&

# Formation préparatoire à la certification professionnelle CISSP

Cette formation a pour but de préparer les candidats à l'examen du CISSP (Certified Information Systems Security Professional), la certification internationale délivrée par l'ISC2, examen qui se déroule chaque année en juillet et octobre.

La formation couvre l'ensemble du CBK (Common Body of Knowledge), tronc commun de connaissances en sécurité défini par ISC2®. Le CBK inclus les connaissances en sécurité de l'information dans les dix domaines suivants : Management de la Sécurité, Architecture et Modèles de Sécurité, Contrôle des accès logiques, Sécurité des applications, Sécurité des opérations, Cryptographie, Sécurité physique, Sécurité des Télécommunications et des Réseaux, Continuité des activités, Loi, investigations et éthique.

Tout au cours de la semaine, les participants sont invités à répondre à des questions, en groupe et individuellement, sur chacun des domaines et similaires à l'examen officiel.

## Attention :

L'inscription à cette formation est totalement indépendante de celle à l'examen qui doit se faire sur le site de l'ISC2 (http://www.isc2.org).
SecuCERT en tant que partenaire accrédité peut prendre en charge pour le compte de ces clients, cette inscription.

## Objectifs :

Acquérir les connaissances nécessaires à la réussite de l'examen CISSP® , Maîtriser les connaissances en sécurité de l'information dans les dix domaines du CBK,Comprendre les besoins en sécurité de l'information pour toute l'organisation , Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en management de la sécurité de l'information.

## Participants :

Auditeurs confirmés ou informaticiens (DSI, RSSI, Managers, Ingénieurs, Experts Consultants) qui souhaitent obtenir la certification CISSP (Certified Information System Security Professional) délivrée par l'ISC2, et préparer l'examen. Celui-ci dure 6 heures Et utilise un questionnaire constitué de 250 questions portant sur l'ensemble des domaines relevant de la sécurité du système d'information. Réussite à l'examen avec au moins 75% de bonnes réponses (*).

## Pré -requis :

Une expérience dans le domaine des réseaux et de la sécurité,
La compréhension de l'anglais est nécessaire car la documentation fournie aux participants est en anglais.

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*

**Bénéfices attendus de la formation :**

Reconnaissance Internationale des compétences en sécurité de l'information, Savoir dialoguer avec le management pour la mise en œuvre des mesures de sécurité, Appréhender le rôle du RSSI dans l'organisation.

**Intervenants :**

Les sessions sont animées par des Experts Seniors certifiés CISA, CISM, CBCP, CISSP®, ISO 27001 Lead Auditor et ISO 27005 Risk Manager.

**Mode :**

Formation inter – entreprises.

**Programme :**

Le programme du séminaire suit les 10 domaines définis pour l'examen :

**Jour 1** :

**Domaine 1** : Management de la Sécurité

- Introduction et Objectifs du management de la sécurité
  - Concepts : Disponibilité, Intégrité, Confidentialité
- Environnement et menaces
- Administration de la Sécurité et Contrôles associés
- Modèles de Sécurité
- Principes de Gestion des Risques
- Politique, Standards, Baselines, Directives et Procédures.
- Classification des Informations
- Politiques et pratiques d'embauche
- Formation de Sensibilisation en Sécurité Informatique
- Questions d'entrainement pour l'examen

**Domaine 2** : Architecture et Modèles de Sécurité

- Introduction et Objectifs de l'architecture et des modèles de sécurité
- Quelques Menaces
- Architecture physique de l'Ordinateur
- Architecture de la sécurité
- Modèles de sécurité
- Modes de sécurité opérationnelle
- Méthodes d'Evaluation et critères des systèmes
  - Le Livre Orange (TCSEC)
  - Le Livre rouge (TNI)
  - IT
    SE
    C
  - Les Critères Communs (CC)
  - Comparaison des niveaux d'évaluation des systèmes
  - Certification et Accréditation.
- Questions d'entrainement pour l'examen

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*

**Jour 2** :

**Domaine 3** : Contrôle des accès logiques

- Introduction et Objectifs du contrôle d'accès logique
- Triade DIC
- Le modèle du « Sujet qui accède à l'objet »
- Qu'est-ce qu'une Politique en matière de Contrôle d'accès ?
- Menaces (perte d'imputabilité, mauvaise configuration, voies clandestins et système, portes dérobées et privilèges administrateur, rémanence des données, extrapolation de l'information)
- Types de Contrôles d'Accès,
- Services de Contrôle d'Accès (IAAA)
- Techniques de Contrôle d'Accès
- Politique de Contrôle d'Accès
- Meilleures pratiques (gestion des mots de passe, …)
- Mécanismes d'assurance
- Questions d'entrainement pour l'examen

**Domaine 4** : Sécurité des applications

- Introduction et Objectifs de la sécurité des applications
- Processus de Développement des Applications
- Cycle de vie du développement des applications
- Contrôle administratif
- Modèles de développement de logiciels
- Contrôle des changements
- Langage de programmation
- Assembleur, compilateur et interpréteur
- Programmation orientée objet (OOP)
- Informatique répartie
- Gestion de base de données
- Système de gestion de base de données
- Modèles de base de données
- Langage d'interface de la base de données
- Entrepôt de données et exploration de données
- Intelligence artificielle
- Système expert
- Réseau neuronal artificiel
- Menaces à la sécurité de l'application
- Code de source ouvert ou de source fermé
- Code malicieux
- Méthodes d'attaque
- Contrôle de l'application
- Questions d'entrainement pour l'examen

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*

**Jour 3** :

**Domaine 5** : Sécurité des opérations

- Introduction et Objectifs de la sécurité des opérations
- Besoins de l'entreprise
- Privilège minimum
- Besoin d'en connaître
- Fonctions privilégiées
- Respect de la vie privée
- Exigences juridiques
- Activités illégales
- Traitement des informations délicates
- Menaces
- Le matériel
- Le logiciel
- Les opérations
- Les données et leur support
- Equipements de télécommunications
- Le système de soutien
- Perte accidentelle
- Le personnel
- Espionnage industriel
- Pirates et intrus
- Activités inappropriées
- Contrôles
- Types de contrôles
- Contrôles administratifs
- Contrôles techniques
- Contrôles physiques
- Questions d'entrainement pour l'examen

**Domaine 6** : Cryptographie

- Introduction et Objectifs du la cryptographie
- Historique de la Cryptographie.
- Définitions
- Encadrement légal
- Concepts de base en cryptographie (méthodes et clés, chiffrement, déchiffrement,…
- Systèmes de chiffrement
- Algorithmes à clés symétriques (DES, IDEA, RC5, RC6)
- Algorithmes à clés asymétriques (RSA, Diffie - Hellman, El-Gamal, ECC)
- Protocoles de Cryptographie (Protocoles Internet)
- Contrôles d'intégrité des messages (concept de fonction de Hachage)
- Signatures numériques
- Infrastructure à clé publique (PKI, Certificat X.509)
- Gestion des clefs
- Cryptanalyse te attaques
- Questions d'entrainement pour l'examen

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*

**Jour 4** :

**Domaine 7** : Sécurité physique

- Introduction et Objectifs de la Sécurité Physique
- Besoins et exigences des entreprises
- Menaces
- Différents types
- 7 sources différentes
- Spécifique – Feu
- Spécifique – Environnement opérationnel
- Contrôles administratifs
- Contrôles techniques
- Contrôles physiques
- Questions d'entrainement pour l'examen

**Domaine 8** : Sécurité des Télécommunications et des Réseaux

- Introduction et Objectifs de la sécurité des Télécommunications et des Réseaux
- Télécommunications, réseaux et Internet
- Réseaux de données
- Protocoles de réseaux
- Menaces liées aux réseaux
- Systèmes de callback et authentification
- Système d'authentification centralisée
- Coupe-feu et sécurité du périmètre
- Filtrage de contenu et inspection
- Détection des intrusions
- Réseaux Privés virtuels (VPN)
- Disponibilité des ressources
- Journaux d'audit de sécurité
- Examens réguliers de la sécurité
- Estimation des vulnérabilités
- Questions d'entrainement pour l'examen

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*

**Jour 5** :

**Domaine 9** : Continuité des activités

- Introduction et Objectifs de la continuité des activités
- Différences entre BCP et DRP
- Définition d'un désastre
- Environnement et menaces
- BCP
- Objectifs
- Phases du processus BCP
- Phase 1 : Management du projet BCP et initiation
- Phase 2 : Business Impact Analysis (BIA)
- Phase 3 : Stratégies de reprise
- Phase 4 : Développement du plan et Implémentation
- Phase 5 : Test, Maintenance, Sensibilisation et Formation
- Objectifs et Types de test
- Maintenance
- Sensibilisation et Formation
- Conditions d'efficacité
- Audit
- Normes
- Vue BCP et DRP
- Questions d'entrainement pour l'examen

**Domaine 10** : Loi, investigations et éthique

- Introduction et Objectifs du domaine Loi, investigations et éthique
- Crimes
- Profils des criminels
- Causes de crimes
- Types de crimes
- Exemples historiques de crimes informatiques
- Avenir du cybercrime
- Droit
- Droit international
- Droit civil
- Common Law
- Exemple : Les Etats-Unis
- Droit de la propriété intellectuelle
- Droit au respect des informations confidentielles
- Code de la confidentialité
- Loi en matière de sécurité informatique, de confidentialité et de crime
- Conformité légale
- Cadre réglementaire
- Diligence nécessaire, diligence raisonnable et responsabilité
- Traitement des incidents
- Expertise judiciaire en informatique et collecte adéquate de preuves
- Preuve
- Types de preuves
- Directives pour intervention en cas d'incident
- Ethique
- Fondements d l'éthique
- Code d'éthique de (ISC)²
- Les 10 commandements de l'infoéthique de l'Institut de Déontologie CEI
- Ethique et Internet (RFC 1087) du IAB (Internet Activities Board)
- Principes généralement acceptés de sécurité du système (GASSAP)
- Questions d'entrainement pour l'examen

Dans chaque exposé, l'accent sera mis sur les éléments organisationnels et technologiques fondamentaux.

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*

**Méthode :**

Ensemble d'exposés couvrant chaque domaine du programme de l'examen,
A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CISSP (ou d'examens comparables), Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

Il est vivement conseillé aux candidats à l'examen d'acquérir avant leur participation à la formation la documentation de préparation de l'examen qu'ils peuvent acquérir auprès de l'ISC2.

**Lieux d'examen :**

Voir sur le site http://www.isc2.org

**Durée :** 5 jours soit 35 heures

**Tarif : 260 000 DA HT**

Les frais d'examen ne sont pas compris dans le prix de cette session,
Le Support de formation et le Manuel Officiel de préparation au CISSP sont fournis à réception de l'inscription,
Un certificat de participation de 35 CPE (Unités d'éducation continue /Continuing Professional Education) est remis aux participants en fin de formation.

**CONTACTE NB.CONSULTING BATNA**

TEL : +213 (0) 558 13 18 88
Fax : +213 (0) 33 85 43 85
Siteweb : www.nb-consulting-dz.com

NB

NB.CONSULTING est le partenaire de secuRCERT qui est accrédité par ISC2 & LSTI

*(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans en cas de diplôme universitaire).*