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

Mis à jour le 11/04/2024

S'inscrire

Formation Préparation à la Certification CISA©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Devenez auditeur en informatique certifié grâce à notre formation CISA© (Certified Information Systems Auditor). Nous vous enseignerons chaque domaine pour que vous soyez préparés au mieux durant l'examen.

Nous reviendrons sur les cinq grands concepts évalués. En premier lieu, le processus d'audit du système d'information, ce chapitre essentiel pour réaliser de bout en bout des audits fiables. Par la suite, vous découvrirez la gestion et la gouvernance informatique.

Une partie où vous apprendrez à définir et à suivre des indicateurs clés afin de garantir le respect des politiques sécuritaires. L'acquisition, le développement et l'implémentation des systèmes d'information vous présentera comment renforcer la clarté des informations à toutes les étapes du cycle de vie IT.

Ensuite, vient le domaine de la résilience, vous découvrirez comment évaluer la pérennité d'une organisation en analysant ses données et les opérations IT. Enfin, vous renforcerez vos compétences en protection des actifs informatiques via différentes méthodes.

Objectifs

- Acquérir les connaissances nécessaires à la réussite de l’examen CISA©
- Maîtriser les compétences d'un auditeur du système informatique
- Connaître les procédures nécessaires pour la protection du patrimoine informatique

Public visé

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

Pré-requis

Au moins 5 ans d'expérience dans l'audit, le contrôle, l'assurance ou la sécurité IS / IT.

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

Programme de la Préparation à la Certification CISA©

Domaine 1 - Processus d'audit des systèmes d'information

- Planifier un audit pour déterminer si les systèmes d'information sont protégés, contrôlés et s'ils apportent une valeur ajoutée à l'organisation
- Réaliser un audit conformément aux normes d'audit des systèmes d'information et à une stratégie d'audit des systèmes d'information basée sur les risques
- Communiquer aux parties prenantes l'état d'avancement de l'audit, les constatations, les résultats et les recommandations
- Effectuer un suivi de l'audit afin d'évaluer si les risques ont été suffisamment pris en compte
- Évaluer la gestion informatique et la surveillance des contrôles
- Utiliser des outils d'analyse de données pour rationaliser les processus d'audit
- Fournir des services de conseil et des orientations à l'organisation afin d'améliorer la qualité et le contrôle des systèmes d'information
- Identifier les possibilités d'amélioration des processus dans les politiques et pratiques informatiques de l'organisation

Domaine 2 - Gouvernance et gestion des technologies de l'information

- Évaluer l'alignement de la stratégie informatique sur les stratégies et les objectifs de l'organisation
- Évaluer l'efficacité de la structure de gouvernance informatique et de la structure organisationnelle informatique
- Évaluer la gestion des politiques et des pratiques informatiques de l'organisation
- Évaluer la conformité des politiques et pratiques informatiques de l'organisation avec les exigences réglementaires et légales
- Évaluer la gestion des ressources et des portefeuilles informatiques en vue de leur alignement sur les stratégies et les objectifs de l'organisation
- Évaluer les politiques et pratiques de gestion des risques de l'organisation
- Évaluer la gestion informatique et le suivi des contrôles
- Évaluer le suivi et le reporting des indicateurs clés de performance (KPI) informatiques
- Évaluer si la sélection et la contractualisation des fournisseurs informatiques
- Évaluer si les processus de sélection des fournisseurs informatiques et de gestion des contrats sont conformes aux exigences de l'entreprise

- Déterminer si les pratiques de gestion des services informatiques sont conformes aux exigences de l'entreprise
- Procéder à un examen périodique des systèmes d'information et de l'architecture d'entreprise
- Évaluer les politiques et les pratiques de gouvernance des données
- Évaluer le programme de sécurité de l'information pour déterminer son efficacité et son alignement sur les stratégies et les objectifs de l'organisation
- Évaluer les opportunités et les menaces potentielles liées aux technologies émergentes, aux réglementations et aux pratiques sectorielles

Domaine 3 - Acquisition, développement et mise en œuvre des systèmes d'information

- Évaluer si l'analyse de rentabilité des changements proposés pour les systèmes d'information répond aux objectifs de l'entreprise
- Évaluer les politiques et les pratiques de l'organisation en matière de gestion de projet
- Évaluer les contrôles à tous les stades du cycle de développement des systèmes d'information
- Évaluer l'état de préparation des systèmes d'information en vue de leur mise en œuvre et de leur migration vers la production
- Procéder à un examen des systèmes après leur mise en œuvre afin de déterminer si les produits livrables, les contrôles et les exigences du projet ont été respectés
- Évaluer les politiques et les pratiques de gestion des changements, des configurations, des versions et des correctifs

Domaine 4 - Exploitation des systèmes d'information et résilience de l'entreprise

- Évaluer la capacité de l'organisation à poursuivre ses activités
- Évaluer si les pratiques de gestion des services informatiques sont conformes aux exigences de l'entreprise
- Procéder à un examen périodique des systèmes d'information et de l'architecture de l'entreprise
- Évaluer les opérations informatiques pour déterminer si elles sont contrôlées efficacement et si elles continuent à soutenir les objectifs de l'organisation
- Évaluer les pratiques de maintenance informatique pour déterminer si elles sont contrôlées efficacement et si elles continuent à soutenir les objectifs de l'organisation
- Évaluer les pratiques de gestion des bases de données
- Évaluer les politiques et les pratiques de gouvernance des données
- Évaluer les politiques et les pratiques de gestion des problèmes et des incidents
- Évaluer les politiques et les pratiques de gestion des changements, des configurations, des versions et des correctifs
- Évaluer l'informatique des utilisateurs finaux afin de déterminer si les processus sont contrôlés de manière efficace

Domaine 5 - Protection du patrimoine informatique

- Réaliser l'audit conformément aux normes d'audit des systèmes d'information et à une stratégie d'audit des systèmes d'information fondée sur les risques
- Évaluer les politiques et les pratiques de gestion des problèmes et des incidents
- Évaluer les politiques et pratiques de l'organisation en matière de sécurité de l'information et de protection de la vie privée

- Évaluer les contrôles physiques et environnementaux afin de déterminer si les actifs informationnels sont correctement protégés
- Évaluer les contrôles de sécurité logiques pour vérifier la confidentialité, l'intégrité et la disponibilité des informations
- Évaluer les pratiques de classification des données pour s'assurer qu'elles sont conformes aux politiques de l'organisation et aux exigences externes applicables
- Évaluer les politiques et les pratiques liées à la gestion du cycle de vie des actifs
- Évaluer le programme de sécurité de l'information pour déterminer son efficacité et sa conformité avec les stratégies et les objectifs de l'organisation
- Effectuer des tests de sécurité technique afin d'identifier les menaces et les vulnérabilités potentielles
- Évaluer les opportunités et les menaces potentielles liées aux technologies émergentes, aux réglementations et aux pratiques du secteur

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.