

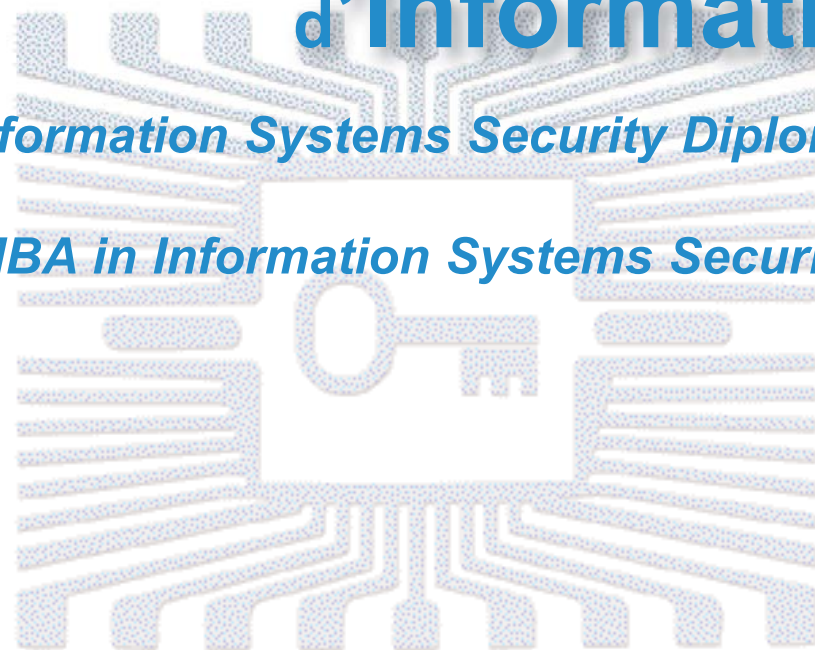


Formation Continue  
Universitaire

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

*Information Systems Security Diploma*

*MBA in Information Systems Security*



**UNIVERSITÉ  
DE GENÈVE**

**HEC**  
GENÈVE

Session 2008-2009

<http://dssi.unige.ch>

## Diplôme de formation continue universitaire

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 deux niveaux.

Candidats ne possédant pas forcément un titre universitaire :

- 1. Diplôme en Sécurité des Systèmes d'Information (DSSI)**  
sur trois semestres

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

- 2. MBA en Sécurité des Systèmes d'Information**  
sur 2 années universitaires



### Sécurité des Systèmes d'Information

· diplôme de formation continue universitaire · contrôle de gestion · diplôme de formation continue universitaire · e-business & e-communication · diplôme de formation continue universitaire · entrepreneurship & business development · diplôme de formation continue universitaire · gestion dans les organismes sans but lucratif · diplôme de formation continue universitaire · gestion de l'environnement et entreprise · diplôme de formation continue universitaire · gestion d'entreprise - licence en sciences de gestion · diplôme de formation continue universitaire · gestion des ressources humaines · diplôme de formation continue universitaire · management de projets · diplôme de formation continue universitaire · management et administration des affaires · diplôme de formation continue universitaire · management des institutions de santé · diplôme de formation continue universitaire · management des institutions sociales · diplôme de formation continue universitaire · management international des affaires · diplôme de formation continue universitaire · management stratégique du processus achats, logistique et approvisionnements · diplôme de formation continue universitaire · sécurité des systèmes d'information · diplôme de formation continue universitaire · stratégie marketing · diplôme de formation continue universitaire · stratégie marketing, communication & e-business · diplôme de formation continue universitaire · international organizations mba · mba master of business administration ·



# Sécurité des Systèmes d'Information

Diplôme de formation continue universitaire

**Septembre 2008 à octobre 2009**

| Page | Sommaire   |
|------|--|
| 2    | ■ Contexte et objectifs de la formation<br>■ Étendue des risques informatiques                     |
| 3    | ■ Objectif de notre formation  |
| 4    | ■ Diplôme ou MBA ?<br>■ Public visé<br>■ Durée de la formation                                     |
| 5    | ■ Évaluation des connaissances<br>■ Charge de travail<br>■ Modules 1 et 2                          |
| 6    | ■ Modules 3 à 7  |
| 7    | ■ Modules 8 à 10   |
| 8    | ■ Intervenants   |
| 9    | ■ Conditions d'obtention et titres délivrés<br>■ MBA mention "Sécurité des Systèmes d'Information" |
| 10   | ■ Renseignements pratiques   |
| 11   | ■ Direction du Diplôme<br>■ Comité Directeur et Conseil Scientifique<br>■ Contacts & Informations  |
| 12   | ■ Bulletin d'inscription   |

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 de leurs traitements. Les référentiels actuels pour la sécurité des informations, tels que la série des normes ISO 27000, 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.

## 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.

# Objectif de 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 250 participants ont suivi nos formations en sécurité des systèmes d'information et constituent un réseau actif. C'est d'ailleurs notre fierté de constater que nombre de nos diplômés sont devenus aujourd'hui des personnalités de premier plan du monde de la sécurité de l'information en Suisse romande.

L'information numérique a envahi les organisations contemporaines en constituant une véritable ressource qui assure, à tous les niveaux, son bon fonctionnement, voire sa survie. A ce titre, les responsables chargés de la sécurité de l'information doivent, avant tout, posséder de solides connaissances des organisations tirées de nombreuses années d'expérience professionnelle, puis avoir su se former pour acquérir les compétences multidisciplinaires indispensables.

Ces professionnels peuvent avoir diverses dénominations et occuper diverses positions hiérarchiques selon la nature des ressources à protéger. La fonction la plus couramment répandue est celle de RSSI (Responsable de la Sécurité des Systèmes d'Information). Il/elle est en charge de la mise en œuvre de la politique organisationnelle de sécurité de l'information dans les entreprises et administrations. Dans les pays anglo-saxons, la dénomination est "*Information Systems Security Officer*", voire "*Chief Information Security Officer (CISO)*".

Pour assurer cette mission, ces spécialistes doivent être formés à la culture multidimensionnelle du champ de la sécurité des informations :

- **dimension managériale** : évaluation et gestion des risques de l'information, mise en place d'indicateurs et métriques, retour sur investissements, organisation de la sécurité, plan de continuité d'activités, méthodologie d'audit, etc.
- **dimension organisationnelle et humaine** : plan d'assurance qualité et référentiels qualité, management de projets, sensibilisation et motivation du personnel, plans de secours informatique, etc.
- **dimension technologique** : nouvelles applications de l'informatique, refonte des systèmes d'information, sécurité des réseaux et des communications internet, architectures de sécurité, etc.
- **dimension juridique** : mise en conformité avec les réglementations (de type IFRS, Sarbanes-Oxley ou Bâle II par exemple), avec les lois actuelles (protection des données, propriété intellectuelle, etc.) et les conventions internationales.

Comme le montre cet inventaire – non exhaustif – des compétences et connaissances requises, les risques sur la sécurité de l'information (et sur les systèmes d'information qui en assurent la saisie-mémorisation, le traitement et la communication) ne se limitent pas aux seuls 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 ses ressources humaines, etc.

Il s'agit donc d'aller au-delà de la seule sécurité informatique pour englober tous les processus liés à la protection du patrimoine informationnel des organisations. Nos programmes de formation continue à la sécurité des systèmes d'information visent à faire acquérir à nos étudiants ces compétences pour qu'ils deviennent les "couteaux suisses" de la sécurité de l'information dans leurs entreprises et administrations.

Bien que dispensé en français, ce Diplôme 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.

## Diplôme ou MBA ?

---

La formation de base est le “**Diplôme de formation continue en Sécurité des Systèmes d’Information (DSSI)**” visant à former des professionnels aguerris aux concepts, moyens et méthodes de la sécurité des S.I. Les 10 modules du Diplôme, représentant 240 heures de cours (30 crédits ECTS - European Credit Transfer and accumulation System).

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 1ère année de formation au management général, ils pourront suivre les modules du DSSI dans le cadre de leur 2e année de spécialisation et obtenir le **MBA en Sécurité des Systèmes d’Information**. Voir p. 9 pour davantage de détails.

## Public visé

---

Ces formations s’adressent 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 Diplôme est composé de 10 modules de 24 heures d’enseignement chacun, y compris le contrôle des connaissances. Chaque module est équivalent à 3 crédits ECTS. Chaque module comporte cinq séances de quatre heures. Une sixième séance est réservée au contrôle des connaissances suivi de la correction de l’épreuve. L’ensemble se déroule sur une année universitaire.

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 Diplôme

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

**1 DATES :** 03/09, 10/09, 17/09, 24/09, 01/10, 08/10 2008

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.

### **ÉVALUATION ET GESTION DES RISQUES DE L'INFORMATION**

**2 DATES :** 08/10, 15/10, 22/10, 29/10, 05/11, 12/11 2008

Concepts fondamentaux de la gestion des risques ; La gestion des risques opérationnels ; Les risques informatiques ; Synthèse des normes ISO 13335-2 et BSI 7799-3 et évolution vers ISO 27005 ; Approches normalisées d'analyse de risques ; Présentation de la méthode EBIOS et de son articulation avec l'ISO 2700x ; La gestion des risques sous l'angle de l'assureur ; RSSI et gestion des risques.

## **SÉCURITÉ PHYSIQUE ET CONTINUITÉ DES ACTIVITÉS**

---

**3**

**DATES** : 12/11, 19/11, 26/11, 03/12, 10/12, 17/12 2008

Stratégies de protection physique pour les ressources (humaines, matérielles et immatérielles) des systèmes d'information : mise en place de solutions adaptées dans le domaine de la sécurité incendie, anti intrusion, le contrôle des accès et la vidéo-surveillance. Éclairage sur les méthodes de recherche d'information : veille, intelligence et espionnage économique.

Stratégies de continuité des affaires : méthodologie, politique, stratégie, scénarios, plans et mesures pour garantir en toutes circonstances la continuité des activités. Identification des risques à prendre en compte et analyse d'impact. Introduction à la gestion de crise.

## **ARCHITECTURES TECHNIQUES DE SÉCURITÉ**

---

**4**

**DATES** : 07/01, 14/01, 21/01, 28/01, 04/02, 11/02 2009

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).

## **PROTOCOLES INTERNET DANS UNE OPTIQUE SÉCURITÉ**

---

**5**

**DATES** : 08/01, 15/01, 22/01, 29/01, 05/02, 12/02 2009

Module subdivisé en une partie théorique (50%) et une partie pratique (50%) dispensée sur l'infrastructure du laboratoire.

Partie théorique : Architecture internet et modèle en couches ; Protocoles de la famille TCP/IP (Ethernet, IP, ARP, ICMP, UDP, TCP, http, DNS, DHCP) ; Composants réseau (hub, switch, routeur) ; Topologie ; Gouvernance internet.

Partie pratique basée sur les outils ipconfig, arp, ping, tracert, whois, superscan, wireshark, TCPView, netstat, nslookup ; Configuration de l'interface Ethernet ; Paramètres et compteurs d'un commutateur Ethernet.

## **SÉCURITÉ DANS LES RÉSEAUX INFORMATIQUES**

---

**6**

**DATES** : 11/02, 18/02, 25/02, 04/03, 11/03, 18/03 2009

Architecture sécurisée des réseaux IP (VLAN, firewall, proxy); Tests de pénétration ; Bonnes pratiques ; 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) ; Infrastructure à clé publique (certificat numérique, 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) ; Épreuves du concours CTF (Defcon).

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

---

**7**

**DATES** : 18/03, 25/03, 01/04, 08/04, 15/04, 22/04 2009

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.

## **QUALITÉ INFORMATIQUE ET MANAGEMENT DE PROJETS**

---

**8** **DATES** : 22/04, 29/04, 06/05, 13/05, 20/05, 27/05 2009

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 : Étude de cas d'une approche qualité en management de projet ; Travail en groupe et restitution ; Évaluation des acquis et restitution avec commentaires.

## **CONCEPT ET MÉTHODOLOGIE D'AUDIT DES SYSTÈMES D'INFORMATION**

---

**9** **DATES** : 27/05, 03/06, 10/06, 17/06, 24/06, 01/07 2009

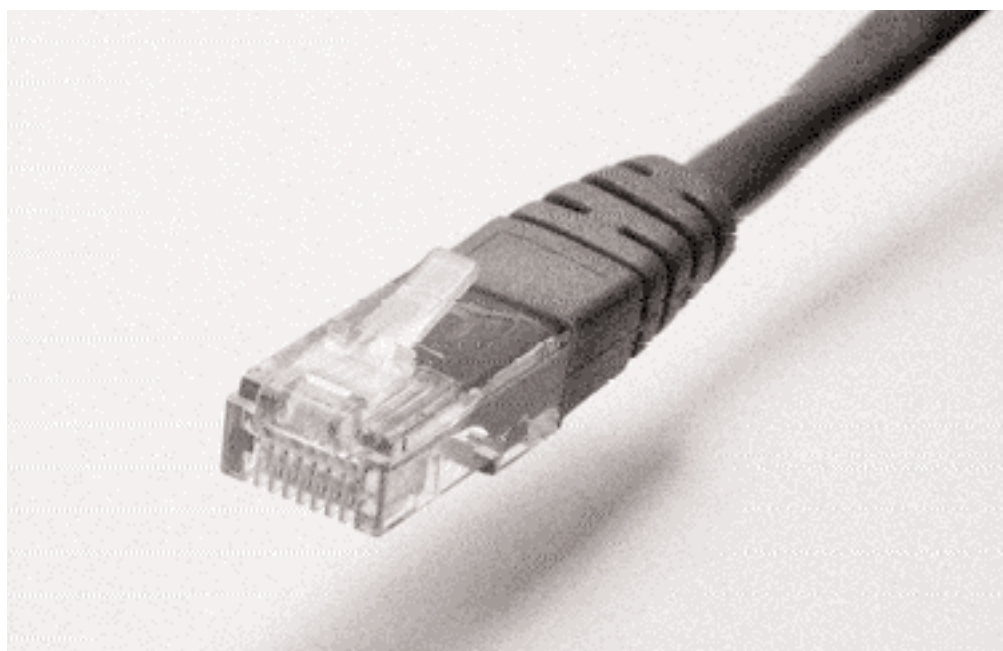
Introduction au référentiel CobiT 4.1 ; Planification d'une mission d'audit IT et établissement d'un plan de mission ; L'audit IT et le contrôle interne ; Concept d'évaluation des risques IT (rappel) ; Introduction à l'IT Assurance Guide (concept CobiT) ; Audit du cycle de développement des systèmes (SDLC) et expériences pratiques d'un auditeur IT ; Établissement d'un rapport d'audit IT ; Audit des accès logiques ; Le tableau de bord du RSSI ; Audit de la gestion des changements et de la gestion de la configuration ; Appréciation des risques sur le personnel ; Audit de la gestion des incidents et de la gestion des problèmes ; Évaluation des acquis et restitution avec commentaires.

## **SÉMINAIRES SUR LA SÉCURITÉ DES INFORMATIONS**

---

**10** **DATES** : de septembre 2008 à octobre 2009

Validation du suivi de six séminaires à choix proposés par les associations partenaires (CLUSIS, GRIFES, FGS, FMQ, etc.) durant la période. Ces séminaires en rapport avec l'un ou l'autre des thèmes abordés dans les modules, visent à initier les étudiants à la pratique d'entretien continu de leurs connaissances par la participation régulière aux travaux de groupes professionnels locaux. Pour chacun des séminaires suivis, l'étudiant devra produire, pour validation, une synthèse faisant ressortir les points-clés de la manifestation et proposant une critique succincte des travaux.



# Intervenants



## **Christophe BARMAN** ■

Change manager, Uniriscgroup, Genève

## **Jean BLOCH** (*Lead Auditor*) ■

Directeur Aud-IT, Genève

## **Antoine BOUR** (*CISSP*) ■

IT Security Expert, SITA Security Services, Paris

## **Olivier BUSOLINI** ■

Consultant, NetExpert, Gland

## **Charles-Henri CARLIN** ■

Consultant, ELCA Informatique SA, Lausanne

## **Gérard CHATELAIN** ■

Head of Operations, HSBC, Genève

## **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

## **Éric DISSON** ■

Enseignant-chercheur, IAE de Lyon, France

## **Frédéric DOMMART** ■

Risk Manager, Banque Cantonale Vaudoise, Lausanne

## **Arnaud DUCROT** (*SEQI, MBA HEC-Genève*) ■

Fondé de pouvoir, Protectas S.A., Genève

## **John FAVRE** ■

Directeur Général, Protectas Systems SA, Genève

## **Bernard FORAY** (*CISSP*) ■

Responsable Sécurité Systèmes d'Information, Groupe Casino, Saint-Etienne, France

## **Christophe GABIOUD** (*CSSI, MBA HEC-Genève*) ■

Directeur, Analyse des risques informatiques, UBS, Zürich

## **Laura GEORG** (*CSSI, Docteur HEC-Genève*) ■

Consultante, Detecon, Zürich

## **John GUNSON** (*Docteur HEC-Genève*) ■

Professeur, University of Wales Institute at Cardiff

## **Dirk LANGER** ■

Avocat-conseil, Étude Lalive, Genève

## **James-Louis LINDER** (*SEQI, CISSP*) ■

Responsable sécurité, Banque Cantonale Vaudoise, Lausanne

## **Gérald LITZISTORF** (*SEQI*) ■

Professeur, HES, École d'Ingénieurs de Genève

## **Olivier LUXEREAU** ■

Consultant, NetExpert, Gland

## **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** (*CSSI, MBA HEC-Genève*) ■

Solution Architect, Sun Microsystems, Gland

## **Christophe NEMETH** ■

Consultant, Nouvel Strategies, Genève

## **Philippe OECHSLIN** (*CISSP*) ■

Chargé de cours EPFL et directeur Objectif Sécurité, Gland

## **Gérald PAGE** (*Docteur en Droit*) ■

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

## **David ROYSTON** ■

Directeur, Royston Consulting, Genève

## **Jean-Marc SOLLEDER** (*CSSI*) ■

Security Engineer, SCRT, Prévèrenges

## **Angelo SORMANI** (*CSSI, CISA*) ■

Responsable de la sécurité, Union Bancaire Privée, Genève

## **Paul SUCH** ■

Directeur, SCRT, Prévèrenges

## **Jean-Pierre THERRE** ■

Chief Security Officer, Pictet & Cie Banquiers, Genève

## **Rémy TEXIER** ■

Application Service Manager, Unicile IT Services, Prilly

## **Michel VAUCHER** (*CSSI, CISSP*) ■

Consultant sécurité informatique, Genève

## **Mauro VIGNATI** ■

Analyst MELANI/Cybercrime, Office Fédéral de la Police, Berne

## **François-Xavier VINCENT** ■

Gouvernance de la sécurité de l'information, Groupe AXA, France

## **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 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.

Titre officiel de l'Université de Genève, le **Diplôme de formation continue en Sécurité des Systèmes d'Information** est délivré aux étudiants ayant satisfait aux conditions d'évaluation des connaissances du Diplôme (30 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 Diplôme en Management et Administration des Affaires (MAA) la première année.

Puis ils s'inscriront au DSSI dont les 10 modules seront crédités comme partie substantielle du programme de leur 2e année et qu'ils complèteront avec trois modules à prendre dans d'autres certificats afin d'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.)
- Avoir réussi le MAA
- Justifier d'une expérience professionnelle pertinente de trois années au minimum
- 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](mailto: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://DSSI.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 2008**, 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 10 modules agencés chaque mercredi de 17h15 à 21h00 (sauf modules 5 et 10). La plupart des séances d'examen clôturant chaque module auront lieu les mercredis de 14h15 à 17h00 avant le début du module suivant. Un planning horaire annuel précis est disponible sur le site du Diplôme (<http://dssi.unige.ch>) et 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 11'500.- pour le Diplôme

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 d'attribution. 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, Président HEC-Genève  
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. Eugène HORBER**, Université de Genève, Faculté des S.E.S., Sciences Sociales

**Prof. Dimitri KONSTANTAS**, Université de Genève, Faculté des S.E.S., Département des  
Systèmes d'Information

**Docteur Mitsuko KONDO OESTREICHER**, Hôpitaux Universitaires de Genève

**Monsieur James LINDER**, Responsable 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, Genève

**Monsieur Maurice WENGER**, Ancien 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 : **dssi@hec.unige.ch**

**http://www.hec.unige.ch**

## Diplôme de formation continue en Sécurité des Systèmes d'Information

### Information Systems Security Officer Diploma

Bulletin d'inscription et dossier complet à envoyer avant le **30 juin 2008** dernier délai à :  
Prof. J.-P. De Blasis, Université de Genève, SES-HEC, 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   MME  M.

Date de naissance (JJ/MM/AAAA) :  Lieu :  Nationalité :  État civil :

Profession/Qualification

Niveau de fin d'études  CFC  Maturité/Bac  HES  École de commerce  Université, EPF  Autre :

Entreprise (en toutes lettres)

Adresse  Professionnelle  Ville

ou  Privée  Ville

Adresse de facturation :

Téléphone  Professionnel  Fax  e-mail

ou  Privé  Fax  e-mail

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

- Je souhaite participer au Diplôme de formation continue universitaire en **Sécurité des Systèmes d'Information** et m'engage à verser la somme de CHF 1'500.- dès réception de la confirmation de mon admission.  Je suis membre du CLUSIS n°..... et bénéficie d'une remise de CHF 500.-.

**SVP joindre les pièces suivantes :**

- 1 fiche résumé-CV à télécharger sur [dssi.unige.ch](http://dssi.unige.ch)  1 CV détaillé + copie des diplômes  1 lettre de motivation  1 lettre de recommandation  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,  7,  8,  9 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.

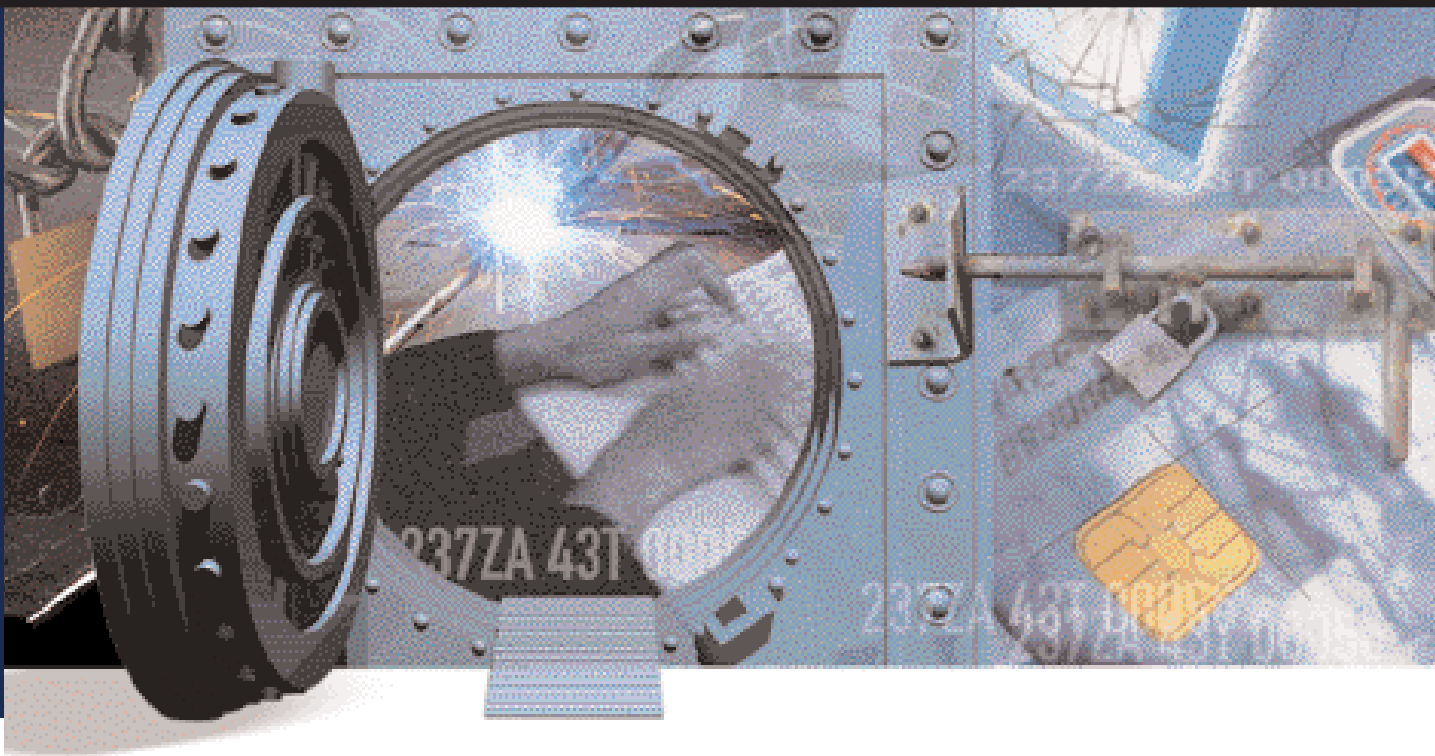
Lieu et date :

Signature :

## Parmi les entreprises ayant participé à nos formations en sécurité des systèmes d'information

---

|                                     |  |
|-------------------------------------|--|
| ABN-AMRO Bank                       | IBM Suisse                               |
| Adecco                              | ILEM                                     |
| Aéroport International Genève       | ING Baring                               |
| Andersen Worldwide                  | Institut Central des Hôpitaux Valaisans  |
| Banque Édouard Constant             | Intra Assurances                         |
| Banque Cantonale de Genève          | J.T. International                       |
| Banque Cantonale du Jura            | Julius Baer Bank                         |
| Banque Cantonale Vaudoise           | KPMG Fides Management                    |
| Banque de Commerce et de Placements | KredietBank Suisse                       |
| Banque Pictet & Cie                 | La Poste Suisse                          |
| Banque Privée Edmond de Rothschild  | Lloyds TSB International Private Banking |
| BIT Bureau International du Travail | Lombard, Odier, Darier, Hentsch & Cie    |
| BNP Paribas Services                | Mairie de Chamonix                       |
| Bordier & Cie                       | Microsoft Suisse                         |
| Bridport & Cie                      | Ministère de la Défense, Burkina Faso    |
| Caran d'Ache                        | Mirabaud & Cie                           |
| Caterpillar                         | Montres Rolex                            |
| Centrale de Compensation            | Morgan Stanley Capital International     |
| CERN                                | Nagra /Kudelski Group                    |
| CISCO Systems                       | National Bank of Koweit                  |
| COLT Telecom                        | NEO Technologies                         |
| Compagnie Bancaire Espirito Santo   | Nestlé Suisse                            |
| Computing Services & Security       | Office des Nations Unies                 |
| Crédit Lyonnais                     | OMM                                      |
| Crédit Suisse                       | OMPI                                     |
| Danzas                              | Oracle Software Suisse                   |
| DAS Protection Juridique            | Pictet & Cie                             |
| Deutsche Bank                       | Proactive Partners                       |
| Discount Bank and Trust Co.         | Providentia Assurances Vie               |
| DSG Damart Somfy                    | Raymond Weil                             |
| EFG Private Bank                    | Royal Bank of Canada                     |
| EDS Information                     | Sanofi                                   |
| EIVD                                | Serono International                     |
| Elca Informatique                   | Services Industriels de Genève           |
| Elvia-Groupe Allianz                | SITA                                     |
| Equant Communication                | Skyguide                                 |
| ERI Bancaire                        | Sté Suisse Employés de Commerce          |
| Ericsson Business Services          | STMicroelectronics                       |
| État de Fribourg                    | Sun Microsystems                         |
| État de Genève                      | Swisscom                                 |
| État de Vaud                        | Tamoil                                   |
| Ferrier Lullin & Cie                | Télévision Suisse Romande                |
| Firmenich                           | TDC Suisse – Sunrise                     |
| Givaudan                            | Thalès Suisse                            |
| Groupe Mutuel                       | The Swatch Group Ltd                     |
| Gucci Group Watches                 | Tetra Laval Finance & Treasury           |
| HES/EIG Genève                      | Total Oil Trading                        |
| HES Yverdon                         | Touring Club Suisse                      |
| Hôpital de Morges                   | T-Systems International                  |
| Hôpitaux Universitaires de Genève   | UBS                                      |
| Hospices Cantonaux                  | UIT                                      |
| Hewlett Packard                     | UNICIBLE IT Services                     |
| HSBC Private Bank                   | Union Bancaire Privée                    |
| Hospice Général                     | Université de Fribourg                   |
| IATA                                | Zürich Assurances                        |



HEC Genève  
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  
<http://www.hec.unige.ch>