Certifiante Sessions garanties disponibles

Formation CISSP (Certified Information Systems Security Professional), avec certification

Réf. SF27998

Boostez votre carrière en cybersécurité grâce à notre formation certifiante CISSP de 5 jours !

5 j Durée	4 250 € HT Inter / participant	12 250 € HT Intra (≤12 pers.)	2 Sessions à venir

Objectifs pédagogiques

✓ Acquérir une vision globale des enjeux et aspects de la sécurité IT

✓ Être en mesure d'optimiser les opérations de sécurité d'une organisation

✓ Comprendre les thèmes, domaines et rubriques du Common Body ok Knowledge (CBK®)

✓ Se préparer et passer l'examen de certification CISSP de l'ISC²

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Auditeurs, Ingénieurs télécoms et réseaux, Managers, Responsables de la sécurité des systèmes d'information (RSSI), Risk managers

PrérequisAvoir lu le CBK ("Official ISC² Guide to the CISSP Exam - (ISC)² Press). Les candidats à l'examen de certification doivent également avoir un minimum de 5 ans d'expérience cumulée de travail rémunéré dans au moins deux des huit domaines du CBK de CISSP. Pour en savoir plus, rendez-vous sur le site de l'ISC².

Programme détaillé

Introduction à la formation CISSP

Présentation et objectifs pédagogiques de cette formation CISSP
Les 8 domaines du CISSP Common Body of Knowledge (CBK)

Gestion du risque et de la sécurité

Comprendre, adhérer et promouvoir l'éthique professionnelle
Comprendre et appliquer les concepts de sécurité
Evaluer et appliquer les principes de gouvernance de sécurité
Déterminer la conformité et les autres exigences
Comprendre les problèmes juridiques et réglementaires relatifs à la sécurité informatique dans un contexte holistique
Comprendre les exigences relatives aux types d'enquêtes (c.-à-d., les normes administratives, criminelles, civiles, réglementaires, industrielles)
Développer, documenter et mettre en œuvre une politique, des normes, des procédures et des directives de sécurité
Identifier, analyser et hiérarchiser les exigences de Continuité Commerciale (BC)
Contribuer et appliquer les politiques et les procédures de sécurité du personnel
Comprendre et appliquer les concepts de gestion du risque
Comprendre et appliquer les concepts et méthodologies de modélisation des menaces
Appliquer les concepts de Gestion des Risques de la Chaîne d'Approvisionnement (SCRM)
Établir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

Sécurité des biens

Identifier et classifier les informations et les biens
Etablir les exigences de traitement de l'information et des biens
Provisionner les ressources en toute sécurité
Gérer la durée de vie des données

Garantir une rétention appropriée des bien (EOL, EOS…)
Déterminer les exigences en terme de contrôle et de conformité de la sécurité des données

Architecture et ingénierie de la sécurité

Rechercher, mettre en œuvre et gérer des processus d'ingénierie en utilisant des principes de conception sécurisée
Comprendre les concepts fondamentaux des modèles de sécurité (p.ex., Biba, Star Model, Bell-LaPadula)
Sélectionner les contrôles en fonction des exigences de sécurité des systèmes
Comprendre les capacités de sécurité des Systèmes Informatiques (IS) (p.ex., protection de la mémoire, Trusted Platform Module (TPM), cryptage / décryptage)
Évaluer et atténuer les vulnérabilités des architectures, des conceptions et des éléments de solution de la sécurité
Sélectionner et déterminer des solutions cryptographiques
Comprendre les méthodes attaques cryptanalytiques
Appliquer les principes de sécurité à la conception du site et des infrastructures
Concevoir les contrôles de sécurité du site et des infrastructures

Sécurité des réseaux et de la communication

Évaluer et mettre en œuvre les principes de conception sécurisée dans les architectures de réseau
Sécuriser les composants réseau
Mettre en œuvre des canaux de communication sécurisés selon la conception

Gestion des identités et des accès (IAM)

Contrôler l'accès physique et logique aux biens
Gérer l'identification et l'authentification des personnes, des appareils et des services
Identité fédérée avec un service tiers
Mettre en œuvre et gérer les mécanismes d'autorisation
Gérer le cycle de vie de l'approvisionnement des identités et des accès
Mettre en œuvre les systèmes d'authentification

Evaluation et tests de sécurité

Concevoir et valider des stratégies d'évaluation, de test et d'audit
Conduire des tests de contrôle de sécurité
Recueillir des données de processus de sécurité (p.ex., techniques et administratives)
Analyser la sortie de test et générer un rapport
Conduire ou faciliter des audits de sécurité

Opérations de sécurité

Comprendre et se conformer aux instructions
Conduire des activités de journalisation et de surveillance
Effectuer la gestion de la configuration (CM) (p.ex., approvisionnement, base de référence, automatisation)
Appliquer les concepts d'opérations de sécurité de base
Appliquer la protection des ressources
Conduire la gestion des incidents
Faire fonctionner et maintenir des mesures de détection et de prévention
Mettre en œuvre et prendre en charge la gestion des correctifs et des vulnérabilités
Comprendre et participer aux processus de gestion du changement
Mettre en œuvre des stratégies de récupération
Mettre en œuvre des processus de Reprise après Sinistre (DR)
Tester les Plans de Reprise après Sinistre (DRP)
Participer à la planification et aux exercices de Continuité Commerciale (BC)
Mettre en œuvre et gérer la sécurité physique
Répondre aux problèmes de sécurité et de sûreté du personnel

Sécurité du développement logiciel

Comprendre et intégrer la sécurité dans le Cycle de Vie du Développement Logiciel (SDLC)
Identifier et appliquer les contrôles de sécurité dans les écosystèmes de développement logiciel
Évaluer l'efficacité de la sécurité logicielle
Évaluer l'impact sur la sécurité des logiciels acquis
Définir et appliquer des directives et des normes de codage sécurisé

Préparation à l'examen de certification CISSP

Révisions, questions/réponses selon les besoins des apprenants
Trucs et astuces pour réussir l’examen de certification
Lectures recommandées

Modalités d’évaluation CISSP

Langues disponibles : Français, Allemand, Portugais, Espagnol, Japonais, Chinois et Coréen
Durée de l’examen : 6h
Nombre de questions : 250
Types de questions : Questions à choix multiple et de technologie avancée
Note nécessaire pour réussir l’examen : 700 points sur 1000

Prochaines sessions

DATE	LIEU	STATUT
02/11/2026	à distance	Sur confirmation
02/11/2026	Paris	**Session garantie**

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans d'expertise	1 068+ formations	11 178 apprenants formés/an	+67 Net Promoter Score

Avis des participants

4,9/5 — 4 avis

William B. — Prévoir l'envoie à chaque particiapnt du livre de CISS au moins un mois avant la formation.

Raphael B. — Bonjour, Merci beaucoup pour cette formation IC2 ! Ce fut passionnant, captivé pendant une semaine entière, bravo au formateur ! Le support de présentation était très clair et…

Votre formateur

Aurelie B. — Formateur
Aurelie intervient notamment sur les outils de pilotage et collaboratifs, ainsi que sur la gestion de projet et les certifications associées. La conception de supports pédagogiques fait également partie de…

Ils nous font confiance

Cette année notre filière Gouvernance, Risques & Conformité (GRC) a accompagné plus de 6 entreprises dont :

ALSTOM AXA ASSISTANCE FRANCE GLOBAL BEAUTY TECH L'ORÉAL - CORPORATE FINANCE AND LEGAL SALVIA DEVELOPPEMENT TESSI DIGITAL SERVICES

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.

Qualiopi processus certifié — RÉPUBLIQUE FRANÇAISE

ecovadis SILVER | Top 15% Sustainability Rating JAN 2026

Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800
demande@sparks-formation.com