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

Mis à jour le 29/07/2026

S'inscrire

Formation Lead SOC 2 Manager

5 jours (35 heures)

Présentation

Le SOC 2 est devenu un référentiel incontournable pour structurer la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la vie privée dans les organisations de services, notamment dans les environnements cloud où la responsabilité est partagée entre le fournisseur et le client.

Notre formation Lead SOC 2 Manager vous permettra d'aller au-delà des fondamentaux pour maîtriser les enjeux opérationnels et méthodologiques d'un programme SOC 2 en environnement réel.

Vous apprendrez à comprendre les Trust Services Criteria, à analyser un périmètre de contrôle, à préparer les preuves attendues, à suivre les écarts et à contribuer efficacement à la production d'un dossier d'audit exploitable.À l'issue de la formation, vous serez en mesure de piloter la préparation SOC 2, de coordonner les parties prenantes, de renforcer la qualité des contrôles et d'aligner les exigences de conformité avec les pratiques de sécurité de l'organisation.

Cette formation aborde également la gouvernance, la gestion des risques, l'evidence collection, le suivi des remédiations, l'usage des environnements cloud et les bonnes pratiques de communication avec les équipes techniques et métiers.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le cadre SOC 2 et ses critères de référence.
- Identifier les contrôles attendus et structurer un plan de conformité.
- Collecter, qualifier et organiser les preuves d'audit.

- Suivre les écarts, les remédiations et les actions correctives.
- Coordonner les échanges entre sécurité, IT, conformité et métiers.
- Préparer un dossier opérationnel pour soutenir une démarche d'audit.

Public visé

- Analyste SOC
- Responsable conformité
- Chef de projet cybersécurité
- Auditeur interne
- Responsable sécurité des systèmes d'information

Pré-requis

- Connaissance des principes de cybersécurité et de gestion des risques.
- Compréhension des environnements cloud et des modèles de responsabilité partagée.
- Expérience préalable en audit, conformité ou contrôle interne.
- Maîtrise des notions de gouvernance IT et de documentation opérationnelle.
- Capacité à lire des procédures, des indicateurs et des preuves techniques.

Pré-requis techniques

- Accès à un tableur et à un outil de prise de notes pour structurer les contrôles et les preuves.
- Micro et casque recommandés pour les sessions à distance et les travaux collaboratifs.
- Si besoin, accès à un espace de travail partagé ou à un environnement cloud de démonstration.

Programme de notre formation Lead SOC 2 Manager

[Jour 1 - Matin]

Fondamentaux SOC 2

- Comprendre la finalité d’un audit SOC 2 et ses usages côté client et fournisseur.
- Identifier les cinq critères de référence, sécurité, disponibilité, intégrité du traitement, confidentialité et vie privée.
- Différencier le rôle du service organization, du management et du praticien.
- Relier les attentes d’audit aux enjeux de gouvernance et de contrôle interne.
- Positionner le périmètre d’un programme SOC 2 dans une organisation de services.
- Atelier pratique : cartographier un cas d’usage et associer chaque exigence SOC 2 au bon critère.

[Jour 1 - Après-midi]

Critères et périmètre

- Analyser la structure des Trust Services Criteria et leur logique de lecture.
- Comprendre la notion de système, de services inclus et d’objectifs de contrôle.
- Identifier les limites de périmètre et les dépendances externes à documenter.
- Repérer les risques de mauvaise qualification du scope et leurs impacts.
- Préparer une première lecture du dispositif de contrôle pour un environnement cloud.
- Atelier pratique : construire un périmètre SOC 2 à partir d’une architecture simplifiée.

[Jour 2 - Matin]

Gouvernance et responsabilités

- Structurer la gouvernance d’un programme SOC 2 et les circuits de validation.
- Définir les responsabilités entre sécurité, opérations, conformité et direction.
- Comprendre l’effet de la responsabilité partagée dans les environnements cloud.
- Organiser les rituels de suivi, les comités et les points d’arbitrage.
- Mettre en place une matrice RACI adaptée aux exigences d’audit.
- Atelier pratique : élaborer une matrice de responsabilités pour un programme SOC 2.

[Jour 2 - Après-midi]

Contrôles et risques

- Identifier les familles de contrôles attendues dans un dispositif mature.
- Relier chaque contrôle à un risque métier, technique ou réglementaire.
- Hiérarchiser les contrôles selon leur criticité et leur maturité.
- Décrire les preuves attendues pour démontrer la conception et l’exécution.
- Préparer une grille de lecture pour évaluer l’efficacité opérationnelle.
- Atelier pratique : transformer une liste de risques en plan de contrôles priorisé.

[Jour 3 - Matin]

Documentation et preuves

- Structurer la documentation attendue pour soutenir un audit SOC 2.
- Qualifier une preuve utile, exploitable et traçable.
- Organiser la collecte des éléments auprès des équipes techniques et métiers.
- Éviter les preuves incomplètes, non datées ou non reliées au contrôle.
- Mettre en place un référentiel documentaire simple et maintenable.
- Atelier pratique : constituer un dossier de preuves à partir d’un scénario d’audit.

[Jour 3 - Après-midi]

Cloud et sécurité opérationnelle

- Appliquer le modèle de responsabilité partagée aux services cloud.
- Relier les contrôles aux configurations de sécurité, d’accès et de journalisation.
- Comprendre l’impact des paramètres d’infrastructure sur la conformité.
- Identifier les écarts fréquents liés aux comptes, aux rôles et aux permissions.
- Intégrer les exigences de sécurité opérationnelle dans le suivi SOC 2.
- Atelier pratique : analyser un environnement cloud fictif et détecter les points de contrôle manquants.

[Jour 4 - Matin]

Audit readiness

- Préparer la phase de readiness avant une revue formelle.
- Identifier les écarts de conception et les écarts d’exécution.
- Construire un plan de remédiation réaliste, daté et suivi.
- Prioriser les actions selon l’impact sur l’éligibilité audit.
- Anticiper les questions récurrentes des auditeurs et des parties prenantes.
- Atelier pratique : rédiger un plan d’actions correctives à partir d’un rapport de constats.

[Jour 4 - Après-midi]

Suivi et pilotage

- Mettre en place des indicateurs de suivi pour le programme SOC 2.
- Mesurer l’avancement des contrôles, des preuves et des remédiations.
- Définir des tableaux de bord lisibles pour le management.
- Gérer les dépendances entre équipes et les points de blocage.
- Préparer une communication claire pour les comités de pilotage.
- Atelier pratique : concevoir un tableau de bord de pilotage SOC 2 avec indicateurs clés.

[Jour 5 - Matin]

Préparation de l’audit

- Ordonner les livrables attendus dans une phase de préparation finale.
- Vérifier la cohérence entre périmètre, contrôles, preuves et remédiations.
- Préparer les échanges avec les auditeurs et les contributeurs internes.
- Anticiper les questions sur la conception, l’exécution et la traçabilité.
- Finaliser un dossier prêt à être présenté dans une logique d’audit.
- Atelier pratique : simuler une revue de préparation et corriger les points de fragilité.

[Jour 5 - Après-midi]

Consolidation et mise en œuvre

- Revoir les acquis essentiels de la semaine et les points de vigilance.
- Structurer une feuille de route de mise en œuvre post-formation.
- Identifier les bonnes pratiques pour pérenniser le dispositif SOC 2.
- Formaliser les rôles, les rituels et les livrables de suivi.
- Préparer les prochaines étapes pour industrialiser la démarche.
- Atelier pratique : élaborer un plan d’action personnel pour déployer SOC 2 dans son contexte.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.