

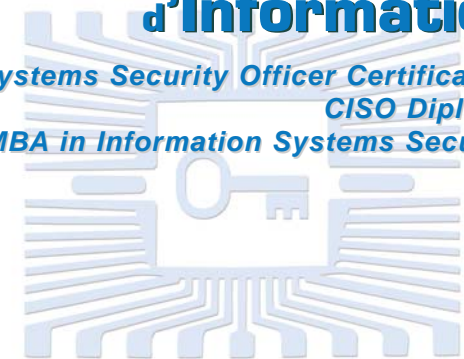
Formation Continue  
Universitaire

Session 2007-2008

<http://cssi.unige.ch>

Certificat, Diplôme et MBA en  
**Sécurité des Systèmes  
d'Information**

*Information Systems Security Officer Certification  
CISO Diploma  
MBA in Information Systems Security*



© 2003 • Graphic Design blueBOX Marketing & Concepts • www.bluebox-

HEC  
Hautes Études Commerciales  
FACULTÉ DES SCIENCES ÉCONOMIQUES ET SOCIALES

Université de Genève  
UNI MAIL | 40, Boulevard du Pont-d'Arve | CH-1211 Genève 4 | Suisse  
Tél. 022 379 88 00  
Fax 022 379 81 04  
e-mail : [cssi@hec.unige.ch](mailto:cssi@hec.unige.ch)  
<http://cssi.unige.ch>



# Sécurité des Systèmes d'Information

Certificat et Diplôme de formation continue universitaire

Septembre 2007 à juin 2008

Page	Sommaire
2	■ Contexte et objectifs de la formation ■ Étendue des risques informatiques
3	■ Notre formation ■ Certificat ou Diplôme ? ■ Public visé
4	■ Méthodes pédagogiques ■ Durée ■ Contrôles ■ Charge de travail
5-6	■ Modules
7	■ Intervenants
8	■ Évaluation et titres délivrés ■ MBA mention "Sécurité des Systèmes d'Information"
9	■ Renseignements pratiques
10	■ Direction du Certificat ■ Comité Directeur et Conseil Scientifique ■ Contacts & Informations
11	■ Bulletin d'inscription

## Un programme complet de formation continue universitaire spécialisée

- pouvant être suivi en emploi pour valoriser votre carrière,
- accessible si vous avez plusieurs années d'expérience professionnelle,
- proposé selon trois niveaux.

Candidats ne possédant pas forcément un titre universitaire :

- 1. Certificat en Sécurité des Systèmes d'Information (CSSI)**  
sur une année universitaire
- 2. Diplôme d'Expert en Sécurité des Systèmes d'Information (DESSI)**  
sur une 2<sup>e</sup> année universitaire pour les titulaires du CSSI

Candidats détenteurs d'un titre universitaire ou titre jugé équivalent :

- 3. MBA en Sécurité des Systèmes d'Information**

Certificat et Diplôme de formation continue en

## «Sécurité des Systèmes d'Information»



### Contexte et objectifs de la formation

La prolifération des nouvelles technologies d'information et de communication, l'utilisation croissante de la messagerie électronique, l'essor des intranets et extranets ainsi que la mise en place rapide d'applications de commerce électronique fondées sur internet génèrent de nouveaux risques par une plus grande exposition des systèmes d'information (S.I.) d'une organisation vers l'extérieur. Or, les entreprises amenées à créer très rapidement des services sur internet, privilégient souvent les aspects commerciaux au détriment de la sécurité de leurs S.I. La pression réglementaire (Bâle II et SOX par exemple) pousse à la refonte des systèmes d'information pour une mise en conformité (*Compliance*) en termes de gouvernance, de prise en compte des risques opérationnels, et donc de sécurité des informations et leurs traitements. Les référentiels actuels pour la sécurité des informations, tels que les normes ISO 17799, ISO 27001, et les bonnes pratiques telles que le CobiT, COSO et ITIL, fournissent le cadre de référence pour cette mise en conformité.

Ces évolutions exigent de nouvelles compétences de la part des professionnels en charge de la sécurité de l'information et des S.I. Ils se doivent d'être en mesure d'identifier les risques nouveaux, de planifier et d'assurer le suivi de la mise en place des mesures préventives et curatives adéquates pour y faire face, et surtout de sensibiliser la direction et le personnel.

La fonction occupée est celle d'un "Responsable de la Sécurité des Systèmes d'Information" (RSSI), en charge de la mise en œuvre de la politique de sécurité des S.I. dans les entreprises et administrations. Dans les pays anglo-saxons, la dénomination est "*Information Systems Security Officer*", voire *Chief Information Security Officer (CISO)*. Bien que dispensé en français, ce Certificat peut représenter un bon moyen de préparation pour ceux qui seraient intéressés à se présenter aux examens de certaines certifications nord-américaines telles que le CISSP/SSCP, CISA/CISM, etc.

### Étendue des risques informatiques

De nombreux facteurs expliquent la prise en compte croissante de la dimension sécurité dans le management des S.I. : les nouvelles applications de l'informatique, l'ouverture vers internet et l'explosion des attaques, la multiplication des projets complexes de refonte des S.I., leur mise en conformité avec les réglementations et les normes actuelles, le déploiement d'architectures informatiques complexes, l'avènement des technologies sans fil, la généralisation des services à distance ou l'élaboration de plans de continuité d'activités.

Les risques en termes de sécurité des S.I. ne se limitent pas aux risques technologiques des plates-formes informatiques ou des réseaux, mais incluent aussi les risques liés à l'organisation même de l'entreprise, à ses processus métiers, à ses méthodes de travail, à son personnel, etc.

Par ailleurs, les contraintes juridiques et légales engendrent également des risques qui vont désormais au-delà des frontières. Chaque entreprise doit veiller à respecter non seulement les lois de son pays (protection des données, propriété intellectuelle, etc.), mais aussi les conventions internationales et les lois des pays avec lesquels elle échange des données.

Ce sont autant de thèmes d'étude et de domaines de connaissances qui sont couverts par nos programmes dont l'ambition est de former les étudiants à la **culture multidimensionnelle du champ de la sécurité des S.I.** qui est aujourd'hui requise.

### Notre formation

Les risques informatiques, la pression réglementaire pour la révision des processus internes et la mise en conformité, génèrent de nouveaux besoins dans les entreprises. Il s'agit non seulement d'une prise de conscience des dangers de l'ouverture des systèmes d'information au monde extérieur, mais également de l'augmentation du degré de sensibilité à la sécurité des informations à tous les échelons de l'organisation.

Force est de constater l'amplification de ce phénomène depuis ces dernières années qui a entraîné une demande accrue de formation et d'approfondissement dans ce domaine. Ainsi, depuis 1997, plus de 200 participants ont suivi nos formations en sécurité des systèmes d'information.

### Certificat ou Diplôme ou MBA ?

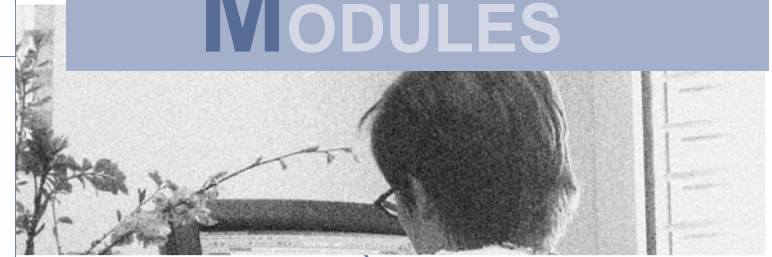
Désormais la formation est dispensée selon trois niveaux : un "**Certificat de formation continue en Sécurité des Systèmes d'Information (CSSI)**" durant la 1<sup>ère</sup> année et, pour ceux qui le souhaitent, une 2<sup>e</sup> année de spécialisation et d'approfondissement conduisant au "**Diplôme de formation continue d'Expert en Sécurité des Systèmes d'Information (DESSI)**", chacun visant à former des professionnels aguerris aux concepts, moyens et méthodes de la sécurité des S.I. D'un point de vue pratique, les étudiants de formation continue suivent les six modules du Certificat, représentant 168 heures de cours (18 crédits ECTS - European Credit Transfer and accumulation System). En cas de succès, ils peuvent accéder à la 2<sup>e</sup> année optionnelle représentant également 18 crédits et comprenant trois modules complémentaires à choix ainsi que la rédaction d'un mémoire de diplôme. Les 36 crédits ECTS accumulés leur permettront de se voir délivrer le titre de Diplôme d'Expert en Sécurité des Systèmes d'Information.

Pour les candidats déjà titulaires d'un diplôme universitaire, il est judicieux de postuler d'abord à l'admission au programme du **Master en Business Administration (MBA)** de HEC-Genève. Après une 1<sup>ère</sup> année de formation au management général, ils pourront suivre les modules du CSSI dans le cadre de leur 2<sup>e</sup> année de spécialisation et obtenir le **MBA en Sécurité des Systèmes d'Information**. Voir p. 8 pour davantage de détails.

### Public visé

Ce Certificat s'adresse tout particulièrement aux différents responsables œuvrant dans le domaine de la sécurité des systèmes d'information :

- Responsables des systèmes d'information
- Responsables sécurité des réseaux et systèmes
- Risk Managers et responsables des politiques de protection des ressources liées aux systèmes d'information et de communication
- Chefs de projets d'informatisation, de projets en e-commerce et e-business
- Consultants en informatique, en sécurité, en risk management
- Responsables chargés de l'évaluation des risques opérationnels
- Auditeurs informatiques
- Juristes d'entreprises chargés des questions de sécurité et de conformité des systèmes d'information



## Méthodes pédagogiques

Le programme est animé par des universitaires et des professionnels, tous spécialistes des domaines relatifs à la sécurité de l'information et des systèmes d'information. La diversité des compétences des enseignants et intervenants assure la pluridisciplinarité de cette formation.

Les méthodes pédagogiques utilisées offrent un environnement propice aux échanges d'idées et d'expériences et encouragent la constitution d'un "réseau de compétences" entre les participants d'une volée et des volées précédentes.

L'enseignement donné de manière didactique fait recours à des études de cas, à des exercices pratiques ainsi qu'à l'étude de sites web dédiés à la sécurité des systèmes d'information.

Le pilier central d'échange entre les enseignants et les participants est le site web du programme qui leur est réservé.

## Durée de la formation

Le programme du **Certificat** de la 1<sup>ère</sup> année est composé de 6 modules de 28 heures d'enseignement chacun, y compris le contrôle des connaissances. Chaque module est équivalent à 3 crédits ECTS. En complément, un module de 24 heures, sans crédit, est proposé en option pour ceux qui souhaitent se mettre à niveau sur les concepts et pratiques des communications internet. Chaque module comporte six séances de quatre heures et une septième séance réservée au contrôle des connaissances est suivie de la correction de l'épreuve. L'ensemble se déroule sur une année universitaire.

Le programme de la 2<sup>e</sup> année conduisant au **Diplôme** est réservé aux titulaires du Certificat. Il se déroule également sur une année universitaire et comporte trois modules spécialisés de 3 crédits à choix ainsi que la rédaction d'un mémoire dont l'encadrement est assuré par un membre du comité scientifique.

Sous réserve de places disponibles, les personnes ne souhaitant pas suivre l'intégralité du Certificat peuvent s'inscrire à un ou plusieurs modules isolés.

## Évaluation des connaissances

Chaque module est validé par un contrôle des connaissances comportant, en principe, l'évaluation d'un travail individuel, d'un travail en groupe et d'un examen final formel.

## Charge de travail

Pour chaque heure d'enseignement, il faut compter de deux à trois heures de travail personnel sous forme de lectures pour la préparation des séances, de rédaction des travaux d'évaluation, individuels ou en groupe, ainsi que le temps consacré à la révision de l'examen final de chaque module.

D'après l'enquête réalisée auprès des étudiants des volées précédentes, il ressort qu'en moyenne, ils ont consacré environ 12 heures par semaine à leur formation.

## Modules du certificat de 1<sup>ère</sup> année

### 1 FONDEMENTS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

**DATES** : 19/09, 26/09, 03/10, 10/10, 17/10, 24/10, 31/10/2007

Étendue des risques liés aux technologies d'information et de communication, aux méthodes d'organisation du travail et aux personnels ; Sécurité de l'information, Identification des failles de sécurité ainsi que des mesures préventives et curatives correspondantes ; Sécurité dans l'organisation des systèmes d'information (SI) de l'entreprise ; Sécurité et qualité dans les applications exemplaires actuelles et le développement de systèmes ; Gouvernance de l'entreprise et gouvernance des SI, Cadres réglementaires pour la conformité (*Compliance*) des processus métiers et des SI correspondants ; Introduction aux principaux référentiels pour la sécurité de l'information et des SI, Principes d'élaboration d'une politique organisationnelle de sécurité des systèmes d'information (POSI) ; Études de cas d'entreprises.

### 2 ARCHITECTURES DE SÉCURITÉ

**DATES** : 07/11, 14/11, 21/11, 28/11, 05/12, 12/12, 19/12/2007

Architectures informatiques : structures d'entrées-sorties, programmation et logiciels, architecture distribuée, mécanismes de protection, techniques de "hardening", classification et modes de sécurité, procédures de reprise d'activité, satisfaction des besoins en sécurité, connaître ses ennemis, accréditation et certification; Modèles de sécurité de l'information : modèles de contrôle d'accès (matrice d'accès, Bell-LaPadula), modèles d'intégrité des données (Biba, Clark-Wilson), modèles d'accès basés sur les rôles (RBAC). Architectures de sécurité physique : menaces, contrôles (administratifs, environnementaux, vitaux, physiques et techniques) ; Plans de secours/Disaster Recovery Planning, Plan de continuité d'activité/Business Continuity Planning, reprise en cas de désastre : processus, tests, procédures.

### MODULE OPTIONNEL (détails du programme dans le fichier pdf sur <http://cssi.unige.ch>) CONCEPTS, PRATIQUES ET ASPECTS DE SÉCURITÉ DES COMMUNICATIONS INTERNET

**DATES** : 22/11, 29/11, 06/12, 13/12/07, 24/01/08, 07/02/08

Module sans crédit, en deux parties : **A.** 4 séances consacrées aux protocoles de la famille TCP/IP et à l'architecture internet (50% de théorie et 50% de mise en pratique directement sur l'infrastructure du laboratoire). Ces séances sont destinées aux participants inscrits au CSSI qui ont besoin d'une formation au socle de connaissances indispensables sur les réseaux informatiques avant de pouvoir aborder dans le module 3, les aspects spécifiques de leur sécurité. **B.** 2 séances pratiques en laboratoire dans le cadre du module 3 pour les participants qui souhaitent configurer un firewall personnel, utiliser des outils tels que nmap et nessus, cracker un mot de passe, chiffrer-signer des données, mettre en œuvre les mécanismes d'une infrastructure à clé publique.

### 3 SÉCURITÉ DANS LES RÉSEAUX INFORMATIQUES

**DATES :** 09/01/08, 16/01, 23/01, 24/01(opt.), 30/01, 06/02, 07/02(opt.), 13/02, 20/02

Architecture sécurisée des réseaux IP (VLAN, firewall, proxy); Attaques et menaces sur internet (email, virus, vers, code mobile, cheval de Troie, exploit); Détection d'intrusions; Introduction à la cryptographie (chiffrement, contrôle d'intégrité, signature numérique, certificat numérique); Infrastructure à clé publique (application e-commerce avec SSL); Efficacité des mots de passe; Identité numérique et authentification forte (OTP, token, biométrie); Intégration de l'authentification en entreprise; Réseaux privés (historique, VPN, IPSec); Techniques de hacking (méthodologie, exemples); Thèmes de la conférence Blackhat; Travaux en laboratoire (optionnels).

### 4 QUALITÉ INFORMATIQUE ET MANAGEMENT DE PROJETS

**DATES :** 27/02, 05/03, 12/03, 19/03, 26/03, 02/04, 09/04

Management de la qualité et entreprise : place des différents référentiels qualité dans la gestion d'une entreprise ; Exemple de management de la qualité dans la gestion du système d'information d'une industrie ; Quelques outils en management de la qualité informatique et leurs champs d'application ; Utilisation pratique des outils de management de la qualité dans un secteur informatique ; La place de la qualité en management de projet : présentation d'une méthodologie concrète, travail en groupe et restitution; Étude de cas d'une approche qualité en management de projet ; Évaluation des acquis et restitution avec commentaires.

### 5 ASPECTS JURIDIQUES DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

**DATES :** 09/04, 16/04, 23/04, 30/04, 07/05, 14/05, 21/05

Aspects préventifs : validité des documents et données, archivage, valeur de preuve, protection des données, secret et confidentialité; Aspects répressifs : responsabilité civile et pénale, propriété intellectuelle, concurrence déloyale ; Conséquences fiscales des échanges électroniques : archivage, imposition des revenus du e-commerce, TVA ; Particularités dans la conclusion des contrats : signatures électroniques, contrats à distance, contrats de consommation, contrats de sites web ; Particularités dans la gestion des litiges : sauvegarde et administration des preuves - "Computer Forensics"; Particularités de l'organisation des groupes d'entreprise et flux transfrontières de données.

### 6 MÉTHODES D'ÉVALUATION DES RISQUES ET D'AUDIT DES S.I.

**DATES :** 21/05, 28/05, 04/06, 11/06, 18/06, 25/06, 27/06

Méthode de gestion des risques des systèmes d'information ; Domaines de contrôle et principaux processus informatiques avec examen de quelques référentiels, dont ceux proposés par le CobIT de l'ISACA et l'ISO/IEC 17799 et 27001 ; Planification et exécution des missions d'évaluation des risques des systèmes d'information selon les exigences de l'entreprise ; Propositions de solutions pour réduire les faiblesses et améliorer la sécurité ; Démarche pour réaliser une politique de sécurité des systèmes d'information.

## Intervenants



**Christophe BARMAN** ■  
Change manager, Uniriscgroup, Genève

**Jean BLOCH** ■  
Directeur Aud-IT, Genève

**Antoine BOUR (CISSP)** ■  
IT Security Expert, SITA Security Services, Paris

**Charles-Henri CARLIN** ■  
Consultant, ELCA Informatique SA, Lausanne

**Alessandro COLARUSSO** ■  
Responsable Audit informatique, Lombard Odier Darier Hentsch & Cie, Genève

**Christian CRETENAND** ■  
Contre-espionnage, crime organisé et contre prolifération, Office Fédéral de la Police, Berne

**Jean-Paul DE BLASIS** ■  
Professeur ordinaire, HEC-Genève, Faculté des Sciences Economiques et Sociales, Université de Genève

**Eric DISSON** ■  
Enseignant-chercheur, IAE de Lyon, France

**Arnaud DUCROT** ■  
Fondé de pouvoir, Protectas S.A., Genève

**John FAVRE** ■  
Directeur Général, Protectas Systems SA, Genève

**Bernard FORAY (CISSP)** ■  
Responsable Sécurité Systèmes d'Information, Gemalto, Marseille

**Dirk LANGER** ■  
Avocat-conseil, Lalive & Associés Avocats, Genève

**James-Louis LINDER (CISSP)** ■  
Responsable sécurité, Banque Cantonale Vaudoise, Lausanne

**Gérald LITZISTORF** ■  
Professeur, HES, École d'Ingénieurs de Genève

**Sylvain MARET** ■  
Strategic Director, e-Xpert Solutions, Genève

**Patrick MARIET** ■  
Service Delivery Manager, Safe Host SA, Genève

**Claude MAURY (Lead Auditor)** ■  
Président du CLUSIS, Lausanne

**Jean MENTHONNEX** ■  
Professeur, Université de Besançon et Directeur du Centre EUROQUAL, Lausanne

**Jean-François MILHOMME** ■  
Solution Architect, Sun Microsystems, Gland

**Christophe NEMETH** ■  
Consultant, Nouvel Strategies, Genève

**Philippe OECHSLIN (CISSP)** ■  
Senior Researcher, LASEC/EPFL et conseil en sécurité informatique, Lausanne

**Gérald PAGE** ■  
Avocat-conseil, Étude Lalive, Genève

**Bernie PERROUD** ■  
Analyste non-prolifération, Office Fédéral de la Police, Berne

**Pierre-Alex RISSE** ■  
Corporate Quality Assessment System Auditor, Logitech., Romanel-sur-Morges

**Angelo SORMANI (CISA)** ■  
Chief Information Security Officer, Union Bancaire Privée, Genève

**Rémy TEXIER** ■  
Application Service Manager, Unicile IT Services, Prilly

**Michel VAUCHER (CISSP)** ■  
Consultant sécurité informatique, Genève

**Charl van der WALT (CISSP)** ■  
Consultant, SensePost Co., Centurion, Afrique du Sud

**Maurice WENGER** ■  
Responsable Cellule Sécurité des systèmes d'information, État de Genève

## Conditions d'obtention et titres délivrés

Les modalités d'évaluation des connaissances sont définies dans le règlement d'étude du programme remis aux participants en début de formation.

L'obtention du certificat ou diplôme est conditionnée à la fréquentation assidue de tous les modules et à l'exécution de tous les travaux requis à la satisfaction des enseignants. Toute absence doit être justifiée. Une moyenne générale de 4.0/6.0 est exigée pour réussir le programme. Une seule note entre 3.0 et 3.75 à un module peut être compensée pour autant que la moyenne générale soit au moins égale à 4.0. Une note inférieure à 3.0 ne donne pas droit aux crédits et nécessite la répétition du module l'année suivante.

Titres officiels de l'Université de Genève, le **Certificat de formation continue en Sécurité des Systèmes d'Information** ainsi que le **Diplôme de formation continue d'Expert en Sécurité des Systèmes d'Information** seront délivrés aux étudiants ayant satisfait aux conditions d'évaluation des connaissances du Certificat (18 crédits) ou du Diplôme (36 crédits).

Les participants inscrits à un ou plusieurs modules isolés recevront une attestation de réussite s'ils satisfont aux conditions d'attribution des crédits correspondants.

## MBA mention "sécurité des systèmes d'information"

Plusieurs de nos anciens étudiants ont obtenu le Master in Business Administration (MBA) avec la mention "sécurité des systèmes d'information". Les candidats déjà titulaires d'un diplôme universitaire, qui souhaitent s'inscrire au MBA doivent d'abord obtenir le Certificat en Management et Administration des Affaires (MAA) la 1<sup>ère</sup> année. Puis ils s'inscriront au CSSI dont les modules seront crédités comme partie substantielle du programme de leur 2<sup>e</sup> année et qu'ils complèteront avec quelques modules à prendre dans d'autres certificats pour obtenir le nombre de crédits ECTS requis pour le MBA. Par principe, le mémoire de MBA se fera dans une matière relevant du CSSI.

Les conditions d'admission au MBA sont les suivantes :

- Être titulaire d'un diplôme universitaire ou titre jugé équivalent (HES par ex.)
- Justifier d'une expérience professionnelle pertinente de trois années au minimum
- Avoir réussi le Certificat MAA
- Posséder une excellente maîtrise parlée et écrite du français comme de l'anglais
- Avoir la pratique des logiciels bureautiques de base
- GMAT ou autres bases en gestion et informatique

Pour toute information complémentaire, prière de s'adresser directement au :

Programme MBA  
HEC – Université de Genève  
Uni Mail – 40, bd du Pont-d'Arve – 1211 Genève 4  
Tél. : 022 379 88 09  
e-mail : mba@hec.unige.ch  
<http://mba.unige.ch>



## Renseignements pratiques

### CONDITIONS D'ADMISSION

L'admission des candidats est prononcée par le Comité scientifique du Certificat sur examen d'un dossier constitué du bulletin d'inscription, auquel doivent être annexés :

- 1) un curriculum vitæ résumé (formulaire à télécharger sur <http://CSSI.unige.ch>)
- 2) un curriculum vitæ complet
- 3) une lettre de motivation
- 4) une lettre de recommandation, si possible
- 5) 1 photo passeport

Aucune candidature ne sera recevable après le début des cours.

### CONNAISSANCES PRÉALABLES REQUISES

Les candidats doivent être familiarisés avec les outils, méthodes et normes de base de gestion et d'utilisation des systèmes d'information. La connaissance de l'anglais technique est recommandée.

### DÉLAI D'INSCRIPTION

La candidature d'inscription doit parvenir **avant le 30 juin 2007**, adressée à :

Jean-Paul De Blasis, Formation en Sécurité des Systèmes d'Information  
HEC-Genève, Université de Genève, Bd du Pont-d'Arve 40, 1211 Genève 4

Les demandes arrivées après ce délai seront prises en compte selon les places disponibles.

### HORAIRE / ORGANISATION

Le certificat est organisé en 6 modules agencés chaque mercredi de 17h15 à 21h00. Un planning horaire précis sera remis en début de programme.

### LIEU

Université de Genève, Uni-Mail, Bd du Pont-d'Arve 40, 1211 Genève 4

### FRAIS DE PARTICIPATION

CHF 9'000.- pour le Certificat de 1<sup>ère</sup> année + CHF 1'500.- pour le module en option.

CHF 9'000.- pour le programme du Diplôme de 2<sup>e</sup> année.

L'admission à un ou plusieurs modules isolés est subordonnée au nombre de places disponibles. Le coût est de CHF 1'800.- par module.

L'État de Genève encourageant la formation professionnelle des adultes, un chèque annuel de CHF 750.- peut être demandé **avant le début des cours** par les étudiants répondant aux critères. Informations disponibles sur : <http://www.geneve.ch/bourses>

### PRINCIPES DE VALIDATION DES CANDIDATURES ET RÈGLES D'ANNULATION

Après délibération du comité scientifique, les candidats sont informés par courrier de l'acceptation ou non de leur dossier. Les candidats retenus doivent avoir réglé la finance d'inscription à la date indiquée sur le courrier pour valider leur inscription sinon elle est annulée de fait. Tout renoncement dans les 30 jours suivants, mais avant le début des cours, entraîne la perception d'une retenue de CHF 500.- pour frais administratifs. Tout renoncement après le début des cours donne lieu au remboursement de 50 % du montant au prorata des modules non intégralement suivis. Les demandes de report ou d'annulation doivent être formulées par écrit.

## Direction

**Jean-Paul DE BLASIS**,  
Professeur HEC,  
Université de Genève



## Comité directeur

**Monsieur Jean BLOCH**, Directeur, Aud-IT, Genève  
**Prof. Jean-Paul DE BLASIS**, Faculté des S.E.S./HEC, Université de Genève  
**Monsieur Arnaud DUCROT**, Fondé de pouvoir, Protectas SA, Genève  
**Prof. Gérald LITZISTORF**, HES-SO/EIG, Genève  
**Monsieur Jean-Pierre THERRE**, CSO, Pictet & Cie, Genève

## Conseil scientifique

**Monsieur Pierre DELETRAZ**, Directeur, Computing Services & Security, Genève  
**Prof. Pascal DUMONTIER**, Faculté des S.E.S., HEC-Genève  
**Prof. Eugène HORBER**, Faculté des S.E.S., Sciences Sociales  
**Docteur Mitsuko KONDO OESTREICHER**, Hôpitaux Universitaires de Genève  
**Monsieur James LINDER**, Resp. Sécurité, Banque Cantonale Vaudoise, Lausanne  
**Monsieur Claude MAURY**, Président du CLUSIS (Association suisse de la sécurité des systèmes d'information, Lausanne)  
**Prof. Jean MENTHONNEX**, Université de Franche-Comté et Directeur du Centre inter-universitaire EUROQUAL, Lausanne  
**Maître Gérald PAGE**, Avocat, Étude Lalive, Genève  
**Monsieur Angelo SORMANI**, Responsable sécurité, Union Bancaire Privée, Genève  
**Monsieur Michel VAUCHER**, Consultant en sécurité informatique, Valleiry  
**Monsieur Maurice WENGER**, Responsable de la cellule de sécurité des systèmes d'information, État de Genève

## Contacts et Informations

Le Professeur Jean-Paul De Blasis, responsable de la formation, se tient volontiers à disposition pour tout renseignement complémentaire sur le contenu du programme :  
tél. **022 379 81 28** fax : **022 379 81 04** email : **deblasis@hec.unige.ch**

Pour toute autre question, contacter :  
Secrétariat formation continue, HEC-Genève  
UNI MAIL  
Bd du Pont-d'Arve 40  
1211 Genève 4

Tél. : 022 379 88 00  
Fax : 022 379 81 04  
Email : **CSSI@hec.unige.ch**  
**http://www.hec.unige.ch**

## Formation Continue Universitaire • Bulletin d'Inscription Programme de formation continue en Sécurité des Systèmes d'Information Information Systems Security Officer Certification

UNIVERSITÉ  
DE GENÈVE



Bulletin d'inscription et dossier complet à envoyer **avant le 30 juin 2007 dernier délai** à :  
Prof. J.-P. De Blasis, SES-HEC, Université de Genève, Bd du Pont-d'Arve 40, CH-1211 Genève 4 (ou par fax: 022 379 81 04)  
**(s.v.p., à remplir en lettres majuscules)**

Nom	Prénom	<input type="checkbox"/> MME	<input type="checkbox"/> M.			
Date de naissance (JJ/MM/AAAA) :	Lieu :	Nationalité :	État civil :			
Profession/Qualification						
Niveau de fin d'études	<input type="checkbox"/> CFC	<input type="checkbox"/> Maturité/Bac	<input type="checkbox"/> HES	<input type="checkbox"/> École de commerce	<input type="checkbox"/> Université, EPF	<input type="checkbox"/> Autre :
Entreprise (en toutes lettres)						
Adresse	<input type="checkbox"/> Professionnelle	Ville				
	ou <input type="checkbox"/> Privée	Ville				
Adresse de facturation :						
Téléphone	<input type="checkbox"/> Professionnel	Fax	<input type="checkbox"/> e-mail			
	ou <input type="checkbox"/> Privé	Fax	<input type="checkbox"/> e-mail			

Adresse pour l'envoi postal :  professionnelle  privée (ne cocher qu'une seule case)

- Je souhaite participer au **Certificat** de formation continue universitaire en Sécurité des Systèmes d'Information et m'engage à verser la somme de CHF 9'000.- dès réception de la confirmation de mon admission.  Je suis membre du CLUSIS n° ..... et bénéficie d'une remise de CHF 500.-.
- Je souhaite aussi participer au module optionnel "Concepts, pratiques et aspects de sécurité des communications internet" et m'engage à verser la somme de CHF 1'500.- (à régler en même temps que l'inscription par les participants retenus).
- Je suis déjà titulaire du CSSI année : ..... et je souhaite m'inscrire au programme du **Diplôme** de formation continue universitaire d'Expert en Sécurité des Systèmes d'Information. Je m'engage à verser la somme de CHF 9'000.- dès réception de la confirmation de mon admission.

**SVP joindre les pièces suivantes :**

- 1 fiche résumé-CV à télécharger  1 CV détaillé + copie des diplômes  1 lettre de motivation  1 lettre de recommandation si possible  1 photo ID
- En cas d'inscription à un ou plusieurs modules isolés, je souhaite participer au(x) module(s) suivant(s) : Module  1,  2,  3,  4,  5,  6 et je m'engage à verser la somme de CHF 1'800.- par module dès réception de la confirmation d'inscription.

J'ai connaissance que, si ma candidature est acceptée, mon inscription doit être confirmée par le versement des frais de participation. Si je me désiste avant le début des cours, je m'engage à régler CHF 500.- pour frais administratifs. Si je renonce après, je ne serais remboursé que de 50 % des modules que je n'aurais pas suivis entièrement.

Lieu et date :

Signature :



## Sécurité des Systèmes d'Information

· CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · CONTRÔLE DE GESTION · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · E-BUSINESS & E-COMMUNICATION · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · ENTREPRENEURSHIP · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · FINANCE D'ENTREPRISE CONTEMPORAINE · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · GESTION DANS LES ORGANISMES SANS BUT LUCRATIF · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · GESTION DE L'ENVIRONNEMENT ET ENTREPRISE · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · GESTION DES RESSOURCES HUMAINES · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MANAGEMENT DE PROJETS · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MANAGEMENT DES INSTITUTIONS DE SANTÉ · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MANAGEMENT DES INSTITUTIONS SOCIALES · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MANAGEMENT ET ADMINISTRATION DES AFFAIRES · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MANAGEMENT INTERNATIONAL DES AFFAIRES · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MANAGEMENT STRATÉGIQUE DU PROCESSUS ACHATS, LOGISTIQUE ET APPROVISIONNEMENTS · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MARKETING · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · SÉCURITÉ DES SYSTÈMES D'INFORMATION · CERTIFICAT DE FORMATION CONTINUE UNIVERSITAIRE · MBA MASTER OF BUSINESS ADMINISTRATION · DOCTORAT EN GESTION D'ENTREPRISE · DEA EN GESTION D'ENTREPRISE · DEA EN ÉCONOMIE ET FINANCE · LICENCE EN GESTION D'ENTREPRISE · INTERNATIONAL ORGANIZATIONS MBA

## Parmi les entreprises ayant participé au certificat

ABN-AMRO Bank	HSBC Republic Bank
Adecco	IATA
Andersen Worlwide	IBM Suisse
Banque Édouard Constant	ILEM
Banque Cantonale de Genève	ING Baring
Banque Cantonale du Jura	Institut Central des Hôpitaux Valaisans
Banque Cantonale Vaudoise	Intra Assurances
Banque de Commerce et de Placements	J. T. International
Banque Pictet & Cie	Julius Baer Bank
Banque Privée Edmond de Rothschild	KPMG FidesManagement
BIT Bureau International du Travail	La Poste Suisse
BNP Paribas Services	Lloyds TSB International Private Banking
Bordier & Cie	Lombard, Odier, Darier, Hentsch & Cie
Bridport & Cie	Ministère de la Défense, Burkina Faso
Caterpillar	Mirabaud & Cie
Centrale de Compensation	Montres Rolex
CERN	Morgan Stanley Capital International
CISCO Systems	Nagra / Kudelski Group
COLT Telecom	National Bank of Koweit
Compagnie Bancaire Espirito Santo SA	NEO Technologies
Computing Services & Security	Nestlé Suisse
Crédit Lyonnais	Office des Nations Unies
Crédit Suisse	OMM
Danzas	OMPI
Darier Hentsch & Cie	Pictet & Cie
DAS Protection Juridique	Proactive Partners
Deutsche Bank	Providentia Assurances Vie
Discount Bank and Trust Co.	Royal Bank of Canada
DSG Damart Somfy	Sanofi
EFG Private Bank	Serono International
EDS Information	Services Industriels de Genève
EIVD	SITA
Elca Informatique	Skyguide
Elvia-Groupe Allianz	Société Suisse des Employés de Commerce
Eqant Communication	STMicroelectronics
ERI Bancaire	Sun Microsystems
Ericsson Business Services	Swisscom
État de Fribourg	Tamoil
État de Genève	Télévision Suisse Romande
État de Vaud	Thalès Suisse
Ferrier Lullin & Cie	The Swatch Group Ltd
Firmenich	Tetra Laval Finance & Treasury
Givaudan	Total Oil Trading
Groupe Mutuel	Touring Club Suisse
Gucci Group Watches	T-Systems International
HES/EIG Genève	UBS
HES Yverdon	UIT
Hôpital de Morges	UNICIBLE IT Services
Hôpitaux Universitaires de Genève	Union Bancaire Privée
Hospices Cantonaux	Université de Fribourg
Hewlett Packard	Zürich Assurances