+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

Senior Lead SOC 2 Manager Training

5 days (35 hours)

Overview

SOC 2 has become a key framework for demonstrating mastery of security controls, availability, confidentiality, and integrity. This training prepares you to lead an audit-ready and production-ready approach in demanding environments.

Our Senior Lead SOC 2 Manager training enables you to go beyond a basic understanding of the framework to structure operational governance, align evidence, and ensure compliance processes over the long term.

You will learn to interpret the Trust Services Criteria, organize the collection of evidence, track control deficiencies, coordinate stakeholders, and effectively prepare for internal and external audits.

Upon completion of the training, you will be able to strengthen a SOC 2 framework, prioritize remediation efforts, standardize control monitoring, and ensure the reliable production of deliverables expected by auditors and security teams.

This training also covers monitoring, incident management, traceability, documentation, and best practices for governance to help you establish a sustainable compliance posture.

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

Objectives

- Master the requirements of the SOC 2 framework and the Trust Services Criteria.
- Establish a compliance governance framework focused on evidence, controls, and accountability.

- Organize the collection, qualification, and retention of audit evidence.
- Analyze gaps, prioritize remediation, and track action plans.
- Prepare a Type 1 or Type 2 audit using a standardized approach.
- Strengthen incident management, monitoring, and traceability.

Target Audience

- SOC Analyst
- Compliance Manager
- Cybersecurity Consultant
- Security Auditor
- GRC Manager

Prerequisites

- Knowledge of the fundamentals of cybersecurity and internal controls.
- Previous experience in SOC, GRC, or compliance management.
- Proficiency in the concepts of risk, evidence, and traceability.
- Understanding of cloud, SaaS, or hybrid environments.
- Ability to interpret security documentation and audit procedures in a practical context.

Technical Prerequisites

- A recent computer with an up-to-date web browser and sufficient disk space for course materials.
- Stable Wi-Fi or Ethernet connection for discussions, workshops, and demonstrations.
- Office suite installed, including Microsoft Excel or equivalent for tracking controls.
- Access to a PDF reader and a note-taking tool for training deliverables.
- A microphone and headset are recommended for remote sessions and collaborative work.

Curriculum for our Senior Lead SOC 2 Manager Training

[Day 1 - Morning]

Foundations of the SOC 2

Framework

- The role of SOC 2 in a compliance and trust strategy.
- Structured review of the Trust Services Criteria and their operational requirements.
- Differences between Type 1 and Type 2, and their impact on management and evidence.
- Roles of the Senior Lead Analyst, security teams, and business stakeholders.
- Initial mapping of controls, risks, and documentation dependencies.
- Hands-on workshop: Building an initial mapping matrix between SOC 2 criteria and existing controls.

[Day 1 - Afternoon]

Governance and Scope

- Definition of the audit scope, affected systems, and justified exclusions.
- Structuring governance, RACI, and approval workflows.
- Identifying sources of evidence, internal policies, and retention requirements.
- Alignment of compliance objectives, operational constraints, and remediation priorities.
- Management of dependencies with suppliers, subcontractors, and cloud environments.
- Hands-on workshop: formalizing a SOC 2 scope and a responsibility matrix for a fictional organization.

[Day 2 - Morning]

Security Controls

- Analysis of controls related to access, authentication, and the principle of least privilege.
- Requirements for change management, approvals, and segregation of duties.
- Controls for logging, monitoring, and audit trail retention.
- Review of requirements for confidentiality, integrity, and data protection.
- Assessing the maturity of controls and identifying areas of vulnerability.
- Hands-on workshop: auditing a set of controls and classifying discrepancies by criticality.

[Day 2 - Afternoon] Evidence

and Documentation

- Developing a reliable and repeatable evidence-gathering strategy.
- Criteria for evidence quality, traceability, timestamping, and chain of custody.
- Document organization, naming conventions, versioning, and secure storage of deliverables.
- Preparing audit files to minimize follow-up requests.
- Managing sensitive evidence and document access restrictions.
- Hands-on workshop: Compiling a comprehensive evidence file for a specific SOC 2 audit.

[Day 3 - Morning]

Advanced Risk Assessment

- Risk Analysis Methodology Applied to the SOC 2 Context.
- Identification of failure scenarios, impacts, and aggravating factors.
- Prioritization of risks based on exposure, likelihood, and business criticality.
- Definition of risk treatments, risk acceptance levels, and remediation plans.
- Monitoring of residual risks and integration with compliance management.
- Hands-on workshop: creating a mini risk map with associated action plans.

[Day 3 - Afternoon]

Monitoring and Detection

- The role of monitoring in continuously demonstrating control effectiveness.
- Useful indicators for tracking the status of controls and compliance deviations.
- Monitoring of security events, correlation, and escalation.
- Integration between logging, monitoring, and anomaly detection.
- Using metrics to support compliance reporting.
- Hands-on workshop: Defining a SOC 2 management dashboard with key metrics.

[Day 4 - Morning]

Incidents and Response

- Organizing an incident response capability aligned with audit requirements.
- The incident lifecycle, from detection to documented closure.
- Procedures for notification, escalation, and cross-team coordination.
- Post-incident lessons learned, feedback, and continuous improvement.
- Traceability requirements for incidents, decisions, and corrective actions.
- Hands-on workshop: Simulate incident handling and produce the associated documentation.

[Day 4 - Afternoon] Remediation

and Action Plans

- Developing a realistic, measurable, and prioritized remediation plan.
- Coordinating actions across security, product, infrastructure, and governance.
- Tracking milestones, dependencies, and evidence of correction.
- Managing exceptions, accepted risks, and executive decisions.
- Preparing justification documentation for unresolved issues.
- Hands-on workshop: transforming a list of discrepancies into a time-bound action plan.

[Day 5 - Morning] Audit

Preparation

- Organizing the preparation file for an internal or external audit.
- Anticipating audit questions and requests for clarification.
- Techniques for cross-checking evidence and critical controls.
- Managing interviews, demonstrations, and validation procedures.
- Best practices for ensuring consistency between the narrative, evidence, and operational reality.
- Hands-on workshop: conducting a simulated audit review using a preparation and debriefing checklist.

[Day 5 - Afternoon] Consolidation

and Sustainable Management

- Summary of key takeaways and development of a maturity improvement plan.
- Standardizing the tracking of controls, evidence, and periodic reviews.
- Integrating compliance into management processes and security committee meetings.
- Defining continuity measures to maintain a robust SOC 2 framework.
- Post-training roadmap to stabilize governance and prepare for upcoming audit cycles.
- Hands-on workshop: developing a 90-day SOC 2 roadmap with priorities, responsible parties, and deliverables.

Target Audience

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

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.