



# Continuous Auditing Design and Operations Training Course

1 – 5 August 2027  
Geneva

## Continuous Auditing Design and Operations Training Course

**Ref:** 366\_130090 **Date:** 1 – 5 August 2027 **Location:** Geneva **Fees:** 6200 Euro

### Overview

Continuous Auditing Design and Operations Training Course is a five-day course for internal auditors, audit managers, assurance professionals, data-enabled audit teams, and control monitoring specialists who leave with a Continuous Audit Operating Toolkit. The course connects continuous auditing, risk-based test selection, automated audit tests, risk indicators, exception handling, alert triage, evidence retention, control validation, continuous audit reporting, governance, and improvement while distinguishing audit-owned work from continuous monitoring. Agile Leaders Training Center delivers this course on continuous auditing.

### Who Should Attend

- Internal audit functions responsible for ongoing risk and control assessment
- Audit management functions responsible for continuous-assurance strategy and governance
- Data-enabled audit teams responsible for automated tests and exception analysis
- Risk and compliance functions responsible for indicators and control insight
- Control monitoring functions responsible for management-owned monitoring activities

The course assumes participants already contribute to audit, assurance, risk, compliance, data analysis, or control monitoring and leaves out software coding and external certification preparation.

### Departments and Industries

The course supports continuous audit operations across transactional, technology, and service environments.

- Internal audit, assurance, risk, and compliance departments
- Financial services and professional-services organizations
- Manufacturing and supply-chain operations
- Healthcare and education institutions
- Technology and digital-service functions
- Public-service and nonprofit organizations

### Learning Objectives

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



- Compare continuous auditing, continuous monitoring, and periodic audit roles
- Prioritize risks, processes, controls, and data sources
- Build automated audit tests, indicators, and alert criteria
- Evaluate exceptions, false positives, and evidence quality
- Use governance, access, retention, and validation controls
- Build reporting, escalation, and improvement routines

## **Course Agenda**

### **Day 1: Continuous Audit Context and Governance**

- Continuous Auditing and Monitoring Role Matrix
- Periodic and Continuous Assurance Comparison Map
- Continuous Audit Governance Charter
- Independence and Management Ownership Boundary Checklist
- Continuous Audit Maturity Diagnostic

### **Day 2: Risk Selection and Test Design**

- Risk-to-Process Prioritization Matrix
- Control and Data Source Inventory
- Automated Audit Test Design Canvas
- Risk Indicator Definition Sheet
- Population Coverage and Frequency Decision Grid

### **Day 3: Exceptions and Evidence**

- Exception Detection Rule Catalogue
- Alert Threshold and Tolerance Matrix
- False-Positive Triage Workflow
- Exception Investigation Case Log
- Audit Evidence Retention and Traceability Register

### **Day 4: Validation and Reporting**

- Data Quality and Access Control Checklist
- Automated Test Validation Protocol
- Control Failure Escalation Matrix
- Continuous Audit Reporting Dashboard Specification
- Performance Review and Improvement Backlog



## **Day 5: Continuous Audit Practice and Capstone**

- Suggested Exercise: Governance and Role Boundary Review
- Suggested Exercise: Risk Indicator and Test Design
- Suggested Exercise: Alert Triage and Evidence Assessment
- Suggested Exercise: Validation and Reporting Challenge
- Capstone Exercise: Continuous Audit Operating Toolkit

## **Practical Exercises**

The course uses suggested activities to connect automated testing with audit judgment and control evidence.

- Suggested activity: select financial-service risks, controls, data, tests, indicators, and frequencies for continuous assessment.
- Suggested activity: triage manufacturing exceptions and distinguish actionable alerts from false positives.
- Suggested activity: validate a healthcare audit test for access, data quality, logic, evidence, and traceability.
- Suggested activity: design a reporting and escalation routine with an improvement backlog.

## **FAQs**

### **Who suits continuous auditing design and operations, and what does the course assume?**

Continuous auditing design and operations suit professionals who already contribute to audit, assurance, risk, compliance, data analysis, or control monitoring and need an operating approach for ongoing assessment.

### **How does continuous auditing differ from continuous monitoring?**

Continuous auditing is audit-owned ongoing assessment that supports assurance, while continuous monitoring is management-owned observation of operations, risks, and controls.

### **How are automated audit tests selected for continuous auditing?**

Automated audit tests are selected by prioritizing risk, control importance, data availability, reliability, expected exception value, ownership, and the practical frequency of assessment.

### **How should continuous auditing teams handle false-positive alerts?**

Continuous auditing teams should document alert logic, apply triage criteria, validate source data, investigate causes, tune thresholds, preserve decisions, and monitor recurring false-positive patterns.



## **What evidence should continuous auditing retain?**

Continuous auditing should retain test logic, data lineage, run records, exceptions, investigation decisions, validation results, approvals, escalations, reports, and changes to rules or thresholds.

## **Conclusion**

Participants leave with a Continuous Audit Operating Toolkit linking governance, risk selection, test design, indicators, alerts, evidence, validation, reporting, and improvement. The toolkit changes isolated automated checks into a governed audit capability. It provides a working basis for prioritizing coverage, assessing exceptions, preserving traceability, and refining continuous audit operations.