

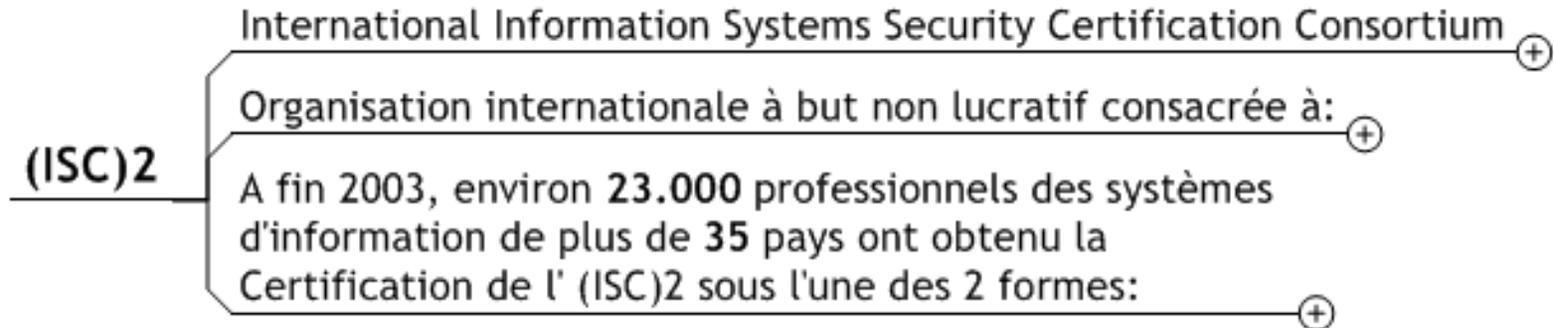
# Certified Information System Security Professional (CISSP)



Christian Simatos  
12-01-2004

# (ISC)2

[www.isc2.org](http://www.isc2.org)



# Organisation internationale à but non lucratif consacrée à:

- Maintenir un tronc commun de connaissances de sécurité (Common Body of Knowledge)
- Certifier les professionnels et praticiens de l'industrie d'un standard international de sécurité de l'information.
- Administrer des séminaires de révision et des examens de certification.
- Assurer que les compétences sont maintenues dans le temps.

A fin 2003, environ 23.000 professionnels des systèmes d'information de plus de 35 pays ont obtenu la Certification de l' (ISC)2 sous l'une des 2 formes:

- Certified Information Systems Security Professional (CISSP)
- System Security Certified Practitioner (SSCP)

# Certification CISSP

La certification CISSP a été conçue pour sanctionner la maîtrise d'un standard international de sécurité de l'information et la compréhension d'un tronc commun de connaissances en sécurité (Common Body of Knowledge CBK).

La certification CISSP assure une crédibilité supplémentaire en sécurité pour les individus et les organisations au **niveau International**.

Certification CISSP

Common Body of Knowledge  
(CBK)



Bénéfices de la Certification  
CISSP pour les **Professionnels**



Bénéfices de la Certification  
CISSP pour les **Organisations**



# Common Body of Knowledge (CBK)

## Définition:

- Taxinomie des domaines de la sécurité de l'information qu'un professionnel doit connaître et comprendre suffisamment pour tenir des discussions sensées avec des pairs.

# Bénéfices de la Certification CISSP pour les Professionnels

- Valide une expertise et une expérience en passant un examen rigoureux.
- Peut être un différentiateur professionnel, par des relations avec vos pairs et une crédibilité accrue.
- Enrichit vos références professionnelles - de nombreuses organisations exigent une "Certifications CISSP" dans leurs annonces.

# Bénéfices de la Certification CISSP pour les Organisations

- Fournit aux employés une orientation vers des solutions plutôt que vers des spécialisations, en particulier par une compréhension élargie de la sécurité des systèmes d'information
- Permet l'accès à un réseau global d'experts de l'industrie et de domaines/problèmes associés.
- Augmente la crédibilité de l'organisation concernant la sécurité des informations qu'elle gère car ses employés ont réussi la certification.

# Le Candidat CISSP

## Le Candidat CISSP

Comprend et accepte les principes énoncés dans le code d'éthique de la Certification (ISC)2

Possède au moins 3 années d'expérience dans un ou plusieurs des 10 domaines de la sécurité des informations.

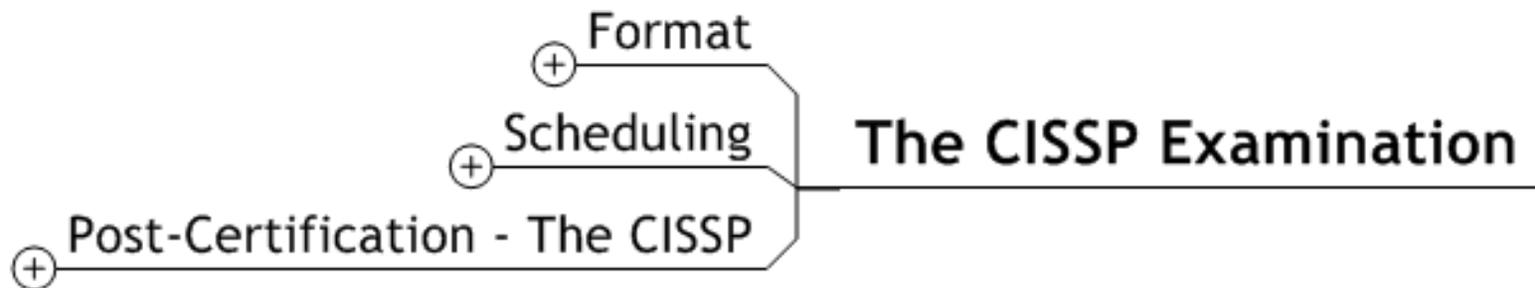
A une vaste compréhension des domaines, acquise ⊕

Obtient une reconnaissance professionnelle en réussissant l'examen de certification CISSP.

# A une vaste compréhension des domaines, acquise:

- par l'étude et l'activité professionnelle,
- en assistant aux séminaires de revue,
- et en se tenant constamment au courant des avancées technologiques de l'industrie.

# The CISSP Examination



# Format

- 250 multiple choice questions
- **Le tout en Anglais**
- Up to six hours to complete

Une maitrise suffisante de l'anglais est  
nécessaire

# Dates Certification Paris

- World-Wide Locations
- Paris
  - [www.Auditware.fr](http://www.Auditware.fr)
  - 27 Mars 2004
  - 26 Juin 2004
  - 23 Octobre 2004
  - 499 \$ - 460 €

# Post-Certification - The CISSP

- Maintenir votre status par la formation continue ou en re-certifiant tous les 3 ans.
  - 120 Continuing Professional Education Credits
- Cotisation annuelle de maintenance
- Respecter le Code d'Ethique de l'(ISC)<sup>2</sup>

# CBK Review Seminar

Des séminaires de révision du CBK sont tenus régulièrement dans le monde entier donnant une opportunité aux professionnels de parcourir le CBK afin de préparer l'examen de certification et de se tenir à jour sur les domaines évoluant en permanence de la sécurité de l'information.



# Objectifs

- Revue des principaux sujets
- Identifie les domaines que les candidats doivent approfondir pour l'examen
- N'a pas pour finalité "d'enseigner l'examen"
- Fournir les éléments permettant de valider:
  - Une connaissance et une compréhension professionnelle
  - Une capacité à mettre en oeuvre le spectre entier des concepts de sécurité

# Les séminaires

- Sessions de 5 jour
- Le sujet est séparé en 10 domaines de connaissance
- Chaque domaine inclut 5 domaines fonctionnels
- Programme CISSP 2004 en France (Paris)

# Le sujet est séparé en 10 domaines de connaissance

- Security Management Practices
- Security Architecture and Models
- Access Control Systems and Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network, and Internet Security
- Business Continuity Planning
- Law, Investigations, and Ethics

# Chaque domaine inclut 5 domaines fonctionnels

- Information Protection Requirements
  - Décrit les connaissances qu'un professionnel doit posséder concernant les besoins, leur origine ou leur prescripteur,
  - Le professionnel est sensé avoir une compréhension suffisante des motivations sociales, légales, financières et industrielles afin de prendre des décisions raisonnables concernant la protection des information.
- Information Protection Environment
  - Ce que le candidat doit connaître concernant les technologies de l'information, les réseaux, les systèmes et les applications qui forment le contexte dans lequel les besoins doivent être satisfaits.
  - Les Professionnels sont sensés connaître les risques, vulnérabilités et possibilité de protection de l'environnement dans lequel l'information est traitée, transmise ou stockée.
- Security Technology and Tools
  - Ce qu'un Professionnel de la sécurité des SI doit connaître concernant les technologies, les mécanismes et les outils qu'il peut être amené à utiliser pour assurer les besoins de sécurité.
    - Connaissance approfondie des technologies et des techniques utilisées pour la protection de l'information.
    - Capacité de prendre les décisions adéquates concernant l'utilisation d'une technique ou d'une technologie spécifique pour assurer les objectifs de la politique de sécurité.
- Assurance, Trust, and Confidence Mechanisms
  - Ce qu'un Professionnel doit connaître concernant les outils et mécanismes qui permettent de s'assurer que les contrôles mis en place sont fiables, efficaces et fonctionnent comme supposés.
  - Il doit comprendre la nécessité et l'utilisation des outils, techniques, standards et autre critères mis en oeuvre pour fournir une assurance à toutes les parties prenantes que les contrôles satisfont les impératifs.
- Information Protection and Management Services
  - Connaissances des organisations et services sous l'autorité directe des responsables de la sécurité des information ou du management.
  - Le professionnel est sensé connaître les principes, les pratiques usuelles et les activités professionnelles mises en oeuvre pour promouvoir des comportements surs.

# Dates des séminaires Paris

- [www.Auditware.fr](http://www.Auditware.fr)
- 8-12 Mars 2004
- 7-11 Juin 2004
- 4-8 Octobre 2004
- 2.595 €