Formation : CCSP - Certified Cloud Security Professional, préparation à la certification ISC2

Formation pratique - 5j - 35h00 - Réf. CCN
Prix : 4040 CHF H.T.

Nouvelle édition

Cette formation CCSP Certified Cloud Security Professional vous permet de gérer tous les risques induits par les services cloud computing en termes de sécurité de l'information.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Obtenir une vision pointue des offres de cloud computing
- Appréhender précisément tous les risques induits par ces services en ce qui concerne la sécurité de l'information
- Connaître l'ensemble des aspects légaux et de conformité (juridique, niveaux de service, audit, standards...)
- Comprendre la sécurité des plateformes et infrastructures de cloud computing
- Comprendre la sécurité des applications
- Comprendre la sécurité des opérations
- Savoir répondre efficacement à un incident de sécurité cloud

Public concerné

Responsables sécurité des systèmes d'Information, consultants en sécurité des systèmes d'information.

Prérequis

A
voir lu le CBK ("Official ISC2
Guide to the CCSP CBK" -
Sybex
).

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

PARTICIPANTS

Responsables sécurité des systèmes d'Information, consultants en sécurité des systèmes d'information.

PRÉREQUIS

A
voir lu le CBK ("Official ISC2
Guide to the CCSP CBK" -
Sybex
).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Certification

Pour passer la certification, vous devez vous inscrire sur le site de l'ISC2 et déposer un dossier d'éligibilité (justifier de 5 années d'expérience professionnelle en technologies de l'information).

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Domaine 1 - exigences et concepts en matière de conception en architecture cloud computing

- Les concepts du cloud computing.
- Les architectures de référence du cloud computing.
- Les concepts de sécurité associés au cloud computing.
- Les principes de conception de sécurité du cloud computing.
- L'identification des services de cloud computing de confiance.

2 Domaine 2 - la sécurité des données dans le cloud computing

- Le cycle de vie des données du cloud computing.
- Conception et déploiement des architectures de stockage en cloud computing.
- Conception et application des stratégies de sécurité des données.
- Connaissances et déploiement des technologies de classification et de découverte des données.
- Conception des exigences légales de sécurité des données concernant l'identification des informations personnelles.
- Conception et déploiement du Data Rights Management.
- Planification et mise en œuvre des politiques de rétention, de suppression et d'archivage des données.
- Conception et déploiement des démarches d'audit, de détection et de démontrabilité.

3 Domaine 3 - la sécurité des infrastructures et des plateformes de cloud computing

- Les composants de l'infrastructure du cloud computing.
- Évaluation des risques de l'infrastructure du cloud computing.
- Conception et planification des contrôles de sécurité.
- Conception et déploiement de plan de reprise et de continuité des services et des métiers.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

4 Domaine 4 - la sécurité des applications de cloud computing

- Formation et sensibilisation de la sécurité autour des services du cloud computing.
- Validation et assurance des solutions logicielles du cloud computing.
- Utilisation des logiciels vérifiés, approbation des API.
- SDLS : cycle de vie du développement de la sécurité logicielle.
- Les architectures applicatives du cloud computing.
- Conception et déploiement d'une solution d'IAM (Identity & Access Management).

5 Domaine 5 - gestion des opérations

- Planification des processus de conception du data center.
- Développement et mise en œuvre d'une infrastructure physique du cloud.
- Gestion opérationnelle et maintenance d'une infrastructure physique de cloud computing.
- Conception, maintenance et gestion d'une infrastructure logique de cloud computing.
- Conformité avec les normes de type ISO 20000-1 ou des référentiels comme ITIL.
- Évaluation des risques d'une infrastructure logique et physique du cloud computing.
- Collecte et conservation des preuves numériques (forensic).
- Communication avec les parties prenantes.

6 Domaine 6 - les exigences légales et la conformité

- Risques et exigences légales d'un environnement de cloud computing.
- La gestion de la vie privée, diversité des exigences légales en fonction des pays.
- Méthodes et processus d'audit d'un environnement de cloud computing.
- La gestion des risques au niveau de l'entreprise d'un écosystème cloud computing.
- Conception et gestion des contrats, notamment dans le cadre d'une démarche d'externalisation.
- Gestion des fournisseurs du cloud computing.

Dates et lieux

CLASSE À DISTANCE
2026 : 8 juin, 21 sep., 30 nov.