+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 07/29/2026

Sign Up

SOC 2 Lead Manager Training

5 days (35 hours)

Overview

SOC 2 has become an essential framework for structuring security, availability, data integrity, confidentiality, and privacy in service organizations, particularly in cloud environments where responsibility is shared between the provider and the client.

Our Lead SOC 2 Manager training will enable you to go beyond the fundamentals and master the operational and methodological challenges of a SOC 2 program in a real-world environment.

You will learn to understand the Trust Services Criteria, analyze a scope of control, prepare the required evidence, track discrepancies, and effectively contribute to the production of a usable audit report.Upon completion of the training, you will be able to lead SOC 2 preparation, coordinate stakeholders, enhance the quality of controls, and align compliance requirements with the organization’s security practices.

This training also covers governance, risk management, evidence collection, remediation tracking, the use of cloud environments, and best practices for communicating with technical and business teams.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the SOC 2 framework and its criteria.
- Identify the expected controls and develop a compliance plan.
- Collect, qualify, and organize audit evidence.

- Track discrepancies, remediation efforts, and corrective actions.
- Coordinate communication between security, IT, compliance, and business units.
- Prepare an operational dossier to support the audit process.

Target Audience

- SOC Analyst
- Compliance Manager
- Cybersecurity Project Manager
- Internal Auditor
- Information Systems Security Manager

Prerequisites

- Knowledge of cybersecurity principles and risk management.
- Understanding of cloud environments and shared responsibility models.
- Prior experience in auditing, compliance, or internal control.
- Proficiency in IT governance and operational documentation.
- Ability to interpret procedures, metrics, and technical evidence.

Technical Requirements

- Access to a spreadsheet program and a note-taking tool to organize controls and evidence.
- A microphone and headset are recommended for remote sessions and collaborative work.
- If needed, access to a shared workspace or a cloud-based demo environment.

Lead SOC 2 Manager Training Program

[Day 1 - Morning] SOC 2

Fundamentals

- Understand the purpose of a SOC 2 audit and its applications from both the client’s and the provider’s perspectives.
- Identify the five criteria: security, availability, processing integrity, confidentiality, and privacy.
- Distinguish between the roles of the service organization, management, and the practitioner.
- Link audit expectations to governance and internal control issues.
- Define the scope of a SOC 2 program within a service organization.
- Hands-on workshop: Map out a use case and match each SOC 2 requirement to the correct criterion.

[Day 1 – Afternoon] Criteria

and Scope

- Analyze the structure of the Trust Services Criteria and how to interpret them.
- Understand the concepts of a system, included services, and control objectives.
- Identify scope boundaries and external dependencies that need to be documented.
- Identify the risks of incorrectly defining the scope and their impacts.
- Prepare an initial review of the control framework for a cloud environment.
- Hands-on workshop: Build a SOC 2 scope based on a simplified architecture.

[Day 2 - Morning]

Governance and Responsibilities

- Structure the governance of a SOC 2 program and its approval processes.
- Define responsibilities among security, operations, compliance, and management.
- Understand the impact of shared responsibility in cloud environments.
- Organize monitoring processes, committees, and escalation procedures.
- Implement a RACI matrix tailored to audit requirements.
- Hands-on workshop: Develop a responsibility matrix for a SOC 2 program.

[Day 2 - Afternoon]

Controls and Risks

- Identify the categories of controls expected in a mature framework.
- Link each control to a business, technical, or regulatory risk.
- Prioritize controls based on their criticality and maturity.
- Describe the evidence required to demonstrate design and operation.
- Prepare an evaluation framework to assess operational effectiveness.
- Hands-on workshop: transforming a list of risks into a prioritized control plan.

[Day 3 - Morning]

Documentation and

Evidence

- Structure the documentation required to support a SOC 2 audit.
- Define what constitutes useful, actionable, and traceable evidence.
- Organize the collection of evidence from technical and business teams.
- Avoid evidence that is incomplete, undated, or unrelated to the control.
- Set up a simple and maintainable document management system.
- Hands-on workshop: Compile a file of evidence based on an audit scenario.

[Day 3 - Afternoon]

Cloud and Operational Security

- Apply the shared responsibility model to cloud services.
- Link controls to security, access, and logging configurations.
- Understand the impact of infrastructure settings on compliance.
- Identify common gaps related to accounts, roles, and permissions.
- Integrate operational security requirements into SOC 2 monitoring.
- Hands-on workshop: Analyze a mock cloud environment and identify missing control points.

[Day 4 - Morning]

Audit Readiness

- Prepare for the readiness phase prior to a formal review.
- Identify design and implementation gaps.
- Develop a realistic, time-bound, and trackable remediation plan.
- Prioritize actions based on their impact on audit eligibility.
- Anticipate recurring questions from auditors and stakeholders.
- Hands-on workshop: Drafting a corrective action plan based on a findings report.

[Day 4 - Afternoon]

Monitoring and

Management

- Establish monitoring metrics for the SOC 2 program.
- Measure the progress of controls, evidence, and remediation efforts.
- Define easy-to-read dashboards for management.
- Manage dependencies between teams and resolve bottlenecks.
- Prepare clear communications for steering committees.
- Hands-on workshop: Design a SOC 2 management dashboard with key metrics.

[Day 5 - Morning] Audit

Preparation

- Organize the expected deliverables during the final preparation phase.
- Verify consistency between scope, controls, evidence, and corrective actions.
- Prepare for discussions with auditors and internal contributors.
- Anticipate questions regarding design, execution, and traceability.
- Finalize a dossier ready for presentation in an audit context.
- Hands-on workshop: Simulate a preparation review and address any weaknesses.

[Day 5 - Afternoon] Consolidation

and Implementation

- Review the key takeaways from the week and areas requiring attention.
- Develop a post-training implementation roadmap.
- Identify best practices to ensure the long-term sustainability of the SOC 2 program.
- Define roles, processes, and follow-up deliverables.
- Prepare the next steps to scale up the initiative.
- Hands-on workshop: Develop a personal action plan to implement SOC 2 in your specific context.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methods.

Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg