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

Mis à jour le 16/09/2024

S'inscrire

Formation Préparation à la Certification CISMP

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

3 jours (21 heures)

Présentation

Notre préparation à la certification CISMP (Certified Information Security Management Principles) vous aidera à fournir une base solide sur les principes de sécurité informatique, couvrant des aspects techniques et managériaux pour une gestion efficace des risques liés à la sécurité.

Le programme de formation CISMP vous initiera aux concepts clés de la sécurité de l'information tels que la gestion des risques, les cadres de contrôle ou la législation et conformité. Vous apprendrez également à identifier, atténuer et évaluer les risques dans un environnement professionnel.

La préparation couvre d'autres concepts comme la continuité des activités, la réponse aux incidents et la gestion des fournisseurs tiers. Cette approche inclut la compréhension de l'infrastructure réseau, les mesures de contrôle d'accès et la protection des données sensibles.

Grâce à CISMP, vous pourrez maîtriser les meilleures pratiques de gestion de la sécurité de l'information, vous développerez des compétences en audit des incidents et vous comprendrez comment assurer la sécurité tout en respectant les exigences légales et réglementaires d'une organisation.

Comme pour toutes nos formations, celle-ci vous présentera les toutes dernières nouveautés concernant CISMP.

Objectifs

- Comprendre les principes fondamentaux de la sécurité de l'information
- Identifier et gérer les risques liés aux systèmes d'information
- Appliquer un cadre de sécurité adapté aux organisations

- Mettre en œuvre des contrôles de sécurité technique et humaine
- Élaborer des plans de continuité et de reprise après sinistre

Public visé

- **Analystes cybersécurité**
- Responsables de la sécurité informatique
- Professionnels IT

Pré-requis

Compréhension général des systèmes d'information et des concepts de gestion des risques.

Note : Ambient IT n’est pas propriétaire de CISMP, cette certification appartient à BCS The Chartered Institute for IT.

PROGRAMME DE NOTRE FORMATION CISMP

LES PRINCIPES DE LA SÉCURITÉ DE L'INFORMATION

- Concepts et définitions
- Nécessité et avantages de la sécurité de l'information
- Exemples de questions

RISQUES LIÉS À L'INFORMATION

- Menaces et vulnérabilités des systèmes d'information
- La gestion des risques
- Exemples de questions
- Références et lectures complémentaires

CADRE DE LA SÉCURITÉ DE L'INFORMATION

- Organisation et responsabilités
- Politique, normes et procédures de l'organisation
- Gouvernance de la sécurité de l'information
- Mise en œuvre du programme d'assurance de l'information
- Gestion des incidents de sécurité
- Cadre juridique
- Normes et procédures de sécurité
- Exemples de questions
- Références

CYCLES DE VIE DE LA SÉCURITÉ

- Le cycle de vie de l'information
- Test, audit et révision
- Développement et support des systèmes

CONTRÔLES DE LA SÉCURITÉ DES PROCÉDURES ET DES PERSONNES

- Contrôles généraux
- Sécurité des personnes
- Contrôles d'accès des utilisateurs
- Formation et sensibilisation

CONTRÔLES DE SÉCURITÉ TECHNIQUE

- Sécurité technique
- Protection contre les logiciels malveillants
- Réseaux et communications
- Technologie opérationnelle
- Services externes
- Informatique en nuage
- Infrastructure informatique
- Exemples de questions

SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

- Sécurité physique
- Différentes utilisations des contrôles
- Exemples de questions

GESTION DE LA REPRISE APRÈS SINISTRE ET DE LA CONTINUITÉ DES ACTIVITÉS

- Relation entre la reprise après sinistre et la gestion de la continuité des activités, l'évaluation des risques et l'analyse d'impact
- Résilience et redondance
- Approches de la rédaction et de la mise en œuvre des plans
- Nécessité d'une documentation, d'une maintenance et de tests
- Nécessité d'établir des liens avec la fourniture de services gérés et l'externalisation
- Nécessité d'un stockage hors site sécurisé du matériel vital
- Nécessité d'impliquer le personnel, les fournisseurs et les prestataires de systèmes informatiques
- Relation avec la gestion des incidents de sécurité
- Conformité avec les normes
- Exemples de questions

AUTRES ASPECTS TECHNIQUES

- Enquêtes et criminalistique
- Rôle de la cryptographie
- Renseignements sur les menaces
- Conclusion

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.