Aviation IT Audit Training Course: Airline and Airport Platforms, Risk and Evidence

23 – 27 May 2027
Zoom

Aviation IT Audit Training Course: Airline and Airport Platforms, Risk and Evidence

Ref: 937_42336 **Date:** 23 – 27 May 2027 **Location:** Zoom **Fees:** 1700 GBP

Programme Summary

Aviation IT audit is the subject of this one-week training course for audit, risk and compliance leaders in airlines and airports, taught at managerial level and ending in an audit report for one operator. Reservations, flight operations, maintenance records and ground systems now depend on connected technology, yet many audit teams lack a method fitted to it. The programme moves from scope and criteria to risk ranking, control testing, third-party review and reporting, using prepared records from an airline and an airport. Mars Training Centre UK delivers this programme on aviation IT audit to mixed-organisation cohorts.

The Business Case

Operators that audit their technology against clear criteria find weak access rights, untested recovery plans and unmanaged suppliers before they disrupt flights or expose passenger data. Where audit coverage of aviation systems is thin, boards receive assurance that rests on assumption rather than tested evidence, and suppliers with privileged access escape review. The programme works on the measures below.

- Repeat Control Failures: Fall when findings are rated, owned and followed up.
- Operational Disruption Exposure: Reduces when recovery and change controls are tested on critical systems.
- Audit Coverage of Critical Systems: Rises when the audit plan follows a ranked risk view.

Principles and Evidence Base

- ISO/IEC 27001 and ISO/IEC 27002: International standards for information security management and its control catalogue, applied in Sessions 1 and 3 as criteria for testing.
- COBIT and ISACA ITAF: Frameworks for IT governance and for the practice of IT audit, applied in Session 3 to design tests and rate evidence.
- NIST Cybersecurity Framework: A structure for identifying gaps in security capability, applied in Session 2 to rank exposure.
- ICAO Annex 17: The international standards on aviation security, applied in Session 1 to set sector obligations for the audit scope.

Intended Participants

- Heads of IT audit who plan and supervise technology reviews.
- Internal audit managers who answer to an audit committee for assurance coverage.
- Risk and compliance leaders who own technology controls in an operator.
- Inspectors who review the information systems of aviation operators.

Typical settings include airlines, airports, ground handling companies and aviation oversight bodies.

Learning Outcomes

1. Participants will be able to construct an audit scope for the systems of an airline or airport.
2. Participants will be able to prioritise audit areas by technology risk to flight and ground operations.
3. Participants will be able to design control tests against recognised standards.
4. Participants will be able to evaluate the reliability of audit evidence.
5. Participants will be able to diagnose weaknesses in supplier, cloud and recovery arrangements.
6. Participants will be able to justify audit findings and ratings to management and an audit committee.

Programme Structure

Day 1: Aviation IT Audit Scope and Criteria

Which aviation systems carry the greatest exposure, and which standards set the criteria?

- Aviation Systems Inventory Map
- ISO/IEC 27001 Control Mapping
- ISO/IEC 27002 Control Catalogue Review
- ICAO Annex 17 Obligations Matrix
- Audit Universe and Scoping Sheet

Day 2: Risk Ranking for Airline and Airport Platforms

How is technology risk to flight and ground operations quantified and ranked?

- Reservations and Departure Control Risk Profile
- Maintenance Records Integrity Assessment
- Operational Technology Exposure Review
- NIST Cybersecurity Framework Gap Profile
- Risk-Based Audit Plan

Day 3: Control Testing and Audit Evidence

How are controls tested, and how is the evidence made reliable?

- COBIT Control Objective Testing
- Privileged Access Sampling
- Change and Release Walkthrough
- ISACA ITAF Evidence Rating
- Working Paper Review Checklist

Day 4: Third Parties, Recovery and Findings

How are outsourced systems and recovery arrangements audited, and findings written?

- Cloud and Supplier Assurance Review
- Backup and Recovery Test Observation
- Incident Log Trend Analysis
- Finding and Rating Statement
- Management Action Plan Draft

Day 5: Aviation IT Audit Report for One Operator

Do the earlier results join into one report that an audit committee can act on?

- Applying the Session 1 Scope Sheet
- Testing the Session 2 Risk Ranking
- Checking the Session 3 Evidence Ratings
- Reviewing the Session 4 Findings
- Completing the Operator Audit Report

Methodology

The programme is a field-style audit simulation built on prepared records from an airline and an airport: system inventories, access listings, change logs, supplier contracts and recovery test results. Participants scope an audit, rank risk, test controls, rate evidence and defend findings to peers acting as an audit committee.

- Suggested activity: Ranking six systems of an airline by operational and data risk.
- Suggested activity: Sampling privileged access records and recording exceptions.
- Suggested activity: Rating a draft finding on a supplier outage.

Capstone Output

Each participant completes an audit report for one airline or airport. It holds a scope statement, a ranked risk view, a control test summary, rated findings and an agreed action plan. At work it goes to the audit committee, and its test steps become the basis of the next technology audit cycle.

Frequently Asked Questions

Is aviation IT audit training suitable for auditors new to aviation?

Yes. Aviation IT audit is taught through prepared records and templates. You need responsibility for audit, risk or technology controls and a working grasp of audit practice, but no aviation operating background.

Which standards does aviation IT audit rest on in this training?

Aviation IT audit here rests on ISO/IEC 27001 and ISO/IEC 27002 for controls, COBIT and ISACA ITAF for audit practice, the NIST Cybersecurity Framework for gaps, and ICAO Annex 17 for sector obligations.

How is the report from aviation IT audit training used at work?

You take the operator audit report to your audit committee, use its test steps for the next audit cycle and keep its action plan to track management responses.