IT Auditing Fundamentals and Evidence Training Course

1 – 5 November 2026
Nairobi

AGILE LEADERS
Training Center

IT Auditing Fundamentals and Evidence Training Course

Ref: 1688_226930 **Date:** 1 – 5 November 2026 **Location:** Nairobi **Fees:** 4500 Euro

Overview

IT Auditing Fundamentals Training Course is a one-week foundation course for audit, risk and technology teams, who leave with an IT Audit Engagement Pack. The course connects engagement objectives, scope, risk assessment, control criteria, work programs, evidence collection, sampling, testing, workpapers, findings, reporting and remediation follow-up. Participants create traceable assurance records without preparing for a certification or configuring audit software. Agile Leaders Training Center develops practical IT auditing fundamentals.

Who Should Attend

- Teams responsible for planning and conducting internal audit engagements
- Teams responsible for technology controls and assurance evidence
- Teams responsible for risk, compliance and remediation oversight
- Teams responsible for system ownership and control operation
- Managers responsible for reviewing IT audit results and actions

The course assumes participants can read basic policies, process maps and system records at work, and leaves out certification preparation, advanced data analytics and product configuration.

Departments and Industries

The course supports departments that assess technology governance, risk and controls across service environments.

- Internal audit and assurance
- Information technology and cybersecurity
- Risk, compliance and governance
- Financial services and digital commerce
- Healthcare, manufacturing and infrastructure services

Learning Objectives

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

- Build risk-informed objectives and audit scope
- Use risk and control matrices and work programs
- Apply examine, interview and test methods
- Evaluate evidence relevance, reliability and sufficiency
- Analyze control gaps and formulate findings
- Prioritize recommendations and remediation follow-up

Course Agenda

Day 1: Engagement Planning and Scope

- IT Audit Mandate and Engagement Purpose Canvas
- Process, System and Stakeholder Boundary Map
- Preliminary Risk Assessment and Heat Map
- Engagement Objective, Scope and Limitation Statement
- Audit Resource and Communication Plan

Day 2: Criteria and Work Programs

- Risk and Control Matrix Design
- Policy, Standard and Procedure Criteria Register
- Control Objective and Expected Condition Map
- IT Audit Work Program Template
- Sampling Population and Selection Plan

Day 3: Evidence and Control Testing

- NIST SP 800-53A Examine, Interview and Test Method
- Evidence Relevance, Reliability and Sufficiency Checklist
- Access, Change and Operations Control Test Sheet
- Exception, Cause and Impact Analysis Record
- Audit Workpaper Index and Cross-Reference Method

Day 4: Findings and Follow-Up

- Criteria, Condition, Cause and Effect Finding Model
- Finding Significance and Risk Rating Matrix
- Recommendation and Management Action Template
- Final Audit Communication and Conclusion Outline
- Remediation Owner, Due Action and Status Tracker

Day 5: Audit Practice and Capstone

- Exercise: Scope an IT Audit Engagement
- Exercise: Build a Risk and Control Work Program
- Exercise: Evaluate Evidence and Record Test Results
- Exercise: Draft a Finding and Follow-Up Action
- Capstone: IT Audit Engagement Pack

Practical Exercises

The course uses suggested activities based on access management, system changes and technology operations.

- Suggested activity: convert a process concern into objectives, scope and risk statements
- Suggested activity: map risks, controls, criteria and audit procedures
- Suggested activity: evaluate documents, interview notes and test evidence
- Suggested activity: draft a finding, agreed action and follow-up record

FAQs

Who suits IT auditing fundamentals training and what does it assume?

IT auditing fundamentals training suits auditors, control owners, compliance analysts, risk coordinators and technology managers beginning assurance work. It assumes basic literacy in policies, processes and system records while excluding certification and advanced analytics.

How does IT auditing fundamentals training differ from advanced cybersecurity assessment?

IT auditing fundamentals training covers engagement planning, criteria, evidence, workpapers, findings and follow-up across technology controls. Advanced cybersecurity assessment usually requires deeper technical testing, specialized tools and detailed vulnerability analysis.

What makes IT audit evidence sufficient and reliable?

IT audit evidence is sufficient when its quantity supports a reasonable conclusion and reliable when its source, quality and collection method can be trusted. Relevance connects the evidence directly to the audit objective and criteria.

Why does an IT audit use a risk and control matrix?

An IT audit uses a risk and control matrix to connect objectives, risks, controls, criteria, procedures and results. The matrix keeps testing traceable and helps reviewers identify coverage gaps or unsupported conclusions.

AGILE LEADERS
Training Center

Conclusion

Participants take back an IT Audit Engagement Pack containing scope statements, risk assessments, control matrices, work programs, test records, workpapers, findings, reports and follow-up actions. The pack creates traceability from audit objective to conclusion. It also gives audit and technology teams a shared basis for evidence review and remediation monitoring.