ICT Security Expert
avec diplôme fédéral

ISEIG
Institut Suisse d'Enseignement de l'Informatique de Gestion

ISEIG - Institut Suisse d'Enseignement de l'Informatique de Gestion
Avenue des Boveresses 52, CH - 1010 Lausanne
Tél. +41 (0)21 654 40 60, E-mail : info@iseig.ch, URL : www.iseig.ch

ISEIG
Institut Suisse d'Enseignement de l'Informatique de Gestion

ICT Berufsbildung
Formation professionnelle
Formazione professionale

ICT Security Expert

avec diplôme fédéral

Introduction

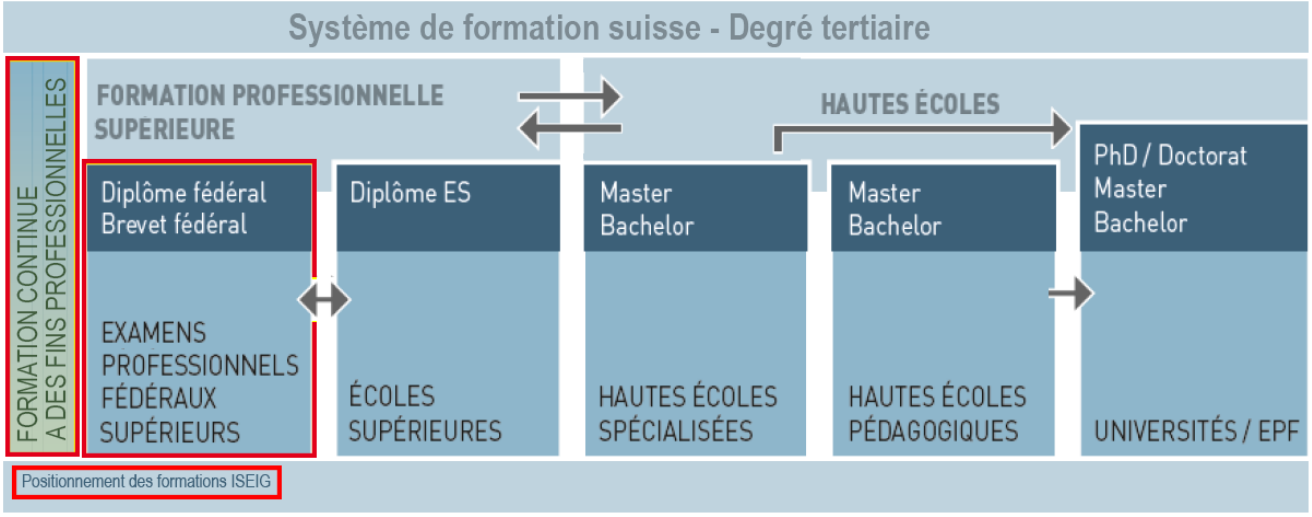
L'examen du diplôme fédéral de « ICT Security Expert » fait partie de la formation professionnelle supérieure et permet d'acquérir des qualifications en vue d'exercer des activités professionnelles complexes impliquant des responsabilités élevées.

Les exigences de l'examen pour l'obtention du titre « ICT Security Expert » avec diplôme fédéral sont définies par « ICT-Formation professionnelle Suisse », l'organisation nationale du travail (OrTra) pour les métiers des technologies de l'information et de la communication (www.ict-formationprofessionnelle.ch), en collaboration avec l'Unité de pilotage informatique de la Confédération (UPIC) et des représentants de l'économie. « ICT-Formation professionnelle Suisse » est également responsable de la définition et de l'organisation des examens.

Le diplôme fédéral est le plus haut diplôme de la formation professionnelle supérieure. Il s'agit de formation continue qui permet l'obtention d'une reconnaissance officielle des connaissances et compétences sans recommencer une longue formation de base déjà acquise. Il est la suite du brevet fédéral qui est le premier diplôme de la formation professionnelle supérieure. Le diplôme fédéral permet à son tour d'accéder aux études HES ou universités en vue de l'obtention d'un MAS (Master of Advanced Studies), d'un CAS (Certificate of Advanced Studies) ou d'un MBA (Master of Business Administration).

Sur la base de son expérience dans la mise en place de formations pointues dans l'informatique et la gouvernance des systèmes d'information, l'ISEIG a mis en place une filière de formation préparant aux examens du diplôme fédéral d'ICT Security Expert.

Le programme se base sur des standards internationaux reconnus tels que **COBIT 5, CISM, CRISC, ISO 2700x, CISSP, BCI, HERMES**, ..., standards faisant partie de l'offre ISEIG depuis de nombreuses années.



Pour qui

La filière du diplôme fédéral de « ICT Security Expert » s'adresse à des **informaticien(ne)s** ou à **tou(te)s professionnel(le)s**[1] dont la carrière les a amené(e)s à prendre des responsabilités dans la sécurité de

[1]Afin de faciliter la lecture, par la suite, seul le masculin est utilisé pour désigner les deux genres.

l'information et qui souhaitent approfondir et systématiser leurs connaissances et compétences dans le domaine, et obtenir un titre de qualification élevé reconnu au niveau fédéral.

Domaine d'activité du « ICT Security Expert »

Le « ICT Security Expert » travaille dans le domaine de la sécurité de l'information pour des entreprises privées et des institutions publiques.

Indépendamment de la taille de l'organisation, son activité recouvre le contexte global de la sécurité de l'information de l'organisation. Grâce à sa compréhension approfondie des domaines d'activités et des processus de l'organisation, il collabore avec les parties prenantes les plus diverses dans les domaines relevant de la sécurité. En font partie les membres de la direction et du conseil d'administration, les spécialistes et responsables d'unités fonctionnelles et de processus ainsi que les prestataires externes.

Le « ICT Security Expert » réduit les risques relatifs à la sécurité de l'information de l'organisation au niveau prescrit par la direction et le conseil d'administration. Il détecte d'éventuels manques dans la stratégie de sécurité et élabore des mesures permettant de parer à ces manques. Il conseille le comité de crise de l'organisation concernant tous les aspects de la sécurité ICT. Il crée à tous les niveaux une prise de conscience envers la sécurité en élaborant et réalisant des campagnes de sensibilisation adéquates.

Compétences opérationnelles principales

Le « ICT Security Expert » est en mesure d'effectuer les missions suivantes :

- Ancrer la stratégie de sécurité
  - Développer les bases de la sécurité de l'information
  - Ancrer la sécurité de l'information auprès de la direction et du conseil d'administration
  - Manager la gestion et le contrôle de la sécurité de l'information
  - Mettre en place l'organisation de la sécurité
  - Piloter professionnellement les spécialistes de la sécurité de l'information
- Etablir le système de management de la sécurité de l'information (ISMS)
  - Piloter l'ISMS
  - Mettre en place les processus de management de la sécurité
  - Manager les risques
  - Intégrer les exigences de sécurité de l'information dans tous les processus
  - Définir des exigences de sécurité
  - Assurer le contrôle de la sécurité
  - Superviser la sécurité externalisée
  - Mesurer les performances
  - Définir les exigences en surveillance de sécurité des personnes en relation avec l'information
- Piloter le programme de sécurité
  - Elaborer une architecture de sécurité ICT
  - Manager le portfolio de produits et services
  - Elaborer le Portfoliomanagement Security-Programm
  - Développer le Business Case
  - Evaluer les solutions de sécurité de l'information
  - Assurer la mise en place des mesures décidées
  - Piloter les projets
  - Intégrer les innovations dans la sécurité de l'information
- Manager les parties prenantes

Confédération suisse

DIPLÔME

Leonhard EULER

né le 20 janvier 1985, originaire de Fribourg

a prouvé qu'il satisfait aux exigences requises pour l'obtention du diplôme en vertu de la loi du 13 décembre 2002 sur la formation professionnelle et conformément au règlement du 23 juillet 2015 approuvé par le Département fédéral de l'économie.

Le présent diplôme autorise le titulaire à porter la dénomination légalement protégée de

ICT Security Expert

Berne, le 24 août 2018

Secrétariat d'Etat à la formation, à la recherche et à l'innovation

La directrice

Pour l'organe responsable de l'examen

Le président de la Commission d'examen

Spécimen

  - Entretenir un réseautage fiable
  - Conseiller de manière professionnelle les parties prenantes
  - Exiger la conformité de la sécurité de l'information
  - Accompagner les projets
  - Prendre en compte les aspects de sécurité dans les études de faisabilité
- Sensibiliser à la sécurité
  - Effectuer une campagne de sensibilisation
  - Assurer la communication de la sécurité en interne et en externe
- Gérer les événements
  - Assurer l'analyse de l'impact sur les affaires
  - Assurer l'organisation d'urgence pour les incidents de sécurité
  - Manager les incidents de sécurité
  - Intégrer les aspects de sécurité de l'information dans la gestion de la continuité des affaires (BCM)
- Sécuriser les informations
  - Assurer la classification des informations
  - Assurer la sécurité des données lors de la transmission
  - Assurer la sécurité des données dans le cadre du stockage et de l'archivage.

Afin de pouvoir exercer cette activité avec professionnalisme, il connaît parfaitement son organisation ainsi que ses produits, ses processus et ses informations et est en mesure de garantir une sécurité de l'information appropriée. Il détecte et évalue les risques, définit et coordonne des mesures de protection et assure l'efficacité de ces mesures de défense.

Exercice de la profession

Le « ICT Security Expert » assume différentes fonctions. Il conseille, dirige des projets, apporte ses connaissances spécialisées dans les équipes et travaille de façon autonome. Son environnement de travail englobe l'ensemble de l'organisation.

Le « ICT Security Expert » communique avec les différentes parties prenantes de façon adaptée aux groupes cibles. Ses connaissances de tous les domaines d'activité de l'organisation lui permettent de traiter les questions portant sur la sécurité dans toute l'organisation. Ce faisant, il a aussi recours à ses connaissances de base en économie d'entreprise. Les directives légales qui s'appliquent à la branche correspondante et la stratégie de l'organisation constituent le cadre de ses activités.

La sécurité de l'information d'une organisation est soumise à des menaces permanentes. C'est pourquoi le « ICT Security Expert » analyse et teste en permanence les technologies et les processus afin de modifier le cas échéant le panorama des produits et des processus dans son propre domaine de responsabilité. Cela requiert une capacité d'innovation importante.

Le « ICT Security Expert » échange ses connaissances sur la situation des menaces et la protection contre les dangers avec des spécialistes. L'échange de données sensibles nécessite des réseaux viables. Le « ICT Security Expert » met en place de tels réseaux et les entretient.

Apport de la profession à la société, l'économie, la nature et la culture

Le « ICT Security Expert » contribue à ce que les informations soient mieux protégées contre des accès non autorisés. Dans tous les domaines de vie, les technologies de l'information et de la communication occupent une place de plus en plus importante, ce qui augmente dans le même temps la vulnérabilité de l'économie et de la société. Il contribue à sensibiliser la société à ce thème.

La sécurité ICT est un facteur d'implantation pour la Suisse et renforce son image de pays fiable. Le « ICT Security Expert » y apporte une contribution importante.

Plan de formation et compétences à acquérir

Le programme de la formation se base sur des standards internationaux reconnus qui font partie de l'offre ISEIG depuis de nombreuses années. Parmi ces standards, il faut citer :

- **COBIT 5 - Control Objectives for Information and related Technology**
  Ce cadre de références pour la gouvernance et la gestion des systèmes d'information intègre

l'évolution des dernières réflexions en matière de gouvernance d'entreprise et de gestion, et fournit des principes acceptés au niveau mondial, des pratiques, des outils analytiques et des modèles pour aider à accroître la confiance dans la valeur des systèmes d'information.
COBIT 5 fournit des principes, pratiques, outils d'analyse et modèles généralement acceptés à l'échelle mondiale pour aider les chefs d'entreprise et les responsables informatiques à maximiser la confiance en leur système d'information et maximiser les bénéfices qui en sont générés.
COBIT 5 simplifie les défis de la gouvernance grâce à seulement 5 principes et 7 catalyseurs. Il intègre de nombreux référentiels, normes ou ressources, comme entre autres : la Val IT et le IT Risk de l'ISACA, le référentiel ITIL et les normes connexes de l'ISO, TOGAF, PMBOK, Prince2, COSO, PCI DSS, la loi Sarbanes-Oxley Act et Bâle III.

- **CISM - Certified Information Security Manager**
  La matière couverte par ce module est structurée dans les 4 domaines suivants :
  1. Gouvervance de la sécurité des informations
     Etablir et maintenir un cadre de gouvernance de la sécurité des informations et des processus de soutien pour assurer que la stratégie de sécurité des informations est alignée sur les objectifs et les finalités organisationnels, que les risques des informations sont gérés de façon appropriée et que les ressources du programme sont gérées de manière responsable.
  2. Gestion des risques de l'information et conformité
     Gérer les risques liés aux informations à un niveau acceptable pour répondre aux exigences du business et de la conformité de l'organisation.
  3. Développement et gestion du programme de la sécurité des informations
     Mettre en place et gérer le programme de la sécurité des informations en alignement avec la stratégie de la sécurité des informations.
  4. Gestion des incidents de sécurité des informations
     Planifier, mettre en place et gérer la capacité de détection, d'investigation, de réponse et de récupération des incidents de sécurité des informations pour en minimiser leur impact sur le business.
- **CRISC - Certified in Risk and Information Systems Control Certification**
  La matière couverte par ce module est structurée dans les 4 domaines suivants :
  1. Identification des risques IT
     Identifier l'univers des risques IT pour contribuer à l'application de la stratégie de la gestion des risques IT en support aux objectifs business et en alignement à la stratégie de la gestion des risques de l'entreprise.
  2. Evaluation des risques IT
     Analyser et évaluer les risques IT pour en déterminer la probabilité et l'impact sur les objectifs business afin de permettre une prise de décision basée sur les risques.
  3. Réponse aux risques et atténuation
     Déterminer les options de réponse aux risques et évaluer leur efficience et leur efficacité pour gérer les risques en alignement aux objectifs business.
  4. Gestion des risques et des contrôles et reporting
     Surveiller continuellement et rapporter les risques IT et les contrôles aux parties prenantes concernées pour garantir continuellement l'efficacité et l'efficience de la stratégie de gestion des risques IT et son alignement sur les objectifs business.
- **La famille des normes ISO 27000**
  La famille de normes ISO/IEC 27000 aide à assurer la sécurité de leurs informations.
  Ces normes facilitent le management de la sécurité des informations, comme les données financières, les documents soumis à la propriété intellectuelle, les informations relatives au personnel ou les données confiées par des tiers.
  ISO/IEC 27001, qui expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI), est la norme la plus célèbre de cette famille. Elle énumère un ensemble de points de contrôles à respecter pour s'assurer de la pertinence du SMSI, pour permettre de l'exploiter et de le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002.

La version 2016 ne fait plus explicitement allusion au PDCA (ou roue de Deming) pour l'évaluation et l'amélioration des processus. Elle utilise les cycles de vie des processus et les concepts hérités des modèles de maturité tel le Capability Maturity Model.
L'objectif de la formation est d'apprendre à implémenter un système de management des SI conforme à la norme ISO 27001:2016 et aux guides associés (ISO 27002, 27003, 27004 et 27005). Il existe plus d'une douzaine de normes dans la famille ISO/IEC 27000

- **CISSP - Certified Information Systems Security Professional**
  La matière couverte par ce module est structurée dans les 8 domaines suivants :
  1. Management de la sécurité et des risques
     Ce domaine présente les concepts de base de la sécurité des informations, en mettant l'accent sur la confidentialité, l'intégrité et la disponibilité. Il traite des aspects liés à l'implémentation des politiques et procédures de sécurité, à l'amélioration de la planification de la continuité du business et des points de restauration, et à la mise en oeuvre de programmes de sensibilisation des utilisateurs. L'accent est mis sur la gestion des risques, notamment en ce qui concerne l'acquisition en toute sécurité de nouveaux logiciels, matériels et services.
  2. Sécurité des actifs
     Ce domaine traite des questions liées à la gestion des données et au concept de propriété des informations. Cela inclut la connaissance des différents rôles concernant le traitement des données (propriétaire, processeur, etc.) et des problèmes de confidentialité.
  3. Ingénierie de la sécurité
     Ce domaine couvre plusieurs concepts importants en matière de sécurité des informations comme les processus d'ingénierie de sécurité, les modèles et les principes de conception, les vulnérabilités, la sécurité des bases de données, les systèmes cryptographiques et la problématique du Cloud.
  4. Sécurité des communications et des réseaux
     Ce domaine traite de la sécurité des réseaux et les possibilités de créer des canaux de communication sécurisés, des différents aspects de l'architecture des réseaux, des protocoles de communication, des segmentations, du routage et des transmissions sans fil.
  5. Gestion de l'identité et des accès
     Ce domaine traite des attaques qui exploitent le composant humain pour accéder aux données et des moyens d'identifier ceux qui ont des droits d'accès aux serveurs et aux informations. Il couvre le concept de sessions, d'authentification multifactorielle, d'épreuvage, d'informations d'identification, du contrôle d'accès basé sur les rôles ou les règles, du MAC et du DAC.
  6. Evaluation et test de la sécurité
     Ce domaine couvre les outils et techniques utilisés pour évaluer la sécurité des systèmes et trouver des vulnérabilités, des erreurs de codage ou de conception, des faiblesses et des domaines de préoccupations possibles non corrigés par les politiques et les procédures. Il traite également l'évaluation de la vulnérabilité et les tests de pénétration, les plans de reprise après sinistre et de continuité, ainsi que la formation de sensibilisation à la sécurité des utilisateurs.
  7. Opérations de sécurité
     Ce domaine met en évidence les concepts fondamentaux, les enquêtes, la gestion des incidents, la récupération après sinistre. Il traite en particulier de l'examen de la criminalité numérique et des enquêtes aux outils de prévention et de détection des intrusions, aux pare-feu et au sandboxing.
  8. Sécurité du développement de logiciel
     Ce domaine concerne la mise en œuvre de contrôles de sécurité des logiciels. Il traite entre autres de l'audit, de l'analyse des risques et de l'identification des vulnérabilités dans les codes.
- **BCI - Business Continuity Institute**
  La matière couverte par ce module comprend 6 domaines :
  - Politique et gestion de programme
  - Intégrer le management de la continuité du business (BCM) dans la culture de l'organisation
  - Comprendre l'organisation
  - Déterminer la stratégie BCM
  - Développer et mettre en œuvre une réponse BCM

- Exercer, maintenir et réviser
- **HERMES - La méthode suisse de gestion de projet**
  Les points traités dans ce module sont : notion de projet; types de projet; catégories de projet; les trois points de vue d'un projet : résultats, démarche, rôles; modèle de phases; scénarios pour projets types; modules, tâches, résultats et rôles; structure détaillée des tâches; pilotage du projet; conduite de projet; structure organisationnelle; organisation du déploiement.

Conditions d'admission à la formation et aux examens

Est admis à l'examen professionnel supérieur le candidat qui remplit une des 4 conditions suivantes :

- être titulaire d'un diplôme tertiaire dans le domaine informatique (brevet fédéral; diplôme fédéral; diplôme ES; Bachelor; Master) ou d'une qualification équivalente et justifier d'au moins trois ans d'expérience professionnelle dans le domaine de la sécurité ICT, ou
- être titulaire d'un diplôme tertiaire dans un autre domaine informatique (brevet fédéral; diplôme fédéral; diplôme ES; Bachelor; Master) ou d'une qualification équivalente et justifier d'au moins quatre ans d'expérience professionnelle dans le domaine de la sécurité ICT, ou
- être titulaire d'un diplôme du degré secondaire II dans le domaine informatique ou d'une qualification équivalente et justifier d'au moins six ans d'expérience professionnelle dans le domaine de la sécurité ICT, ou
- être titulaire d'un diplôme du degré secondaire II dans un autre domaine (certificat de capacité fédéral; maturité gymnasiale; certificat d'école de culture générale; maturité spécialisée) ou d'une qualification équivalente et justifier d'au moins huit ans d'expérience professionnelle dans le domaine de la sécurité ICT.

Prérequis

En plus des conditions d'admission à la formation et aux examens, connaissances de l'anglais technique écrit, le matériel pédagogique étant majoritairement en anglais.

Déroulement des examens

L'examen est organisé selon les épreuves et durées suivantes :

	Partie de l'examen	Type d'examen	Durée
1	Préparation d'un portefeuille sur la base de directives Entretien avec les experts sur le portefeuille	écrit oral	à domicile ~ 40 minutes
2	Etudes de cas	écrit	~ 120 minutes
3	Simulations de cas	pratique	~ 300 minutes

Selon l'expérience, la réussite des examens implique en plus du cours et des exercices dirigés, un travail personnel d´assimilation conséquent dont la charge est estimée à 2 jours par jour de cours.

Titre obtenu

Le diplôme fédéral est délivré par le SEFRI - Secrétariat d'Etat à la formation, à la recherche et à l'innovation.

La ou le titulaire du diplôme fédéral est autorisé(e) à porter le titre protégé de :

- **ICT Security Expert avec diplôme fédéral**
- ICT Security Expert mit eidgenössischem Diplom
- ICT Security Expert con diploma federale.

La traduction anglaise recommandée est :

- **ICT Security Expert, Advanced Federal Diploma of Higher Education.**

Durée et prix

Dates	Formation	Durée	Prix	Prix/j
Voir détail sur www.iseig.ch	ICT Security Expert avec diplôme fédéral	35 jours	12'250.-	350.-

selon conditions générales. Le prix comprend toute la doc. distribuée.
Le prix du cours n'inclut pas la taxe d'examens de CHF 3'400.- (tarif 2017), non soumis à la TVA, montant facturé par ICT-FP Suisse.
Les cours se déroulent en journée de 9 h 00 à 12 h 00 et 13 h 30 à 17 h 00

Cinq bonnes raisons :

- **de se perfectionner à l'ISEIG et**
- **de profiter de plus de 30 ans d'expérience ...**

... vos avantages :

1. Restez compétitif et toujours au top

- Vous apprendrez des contenus basés sur les meilleures pratiques développées par des experts au niveau international. Les méthodes et techniques sont éprouvées et évoluent constamment pour répondre aux besoins en constante évolution. Par vos nouvelles connaissances et compétences, vous vous différencierez sur le marché et serez plus attractif.

2. Garantissez votre investissement formation

- La majorité des formations aboutissent à des certifications qui prouvent vos acquis à votre employeur, partenaires et clients. Vous vous différenciez ainsi positivement et restez attractif sur le marché du travail.
- Votre réussite est optimisée par notre soutien. Si vous considérez que la matière n'a pas été assimilée, nous vous offrons généralement la possibilité de refaire gratuitement tout ou partie de la formation dans les 6 mois, dans une session organisée. Vous ne payerez que les éventuels nouveaux documents pédagogiques ou taxes d'examen. Le reste est à notre charge.

3. Gagnez de l'argent

- Vos nouvelles compétences vous permettront d'être plus productif et d'obtenir une promotion.
- ISEIG, fondation à but non lucratif, offre des formations au meilleur prix. Pour un montant donné, vous obtenez plus.
- Investissez sur vos compétences pour assurer votre rendement, il ne s'agit pas d'une loterie au gain des plus illusoires.

4. Gagnez du temps

- Mettez immédiatement en pratique vos nouvelles compétences. Les ateliers pratiques basés sur des cas réels assurent un transfert de connaissances aisé et l'utilisation des acquis dans votre environnement professionnel.

5. Evitez les mauvaises surprises

- Tout est inclus dans le prix de la formation : supports pédagogiques, énoncés de travaux pratiques avec corrigés, examens à blanc avec corrigés.
- Vous choisissez votre formation sur la base de programmes d'actualité clairement définis.