases
- Committee Briefing Rehearsal — Presenting Findings Under Challenge
- Incident Investigation Report — Facts, Root Causes, Loss Data and Remediation

Applying Bank Incident Reporting and Investigation After the Course

- Re-code the last quarter's incidents using the event type, cause and impact taxonomy and report data quality gaps to the operational risk committee.
- Run a root cause review on one recurring incident using fishbone and barrier analysis, and agree dated remediation actions with the process owner.

Bank Incident Reporting and Investigation Questions FAQ

What is advanced bank incident reporting and investigation and why does it matter now?

Advanced bank incident reporting and investigation is the discipline of capturing, escalating, examining and explaining operational loss events in financial institutions. It matters now because fraud and outages spread faster through digital channels, and boards expect evidenced root causes.

Which roles gain most from advanced bank incident reporting and investigation training?

Operational risk officers, compliance investigators and internal auditors in banks gain most. Risk officers improve loss capture, investigators strengthen evidence handling and interviews, and auditors gain methods to verify that remediation truly closed control gaps.

How does advanced bank incident reporting and investigation differ from a workplace accident investigation course?

Advanced bank incident reporting and investigation addresses financial and operational loss events, not physical safety accidents. It covers fraud, technology outages, process errors, loss data and board reporting inside banks, whereas safety courses focus on injuries and site hazards.

What do you bring back from advanced bank incident reporting and investigation training?

You bring back a drafted investigation report structure covering facts, root causes, loss data and remediation. You also return with taxonomy rules, escalation matrices, evidence checklists and interview templates your control function can use immediately.

Bank Incident Reporting and Investigation: The Way Forward

The Incident Investigation Report records facts, root causes, loss data and dated remediation for one event. Its first use is the next material incident, where the operational risk lead and process owner agree which controls must change. Revisit its taxonomy and escalation thresholds after a quarter of use, when loss data trends show whether events are being captured consistently.