CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

Aperçu de l'Examen de Certification

Date Effective : 1er Mai 2021

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

À propos de CISSP

Certified Information Systems Security Professional (CISSP) est la certification la plus reconnue mondialement sur le marché de la sécurité informatique. CISSP valide les connaissances et l'expérience de gestion et techniques approfondies d'un professionnel de la sécurité informatique pour concevoir, construire et gérer efficacement la posture générale de sécurité d'une organisation.

La large gamme de sujets inclus dans le Corps Commun de Connaissances (CBK®) de CISSP garantit sa pertinence dans toutes les disciplines du domaine de la sécurité informatique. Les candidats retenus sont compétents dans les huit domaines suivants :

- Gestion du Risque et de la Sécurité
- Sécurité des Biens
- Architecture et Ingénierie de la Sécurité
- Sécurité des Réseaux et de la Communication
- Gestion des Identités et des Accés (IAM)
- Évaluation et Tests de Sécurité
- Operations de Sécurité
- Sécurité du Développement Logiciel

Exigences d'Expérience

Les candidats doivent avoir un minimum de cinq ans d'expérience cumulée de travail rémunéré dans au moins deux des huit domaines du CBK de CISSP. Obtenir un diplôme universitaire de quatre ans ou l'équivalent régional ou un diplôme supplémentaire de la liste approuvée de (ISC)² remplira un an d'expérience requise. Le crédit d'études ne remplira qu'une année d'expérience.

Un candidat n'ayant pas l'expérience requise pour devenir un CISSP peut devenir un Associé de (ISC)² en passant avec succès l'examen CISSP. L'Associé de (ISC)² aura alors six ans pour obtenir les cinq ans d'expérience nécessaires. Vous pouvez en savoir plus sur les exigences en matière d'expérience CISSP et sur la façon de comptabiliser le travail à temps partiel et les stages à www.isc2.org/Certifications/CISSP/experience-requirements.

Accréditation

CISSP a été le premier diplôme dans le domaine de la sécurité informatique à répondre aux exigences strictes de la Norme ANSI/ISO/IEC 17024.

Analyse des Tâches du Poste (JTA)

(ISC)² a une obligation pour ses membres de maintenir la pertinence de CISSP. Conduite à intervalles réguliers, l'Analyse des Tâches du Poste (JTA) est un processus méthodique et critique de détermination des tâches effectuées par des professionnels de la sécurité exerçant la profession définie par CISSP. Les résultats de la JTA sont utilisés pour mettre à jour l'examen. Ce processus garantit que les candidats sont testés sur les sujets correspondants aux rôles et responsabilités des professionnels de la sécurité informatique en exercice aujourd'hui.

Informations sur l'Examen CAT de CISSP

L'examen CISSP utilise le Test Adapatif Informatisé (CAT) pour tous les examens en anglais. Les examens CISSP dans toutes les autres langues sont administrés sous forme d'examens linéaires de forme fixe. Vous pouvez en apprendre plus sur le CAT de CISSP à www.isc2.org/certificatons/CISSP-CAT.

Durée de l'examen	3 heures
Nombre d'éléments	100 - 150
Format de l'élément	Questions à choix multiple et de technologie avancée
Note de passage	700 points sur 1000
Disponibilité de la langue d'examen	Anglais
Centre de test	Centres de Test Pearson VUE PPC et PVTC Select Autorisés par (ISC)²

Pondérations de l'Examen CAT de CISSP

Domaines	Pondération Moyenne
1. Gestion du Risque et de la Sécurité	15 %
2. Sécurité des Biens	10 %
3. Architecture et Ingénierie de la Sécurité	13 %
4. Sécurité des Réseaux et de la Communication	13 %
5. Gestion des Identités et des Accés (IAM)	13 %
6. Évaluation et Tests de Sécurité	12 %
7. Operations de Sécurité	13 %
8. Sécurité du Développement Logiciel	11 %
Total :	**100 %**

Informations sur l'Examen Linéaire de CISSP

Durée de l'examen	6 heures
Nombre d'éléments	250
Format de l'élément	Questions à choix multiple et de technologie avancée
Note de passage	700 points sur 1000
Disponibilité de la langue d'examen	Français, Allemand, Portugais (Brésil), Espagnol moderne, Japonais, Chinois Simplifié, Coréen
Centre de test	Centres de Test Pearson VUE PPC et PVTC Select Autorisés par (ISC)²

Pondérations sur l'Examen Linéaire de CISSP

Domaines	Pondérations
1. Gestion du Risque et de la Sécurité	15 %
2. Sécurité des Biens	10 %
3. Architecture et Ingénierie de la Sécurité	13 %
4. Sécurité des Réseaux et de la Communication	13 %
5. Gestion des Identités et des Accés (IAM)	13 %
6. Évaluation et Tests de Sécurité	12 %
7. Operations de Sécurité	13 %
8. Sécurité du Développement Logiciel	11 %
Total :	**100 %**

Domaine 1 : Gestion du Risque et de la Sécurité

1.1 Comprendre, adhèrer et promouvoir l'éthique professionnelle

- Code d'Éthique Professionnelle de (ISC)²
- Code d'éthique organisationnelle

1.2 Comprendre et appliquer les concepts de sécurité

- Confidentialité, intégrité et disponibilité, authenticité et non-répudiation

1.3 Évaluer et appliquer les principes de gouvernance de sécurité

- Alignement de la fonction de sécurité sur la stratégie commerciale, les buts, la mission et les objectifs
- Processus organisationnels (p.ex., acquisitions, désinvestissements, comités de gouvernance)
- Rôles et responsabilités organisationnelles
- Cadres de contrôle de la sécurité
- Attention nécessaire / diligence nécessaire

1.4 Déterminer la conformité et les autres exigences

- Normes contractuelles, légales, industrielles et exigences réglementaires
- Exigences de confidentialité

1.5 Comprendre les problèmes juridiques et réglementaires relatifs à la sécurité informatique dans un contexte holistique

- Cybercrimes et fuites des données
- Exigences en matière de Licences et de Propriété Intellectuelle (IP)
- Contrôles d'importation / exportation
- Flux de données transfrontalier
- Confidentialité

1.6 Comprendre les exigences relatives aux types d'enquêtes (c.-à-d., les normes administratives, criminelles, civiles, réglementaires, industrielles)

1.7 Développer, documenter et mettre en œuvre une politique, des normes, des procédures et des directives de sécurité

1.8 Identifier, analyser et hiérarchiser les exigences de Continuité Commerciale (BC)

- Analyse d'Impact sur les Entreprises (BIA)
- Développer et documenter la portée et le plan

1.9 Contribuer et appliquer les politiques et les procédures de sécurité du personnel

- Sélection et recrutement des candidats
- Contrats d'embauche et politiques d'emploi
- Processus d'intégration, de transferts et de résiliation
- Accords et contrôles entre fournisseurs, consultants et contractuels
- Exigences de politique de conformité
- Exigences de politique de confidentialité

1.10 Comprendre et appliquer les concepts de gestion du risque

- Identifier les menaces et les vulnérabilités
- Évaluation / analyse des risques
- Réponse au risque
- Sélection et mise en œuvre des contre-mesures
- Types de contrôles applicables (p.ex., préventif, de détection, correctif)
- Évaluations de contrôle (sécurité et confidentialité)
- Surveillance et mesure
- Rapport
- Amélioration continue (p.ex., Modélisation de la maturité des risques)
- Cadres de risque

1.11 Comprendre et appliquer les concepts et méthodologies de modélisation des menaces

1.12 Appliquer les concepts de Gestion des Risques de la Chaîne d'Approvisionnement (SCRM)

- Risques associés au matériel, aux logiciels, et aux services
- Évaluation et surveillance par des tiers
- Exigences minimales de sécurité
- Exigences de niveau de service

1.13 Établir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

- Méthodes et techniques de sensibilisation et de formation (p.ex., ingénierie sociale, phishing, champions de la sécurité, ludification)
- Révisions périodiques du contenu
- Évaluation de l'efficacité du programme

Domaine 2 : Sécurité des Biens

2.1 Identifier et classer les informations et les biens

- Classification des données
- Classification des biens

2.2 Établir les exigences de traitement de l'information et des biens

2.3 Provisionner les ressources en toute sécurité

- Informations et propriété des biens
- Inventaire des biens (p.ex., tangibles, intangibles)
- Gestion des biens

2.4 Gérer la durée de vie des données

- Rôles des données (c.-à-d., propriétaires, contrôleurs, gardiens, sous-traitants, utilisateurs / sujets)
- Collecte des données
- Emplacement des données
- Maintenance des données
- Conservation des données
- Rémanence des données
- Destruction des données

2.5 Garantir une rétention appropriée des biens (p.ex., End-of-Life (EOL), End-of-Support (EOS))

2.6 Déterminer les exigences en terme de contrôle et de conformité de la sécurité des données

- États des données (p.ex., en cours d'utilisation, en transit, au repos)
- Cadrage et adaptation
- Sélection des normes
- Méthodes de protection des données (p.ex., Gestion des Droits Numériques (DRM), Prévention contre la Fuite d'Information (DLP), Cloud Access Security Broker (CASB))

Domaine 3 : Architecture et Ingénierie de la Sécurité

3.1 Rechercher, mettre en œuvre et gérer des processus d'ingénierie en utilisant des principes de conception sécurisée

- Modélisation de menaces
- Moindre privilège
- Défense en profondeur
- Défauts sécurisés
- Défaillance en toute sécurité
- Séparation des Fonctions (SoD)
- Keep it simple
- Zéro Trust
- Vie privée dès la conception
- Faire confiance mais vérifier
- Responsabilité partagée

3.2 Comprendre les concepts fondamentaux des modèles de sécurité (p.ex., Biba, Star Model, Bell-LaPadula)

3.3 Sélectionner les contrôles en fonction des exigences de sécurité des systèmes

3.4 Comprendre les capacités de sécurité des Systèmes Informatiques (IS) (p.ex., protection de la mémoire, Trusted Platform Module (TPM), cryptage / décryptage)

3.5 Évaluer et atténuer les vulnérabilités des architectures, des conceptions et des éléments de solution de la sécurité

- Systèmes basés sur client
- Systèmes basés sur serveur
- Systèmes de base de données
- Systèmes cryptographiques
- Systèmes de Contrôle Industriel (ICS)
- Systèmes basés sur Cloud (p.ex., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Systèmes distribués
- Internet des objets (IoT)
- Microservices
- Conteneurisation
- Sans serveur
- Systèmes embarqués
- Systèmes de Calcul de Haute Performance (HPC)
- Systèmes d'edge computing
- Systèmes virtualisés

3.6 Sélectionner et déterminer des solutions cryptographiques

- Cycle de vie cryptographique (p.ex., clés, sélection d'algorithmes)
- Méthodes cryptographiques (p.ex., courbes symétriques, asymétriques, elliptiques, quantiques)
- Infrastructure à Clé Publique (PKI)
- Pratiques principales de gestion
- Signatures numériques et certificats numériques
- Non-répudiation
- Integrité (p.ex., hachage)

3.7 Comprendre les méthodes attaques cryptanalytiques

- Force brute
- Chiffre-texte uniquement
- Plain-texte connu
- Analyse de la fréquence
- Chiffre-texte choisi
- Attaques de la mise en œuvre
- Canal auxiliaire
- Injection de fautes
- Timing
- Attaques de l'Homme du Milieu
- Pass the hash
- Exploitation Kerberos
- Ransomware

3.8 Appliquer les principes de sécurité à la conception du site et des infrastructures

3.9 Concevoir les contrôles de sécurité du site et des infrastructures

- Armoires de câblage / installations de distribution intermédiaires
- Salles de serveurs / centres de données
- Installations de stockage média
- Stockage de preuves
- Sécurité des zones restreintes et de travail
- Services Publics et Chauffage, Ventilation et Climatisation (HVAC)
- Problèmes Environnementaux
- Prévention, détection et suppresion des incendies
- Alimentation (p.ex., redondante, de secours)

Domaine 4 : Sécurité des Réseaux et de la Communication

4.1 Évaluer et mettre en œuvre les principes de conception sécurisée dans les architectures de réseau

- Modèles Interconnexion de Système Ouvert (OSI) et Protocole de Contrôle de Transmission / Protocole Internet (TCP / IP)
- Réseautage de Protocole Internet (IP) (p.ex., Sécurité du Protocole Internet (IPSec), Protocole Internet (IP) v4/6)
- Protocoles sécurisés
- Implications des protocoles multicouches
- Protocoles Convergés (p.ex., Fiber Channel Over Ethernet (FCoE), Interface Internet pour Petit Ordinateur (iSCSI), Voice over Internet Protocol (VoIP))
- Microsegmentation (p.ex., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
- Réseaux sans fil (p.ex., Li-Fi, Wi-Fi, Zigbee, satellite)
- Réseaux cellulaires (p.ex., 4G, 5G)
- Réseaux de Distribution de Contenu (CDN)

4.2 Sécuriser les composants réseau

- Fonctionnement du matériel (p.ex, alimentation redondante, garantie, assistance)
- Médias de transmission
- Appareils de Contrôle d'Accès au Réseau (NAC)
- Sécurité des points d'extrémité

4.3 Mettre en œuvre des canaux de communication sécurisés selon la conception

- Voix
- Collaboration multimédia
- Accès à distance
- Communications des données
- Réseaux virtualisés
- Connectivité des tiers

Domaine 5 : Gestion des Identités et des Accés (IAM)

5.1 Contrôler l'accès physique et logique aux biens

- Information
- Systèmes
- Appareils
- Infrastructures
- Applications

5.2 Gérer l'identification et l'authentification des personnes, des appareils et des services

- Mise en œuvre de la Gestion des Identités (IdM)
- Authentification Unique / Multi-Facteur (MFA)
- Responsabilité
- Gestion de la session
- Enregistrement, vérification et établissement de l'identité
- Gestion des Identités Fédérées (FIM)
- Systèmes de gestion des identifiants
- Authentification Unique (SSO)
- Juste-À-Temps (JIT)

5.3 Identité fédérée avec un service tiers

- Sur place
- Cloud
- Hybride

5.4 Mettre en œuvre et gérer les mécanismes d'autorisation

- Contrôle d'Accès Basé sur Rôle (RBAC)
- Contrôle d'accès basé sur règle
- Contrôle d'Accès Obligatoire (MAC)
- Contrôle d'Accès Discrétionnaire (DAC)
- Contrôle d'Accès Basé sur Attribut (ABAC)
- Contrôle d'accès basé sur risque

5.5 Gérer le cycle de vie de l'approvisionnement des identités et des accès

- Revue d'accès au compte (p.ex., utilisateur, système, service)
- Approvisionnement et deprovisioning (p.ex., embarquement on / off et transferts)
- Définition de rôle (p.ex., personnes affectées à de nouveaux rôles)
- Augmentation des privilèges (p.ex., comptes de service gérés, utilisation de sudo, minimisation de son utilisation)

5.6 Mettre en œuvre les systèmes d'authentification

- OpenID Connect (OIDC) / Open Authorization (Oauth)
- Security Assertion Markup Language (SAML)
- Kerberos
- Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access Control System Plus (TACACS+)

Domaine 6 : Évaluation et Tests de Sécurité

6.1 Concevoir et valider des stratégies d'évaluation, de test et d'audit

- Interne
- Externe
- Tiers

6.2 Conduire des tests de contrôle de sécurité

- Évaluation des vulnérabilités
- Tests de pénétration
- Révisions du journal
- Transactions synthétiques
- Révision et test du code
- Test de cas d'utilisation abusive
- Analyse de la couverture des tests
- Tests de l'interface
- Simulations d'une attaque Breach
- Contrôles de conformité

6.3 Recueillir des données de processus de sécurité (p.ex., techniques et administratives)

- Gestion des comptes
- Révision et approbation de la gestion
- Indicateurs clés de performance et de risque
- Sauvegarde des données de vérification
- Formation et sensibilisation
- Reprise après Sinistre (DR) et Continuité Commerciale (BC)

6.4 Analyser la sortie de test et générer un rapport

- Remédiation
- Traitement des exceptions
- Divulgation éthique

6.5 Conduire ou faciliter des audits de sécurité

- Interne
- Externe
- Tiers

Domaine 7 : Operations de Sécurité

7.1 Comprendre et se conformer aux instructions

- Collecte et traitement des preuves
- Rapports et documentation
- Techniques d'investigation
- Outils, tactiques et procédures de criminalistique numérique
- Artefacts (p.ex., ordinateur, réseau, appareil mobile)

7.2 Conduire des activités de journalisation et de surveillance

- Détection et prévention d'intrusion
- Gestion des Informations et des Événements de Sécurité (SIEM)
- Surveillance continue
- Surveillance de sortie
- Gestion du journal
- Renseignements sur les menaces (p.ex., flux de menaces, chasse aux menaces)
- Analyse Comportementale de l'Utilisateur et de l'Entité (UEBA)

7.3 Effectuer la gestion de la configuration (CM) (p.ex., approvisionnement, base de référence, automatisation)

7.4 Appliquer les concepts d'opérations de sécurité de base

- Besoin de savoir / moindre privilège
- Séparation des Fonctions (SoD) et responsibilités
- Gestion des comptes privilégiés
- Rotation des postes
- Accord sur la Qualité de Service (SLA)

7.5 Appliquer la protection des ressources

- Gestion des médias
- Techniques de protection des médias

7.6 Conduire la gestion des incidents

- Détection
- Réponse
- Atténuation
- Rapport
- Récupération
- Remédiation
- Leçons apprises

7.7 Faire fonctionner et maintenir des mesures de détection et de prévention

- Pare-feu (p.ex., nouvelle génération, application Web, réseau)
- Systèmes de Détection d'Intrusion (IDS) et Systèmes de Prévention d'Intrusion (IPS)
- Liste blanche / liste noire
- Services de sécurité fournis par des tiers
- Bac à sable
- Honeypots / honeynets
- Anti-malware
- Outils basés sur l'apprentissage machine et l'Intelligence Artificielle (IA)

7.8 Mettre en œuvre et prendre en charge la gestion des correctifs et des vulnérabilités

7.9 Comprendre et participer aux processus de gestion du changement

7.10 Mettre en œuvre des stratégies de récupération

- Stratégies de stockage de sauvegarde
- Stratégies de site de récupération
- Sites de traitement multiple
- Résilience du système, Haute Disponibilité (HA), Qualité de Service (QoS) et tolérance aux pannes

7.11 Mettre en œuvre des processus de Reprise après Sinistre (DR)

- Réponse
- Personnel
- Communications
- Évaluation
- Restauration
- Formation et sensibilisation
- Leçons apprises

7.12 Tester les Plans de Reprise après Sinistre (DRP)

- Travail de lecture / sur table
- Procédure
- Simulation
- Parallèle
- Interruption complète

7.13 Participer à la planification et aux exercices de Continuité Commerciale (BC)

7.14 Mettre en œuvre et gérer la sécurité physique

- Contrôles de sécurité du périmètre
- Contrôles de sécurité interne

7.15 Répondre aux problèmes de sécurité et de sûreté du personnel

- Voyage
- Formation et sensibilisation à la Sécurité
- Gestion des urgences
- Contraintes

Domaine 8 : Sécurité du Développement Logiciel

8.1 Comprendre et intégrer la sécurité dans le Cycle de Vie du Développement Logiciel (SDLC)

- Méthodologies de développement (p.ex., Agile, Waterfall, DevOps, DevSecOps)
- Modèles de maturité (p.ex., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Opération et maintenance
- Gestion des modifications
- Equipe Produit Intégré (IPT)

8.2 Identifier et appliquer les contrôles de sécurité dans les écosystèmes de développement logiciel

- Langages de programmation
- Bibliothèques
- Ensembles d'outils
- Environnement de Développement Intégré (IDE)
- Exécution
- Intégration Continue et Livraison Continue (CI / CD)
- Orchestration, Automatisation et Réponse de la Sécurité (SOAR)
- Gestion de la Configuration des Logiciels (SCM)
- Référentiels des codes
- Tests de sécurité des applications (p.ex., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))

8.3 Évaluer l'efficacité de la sécurité logicielle

- Audit et journalisation des modifications
- Analyse et atténuation des risques

8.4 Évaluer l'impact sur la sécurité des logiciels acquis

- Produit informatique standard (COTS)
- Open source
- Tiers
- Services gérés (p.ex., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

8.5 Définir et appliquer des directives et des normes de codage sécurisé

- Faiblesses et vulnérabilités de sécurité au niveau du code source
- Sécurité des Interfaces de Programmation d'Applications (API)
- Pratiques sécurisées de codage
- Sécurité Définie par Logiciel

Informations sur l'Examen Supplémentaire

Références Supplémentaires

Les candidats sont encouragés à compléter leur formation et leur expérience en révisant les ressources pertinentes relatives au CBK et en identifiant les domaines d'études qui pourraient nécessiter une attention supplémentaire.

Voir la liste complète des références supplémentaires à www.isc2.org/certifications/References.

Politiques et Procédures d'Examen

(ISC)² recommande que les candidats CISSP révisent les politiques et procédures d'examen avant de s'inscrire à l'examen. Lisez l'analyse complète de ces informations importantes à www.isc2.org/Register-for-Exam.

Mentions légales

Pour toute question relative aux politiques juridiques de (ISC)², veuillez contacter le Département Légal de (ISC)² à legal@isc2.org.

Des Questions ?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tél. : +1.866.331.ISC2 (4722)
E-mail : info@isc2.org

(ISC)² Asia Pacific
Tél. : +(852) 28506951
E-mail : isc2asia@isc2.org

(ISC)² EMEA
Tél. : +44 (0)203 300 1625
E-mail : info-emea@isc2.org