JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Digital Supervision and Automated Compliance Reporting Training Course

3 – 7 October 2027
Kuala Lumpur

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Digital Supervision and Automated Compliance Reporting Training Course

Ref: 3222_122567 **Date:** 3 – 7 October 2027 **Location:** Kuala Lumpur **Fees:** 4600 GBP

Digital Supervision and Automated Compliance Reporting is a 1-week training course for compliance technology leads, supervisory staff at regulators and risk staff in financial institutions, who leave with a reporting automation roadmap. Supervisors now expect granular, frequent and consistent submissions, while firms face rising rule volumes and pressure on compliance costs. Jupiter Prime Training offers this course on digital supervision and automated compliance reporting for both sides of the supervisory relationship.

Why Digital Supervision and Automated Compliance Reporting Matters Now

Three forces are reshaping supervision. Regulators are moving from periodic template returns towards granular data collection and near-continuous monitoring. Firms are replacing spreadsheet-based reporting chains with automated pipelines that pull figures straight from source ledgers. Boards ask who answers for a rule once it becomes code. Handled well, this means fewer resubmissions and earlier detection of exposures; handled badly, it multiplies reconciliation breaks and hidden manual workarounds. The course rests on widely used principles of risk data aggregation, data lineage and model oversight, described in general terms.

Who Gains Most from Digital Supervision and Automated Compliance Reporting

- Staff who design and run regulatory reporting chains inside banks, insurers and investment firms
- Supervisory analysts who collect returns, check data quality and flag institutions for closer review
- Compliance technology owners who select, configure and maintain monitoring and screening rules
- Risk officers who rely on automated limits, alerts and dashboards for their oversight
- Internal control and assurance staff who test whether coded rules still match the written obligation

Mixed groups from a supervisor's data unit and the reporting function of a regulated firm gain most, because each sees how the other reads a submission.

Digital Supervision and Automated Compliance Reporting Capabilities

Participants move from rule text to data flows and supervisory judgement.

- Map a reporting obligation into data points, validation checks and owners — the scoping decision for any automation effort
- Assess the lineage of a reported figure from source system to submission — the reconciliation question supervisors raise first
- Specify a machine-readable version of a rule with clear test cases — the hand-off between legal interpretation and engineering
- Design supervisory analytics that rank institutions by emerging risk signals — the allocation of scarce inspection time
- Weigh build, buy and shared-utility options for reporting technology — the investment case put to senior management
- Build oversight controls for automated compliance logic — the accountability expected by boards and auditors

Key Digital Supervision and Automated Compliance Reporting Terms

- Granular data collection — supervisors receiving transaction or contract-level records instead of pre-aggregated template totals.
- Machine-readable rule — a regulatory requirement expressed in structured logic that software can execute and test.
- Data lineage — the documented path a figure follows from its source system through every transformation to the submission.
- Validation rule — an automated check that rejects or flags a submitted value failing a defined consistency or plausibility test.
- Supervisory analytics — statistical and pattern-detection techniques supervisors apply to submitted data to prioritise follow-up.
- Rule drift — the gap that opens when coded logic is not updated after the written obligation or its interpretation changes.

Digital Supervision and Automated Compliance Reporting Day by Day

Day 1: The Changing Supervisory Data Relationship

- Template Returns Versus Granular Collection — What Changes for Both Sides
- Supervisory Data Strategies — How Regulators Decide What to Collect
- Reporting Cost Drivers — Where Manual Effort Accumulates in Firms
- Stakeholder Map of the Reporting Chain — Who Owns Each Figure
- Resubmission and Error Patterns — Signals of Weak Reporting Controls

Day 2: From Rule Text to Executable Logic

- Obligation Decomposition — Turning Paragraphs Into Data Points and Conditions
- Machine-Readable Rule Specification — Bridging Legal and Engineering Interpretation
- Test Case Libraries — Proving Coded Rules Match Intended Meaning
- Rule Change Management — Keeping Logic Current After Amendments
- Interpretation Logs — Recording Judgement Calls Behind Each Coded Rule

Day 3: Reporting Pipelines and Data Lineage

- Source-to-Submission Architecture — Locating Transformations and Manual Touchpoints
- Lineage Documentation — Answering Supervisor Reconciliation Questions Quickly
- Validation Rule Design — Catching Errors Before Submission Leaves the Firm
- Reference Data Control — Consistent Identifiers Across Entities and Products
- Build, Buy or Shared Utility — Weighing Reporting Technology Options

Day 4: Supervisory Analytics and Risk Detection

- Peer Comparison Screens — Spotting Outliers Across Reporting Institutions
- Early Warning Indicators — Ranking Firms for Closer Supervisory Attention
- Text Analysis of Filings and Disclosures — Surfacing Hidden Concerns
- Transaction Monitoring Alerts — Tuning Thresholds to Reduce False Positives
- Explainability of Analytical Findings — Defending Conclusions to Supervised Firms

Day 5: Practising Oversight of Automated Compliance

- Accountability Model for Coded Rules — Owners, Reviewers and Escalation Paths
- Rule Drift Testing — Applying Day 2 Test Libraries Periodically
- Lineage and Validation Evidence Pack — Applying Day 3 Controls for Assurance
- Analytics Governance Review — Applying Day 4 Explainability to Model Changes
- Reporting Automation Roadmap — Sequencing Obligations, Controls and Investment

Applying Digital Supervision and Automated Compliance Reporting After the Course

- Lead a lineage walk-through for one high-risk reported figure, documenting each transformation and manual adjustment
- Run a rule drift test on three coded monitoring or reporting rules against the current written obligation

Digital Supervision and Automated Compliance Reporting Questions FAQ

What is digital supervision and automated compliance reporting, and why does it matter now?

It is the use of structured data, coded rules and analytics by supervisors and regulated firms to collect, check and act on regulatory information. It matters now because supervisors want granular data that manual chains cannot deliver.

Which roles gain most from digital supervision and automated compliance reporting?

Reporting chain owners, supervisory data analysts, compliance technology owners, risk officers and assurance staff gain most. Each must explain automated logic to someone else.

How does a digital supervision and automated compliance reporting course differ from a vendor selection course?

It covers the whole supervisory data relationship rather than choosing tools. A selection course compares products; this one teaches rule specification, lineage, supervisory analytics and the oversight of coded compliance logic from both sides.

What do you bring back from digital supervision and automated compliance reporting training?

You bring back a reporting automation roadmap. It sequences which obligations to automate first, the controls they need and who owns each decision.

Digital Supervision and Automated Compliance Reporting: The Way Forward

The reporting automation roadmap first informs which obligation moves from a manual chain to an automated pipeline. Reporting owners and compliance technology leads use it to agree scope. After its first use, revisit the accountability model for coded rules, since ownership gaps surface once automated logic starts failing quietly.