CISSP®

Certified Information Systems Security Professional

Aperçu de l'examen de certification

Effective Date: April 2018

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

A propos du CISSP

La certification CISSP (Professionnel certifié de la sécurité des systèmes d'information) est la certification la plus reconnue globalement sur le marché de la sécurité de l'information. Les CISSP acquièrent une connaissance technique et managériale approfondie des professionnels de la sécurité de l'information et l'expérience pour concevoir, réaliser et gérer la sécurité globale d'une organisation.

Le large spectre de sujets compris dans le CBK (Tronc commun de connaissance) garantit sa pertinence concernant toutes les disciplines dans le domaine de la sécurité de l'information. Les candidats qui ont réussi sont compétents dans les 8 domaines suivants :

- Gestion de la sécurité et des risques
- Sécurité des biens
- Architecture de sécurité et ingénierie
- Sécurité des communications et des réseaux
- Gestion des identités et des accès (IAM)
- Evaluation et test de la sécurité
- Sécurité opérationnelle
- Sécurité du développement des logiciels

Expérience Requise

LLes candidats doivent avoir une expérience d'au moins 5 ans à plein temps dans 2 ou plus domaines du CBK. Les candidats qui possèdent un diplôme universitaire (niveau BAC+4) ou un équivalent régional ou une certification complémentaire dans la liste approuvée par l'(ISC)² ne doivent avoir qu'une année de l'expérience requise. Les candidats bénéficiant de crédit d'éducation doivent avoir 1 année d'expérience.

Un candidat qui n'a pas l'expérience requise pour devenir CISSP peut devenir un associé de l'(ISC)² en réussissant l'examen. Les associés de l'(ISC)² auront besoin de 6 années pour acquérir les 5 années d'expérience requise.

Accréditation

CISSP a été la première certification dans le domaine de la sécurité de l'information à être conforme aux exigences strictes de la norme ANSI/ISO/IEC Standard 17024.

Analyse des tâches (JTA: Job Tasks Analysis)

(ISC)² a l'obligation vis-à-vis de ses membres de maintenir le niveau du CISSP. Conduit à intervalles réguliers, l'analyse des tâches est un processus méthodique et critique qui consiste à déterminer les tâches réalisées par les professionnels de la sécurité qui sont employés dans les professions définies par le CISSP. Les résultats de l'analyse des tâches sont utilisés pour mettre à jour la certification. Ce processus garantit que les candidats sont testés dans les domaines en rapport avec les rôles et responsabilités des professionnels de la sécurité d'aujourd'hui.

Information concernant l'examen CISSP en ligne

L'examen CISSP en ligne (CAT : computerized adaptive testing) est disponible pour tous les examens en anglais. Dans les autres langues, les examens CISSP sont gérés de façon linéaire et fixe. Vous pouvez vous renseigner sur les examens en ligne à www.isc2.org/certificatons/CISSP-CAT.

Durée de l'examen	3 heures
Nombre de questions	100 - 150
Type de questions	Choix multiples et questions avancées innovantes
Note de passage	700 sur 1000 points
Langue disponible	Anglais
Centre d'examen	PPC et PVTC, centres de tests Pearson Vue autorisés par l'(ISC)[2]

CISSP CAT Poids des domaines

Domaines	Poids moyen
1. Gestion de la sécurité et des risques	15%
2. Sécurité des biens	10%
3. Architecture de sécurité et ingénierie	13%
4. Sécurité des communications et des réseaux	14%
5. Gestion des identités et des accès (IAM)	13%
6. Evaluation et tests de la sécurité	12%
7. Sécurité Opérationnelle	13%
8. Sécurité des développements logiciels	10%
Total:	**100%**

Examen CISSP linéaire

Durée de l'examen	6 heures
Nombre de questions	250
Type de questions	Choix multiples et questions avancées innovantes
Note de passage	700 sur 1000 points
Langue disponible	Français, Allemand, Portugais brésilien, Espagnol, Japonais, Chinois simplifié, Coréen
Centre d'examen	PPC et PVTC, centres de tests Pearson Vue autorisés par l'(ISC)[2]

CISSP Linéaire Poids des domaines

Dominios	Peso
1. Gestion de la sécurité et des risques	15%
2. Sécurité des biens	10%
3. Architecture de sécurité et ingénierie	13%
4. Sécurité des communications et des réseaux	14%
5. Gestion des identités et des accès (IAM)	13%
6. Evaluation et tests de la sécurité	12%
7. Sécurité Opérationnelle	13%
8. Sécurité des développements logiciels	10%
Total:	**100%**

Domaine 1: Gestion de la sécurité et des risques

1.1 Comprendre et appliquer les concepts de confidentialité, intégrité et disponibilité

1.2 Evaluer et appliquer les principes de gouvernance de la sécurité

- Alignement des fonctions de sécurité aux métiers, stratégies, buts, missions et objectifs
- Processus organisationnels (par exemple, acquisitions, désinvestissement, comités de gouvernance)
- Rôles organisationnels et responsabilités
- Référentiel des contrôles de sécurité
- Attention requise/ diligence requise

1.3 Déterminer les exigences de conformité

- Contractuelles, légales, standards industriels, et exigences réglementaires
- Exigences concernant les données personnelles

1.4 Comprendre les questions légales et réglementaires qui font partie de la sécurité de l'information dans un contexte global

- Cyber crimes et failles de sécurité
- Exigences concernant les licences et la propriété intellectuelle
- Contrôle import / export
- Flux de données trans frontalier
- Données personnelles

1.5 Comprendre, adhérer, et promouvoir l'éthique professionnelle

- Code d'éthique professionnelle de l'(ISC)²
- Code d'éthique organisationnel

1.6 Développer, documenter, et implémenter les politiques de sécurité, les standards, les procédures, et les lignes directrices

1.7 Identifier, analyser, et déterminer les priorités concernant les exigences de continuité des métiers

- Développer et documenter le périmètre et le plan
- Analyse d'impact sur les métiers (BIA)

1.8 Contribuer et imposer les politiques sécurité et les procédures des ressources humaines

- Sélection et embauche des candidats
- Contrats de travail et politiques
- Processus d'entrée-sortie
- Accord concernant les vendeurs, les consultants et les sous-traitants et contrôles
- Exigences concernant les politiques de conformité
- Exigences concernant la politique sur les données personnelles

1.9 Comprendre et appliquer les concepts de la gestion des risques

- Identifier les menaces et les vulnérabilités
- Evaluation des risques / analyse
- Traitement des risques
- Choix des contre-mesures et implémentation
- Types de contrôles applicables (par exemple, prévention, détection, correction)
- Evaluation des contrôles de sécurité SCA)
- Surveillance et mesures
- Valorisation des biens
- Rapport
- Amélioration continue
- Référentiels des risques

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

- Méthodologie de modélisation des menaces
- Concept de modélisation des menaces

1.11 Appliquer les concepts de gestion basés sur les risques à la chaine d'approvisionnement

- Risques associés au matériel, logiciel, et services
- Evaluation des tierces parties et surveillance
- Exigences de sécurité minimales
- Exigences des niveaux de service

1.12 Etablir et maintenir un programme de sensibilisation, formation et entrainement à la sécurité

- Méthodes et techniques pour présenter la sensibilisation et la formation
- Revues périodiques du contenu
- Evaluation de l'efficacité du programme

Domaine 2: Sécurité des biens

2.1 Identifier et classifier l'information et les biens

- Classification des biens
- Classification des données

2.2 Déterminer et maintenir la propriété de l'information et des biens

2.3 Protéger les données personnelles

- Propriétaires des données
- Propriétaire des processus
- Rémanence des données
- Limite des collectes

2.4 Garantir une rétention appropriée des biens

2.5 Déterminer les contrôles de sécurité des données

- Comprendre les données d'état
- Portée et adaptation
- Choix des standards
- Méthodes de protection des données

2.6 Etablir les exigences concernant la manipulation des informations et des biens

Domaine 3: Architecture de sécurité et ingénierie

3.1 Implémenter et gérer les processus d'ingénierie en utilisant les principes de conception sécurisée

3.2 Comprendre les concepts fondamentaux des modèles de sécurité

3.3 Sélectionner les contrôles en accord avec les exigences de sécurité des systèmes

3.4 Comprendre les aptitudes de sécurité des systèmes d'information (par exemple, la protection de la mémoire, TPM (Trusted Platform Module), chiffrement/déchiffrement)

3.5 Evaluer et atténuer les vulnérabilités des architectures de sécurité, de la conception, et des éléments de la solution

- Systèmes basés sur les clients
- Systèmes basés sur les serveurs
- Systèmes des bases de données
- Systèmes cryptographiques
- Système de contrôle industriel (SCADA)
- Systèmes basés sur le Cloud
- Systèmes distribués
- Internet des objets (IoT)

3.6 Evaluer et atténuer les vulnérabilités des systèmes basés sur le Web

3.7 Evaluer et atténuer les vulnérabilités des systèmes mobiles

3.8 Evaluer et atténuer les vulnérabilités des modules embarqués

3.9 Mettre en œuvre la cryptographie

- Cycle de vie de la cryptographie (par exemple gestion des clés, choix des algorithmes)
- Méthodes cryptographiques (par exemple, symétrique, asymétrique, courbes elliptiques)
- Infrastructure de clés publiques (PKI)
- Pratiques de gestion de clés
- Signatures numériques
- Non-répudiation
- Intégrité (par exemple, hashing)
- Comprendre les méthodes des attaques de cryptanalyse
- Gestion des droits numériques (DRM)

3.10 Appliquer les principes de sécurité à la conception des sites et des bâtiments

3.11 Implémenter les contrôles de sécurité pour les sites et les bâtiments

- Locaux techniques/local de distribution intermédiaire
- Local serveurs/Centre de données
- Local de stockage des media
- Stockage des preuves
- Zones de sécurité restreintes et de travail
- Utilitaires et système de chauffage, de ventilation et d'air conditionné
- Problèmes environnementaux
- Prévention incendie, détection et extinction

Domaine 4: Sécurjté des communications et des réseaux

4.1 Implémenter les principes de conception sécurisée dans les architectures des réseaux

- Modèles Open System Interconnection (OSI) et Transmission Control Protocol/Internet Protocol (TCP/IP)
- Réseaux Internet Protocol (IP)
- Implications des protocoles multicouches
- Protocoles de convergence
- Réseaux logiciels
- Réseaux sans fil

4.2 Composants des réseaux sécurisés

- Fonctionnement du matériel
- Media de transmission
- Dispositifs de contrôle d'accès au réseau (NAC)
- Sécurité des points de terminaison
- Réseau de contenu distribué

4.3 Implémenter des canaux de communication sûrs en accord avec la conception

- Voix
- Collaboration multimédia
- Accès distants
- Communications des données
- Réseaux virtuels

Domaine 5: Gestion des identités et des accès (IAM)

5.1 Contrôle d'accès physique et logique aux biens

- Informations
- Systèmes
- Dispositifs
- Bâtiments

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

- Implémentation de la gestion des identités
- Single/multi-factor Authentification simple/multi facteur
- Traçabilité
- Gestion des sessions
- Enregistrement et preuves des identités
- Gestion fédérées des identités (FIM)
- Systèmes de gestion des certificats

5.3 Intégrer l'identité comme un service tierce partie

- En interne
- Dans le cloud
- Fédéré

5.4 Implémenter et gérer des mécanismes d'autorisation

- Contrôle d'accès basé sur les rôles (RBAC)
- Contrôle d'accès basé sur les règles
- Contrôle d'accès obligatoire (MAC)
- Contrôle d'accès discrétionnaire (DAC)
- Contrôle d'accès basé sur les attributs (ABAC)

5.5 Gérer le cycle de vie des identité et du provisionnement des accès

- Revue des accès des utilisateurs
- Revue des comptes d'accès système
- Provisionnement et déprovisionnement

Domaine 6: Evaluation et test de la sécurité

6.1 Concevoir et valider l'évaluation, les tests et les stratégies d'audit

- Internes
- Externes
- Tierce partie

6.2 Conduire les tests des contrôles de sécurité

- Evaluation des vulnérabilités
- Tests de pénétration
- Revues des logs
- Transactions synthétiques
- Revue du code et test
- Tests des cas d'erreur
- Analyse de la couverture des tests
- Tests des interfaces

6.3 Collecter les données des processus de sécurité (par exemple, technique et administrative)

- Gestion des comptes
- Revue de la gestion et approbation
- Indicateurs de performance clé et des risques
- Vérification des données de sauvegarde
- Formation et sensibilisation
- Reprise après sinistre (DR) et Continuité d'activité (BC)

6.4 Analyser les résultats des tests et générer un rapport

6.5 Conduire ou encourager les audits de sécurité

- Internes
- Externes
- Tierce partie

Domaine 7: Sécurité Opérationnelle

7.1 Comprendre et encourager les investigations

- Collecte des preuves et manipulation
- Rendre compte et documenter
- Investigations techniques
- Outils d'enquête digitales, tactiques et procédures

7.2 Comprendre les exigences des différents types d'investigation

- Administratives
- Criminelles
- Civiles
- Réglementaires
- Standards de l'industrie

7.3 Mener les activités de journalisation et de supervision

- Détection et prévention d'intrusion
- Gestion des informations de sécurité et des événements (SIEM)
- Supervision continue
- Supervision des sorties

7.4 Provisionnement sécurisé des ressources

- Inventaire des biens
- Gestion des biens
- Gestion des configurations

7.5 Comprendre et appliquer les concepts fondamentaux de la sécurité opérationnelle

- Besoin d'en connaître / Moindre privilège
- Séparation des tâches et responsabilités
- Gestion des comptes à privilège
- Rotation des emplois
- Cycle de vie des informations
- Accords sur les niveaux de services (SLA)

7.6 Appliquer les techniques de protection des ressources

- Gestion des média
- Gestion des biens matériels et logiciels

7.7 Conduire la gestion des incidents

- Détection
- Réponse
- Atténuation
- Rapports
- Reprise
- Remédiation
- Leçons apprises

7.8 Opérer et maintenir des mesures de détection et de prévention

- Pare feu
- Systèmes de détection et de prévention d'intrusion
- Listes blanches/noires
- Services de sécurité des tierces parties
- Bac à sable
- Pots de miel/filets
- Anti-malware

7.9 Implémenter et gérer la gestion des patches et des vulnérabilités

7.10 Comprendre et participer au processus de gestion des changements

7.11 Implémenter les stratégies de reprise

- Stratégies de stockage des sauvegardes
- Stratégies des sites de reprise
- Sites multi processing
- Résilience des systèmes, haute disponibilité, Qualité de Service (QoS), et tolérance aux fautes

7.12 Implémenter les processus de reprise après sinistre (DR)

- Réponse
- Personnel
- Communications
- Evaluation
- Restauration
- Formation et sensibilisation

7.13 Tester les plans de reprise après sinistre (DRP)

- Relecture/sommaire
- Parcours
- Simulation
- Parallèle
- Interruption complète

7.14 Participer au plan de continuité d'activité et s'entraîner

7.15 Implémenter et gérer la sécurité physique

- Contrôle du périmètre de sécurité
- Contrôle de sécurité interne

7.16 Prendre en compte la sécurité du personnel et les problèmes de sécurité

- Voyage
- Formation et sensibilisation à la sécurité
- Gestion de crise
- Contrainte

Domaine 8: Sécurité des développements logiciels

8.1 Comprendre et intégrer la sécurité dans le cycle de vie des développements (SDLC)

- Méthodologies de développement
- Modèles de maturité
- Opération et maintenance
- Gestion du changement
- Equipe d'intégration

8.2 Identifier et appliquer les contrôles de sécurité dans les environnements de développement

- Sécurité des environnements logiciels
- Gestion des configurations comme une partie du code sécurisé
- Sécurité du dépôt des sources

8.3 Evaluer la sécurité effective du logiciel

- Auditer et tracer les changements des risques
- Analyse de risques et atténuation

8.4 Evaluer les impacts sécurité des logiciels achetés

8.5 Définir et appliquer les recommandations et standards de développements sécurisés

- Faiblesses de sécurité et vulnérabilités dans le code source
- Sécurité de la programmation des interfaces des applications
- Pratiques de code sécurisé

Informations additionnelles pour l'examen

Références supplémentaires

Les candidats sont encouragés à compléter leur formation et expérience en revoyant les points adéquats qui appartiennent au CBK et à identifier les domaines d'étude nécessitant un supplément de formation.

La liste des références complémentaires est disponible à www.isc2.org/certifications/References.

Règles et procédures de l'examen

(ISC)² recommande que les candidats au CISSP revoient les règles et procédures avant de s'inscrire à l'examen. Lire la description complète de cette information à www.isc2.org/Register-for-Exam.

Informations légales

Pour toute question en rapport avec les politiques légales de l'(ISC)², prière de contacter le département juridique à legal@isc2.org.

Autres Questions?

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

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org

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