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

Mis à jour le 01/03/2024

S'inscrire

Formation Préparation à la Certification CISM©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Devenez expert en analyse et gestion des risques grâce à notre formation CISM© (Certified Information Security Manager). Nous vous enseignerons chaque domaine pour que vous soyez préparés au mieux lors de l'examen.

En effet, nous reviendrons sur les quatre grands concepts évalués. Tout d'abord, la gouvernance en cybersécurité, comprendre le rôle de la gouvernance et les normes régissant la sécurité de l'information.

Ensuite, la gestion des risques, pour savoir comment évaluer les potentielles menaces et s'assurer d'un bon processus de surveillance. Nous poursuivrons avec le programme de sécurité qui explique les différentes composantes de la cybersécurité. Vous apprendrez à créer des mesures et des procédures pour protéger votre organisation.

Enfin, la dernière partie concerne la gestion des incidents, comment les catégoriser et gérer les opérations suite à un sinistre.

Objectifs

- Acquérir les connaissances nécessaires à la réussite de l’examen CISM©
- Comprendre les pratiques de gestion des risques liés à la sécurité informatique
- Pouvoir mettre en place les procédures nécessaires en réponse à un incident

Public visé

- DSI

- RSSI
- Informaticien
- Responsable de la continuité d'activité
- Ingénieur
- Auditeur
- Consultant en cybersécurité

Pré-requis

- Prouver 5 ans d'expérience professionnelle en gestion de la sécurité de l'information
- Connaissances de base des normes en audit
- Connaissances en continuité des activités
- Compréhension de l’anglais technique

Note : Ambient IT n’est pas propriétaire de CISM©, cette certification appartient à ISACA©.

Programme de la Préparation à la Certification CISM©

Domaine 1 - Gouvernance de la sécurité informatique

- Décrire le rôle de la gouvernance dans la création de valeur pour l'entreprise
- Expliquer l'importance de la gouvernance de la sécurité de l'information dans le contexte de la gouvernance globale de l'entreprise
- Décrire l'influence de la direction, de la structure et de la culture de l'entreprise sur l'efficacité d'une stratégie de sécurité de l'information
- Identifier les exigences légales, réglementaires et contractuelles pertinentes qui ont un impact sur l'entreprise
- Décrire les effets de la stratégie de sécurité de l'information sur la gestion des risques de l'entreprise
- Évaluer les cadres et les normes communes utilisées pour régir une stratégie de sécurité de l'information
- Expliquer pourquoi les mesures sont essentielles dans le développement et l'évaluation de la stratégie de sécurité de l'information

Domaine 2 - Gestion des risques liés à la sécurité informatique

- Appliquer des stratégies d'évaluation des risques pour réduire l'impact des risques liés à la sécurité de l'information
- Évaluer les types de menaces auxquelles l'entreprise est confrontée
- Expliquer comment les référentiels de contrôle de sécurité affectent l'analyse des vulnérabilités et des déficiences de contrôle
- Différencier l'application des types de traitements des risques du point de vue de la sécurité de l'information
- Décrire l'influence de la propriété des risques et des contrôles sur le programme de sécurité de l'information
- Décrire le processus de surveillance et de déclaration des risques liés à la sécurité de l'information

Domaine 3 - Programme de sécurité informatique

- Décrire les composantes et les ressources utilisées pour élaborer un programme de sécurité de l'information
- Distinguer les normes et les cadres communs des SI disponibles pour construire un programme de sécurité de l'information
- Expliquer comment aligner les politiques, procédures et lignes directrices en matière de SI sur les besoins de l'entreprise
- Décrire le processus de définition d'une feuille de route pour le programme de sécurité de l'information
- Décrire les mesures clés du programme de sécurité de l'information utilisées pour suivre les progrès et en rendre compte à la direction générale
- Expliquer comment gérer le programme SI à l'aide de contrôle
- Créer une stratégie pour améliorer la sensibilisation et la connaissance du programme de sécurité de l'information
- Décrire le processus d'intégration du programme de sécurité avec les opérations informatiques et les fournisseurs tiers
- Communiquer les informations clés du programme de sécurité de l'information aux parties prenantes concernées

Domaine 4 - Gestion des incidents

- Faire la distinction entre la gestion des incidents et la réponse aux incidents
- Décrire les exigences et les procédures nécessaires à l'élaboration d'un plan de réponse aux incidents
- Identifier les techniques utilisées pour classer ou catégoriser les incidents
- Décrire les types de rôles et de responsabilités nécessaires à une équipe efficace de gestion et de réponse aux incidents
- Distinguer les types d'outils et de technologies de gestion des incidents dont dispose une entreprise
- Décrire les processus et les méthodes utilisés pour enquêter sur un incident, l'évaluer et le contenir
- Identifier les types de communication et de notification utilisés pour informer les principales parties prenantes des incidents et des tests
- Décrire les processus et les procédures utilisés pour éradiquer les incidents et y remédier
- Décrire les exigences et les avantages de la documentation des événements
- Expliquer la relation entre l'impact sur les activités, la continuité et la réponse aux incidents
- Décrire les processus et les résultats liés à la reprise après sinistre
- Expliquer l'impact des mesures et des tests lors de l'évaluation du plan de réponse aux incidents

Stratégies et astuces pour réussir l'examen

Examen blanc

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.