JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Aviation Information Systems Audit Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Aviation Information Systems Audit Training Course

Aviation Information Systems Audit is a 2-week training course for IT auditors, internal auditors and information security leads at airlines and airports, who leave with an aviation information systems audit plan with findings and control recommendations. Departure control, reservation, maintenance and flight operations systems now carry safety, revenue and passenger data in real time, so a weak control can ground flights or expose millions of records. The course is delivered by Jupiter Prime Training.

Why Aviation Information Systems Audit Matters Now

Three forces reshape the audit of aviation systems. Airlines and airports have moved core platforms to cloud services and shared community systems, so control ownership now spans vendors, alliance partners and ground handlers. System outages and cyber incidents at check-in, baggage and crew scheduling have shown audit committees how quickly an IT failure becomes an operational crisis. Aviation authorities and data-protection rules expect evidence that operational and personal data are protected and recoverable. An audit function that reads these systems well protects schedules, safety records and passenger trust; one that tests only generic controls misses the risks that matter. The course rests on the IT general controls ITGC model and risk-based audit planning.

Who Gains Most from Aviation Information Systems Audit

- IT audit leads who plan and execute reviews of operational aviation platforms
- Internal audit leads who report system risks to audit committees
- Information security leads who own access, logging and resilience controls
- Application owners responsible for departure control, reservation or maintenance systems
- Risk and quality leads who track remediation of control findings

An airline or airport gains most when its internal audit, information security and application owners attend together and agree how system findings are rated and closed.

Aviation Information Systems Audit Capabilities

Participants practise turning knowledge of how aviation platforms run into audit tests that reveal real operational and data exposure.

- Assess the risk profile of departure control, reservation, maintenance and flight operations systems — annual audit plan and audit committee
- Design test steps for access, change and operations controls — IT audit fieldwork leads
- Test interfaces and data flows between airline, airport and partner systems — application owners and vendors
- Weigh audit evidence for sufficiency and reliability — audit quality reviewers
- Calculate the operational impact of a control gap on flights and passengers — executive sponsors of remediation
- Communicate findings with ratings, root causes and control recommendations — management and board audit committee

Key Aviation Information Systems Audit Terms

- Departure control system DCS — the airline platform that manages check-in, boarding, seat allocation and load data for each flight.
- Passenger service system PSS — the set of reservation, inventory and ticketing applications an airline uses to sell and manage bookings.
- IT general controls ITGC — controls over access, change, operations and backup that support the reliability of every application.
- Segregation of duties — a control that splits incompatible tasks between people so no one can both make and approve a change.
- Audit evidence — the records, logs, observations and re-performance results that support an auditor's conclusion on a control.
- Control finding — a documented weakness with its condition, criteria, cause, effect and recommended remedy.

Aviation Information Systems Audit Day by Day

Day 1: The Aviation Systems Landscape

- Airline and Airport Application Map — Where Critical Data Lives
- Community Systems and Vendor Platforms — Shared Control Ownership
- Operational Technology at Airports — Baggage, Gates and Building Systems
- Regulatory and Data-Protection Expectations — Evidence Auditors Must Obtain
- Audit Universe Definition — Entities and Systems in Scope

Day 2: Risk-Based Audit Planning

- System Criticality Rating — Safety, Revenue and Passenger Impact
- Risk and Control Matrix Design — Linking Threats to Tests
- Annual IT Audit Plan Construction — Coverage Versus Resources
- Audit Scoping Memos — Boundaries With Vendors and Partners
- Stakeholder Interviews — Application Owners and Security Leads

Day 3: IT General Controls

- Logical Access Reviews — Joiners, Movers and Leavers
- Privileged Account Monitoring — Administrator and Vendor Access
- Change Management Testing — Emergency Fixes During Operations
- Backup and Restore Evidence — Recovery of Flight-Critical Data
- Job Scheduling and Batch Controls — Overnight Interfaces and Reconciliations

Day 4: Passenger and Departure Control Systems

- Reservation and Ticketing Controls — Fare Integrity and Revenue Leakage
- Departure Control Access Profiles — Agent, Supervisor and Handler Rights
- Boarding and Load Data Accuracy — Weight Figures Passed to Flights
- Passenger Data Protection — Personal Records and Retention Rules
- Advance Passenger Information Interfaces — Data Quality to Border Systems

Day 5: Maintenance and Flight Operations Systems

- Maintenance Information System Records — Airworthiness Data Integrity
- Electronic Technical Log Controls — Defect Entries and Sign-Offs
- Crew Scheduling System Rules — Duty Limits and Roster Changes
- Flight Planning and Electronic Flight Bag — Data Updates and Version Control
- Engineering Parts Traceability — Component History and Approval Records

Day 6: Airport Operational Systems

- Airport Operational Database Controls — Flight Information Accuracy
- Baggage Handling System Logs — Sortation Errors and Mishandling
- Common-Use Passenger Processing Platforms — Shared Workstation Security
- Access Control and CCTV Systems — Physical Security Data Integrity
- Resource Management Systems — Stand and Gate Allocation Audit Trails

Day 7: Security, Resilience and Third Parties

- Security Logging and Monitoring Tests — Detection of Misuse
- Vulnerability Management Evidence — Patch Timelines for Critical Systems
- Business Continuity and Disaster Recovery Testing — Outage Readiness
- Cloud and Vendor Assurance Reports — Reliance on Service Organisation Controls
- Contract Right-to-Audit Clauses — Access to Supplier Evidence

Day 8: Audit Evidence and Data Analytics

- Evidence Sufficiency Criteria — Inspection, Observation and Re-Performance
- Sampling Methods for System Controls — Attribute and Judgemental Samples
- Computer-Assisted Audit Techniques — Full-Population Testing of Logs
- Segregation of Duties Analysis — Conflicting Access Combinations
- Working Paper Standards — Traceable Conclusions for Reviewers

Day 9: Findings, Reporting and Follow-Up

- Finding Structure — Condition, Criteria, Cause, Effect and Remedy
- Risk Rating Scales — Operational, Safety and Data Impact
- Audit Committee Reporting — Board-Level Summaries of System Risk
- Management Action Plans — Owners, Dates and Acceptance of Risk
- Remediation Validation — Closing Findings With Fresh Evidence

Day 10: Practising the Aviation Information Systems Audit Plan

- Departure Control Audit Case — Applying ITGC and Access Tests
- Maintenance Records Audit Case — Applying Data Integrity Tests
- Log Analytics Exercise — Applying Computer-Assisted Audit Techniques
- Finding Write-Up Clinic — Applying Rating and Reporting Standards
- Aviation Information Systems Audit Plan — Scope, Tests and Recommendations

Applying Aviation Information Systems Audit After the Course

- Rate the criticality of the organisation's operational systems and propose a revised audit universe to the head of internal audit.
- Run a privileged access review on one flight-critical system and report the results using the finding structure taught.

Aviation Information Systems Audit Questions FAQ

What is aviation information systems audit, and why does it matter now?

Aviation information systems audit is the independent testing of controls over airline and airport platforms such as departure control, reservation and maintenance systems. It matters now because cloud migration, outages and cyber incidents have made these systems a direct operational and regulatory risk.

Which roles gain most from aviation information systems audit training?

IT auditors and internal audit leads gain most, followed by information security leads and application owners. If you plan audits, own system controls or respond to findings, you gain a shared method for testing and rating aviation-specific risks.

How does aviation information systems audit training differ from a general IT audit course?

It applies audit methods to the systems that run flights and airports. A general IT audit course teaches controls in the abstract; this course tests departure control, maintenance, crew scheduling and airport operational platforms with their real interfaces and failure points.

What do you bring back from aviation information systems audit training?

You bring back a scoped audit plan with a risk and control matrix, test steps, sample findings and control recommendations. It gives your audit function a ready reference for the next review of flight-critical systems.

Aviation Information Systems Audit: The Way Forward

The aviation information systems audit plan first informs which operational systems enter next year's audit cycle and in what order. Heads of internal audit, IT audit leads and information security owners use it to agree coverage and remediation priorities. After the first audit under the plan, revisit the criticality ratings and test steps to reflect what the evidence revealed.