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

Mis à jour le 07/10/2025

S'inscrire

Formation certification ISSMP – Information Systems Security Management Professional

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

La certification ISSMP (Information Systems Security Management Professional) du (ISC)² représente le plus haut niveau de reconnaissance en management stratégique de la cybersécurité. Conçue pour les professionnels expérimentés, elle valide votre capacité à diriger des programmes de sécurité complexes, alignés sur les objectifs de l'entreprise. Cette formation officielle prépare aux six domaines du référentiel officiel de compétences (CBK) ISSMP : gouvernance, gestion des risques, conformité, continuité d'activité, opérations et aspects légaux. À travers une approche méthodique et pratique, vous apprendrez à mettre en place une gouvernance sécurité robuste, piloter des plans de gestion de crise, superviser la conformité et accompagner la direction dans la prise de décision stratégique. Vous développerez une compréhension approfondie des référentiels clés et des mécanismes de pilotage (KPI, KRI), tout en renforçant votre posture de leader cybersécurité. La formation se conclut par un examen blanc complet et sa correction détaillée afin de vous préparer efficacement à la réussite de la certification (ISC)² ISSMP. Comme toutes nos formations, celle-ci repose sur la dernière version du référentiel CBK et privilégie une approche opérationnelle, pragmatique et orientée résultat, pour des managers capables de transformer la sécurité en véritable levier de gouvernance.

Objectifs

- Maîtriser la gouvernance et la gestion des risques à un niveau stratégique
- Piloter la conformité, la continuité et les opérations de sécurité
- Développer son leadership et sa capacité à diriger des équipes cybersécurité
- Se préparer efficacement à la certification (ISC)² ISSMP

Public visé

- RSSI
- Consultants GRC

- Chefs de projet / managers IT
- Professionnels certifiés CISSP visant un rôle de leadership stratégique

Pré-requis

- Être certifié CISSP
- Solide expérience en cybersécurité et en management de la sécurité

Programme de formation ISSMP – Information Systems Security Management Professional

[Jour 1 - Matin]

Fondamentaux et rôle du manager sécurité

- Positionnement de l'ISSMP vs CISSP et autres certifications ISC²
- Rôle stratégique du manager sécurité : alignement métier
- Le référentiel officiel de compétences (CBK) ISSMP et la logique de domaines
- Compétences clés : gouvernance, leadership, communication
- Atelier pratique : Autoévaluation des compétences et gap analysis.

[Jour 1 - Après-midi]

Gouvernance et alignement avec l'organisation

- Vision, mission, objectifs sécurité alignés aux objectifs business
- Rôles et responsabilités, comités, chartes
- Cadres de gouvernance : ISO 27014, COBIT, ITIL
- Mesure de maturité et pilotage par les indicateurs
- Atelier pratique : Cartographier la gouvernance sécurité de l'entreprise.

Politiques, normes et procédures

- Hiérarchie : politiques, standards, procédures, guidelines
- Cycle de vie documentaire et approbations
- Diffusion des politiques, formation des équipes et vérification de leur application effective.
- Auditabilité et conformité
- Atelier pratique : Rédiger une politique sécurité conforme ISO 27001.

[Jour 2 - Matin]

Gestion des risques : méthodes et mise en œuvre

- Processus : identification, analyse, traitement, acceptation
- Référentiels : ISO 31000, NIST RMF, EBIOS/FAIR
- Cartographie des risques et appétence au risque
- Plans de remédiation et suivi
- Atelier pratique : Réaliser une analyse de risques complète.

[Jour 2 - Après-midi]

Conformité et exigences réglementaires

- Panorama : RGPD, SOX, HIPAA, PCI DSS, ISO 27001
- Privacy by design et registres de traitement
- Mécanismes de contrôle et audits
- Gestion des écarts et plans d’actions
- Atelier pratique : Mini-audit conformité et plan de correction.

Architecture et gouvernance technique

- Cadres : SABSA, TOGAF, NIST CSF
- Gestion des actifs, configurations et obsolescence
- Sécurité physique, logique, réseau : vues intégrées
- Patterns de défense en profondeur
- Atelier pratique : Cartographier l’architecture sécurité cible.

[Jour 3 - Matin]

Cycle de vie des systèmes

- Intégration de la sécurité dans le SDLC
- Exigences, conception, validation, mise en service
- Changements, décommissionnement et destruction
- Assurance qualité et traçabilité : validation, vérification et preuves de conformité des livrables
- Atelier pratique : Check-list sécurité pour projets critiques.

[Jour 3 - Après-midi]

Opérations de sécurité et pilotage

- Processus SOC : supervision, détection, triage
- Gestion des vulnérabilités et correctifs
- Gestion des accès et IAM, journalisation, SIEM
- Externalisation et fournisseurs managés
- Atelier pratique : Définir des KPI/KRI opérationnels SOC.

Gestion de la performance : KPI, KRI et tableaux de bord

- Choisir des indicateurs utiles pour le COMEX
- Mesure de l’efficacité des contrôles
- Amélioration continue et revue de direction
- Storytelling et data visualisation sécurité
- Atelier pratique : Concevoir un tableau de bord cybersécurité.

[Jour 4 - Matin]

Continuité d’activité, résilience et PRA

- Concepts : RTO, RPO, MTTR, criticité
- PCA/PRA : conception, tests, maintien
- Chaîne d’escalade et communication de crise
- Résilience organisationnelle et dépendances
- Atelier pratique : Exercice de crise et post-mortem.

[Jour 4 - Après-midi]

Gestion des fournisseurs et tiers

- Due diligence et questionnaires sécurité
- Clauses contractuelles, SLA/SLO, droits d’audit
- Surveillance continue et risques supply chain
- Gestion des incidents tiers
- Atelier pratique : Revue d’un contrat fournisseur critique.

Légal, éthique et conformité internationale

- Responsabilités du manager et éthique

- Vie privée, transferts et localisations de données
- Preuves, e-discovery, conservation
- Cyberassurance et aspects contractuels
- Atelier pratique : Gestion d’une violation de données personnelles selon le RGPD.

[Jour 5 - Matin]

Réponse aux incidents et gestion de crise

- Plans IR : préparation, détection, contenance, éradication
- Rôles, cellule de crise et communication
- Coordination partenaires/autorités
- Retour d’expérience et leçons apprises
- Atelier pratique : Simulation d’un incident majeur.

[Jour 5 - Après-midi]

Leadership et management des équipes sécurité

- Culture sécurité et conduite du changement
- Organisation, responsabilités, montée en compétences
- Motivation, conflits, collaboration inter-Directions
- Plan de carrière et rétention des talents
- Atelier pratique : Plan de développement d’une équipe SOC.

Préparation à l’examen ISSMP

- Format, domaines, pondérations et stratégies d’examen
- Gestion du temps, techniques de réponse et pièges courants
- Révision ciblée des points sensibles du CBK
- Atelier pratique : Passage de l’examen blanc + correction.

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2025. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg