# Advanced Aviation Information Systems Audit and Assurance Training Course

6 – 10 September 2027
Frankfurt

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# Advanced Aviation Information Systems Audit and Assurance Training Course

**Ref:** 1197_188408 **Date:** 6 – 10 September 2027 **Location:** Frankfurt **Fees:** 5700 Euro

## Overview

Advanced Aviation Information Systems Audit and Assurance is a one-week course for aviation IT auditors, assurance teams, technology risk specialists, compliance professionals, and governance managers, who leave with an Aviation Information Systems Audit File. The course connects aviation digital systems, IT general controls, application controls, privileged access, change management, data integrity, aviation cybersecurity, operational resilience, third-party assurance, audit evidence, and corrective-action follow-up. Agile Leaders Training Center presents aviation information systems audit and assurance.

## Who Should Attend

- Teams responsible for auditing airline, airport, operational, and connected-system technology
- Functions accountable for IT control design, operation, evidence, and remediation
- Cyber assurance teams responsible for resilience, incident, and security-control reviews
- Technology risk functions responsible for audit universes, risk assessments, and priorities
- Compliance teams responsible for mapping applicable requirements to testable criteria
- Aviation governance teams responsible for findings, action ownership, and oversight reporting

The course assumes participants already perform audit, assurance, technology risk, cybersecurity, or compliance work and leaves out introductory auditing terminology and certification-exam preparation.

## Departments and Industries

The course supports digital assurance work across:

- Airline operations, passenger services, cargo, and engineering systems
- Airport operations, security, baggage, and terminal technology
- Air navigation, aviation communications, and information services
- Aircraft-connected technology and maintenance information environments
- Aviation suppliers, managed services, and technology outsourcing functions
- Internal audit, information security, risk, compliance, and continuity departments

## Learning Objectives

By the end of this course, participants will be able to:

- Build an aviation information-systems audit universe and risk assessment
- Apply ITAF principles to engagement planning, testing, and reporting
- Analyze IT general, application, interface, and data-integrity controls
- Evaluate cyber resilience, incident, continuity, and supplier controls
- Use evidence, sampling, interviews, and reperformance to support findings
- Prioritize recommendations, corrective actions, and assurance follow-up

## Course Agenda

### Day 1: Aviation Audit Universe and Criteria

- Aviation Digital Ecosystem and System Dependency Map
- ITAF Audit and Assurance Engagement Framework
- Information Confidentiality, Integrity, and Availability Criteria Matrix
- Aviation Technology Audit Universe and Entity Register
- Risk-Based Engagement Scope and Objective Worksheet

### Day 2: Core Technology Control Testing

- IT General Controls Design and Operating-Effectiveness Test
- Identity and Privileged Access Review Matrix
- Change, Release, and Configuration Control Walkthrough
- Application and Interface Control Test Script
- Aviation Data Integrity and Reconciliation Worksheet

### Day 3: Cyber and Operational Resilience

- Aviation Cybersecurity Governance and Responsibility Map
- Critical Information Asset and Protection Objective Register
- Incident Response and Operational Continuity Test Plan
- Connected-Aircraft and Operational-Technology Risk Scenario
- Cybersecurity Control Effectiveness Assessment

### Day 4: Evidence, Suppliers, and Reporting

- Third-Party and Aviation Supply-Chain Assurance Matrix
- Audit Evidence Sufficiency and Reliability Checklist
- Technology Audit Sampling and Reperformance Method
- Finding, Cause, Risk, and Control Analysis Template
- Corrective-Action Ownership and Follow-Up Register

## Day 5: Applied Aviation IT Audit Practice

- Exercise: Build an Aviation Systems Audit Universe
- Exercise: Test Access, Change, and Interface Controls
- Exercise: Assess Cyber Resilience and Supplier Assurance
- Exercise: Draft Findings and Corrective Actions
- Capstone Exercise: Aviation Information Systems Audit File

## Practical Exercises

The course uses suggested activities to connect aviation technology risks with evidence and assurance decisions:

- Suggested activity: map dependencies across airline operations, airport services, and external providers
- Suggested activity: test privileged access and system-change evidence against defined criteria
- Suggested activity: evaluate an operational disruption scenario and continuity-control response
- Suggested activity: assemble testing records, findings, actions, and follow-up evidence into an audit file

## FAQs

### Who does advanced aviation information systems audit and assurance suit, and what does it assume?

It suits professionals who perform aviation audit, IT assurance, cyber assurance, technology risk, compliance, or governance work and assumes practical familiarity with controls, evidence, systems, or operational processes.

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

Aviation information systems audit applies audit methods to airline, airport, operational, connected-aircraft, supplier, safety-critical, and continuity contexts, while general IT audit training uses cross-industry systems and control examples.

### What evidence supports an aviation information systems audit finding?

Reliable evidence can include configurations, access records, change tickets, interface reconciliations, incident records, supplier reports, interviews, observations, sampling results, and reperformance documented against defined criteria.

## How does aviation cybersecurity affect information systems assurance?

Aviation cybersecurity adds interconnected operational dependencies, critical information assets, incident response, supply-chain exposure, and continuity requirements that must be incorporated into scoping, testing, findings, and follow-up.

## How are corrective actions followed after an aviation IT audit?

Corrective actions are followed through assigned ownership, due-state evidence, validation testing, residual-risk assessment, escalation criteria, and documented closure decisions.

## Conclusion

Participants take back an Aviation Information Systems Audit File containing the audit universe, risk assessment, control tests, evidence records, resilience assessment, supplier review, findings, corrective actions, and follow-up register. The file changes disconnected technology checks into a traceable aviation assurance engagement. It supports consistent scoping, testing, reporting, remediation validation, and governance oversight.