Diplôme fédéral ICT Security Expert
Cursus classique

Votre profil : vous êtes titulaire d'un diplôme de niveau tertiaire dans le domaine informatique – Brevet fédéral, diplôme ES, Bachelor ou Master – et professionnellement actif dans le domaine de la sécurité ICT.

Durée & horaire

Les cours ont lieu à Renens deux à trois vendredis par mois, de 18h à 21h ainsi qu'un samedi par mois, de 9h à 16h.

La formation comprend 160 périodes réparties sur 15 à 24 mois.

Matériel de formation

Tous les modules sont accompagnés d'un livre rédigé spécifiquement pour cette formation ainsi que d'études de cas réels et de QCM en ligne permettant de valider l'acquisition de compétences.

Ecolage

Réglé par trimestre l'écolage s'élève au total à 13'340 francs dont 6'670 remboursés par la Confédération après l'examen. Les candidats employés dans le canton de Vaud peuvent obtenir une contribution supplémentaire de 2'500 francs versée pendant la formation. Les candidats travaillant ou habitant dans le canton de Genève peuvent bénéficier du Chèque Annuel Formation (CAF) à hauteur de 2'250 francs.

L'écolage inclut le coût de la totalité du matériel de formation, y compris nos livres et les examens blancs. Seule l'inscription à l'examen final n'est pas incluse. Celle-ci est facturée directement par ICT-Formation professionnelle au tarif de 3'400 francs, réglables deux mois avant l'examen. Les candidats employés dans le canton de Vaud peuvent obtenir 3'000 francs de remboursement de cette taxe d'examen.

Un règlement en 24 mensualités successives de 585 francs est possible.

Prochaines sessions

La formation étant modulaire, elle peut débuter chaque trimestre.
Les prochaines dates sont publiées sur notre site web.

accès aux dates

IDEC rue de la Mèbre 2 1020 Renens
021 634 38 55 info@idec.ch www.idec.ch

Diplôme fédéral ICT Security Expert
Cursus VAE & coaching

Si votre expérience ou votre disponibilité professionnelles vous permettent de vous investir dans une formation intensive, nous vous proposons un cursus sur mesure en 12 mois.
Associant coaching et validation des acquis de l'expérience (VAE), cette approche vous permet de vous concentrer uniquement sur les compétences manquant à votre parcours professionnel.

Durée & horaire

La partie présentielle du cursus comprend 8 journées complètes – un samedi par mois, de 9h à 16h – ainsi que 8 soirées sélectionnées en fonction de vos acquis et besoins de compléments. Une durée au moins équivalente doit être réservée pour les travaux de VAE à réaliser chez soi.

Les cours présentiels ont lieu à Renens et/ou en visioconférence.

Le cursus est conçu pour une durée de 12 mois, d'octobre à octobre, les examens ayant lieu en novembre chaque année. La durée peut être étendue sur votre demande, vous permettant par exemple de commencer dès mai ou en septembre.

Contenu

Le calendrier des cours présentiels et des travaux de VAE sur notre plateforme e-learning est établi par votre coach en fonction de votre parcours professionnel et de questionnaires d'évaluation des connaissances. Chaque parcours est unique. Votre coach se charge de votre suivi individuel.

En fonction de vos besoins et sur votre demande, le parcours peut être adapté en cours de formation, par exemple en prolongeant la durée de la préparation et/ou en ajoutant des cours présentiels.

Ecolage

Réglé par trimestre, l'écolage s'élève au total à 7'500 francs dont 3'750 sont remboursés par la Confédération après l'examen. Les candidats employés dans le canton de Vaud peuvent obtenir une contribution supplémentaire de 2'500 francs versée pendant la formation.

Un règlement en 12 mensualités successives de 660 francs est possible.

L'écolage inclut le coût de la totalité du matériel de formation, y compris les livres et les examens blancs (un examen écrit et un examen oral).
Seule l'inscription à l'examen final n'est pas incluse. Celle-ci est facturée directement par ICT-Formation professionnelle au tarif de 3'400 francs, réglables deux mois avant l'examen. Les candidats employés dans le canton de Vaud peuvent obtenir 3'000 francs de remboursement de cette taxe d'examen.

IDEC rue de la Mèbre 2 1020 Renens
021 634 38 55 info@idec.ch www.idec.ch

Programme

Que le cursus soit intensif ou classique, la formation couvre les objectifs de compétences du règlement d'examen dans les domaines qu'il spécifie :

A)	Ancrage de la stratégie en matière de sécurité
	Déterminer le degré de maturité de la sécurité dans l'organisation, élaborer une stratégie de sécurité alignée sur la stratégie d'entreprise.
B)	Mise en place du système de gestion de la sécurité de l'information (SMSI)
	Elaborer, implémenter et gérer en continu un système de gestion de la sécurité de l'information (SMSI) selon les normes ISO 27000.
C)	Direction du programme relatif à la sécurité
	Définir les besoins de sécurité des systèmes et applications, proposer et réaliser une architecture de sécurité, conduire les projets relatifs aux solutions de sécurité.
D)	Gestion des parties prenantes
	Entretenir un réseau d'expertise, rendre compte des résultats des audits de conformité, conseiller les responsables métier et les responsables de projet relativement aux aspects sécuritaires de leurs missions et productions, contrôler la sécurité des prestations et des relations avec les fournisseurs.
E)	Création d'une prise de conscience
	Assurer la sensibilisation de tous les groupes cibles concernés, gérer la communication externe liée à la sécurité.
F)	Maîtrise des événements de sécurité
	Déterminer l'impact, assurer la continuité d'activité, conduire une cellule de réaction aux situations d'urgence, gérer l'évolution des risques.
G)	Garantie de la fourniture d'informations
	Assurer la classification des informations et leur sécurité durant les opérations de transfert, sauvegarde, archivage.

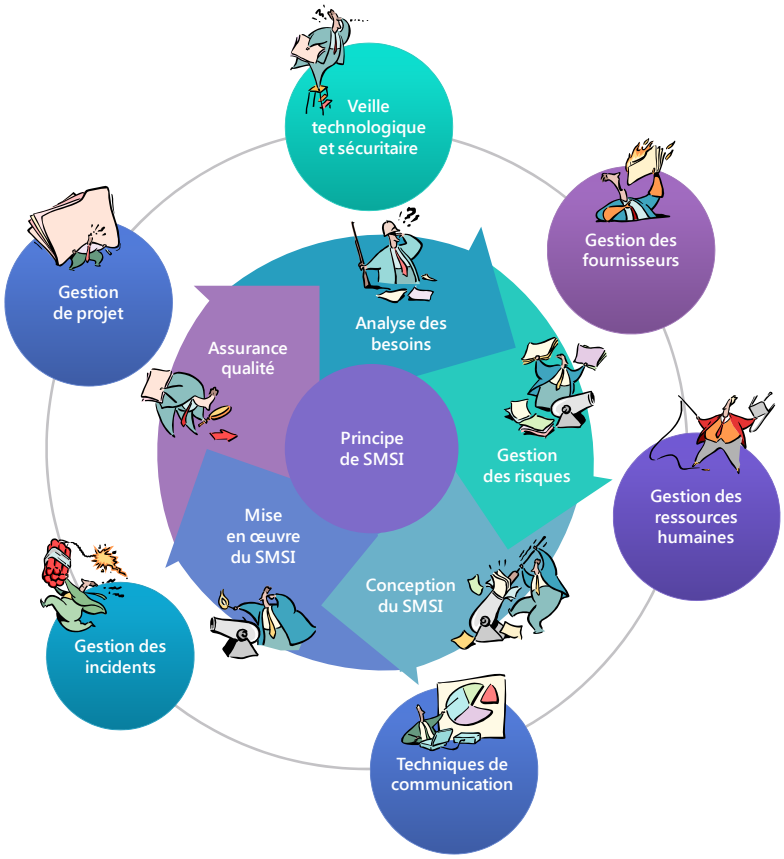
IDEC rue de la Mèbre 2 1020 Renens
021 634 38 55 info@idec.ch www.idec.ch

Des méthodes d'enseignement adaptées aux ICT Security Expert

A l'IDEC, les mots « enseignement professionnel supérieur » prennent véritablement leur sens. Non seulement nous construisons les formations en tenant compte de vos acquis et de vos contraintes professionnelles mais nous mettons aussi à votre disposition un véritable système d'enseignement pensé pour les professionnels en formation continue :

- nos livres rédigés spécifiquement pour la préparation à l'examen ICT Security Expert,
- des questionnaires à choix multiples disponibles en ligne pour valider l'étude de nos livres,
- une participation active durant les cours par le biais de missions à accomplir individuellement ou en équipes, afin d'appliquer concrètement le contenu de nos livres,
- l'entraînement à l'examen pratique par le biais de jeux de rôles simulant des situations réelles,
- des évaluations individuelles notées et des examens blancs afin que vous puissiez clairement situer votre niveau de progression par rapport aux exigences de l'examen,
- l'accompagnement dans l'élaboration du travail de portefeuille à soutenir lors de l'examen.

Le système est modulaire afin de garantir qu'il soit possible de débuter, suspendre ou reprendre le cursus chaque deux mois. Ce principe permet aussi l'indépendance entre les modules, évitant ainsi que quelques absences ou une période professionnelle temporairement plus chargée ne se répercutent sur toute la suite de la formation : si vous n'avez pas pu consacrer le temps nécessaire à l'un des modules, vous pouvez remettre son acquisition à plus tard et néanmoins débuter le module suivant car celui-ci ne s'appuie pas sur les modules précédents.



Chacun des 12 modules représentés ci-contre regroupe thématiquement les compétences spécifiées dans le règlement d'examen.

Les modules spécifiques au SMSI (ISMS) sont délimités et représentés conformément à l'approche PDCA indissociable du concept de SMSI mais demeurent indépendants en termes d'apprentissage.

Chaque module possède son propre livre et ses questionnaires en ligne pour la validation des connaissances acquises.

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Formation professionnelle ICT Suisse

REGLEMENT

Concernant

l'examen professionnel supérieur de l'ICT Security Expert

du 14 août 2017

Vu l'art. 28, al. 2, de la loi fédérale du 13 décembre 2002 sur la formation professionnelle, l'organe responsable au sens du ch.1.3 arrête le règlement d'examen suivant:

1 DISPOSITIONS GÉNÉRALES

1.1 But de l'examen

L'examen professionnel fédéral supérieur a pour but de vérifier de manière exhaustive si les candidates et les candidats ont acquis les compétences nécessaires pour exercer de manière responsable une activité professionnelle exigeante en tant qu'ICT Security Expert.

1.2 Profil de la profession

1.21 Domaine d'activité

Les ICT Security Experts travaillent pour le compte d'entreprises privées et d'institutions publiquesdans le domaine de la sécurité de l'information.

Indépendamment de la taille de l'organisation, leur activité recouvre le contexte global de la sécurité de l'information dans l'organisation. Grâce à leur compréhension approfondie des domaines d'activités et des processus de l'organisation, ils collaborent avec les parties prenantes les plus diversesdans des domaines relevant de la sécurité. En font partie la direction et le Conseil d'administration, des spécialistes, des responsables d'unité de fonction et de processus ainsi que des prestataires externes.

Les ICT Security Experts réduisent le risque relatif à la sécurité de l'information de l'organisation au niveau prescrit par la direction et le Conseil d'administration. Ils détectent d'éventuelles lacunes dans la stratégie de sécurité et élaborent des mesures permettant de combler ces lacunes. Ils conseillent le comité de crise de l'organisation concernant tous les aspects de la sécurité ICT. Ils créent à tous les niveaux une prise de conscience envers la sécurité en élaborant et réalisant des campagnes de sensibilisation adéquates.

1.22 Principales compétences opérationnelles

Les ICT Security Experts

- ancrent la stratégie de sécurité
- mettent en place le système de gestion de la sécurité de l'information (ISMS)
- dirigent le programme relatif à la sécurité
- gèrent les parties prenantes
- créent une prise de conscience envers la sécurité
- maîtrisent des événements
- garantissent la fourniture d'informations

Afin de pouvoir exécuter cette activité avec professionnalisme, ils connaissent parfaitement leur organisation ainsi que ses produits, ses processus et ses informations et sont en mesure de garantir une sécurité de l'information appropriée. Ils détectent et évaluent les risques, définissent et coordonnent des mesures de protection et assurent l'efficacitédes mesures de défense.

1.23 Exercice de la profession

Les ICT Security Experts assument différentes fonctions. Ils conseillent, dirigent des projets, apportent leurs connaissances spécialisées dans les équipes et travaillent de façon autonome. Leur environnement de travail englobe l'ensemble de l'organisation.

Les ICT Security Experts communiquent avec les différentes parties prenantes de façon adaptée aux groupes cibles. Leurs connaissances de tous les domaines d'activité de l'organisation leur permettent de traiter les questions portant sur la sécurité dans toute l'organisation. Ce faisant, ils ont aussi recours à leurs 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 leurs activités.

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

Les ICT Security Experts échangent leurs connaissances sur la situation des menaces et la protection contre les dangersavec des spécialistes. L'échange de données sensibles nécessite des réseaux viables. Les ICT Security Experts mettent en place de tels réseaux et les entretiennent.

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

Les ICT Security Experts contribuent 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. Ils contribuent 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. Les ICT Security Experts y apportent une contribution importante.

Le profil professionnel et de qualification se trouve dans les instructions.

1.3 Organe responsable

1.31 L'organisation du monde du travail suivante constitue l'organe responsable:

Association ICT-Formation professionnelle Suisse

1.32 L'organe responsable est compétent pour toute la Suisse.

2 ORGANISATION

2.1 Composition de la commission d'examen

2.11 Toutes les tâches liées à l'octroi du diplôme sont confiées à une commission d'examen. Celle-ci est composée d'au moins cinq membres, nommés par l'organe responsable pour une période administrative de deux ans.

2.12 L'organe responsable nomme la présidente ou le président pour une durée de fonction de deux ans. Par ailleurs, la commission d'examen se constitue elle-même. Le quorum est atteint lorsque la majorité des membres sont présents. Les décisions se prennent à la majorité des membres présents. Le président tranche en cas d'égalité des voix.

2.13 Les membres de la commission ne sont pas autorisés à exercer une activité dans le cadre des cours de préparation à l'examen.

2.2 Tâches de la commission d'examen

2.21 La commission d'examen:

a) arrête les directives relatives au règlement et les met à jour périodiquement;
b) fixe la taxe de l'examen;
c) fixe la date et le lieu de l'examen;
d) définit le programme d'examen;
e) donne l'ordre de préparer les énoncés de l'examen et organise l'examen;
f) nomme et engage les expertes et les experts et les forme pour accomplir leurs tâches;
g) décide de l'admission à l'examen ainsi que d'une éventuelle exclusion de l'examen;
h) décide de l'octroi du diplôme;
i) traite les requêtes et les recours;
j) s'occupe de la comptabilité et de la correspondance;
k) décide de la reconnaissance ou de la prise en compte d'autres diplômes et d'autres prestations;
l) rend compte de ses activités aux instances supérieures et au Secrétariat d'Etat à la formation, à la recherche et à l'innovation (SEFRI);
m) veille au développement et à l'assurance de la qualité, et en particulier à l'actualisation régulière du profil de qualification en fonction des besoins du marché du travail.

2.22 La commission d'examen délègue les tâches administratives au secrétariat d'ICT-Formation professionnelle Suisse.

2.3 Publicité / surveillance

2.31 L'examen est placé sous la surveillance de la Confédération. Il n'est pas public. Dans des cas particuliers, la commission d'examen peut autoriser des dérogations à cette règle.

2.32 Le SEFRI est invité suffisamment tôt à assister à l'examen et reçoit les dossiers d'examen.

3 PUBLICATION, INSCRIPTION, ADMISSION, FRAIS D'EXAMEN

3.1 Publication

3.11 L'examen est annoncé publiquement dans les trois langues officielles cinq mois au moins avant le début des épreuves.

3.12 La publication informe au moins sur:

- les dates de l'examen;
- la taxe d'examen;
- l'adresse d'inscription;
- le délai d'inscription;
- le déroulement de l'examen.

3.2 Inscription

L'inscription doit comporter

a) un résumé de la formation et des activités professionnelles du candidat;

b) les copies des titres et des certificats de travail requis pour l'admission;

c) la mention de la langue d'examen;

d) la copie d'une pièce d'identité officielle munie d'une photo;

e) la preuve actuelle qu'il n'existe aucune inscription au casier judiciaire inconciliable avec la pratique de la profession;

f) la mention du numéro d'assurance sociale (numéro AVS).[1]

3.3 Admission

3.31 Sont admis à l'examen les candidats qui sont:

a) titulaires d'un diplôme tertiaire dans le domaine informatique (brevet fédéral; diplôme fédéral; diplôme ES; Bachelor; Master) ou d'une qualification équivalente et justifiant d'au moins trois ans d'expérience professionnelle dans le domaine de la sécurité ICT

ou

b) titulaires d'un diplôme tertiaire dans un autre domaine informatique (brevet fédéral; diplôme fédéral; diplôme ES; Bachelor; Master) ou d'une qualification équivalente et justifiant d'au moins quatre ans d'expérience professionnelle dans le domaine de la sécurité ICTou

c) titulaires d'un diplôme du degré secondaire II dans le domaine informatique ou d'une qualification équivalente et justifiant d'au moins six ans d'expérience professionnelle dans le domaine de la sécurité ICT

ou

d) titulaires 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 justifiant d'au moins huit ans d'expérience professionnelle dans le domaine de la sécurité ICT

et fournissant une preuve actuelle qu'il n'existe aucune inscription au casier judiciaire inconciliable avec la pratique de la profession.

Le jour de référence pour la preuve de l'expérience professionnelle est le premier jour de l'examen. Les candidats sont admis sous réserve du paiement de la taxe d'examen, dans les délais impartis, selon le ch. 3.41 ainsi que la remise intégrale et dans les délais du travail de portefeuille conformément au chiffre 5.11. demeurent réservés.

3.32 La décision sur l'admission à l'examen est communiquée par écrit aux candidates et aux candidats au moins trois mois avant le début de l'examen. Une décision négative contient une justification et une indication des voies de droit.

[1] La base juridique de ce relevé est l'ordonnance sur les relevés statistiques (RS **431.012.1**; n° 70 de l'annexe). La commission d'examen ou le SEFRI relève, sur mandat de l'Office fédéral de la statistique, les numéros AVS utiles à des fins purement statistiques.

3.4 Frais

3.41 Après avoir reçu confirmation de son admission, la candidate ou le candidat s'acquitte la taxe d'examen. Les taxes pour l'établissement du diplôme et pour l'inscription de son titulaire dans le registre officiel des titulaires de diplômes ainsi qu'une éventuelle contribution pour frais de matériel sont perçues séparément. Ces frais sont à la charge du candidat.

3.42 Le candidat qui, conformément au chiffre 4.2, se retire dans le délai autorisé ou pour des raisons valables, a droit au remboursement du montant payé, déduction faite des frais occasionnés.

3.43 L'échec à l'examen ne donne droit à aucun remboursement.

3.44 Pour le candidat qui répète l'examen, la taxe d'examen est fixée dans chaque cas par la commission d'examen, compte tenu du nombre d'épreuves répétées.

3.45 Les frais de déplacement, de logement, de subsistance et d'assurance pendant la durée de l'examen sont à la charge du candidat.

4 ORGANISATION DE L'EXAMEN

4.1 Convocation

4.11 En règle générale, un examen a lieu une fois par an. Un examen est réalisé

a) en allemand, dans la mesure où au moins 25 candidats

b) en français, dans la mesure où au moins 8 candidats

c) en italien, dans la mesure où au moins 3 candidats

remplissent les conditions d'admission ou au moins tous les deux ans.

4.12 Les candidats peuvent choisir de passer l'examen dans l'une des trois langues officielles: le français, l'allemand ou l'italien. Des exercices d'examen peuvent contenir des expressions en anglais et des parties d'examen peuvent être réalisées en partie en anglais.

4.13 Les candidats sont convoqués au moins quatre semaines avant le début de l'examen. La convocation comprend:

a) le programme d'examen, avec l'indication du lieu, de la date, de l'heure des épreuves et des moyens auxiliaires dont les candidats sont autorisés ou invités à se munir ;

b) la liste des expertes et des experts.

4.14 Toute demande de récusation d'un expert doit être motivée et adressée à la commission d'examen 14 jours au moins avant le début de l'examen. La commission prend les mesures qui s'imposent.

4.2 Rerait

4.21 Les candidates et les candidats ont la possibilité d'annuler leur inscription jusqu'à six semaines avant le début de l'examen.

4.22 Passé ce délai, le retrait n'est possible que si une raison valable le justifie.
Sont notamment réputées raisons valables:

d) La maternité;

e) La maladie et accident;

f) Le décès d'un proche;

g) Le service militaire, de protection civile ou service civil imprévu.

4.23 Le retrait doit être communiqué sans délai et par écrit à la commission d'examen, assorti de pièces justificatives.

4.3 Non-admission et exclusion

4.31 Les candidates et les candidats qui, en rapport avec les conditions d'admission, donne sciemment de fausses informations ou tente de tromper la commission d'examen d'une autre manière n'est pas admis à l'examen.

4.32 Est exclu de l'examen quiconque:

a) utilise du matériel ou des documents non autorisés;

b) enfreint gravement la discipline de l'examen;

c) tente de tromper les experts.

4.33 La décision d'exclure un candidat de l'examen incombe à la commission d'examen. Le candidat a le droit de passer l'examen sous réserve, jusqu'à ce que la commission d'examen ait arrêté une décision formelle.

4.4 Surveillance de l'examen, expertes et experts

4.41 Au moins une personne de surveillance compétente surveille l'exécution des travaux d'examen écrits et pratiques. Elle consigne ses observations par écrit.

4.42 Au moins deux expertes ou experts évaluent les travaux d'examen écrits et pratiques. Ils s'entendent sur la note à attribuer.

4.43 Au moins deux expertes ou experts procèdent aux examens oraux, prennent des notes sur l'entretien d'examen et sur le déroulement de l'examen, apprécient les prestations fournies et fixent en commun la note.

4.44 Les experts se récusent s'ils sont enseignants aux cours préparatoires, s'ils ont des liens de parenté avec le candidat ou s'ils sont ou ont été ses supérieurs hiérarchiques ou ses collaborateurs.

4.5 Séance d'attribution des notes

4.51 La commission d'examen décide de la réussite ou de l'échec des candidats lors d'une séance mise sur pied après l'examen. La personne représentant le SEFRI est invitée suffisamment tôt à cette séance.

4.52 Les experts se récusent lors de la prise de décision sur l'octroi du diplôme s'ils sont enseignants aux cours préparatoires, s'ils ont des liens de parenté avec le candidat ou s'ils sont ou ont été ses supérieurs hiérarchiques ou ses collaborateurs.

5 EXAMEN

5.1 Parties d'examen et durée de l'examen

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

	Partie de l'examen	Type d'examen	Durée
1	Travail de portefeuille Entretien avec les experts sur le portefeuille	Par écrit Par oral	Au préalable Env. 40 minutes
2	Etudes de cas	Par écrit	Env. 120 minutes
3	Simulations de cas	Pratique	Env. 300 minutes

Partie d'examen 1, travail de portefeuille et entretien avec les experts

Toutes les candidates et les candidats tiennent un portefeuille dans lequel ils font le lien entre la théorie et la pratique. Le portefeuille est un recueil réfléchi et commenté de matériel de différent type dans lequel les candidates et les candidats appliquent les acquis théoriques sur des exemples pratiques du travail quotidien par une prestation de transfert. Les directives sur le plan du contenu et de la forme concernant le portefeuille sont définies dans les instructions. Le portefeuille individuel sert de base à l'entretien avec les experts durant lequel les candidates et les candidats répondent à des questions des expertes et des experts sur leur travail.

Partie d'examen 2, études de cas

Les candidates et les candidats reçoivent des cas proches de la réalité à traiter par écrit. Le choix des cas s'effectue de manière à ce qu'une sélection de compétences opérationnelles de tous les domaines de compétences opérationnelles soit contrôlée.

Partie d'examen 3, simulations de cas

Les candidates et les candidats traitent seul(e)s ou en équipe différentes situations proches de la réalité sur plusieurs postes. L'élaboration de la solution fait l'objet d'une observation, puis est analysée et évaluée. Dans le cadre de la simulation de cas, différentes attitudes sont également contrôlées, une importance particulière étant accordée à l'aptitude au travail en équipe, l'aptitude à la communication et la capacité de jugement. Les directives sur le plan du contenu et de la forme concernant les simulations de cas sont définies dans les instructions.

5.12 Chaque épreuve peut être subdivisée en points d'appréciation. La commission d'examen fixe cette subdivision et la pondération des points d'appréciation dans les directives relatives au présent règlement.

5.2 Exigences

5.21 La commission d'examen arrête les dispositions détaillées concernant l'examen final figurant dans les directives relatives au règlement d'examen (au sens du ch. 2.21, let. a.).

5.22 La commission d'examen décide de l'équivalence des épreuves ou des modules effectués dans le cadre d'autres examens du degré tertiaire ainsi que de la dispense éventuelle des épreuves correspondantes du présent règlement d'examen. Les candidats ne peuvent être dispensés des épreuves qui portent, conformément au profil de la profession, sur les compétences principales.

6 EVALUATION ET ATTRIBUTION DES NOTES

6.1 Généralités

L'évaluation des épreuves et de l'examen est basée sur des notes. Les dispositions des ch. 6.2 et 6.3 du règlement d'examen sont applicables.

6.2 Evaluation

6.21 Une note entière ou une demi-note est attribuée pour les points d'appréciation, conformément au ch. 6.3.

6.22 La note d'une épreuve est la moyenne des notes des points d'appréciation correspondants. Elle est arrondie à la première décimale. Si le mode d'appréciation permet de déterminer directement la note de l'épreuve sans faire usage de points d'appréciation, la note de l'épreuve est attribuée conformément au ch. 6.3.

6.23 La note globale de l'examen correspond à la moyenne pondérée des notes des épreuves. Elle est arrondie à la première décimale.

6.3 Notation

Les prestations des candidats sont évaluées au moyen de notes échelonnées de 6 à 1. Les notes supérieures ou égales à 4,0 désignent des prestations suffisantes.
Seules les demi-notes sont admises comme notes intermédiaires.

6.4 Conditions de réussite de l'examen et de l'octroi du diplôme

6.41 L'examen est réussi si

a) la note générale est supérieure ou égale à 4,0;

b) les notes des parties d'examen 1 et 3 ne sont pas inférieures à 4,0;

c) la note de la partie d'examen 2 n'est pas inférieure à 3,0.

6.42 L'examen final est considéré comme non réussi si la candidate ou le candidat:

a) ne se désiste pas à temps;

b) ne se présente pas à l'examen ou à une épreuve, et ne donne pas de raison valable;

c) se retire après le début de l'examen sans raison valable;

d) est exclu de l'examen.

6.43 La commission d'examen décide de la réussite de l'examen uniquement sur la base des prestations fournies par les candidates et les candidats. Le diplôme fédéral est décerné aux candidats qui ont réussi l'examen.

6.44 La commission d'examen établit un certificat d'examen pour chaque candidate et chaque candidat. Ce certificat doit contenir au moins les informations suivantes:

a) les notes des différentes épreuves et la note globale de l'examen;

b) la mention de réussite ou d'échec à l'examen;

c) les voies de droit, si le diplôme est refusé.

6.5 Répétition

6.51 La candidate ou le candidat qui échoue à l'examen est autorisé à le repasser à deux reprises.

6.52 La première répétition de l'examen ne porte que sur les parties pour lesquelles la note 5,0 (au moins) n'a pas été atteinte; la deuxième répétition, en revanche, sur toutes les parties d'examen de la première répétition de l'examen.

6.53 Les conditions d'inscription et d'admission au premier examen s'appliquent également aux examens répétés.

7 DIPLÔME, TITRE ET PROCÉDURE

7.1 Titre et publication

7.11 Le diplôme fédéral est délivré par le SEFRI à la demande de la commission d'examen et porte la signature de la direction du SEFRI et du président de la commission d'examen.

7.12 Les titulaires du diplôme sont autorisés à porter le titre protégé de:

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

Traduction du titre en anglais

ICT Security Expert, Advanced Federal Diploma of Higher Education

7.13 Les noms des titulaires de diplôme sont inscrits dans un registre tenu par le SEFRI.

7.2 Retrait du diplôme

7.21 Le SEFRI peut retirer tout diplôme obtenu de manière illicite. La poursuite pénale est réservée.

7.22 La décision du SEFRI peut être déférée dans les 30 jours suivant sa notification au Tribunal administratif fédéral.

7.3 Voies de droit

7.31 Les décisions de la commission d'examen concernant la non-admission à l'examen ou le refus du diplôme peuvent faire l'objet d'un recours auprès du SEFRI dans les 30 jours suivant leur notification. Le recours doit mentionner les conclusions et les motifs du recourant.

7.32 Le SEFRI statue en première instance sur les recours. Sa décision peut être déférée dans les 30 jours suivant la notification au Tribunal administratif fédéral.

8 COUVERTURE DES FRAIS D'EXAMEN

8.1 Sur proposition de la commission d'examen, l'organe responsable fixe le montant des indemnités versées aux membres de la commission d'examen et aux expertes et aux experts.

8.2 L'organe responsable assume les frais d'examen qui ne sont pas couverts par la taxe d'examen, la subvention fédérale ou d'autres ressources.

8.3 Conformément aux directives relatives au présent règlement, la commission d'examen remet au SEFRI un compte de résultats détaillé au terme de l'examen. Sur cette base, le SEFRI définit le montant de la subvention fédérale accordée pour l'organisation de l'examen.

9 DISPOSITIONS FINALES

9.1 Entrée en vigueur

Le présent règlement d'examen entre en vigueur à la date de son approbation par le SEFRI.

10 ÉDICTION

Berne, le 10 juillet 2017

Formation professionnelle ICT en Suisse

Andreas Kaelin
Président

Jörg Aebischer
Directeur

Le présent règlement de l'examen est approuvé.

Berne, le 14 août 2017

SECRÉTARIAT D'ETAT À LA FORMATION,

À LA RECHERCHE ET À L'INNOVATION SEFRI

Rémy Hübschi
Chef de la division Formation professionnelle supérieure

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Formation professionnelle ICT en Suisse

DIRECTIVES

Relatives au règlement

L'examen professionnel supérieur ICT Security Expert

du 14 août 2017

Basé sur le chiffre 2.11 du règlement de l'examen relatif à l'examen professionnel supérieur **ICT Security Expert**, la commission d'examen établi la directive suivante:

1 INTRODUCTION

En vertu du chiffre 2.11, let. a du règlement de l'examen relatif à l'examen professionnel supérieur ICT Security Expert du 14.08.2017, la commission d'examen arrête la directive suivante relative au règlement de l'examen précité.

1.1 Objet des instructions

Les directives complètent et précisent les dispositions du règlement de l'examen. Les directives sont arrêtées, périodiquement contrôlées et modifiées si besoin est par la commission d'examen.

1.2 Bases légales

- Loi fédérale sur la formation professionnelle (Loi fédérale sur la formation professionnelle, LFP) du 13 décembre 2002.
- Ordonnance sur la formation professionnelle (Ordonnance sur la formation professionnelle, OFP) du 19 novembre 2003.

1.3 Secrétariat d'examen et interlocuteurs

Le secrétariat assure les tâches administratives en relation avec les examens supérieurs pour toutes les régions linguistiques et constitue l'interlocuteur pour les questions qui s'y rapportent:

Formation professionnelle ICT Suisse
Aarbergergasse 30
3011 Berne
Tél.: +41 58 360 55 50
E-mail: info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

1.4 Explications relatives à l'expérience professionnelle (ch. 3.31 du RE)

a) Les années d'expériences exigées doivent être atteintes au moment de l'examen.

b) On entend par expérience à titre principal une activité à temps complet. Pour les travaux à temps partiel, le calcul se fait au pro rata, autrement dit, la durée d'expérience nécessaire se rallonge en conséquence.

1.5 Description des compétences

Les descriptions des compétences de toutes les compétences indispensables pour l'acquisition du diplôme fédéral se trouvent dans la base de données des compétences de l'organe responsable.
(www.ict-berufsbildung.ch).

2 PROFIL PROFESSIONNEL

Le profil professionnel est représenté au chiffre 1.2 du règlement de l'examen.

3 CONDITIONS D'ADMISSION

Les conditions d'admission sont représentées au chiffre 3.3 du règlement de l'examen.

4 EXAMEN

4.1 Parties d'examen, durée de l'examen et pondération

	Partie de l'examen	Type de contrôle	Durée	Pondération de la partie d'examen
1	Travail de portefeuille Entretien avec les experts sur le portefeuille	Par écrit Par oral	Au préalable Env. 40 minutes	2
2	Etudes de cas	Par écrit	Env. 120 minutes	1
3	Simulations de cas	Pratique	Env. 300 minutes	2

4.2 Description des parties d'examen

Partie d'examen 1, portefeuille et entretien avec les experts

Toutes les candidates et les candidats tiennent un portefeuille dans lequel ils font le lien entre la théorie et la pratique. Le portefeuille est un recueil réfléchi et commenté de matériel de différent type dans lequel les candidates et les candidats appliquent les acquis théoriques sur des exemples pratiques du travail quotidien par une prestation de transfert. Différentes compétences opérationnelles des domaines de compétences opérationnelles doivent être traitées dans le portefeuille (annexe A). Les directives détaillées sur le plan du contenu et de la forme concernant le portefeuille sont définies dans les instructions « Travail de portefeuille ». Le portefeuille individuel sert

de base à l'entretien avec les experts durant lequel les candidates et les candidats répondent à des questions des expertes et des experts sur leur travail.

Partie d'examen 2, études de cas

Les candidates et les candidats reçoivent des cas proches de la réalité à traiter par écrit. Le choix des cas s'effectue de manière à ce qu'une sélection de compétences opérationnelles de tous les domaines de compétences opérationnelles soit contrôlée (annexe A).

Partie d'examen 3, simulations de cas

Les candidates et les candidats traitent seul(e)s ou en équipe différentes situations proches de la réalité professionnelle sur plusieurs postes. La solution des simulations de cas fait l'objet d'une observation, puis est analysée et évaluée. Dans le cadre des simulations de cas, différentes attitudes sont également contrôlées, une importance particulière étant accordée à l'aptitude au travail en équipe, l'aptitude à la communication et la capacité de jugement. Les directives détaillées sur le plan du contenu et de la forme concernant les simulations de cas sont définies dans les instructions « Simulations de cas ».

4.3 Critères d'évaluation

Les directives sur le plan du contenu et de la forme concernant l'évaluation de l'examen sont définies dans les instructions « Travail de portefeuille » et « Simulations de cas ».

4.4 Attribution des notes

L'attribution des notes est représentée au chiffre 1.2 du règlement de l'examen.

5 ORGANISATION DE L'EXAMEN

Avant l'examen	12 mois	Distribution d'informations relatives au contenu et à la forme du travail de portefeuille et démarrage
	5 mois	Publication des dates de l'examen Début de l'inscription, ouverture de la fenêtre d'inscription sur le site.
	4 mois	Date limite d'inscription
	3 mois	Décision sur l'admissibilité
	3 mois	Remise du travail de portefeuille
	6 semaines	Convocation à l'examen oral et écrit
	4 semaines	Demandes de désistement remises.
	La convocation à l'examen oral et écrit ne contient aucune information sur la manière dont le travail du portefeuille a été évaluée.	
Examen	Participation aux parties d'examen 1, 2 et 3	
Après l'examen	La communication des résultats aux candidates et aux candidats s'effectue au plus tard cinq semaines après la dernière journée d'examen.	

5.1 Dossiers d'examen

Le travail d'examen, les exercices, les feuilles de solution, les outils de présentation, les documents de note et les évaluations des examens font partie des dossiers d'examen. Les expertes et les experts sont tenus de garder le secret sur les documents remis et les évaluations. La confidentialité est garantie.

5.2 Site internet d'ICT-Formation professionnelle Suisse

Le site d'ICT-Formation professionnelle Suisse contient toutes les informations et documents pertinents concernant l'examen. Les informations relatives aux contenus des compétences comprises dans la base de données des compétences sont indispensables pour une préparation ciblée:
www.ict-berufsbildung.ch

5.3 Informations à l'attention des candidats

Des informations complémentaires à l'attention des candidats se trouvent sur la page d'accueil du SEFRI. https://www.sbfi.admin.ch/sbfi/fr/home/themes/la-formation-professionnelle-superieure/informations-generales-concernant-les-examens-federaux/candidats-et-diplomes.html

- Notice: Compensation des inégalités frappant les personnes handicapées
- Notice: Droit de consulter des documents
- Notice: Notice concernant les recours contre la non-admission à un examen et contre la non-délivrance du brevet fédéral ou du diplôme fédéral

5.4 Littérature spécialisée

En règle générale, des références bibliographiques ne sont pas prises en compte comme preuves en cas de recours.

6 DECRET

BERNE, le 14 août 2017

Daniel Jäggli
Président de la commission des examens

Mario Rusca
Responsable des examens

ANNEXE A: PROFIL DE QUALIFICATION

SOMMAIRE

– Compétences opérationnelles

Aperçu des compétences opérationnelles

Domaines de compétences opérationnelles		Compétences opérationnelles								
a	Ancrage de la stratégie en matière de sécurité	a1: Elaboration des bases en matière de sécurité de l'information	a2: Ancrage de la sécurité de l'information dans la direction et dans le Conseil d'administration	a3: Gestion de la direction et du pilotage de la sécurité de l'information	a4: Mise en place de l'organisation de sécurité	a5: Gestion spécialisée des spécialistes en sécurité de l'information				
b	Mise en place du système de gestion de la sécurité de l'information (ISMS)	b1: Gestion de l'ISMS	b2: Mise en place des processus	b3: Gestion des risques	b4: Intégration des exigences en matière de sécurité de l'information dans tous les processus	b5: Définition des directives de sécurité	b6: Assurance de la vérification de la sécurité	b7: Surveillance de la sécurité dans le processus d'externalisation	b8: Mesure de la performance	b9: Définition des exigences spécifiques aux informations concernant le contrôle de sécurité des personnes
c	Direction du programme relatif à la sécurité	c1: Elaboration de l'architecture de sécurité ICT	c2: Gestion du portefeuille de produits / services	c3: Elaboration de la gestion de portefeuille du programme de sécurité	c4: Développement des cas commerciaux	c5: Evaluation des solutions de sécurité de l'information	c6: Assurance de la mise en œuvre des mesures décidées	c7: Direction des projets	c8: Intégration des innovations dans la sécurité de l'information	
d	Gestion des parties prenantes	d1: Entretien d'un réseau viable sécurisé	d2: Conseil spécialisé des parties prenantes	d3: Exigence de compliance en termes de sécurité de l'information	d4: Accompagnement des projets	d5: Assurance des aspects relatifs à la sécurité dans la démonstration de faisabilité				
e	Création d'une prise de conscience	e1: Réalisation d'une campagne de prise de conscience	e2: Assurance de la communication sur la sécurité en interne et en externe							
f	Maîtrise d'événements	f1: Assurance d'une Business Impact Analyse	f2: Assurance d'une organisation d'urgence pour les incidents relatifs à la sécurité	f3: Gestion des incidents relatifs à la sécurité	f4: Assurance de l'intégration d'aspects relevant de la sécurité de l'information dans le Business Continuity Management					
g	Garantie de la fourniture d'informations	g1: Assurance de la classification des informations	g2: Assurance de la sécurité des données lors du transfert	g3: Assurance de la sécurité des données lors de la sauvegarde et de l'archivage						

A) Ancrage de la stratégie en matière de sécurité

Description du domaine de compétences opérationnelles:
Les ICT Security Experts élaborent la stratégie en matière de sécurité de l'information pour leur entreprise sur la base de la disposition à prendre des risques en matière d'information de la direction et du Conseil d'administration. Ils définissent les scénarios de menace et l'état visé, analysent les écarts et en dégagent les objectifs stratégiques afin de les éliminer. Ils demandent l'adoption de la stratégie en matière de sécurité de l'information auprès de la direction et du Conseil d'administration. Suite à cela, ils définissent la gouvernance en matière de sécurité de l'information et la mettent en œuvre.

Ils ancrent la sécurité de l'information au sein de l'organisation et dirigent l'organisation de sécurité. La définition du rôle de l'organe de pilotage en coordination avec l'organisation ainsi que la fixation des membres en font partie. Ils définissent la formation des titulaires de rôle de l'organisation de sécurité, assurent leur formation et vérifient le degré de maturité de la sécurité au sein de l'organisation.

Les ICT Security Experts peuvent diriger une équipe de spécialistes en sécurité de l'information sur le plan spécialisé, identifient les lacunes de connaissance et fixent les plans de formation. Par ailleurs, ils garantissent l'échange permanent d'expériences et de connaissances entre les spécialistes en sécurité de l'information.

Contexte:
La stratégie en matière de sécurité de l'information détermine l'activité des ICT Security Experts. Ils définissent les capacités et les contrôles nécessaires au respect de la disposition à prendre des risques en matière d'information. L'analyse des écarts identifie le besoin existant en amélioration. Ils en déduisent les objectifs stratégiques qui traitent ces écarts et, à partir de ces objectifs, l'activité des ICT Security Experts.

L'orientation de la stratégie en matière de sécurité de l'information sur tous les aspects de la sécurité de l'information de l'entreprise constitue un facteur de réussite primordial d'une stratégie en matière de sécurité de l'information. Cela signifie que les ICT Security Experts doivent connaître les processus, la chaîne de création de valeur, les actifs devant être protégés et la stratégie de l'entreprise. La stratégie en matière de sécurité de l'information doit alors être intégrée dans la stratégie d'entreprise.

La direction et le Conseil d'administration jouent un rôle capital dans l'ancrage de la stratégie en matière de sécurité. Ceux-ci définissent la disposition à prendre des risques en matière d'information et ancrent les programmes de sécurité de l'information. Les ICT Security Experts veillent à une compréhension commune des scénarios de risque et des risques liés. Les ICT Security Experts veillent à un large soutien dans l'entreprise lors de la mise en œuvre.

Afin que la sécurité soit perçue comme un élément culturel de l'organisation et soit vécue par tous les collaborateurs, une organisation de sécurité doit être mise en place. Les ICT Security Experts en assument la responsabilité sur le plan organisationnel et spécialisé. Ils assurent que les titulaires de rôle connaissent leurs tâches, responsabilités et compétences dans le domaine de la sécurité de l'information et vivent (en donnant l'exemple) la culture de la sécurité.

Les spécialistes en sécurité de l'information doivent toujours avoir des connaissances actualisées. C'est la seule manière d'éviter des événements portant sur la sécurité et d'en réduire leur impact. Les ICT Security Experts le garantissent par le biais de formations et d'un échange permanent et mutuel d'expériences et d'informations. Cela conduit à une meilleure acceptation des spécialistes en sécurité de l'information au sein de l'entreprise.

Le domaine de compétences opérationnelles A constitue la base pour les domaines de compétences opérationnelles B – Mise en place du système de gestion de la sécurité de l'information (ISMS) et C – Gestion du programme de sécurité.

A) Ancrage de la stratégie en matière de sécurité (aperçu)

Compétences opérationnelles professionnelles	**Thèmes importants / Contenus**	**Critères de performance**
A1 – Elaboration des bases pour la sécurité de l'information	Contenu/éléments d'une stratégie en matière de sécurité de l'information, informatique industrielle	Les ICT Security Experts sont en mesure: - d'analyser une stratégie d'entreprise - de déduire les implications des directives régulatoires pour l'entreprise - de définir les scénarios de menace ayant une pertinence pour l'organisation - d'analyser les risques - d'élaborer une stratégie en matière de sécurité de l'information sur la base de la disposition à prendre des risques de la direction et du Conseil d'administration - de réaliser une analyse des manques - de définir et de mettre en œuvre une gouvernance en matière de sécurité de l'information - d'effectuer des présentations de façon adaptée aux destinataires - de définir les responsabilités en termes d'ICT Security (RACI: Responsible, Accountable, Consulted and Informed) - d'élaborer un dispositif de sécurité ICT et de l'ancrer dans l'organisation - de déterminer le degré de maturité de la sécurité dans l'organisation - de transmettre à leur équipe le contenu des publications sur la sécurité - de soutenir les collaborateurs subordonnés sur le plan spécialisé - de mettre en place une communauté de spécialistes en sécurité de l'information et de garantir l'échange permanent d'expériences et de connaissances - de connaître leur propre besoin en formation ainsi que celui de l'équipe et de mettre en œuvre des mesures
A2 – Ancrage de la sécurité de l'information dans la direction et dans le Conseil d'administration	Technique de présentation	
A3 – Gestion de la direction et du pilotage de la sécurité de l'information		
A4 – Mise en place de l'organisation de sécurité		
A5 – Direction des spécialistes en sécurité de l'information sur le plan spécialisé	Compétences de gestion	

B) Mise en place du système de gestion de la sécurité de l'information (ISMS)

Description du domaine de compétences opérationnelles:
Les ICT Security Experts assurent le support de gestion pour l'ISMS et gèrent l'ensemble de règles Plan-Do-Check-Act. Ils conçoivent et gèrent des processus visant à piloter et à mettre en œuvre la sécurité de l'information. Pour la surveillance des processus, ils définissent des chiffres clés appropriés, les mesurent et les évaluent.

Ils observent le développement dans le domaine des nouvelles technologies et l'environnement pertinent pour la sécurité. Ils déterminent et documentent les menaces, détectent les points faibles internes et en déduisent le besoin en action. Ils vérifient régulièrement l'actualité de la liste des risques de sécurité documentés, mènent des entretiens avec les parties prenantes concernant leur estimation de l'appréciation du risque et rendent compte des conséquences et des potentiels de danger à la direction et au Conseil d'administration.

Ils soutiennent les responsables de processus dans la mise en œuvre des exigences en sécurité pour leurs processus. Avec les responsables de processus, de directives et de projet, ils définissent les directives de sécurité et les intègrent dans les documents normatifs correspondants. Ils déclenchent des contrôles de sécurité réalisés par des auditeurs internes et externes. Ils catégorisent les points faibles, déclenchent leur contrôle et réalisent les vérifications de répétition nécessaires et les retests.

Ils définissent avec les responsables RH les exigences concernant le contrôle de sécurité des personnes (PSÜ), établissent un document PSÜ, fixent le processus et forment les collaborateurs RH à la mise en œuvre du processus PSÜ.

Contexte:
Un ISMS peut piloter toute la sécurité de l'information d'une organisation. L'ISMS doit être contrôlé et modifié en permanence. Les ICT Security Experts doivent assurer que les processus sont toujours actualisés conformément aux exigences de l'ISMS.

Les connaissances des ICT Security Experts doivent à tout moment être actualisées (évolution des menaces, technologies, standards, réglementations, lois et concurrents). Cela constitue l'unique moyen de réagir aux évolutions et d'assurer la sécurité de l'information de l'organisation nécessaire.

Les applications, les systèmes et les informations sont régulièrement soumis à un contrôle de la sécurité. Cela permet de détecter et d'éliminer les points faibles et donc d'augmenter la sécurité. Par ailleurs, de nouvelles fonctions sont soumises à un contrôle de sécurité avant la mise en service. Il convient de vérifier si les prestations externalisées répondent aux exigences en matière de sécurité. D'éventuelles mesures sont déduites sur cette base.

Les chiffres clés permettent de mesurer l'état de sécurité d'une organisation. Dans ce but, les ICT Security Experts se concertent régulièrement sur les chiffres clés avec les parties prenantes.

Le domaine de compétences opérationnelles B se fonde sur le DCO A – Ancrage de la stratégie en matière de sécurité.

B) Mise en place du système de gestion de la sécurité de l'information (ISMS) (aperçu)

Compétences opérationnelles professionnelles	**Thèmes importants / Contenus**	**Critères de performance**
B1 – Direction de l'ISMS	ISO 27001 Méthodologie	Les ICT Security Experts sont en mesure: - d'élaborer un ISMS. Cela comprend la définition du volume de l'ISMS, la réalisation d'une analyse du risque, l'élaboration d'un plan de traitement du risque, la définition d'un système de contrôle des mesures ainsi que l'implémentation de mesures de sécurité et de processus - de piloter, de contrôler et de maintenir le fonctionnement d'un ISMS, de contrôler et si nécessaire, de modifier l'efficacité des mesures et des processus - d'assurer l'amélioration permanente de l'ISMS - de connaître et de détailler les risques ICT stratégiques - de définir et d'introduire des processus - de former les parties prenantes à la mise en œuvre des processus - de contrôler les chiffres clés et de réagir en cas de différences par rapport aux valeurs à atteindre - de réaliser des reviews en vue d'améliorer les processus, de dégager et de mettre en œuvre des mesures à partir des résultats - de s'informer en continu sur les thèmes relevant de la sécurité comme les nouvelles technologies, les scénarios d'attaques et les concurrents, et de faire intégrer les nouveaux enseignements dans les règlements internes et dans la gestion des risques - de définir des exigences en sécurité concernant les processus, de les coordonner et de les finaliser avec le responsable des processus - de définir les directives de sécurité, de les intégrer dans les documents normatifs comme les directives et la documentation de processus et de définir le contrôle - de déterminer sur la base de l'exposition aux risques les applications, systèmes et projets devant être contrôlés - de catégoriser les points faibles et de les corriger - d'intégrer et de réaliser le contrôle de la sécurité dans le processus d'autorisation externalisé - d'évaluer les Service Level Reports et les rapports d'audit sur les fournisseurs tiers et d'en dégager des mesures - de définir des niveaux de sécurité par domaine d'affectation du personnel - de définir le type de contrôle ou la méthode par exigence et par niveau - d'élaborer un document de contrôle de sécurité des personnes et le processus correspondant - de former les collaborateurs RH à la mise en œuvre du processus PSÜ
B2 – Mise en place des processus		
B3 – Gestion des risques		
B4 – Intégration des exigences en matière de sécurité de l'information dans tous les processus		
B5 – Définition des directives de sécurité	Informatique industrielle Robotique Internet des objets AI Cloud	
B6 – Assurance du contrôle de la sécurité	ISO 27002 Protection IT de base Test de pénétration Révision des codes	
B7 – Surveillance de la sécurité dans le processus d'externalisation		
B8 – Mesure de la performance		
B9 – Définition des exigences spécifiques aux informations concernant le contrôle de sécurité des personnes		

C) Direction du programme relatif à la sécurité

Description du domaine de compétences opérationnelles:
Les ICT Security Experts élaborent une architecture de sécurité IT à l'échelle de toute l'organisation. Ils identifient les différences entre l'architecture effective et visée et en déduisent les exigences techniques visant à garantir la confidentialité, la disponibilité et l'intégrité des informations.

Ils planifient et conçoivent le portefeuille de produits / services de sécurité et le développent. Les projets dans le domaine de la sécurité de l'information sont déduits de la stratégie en matière de sécurité de l'information. Pour les achats prévus de nouveaux produits / services, ils fournissent une preuve de la rentabilité Ils dirigent des projets dans le domaine de la sécurité de l'information, observent le marché et évaluent les nouveaux produits et processus.

Contexte:
L'architecture de sécurité de l'information constitue les objectifs en termes de sécurité de l'entreprise et sert de base à l'organisation du projet. Pour l'élaboration, les ICT Security Experts utilisent un modèle d'architecture en coordination avec les différentes parties prenantes.

Le portefeuille de produits et de services doit être développé en permanence. Pour le programme de sécurité de l'organisation, cela signifie adapter en permanence le portefeuille aux processus commerciaux. Dans ce cadre, les ICT Security Experts veillent à la transparence sur les investissements réalisés dans leur domaine.

Le domaine de compétences opérationnelles C se fonde sur le domaine de compétences opérationnelles A – Ancrage de la stratégie en matière de sécurité.

C) Direction du programme relatif à la sécurité (aperçu)

Compétences opérationnelles professionnelles	**Thèmes importants / Contenus**	**Critères de performance**
C1 – Elaboration d'une architecture ICT Security	Modèles d'architecture	Les ICT Security Experts sont en mesure: - d'analyser la situation actuelle du panorama des systèmes et des applications informatiques et d'évaluer la situation de menace, - d'esquisser des exigences concernant le modèle technique visé du panorama des systèmes et des applications informatiques - d'élaborer une analyse des écarts entre l'état effectif et l'état visé et de la coordonner avec les parties prenantes correspondantes - de définir des mesures de protection à partir des écarts par rapport aux exigences techniques - de déduire des solutions de protection techniques coordonnées avec les parties prenantes - d'évaluer de nouvelles exigences concernant les produits et les services - de fixer des priorités pour les projets sur la base de critères transparents - de participer à la création d'un budget pour la sécurité de l'information - d'estimer les risques de nouvelles acquisitions - de planifier, de réaliser des projets dans le domaine de la sécurité de l'information et d'évaluer des produits
C2 – Gestion du portefeuille de produits / services		
C3 – Elaboration du programme de sécurité de la gestion du portefeuille		
C4 – Développement de cas commerciaux		
C5 – Evaluation des solutions de sécurité de l'information		
C6 – Assurance de la mise en œuvre des mesures décidées		
C7 – Direction des projets	Méthode de projet Logiciel de gestion de projets	
C8 – Intégration des innovations dans la sécurité de l'information	Portails de recherche (p. ex. Gartner) Conférences pour la sécurité de l'information Ethique	

D) Gestion des parties prenantes

Description du domaine de compétences opérationnelles:
Les ICT Security Experts entretiennent un réseau de relation viable et fiable dans le domaine de la sécurité de l'information en vue de l'échange sur des thèmes relevant de la sécurité de l'information.

Dans l'organisation, ils répondent aux questions portant sur la sécurité de façon adaptée aux groupes cibles. Ils effectuent des activités de conseil dans les projets, les analysent et les évaluent en termes de risques concernant la sécurité de l'information. Ils déduisent les exigences de sécurité concernant un produit à partir des exigences commerciales. Dans le même temps, ils fixent l'intégration minimale d'un produit dans l'architecture de sécurité existante pour la démonstration de faisabilité. Ils élaborent le plan de contrôle de sécurité et participent au contrôle de la démonstration de faisabilité. Ils définissent et réalisent le sign-off.

La gestion des parties prenantes comprend également le contrôle du respect de la compliance pour les activités relevant de la sécurité. Ils documentent et rendent compte des résultats à l'organisation de compliance.

Contexte:
Seul un ancrage de la sécurité de l'information dans toute l'organisation apporte une protection optimale contre les événements de sécurité. Cela requiert des ICT Security Experts qu'ils puissent répondre de façon compétente et compréhensible aux questions portant sur la sécurité.

Dans le même temps, le respect de la sécurité de l'information des nouveaux produits et processus doit être contrôlé dans toute l'entreprise. L'intégration d'un nouveau produit dans l'architecture de sécurité existante joue un rôle central. Les ICT Security Experts intègrent les produits dans l'architecture de sécurité existante.

Le dialogue avec d'autres spécialistes dans le domaine de la sécurité de l'information permet d'échanger des connaissances et des expériences. Les ICT Security Experts connaissent l'importance de ce réseau, le mettent en place et l'entretiennent.

Le domaine de compétences opérationnelles D est en relation avec les domaines de compétences opérationnelles A – Ancrage de la stratégie en matière de sécurité de l'information, B – Mise en place du système de gestion de la sécurité de l'information (ISMS) et C – Direction du programme de sécurité.

D) Gestion des parties prenantes (aperçu)

Compétences opérationnelles professionnelles	**Thèmes importants / Contenus**	**Critères de performance**
D1 – Entretien d'un réseau viable		Les ICT Security Experts sont en mesure: - de mettre en place et d'entretenir un réseau de relation dans le domaine de la sécurité de l'information - de collaborer avec des organisations de sécurité de l'information externes - d'enregistrer des questions de parties prenantes et d'y répondre de façon adaptée aux groupes cibles - de documenter et de rendre compte des résultats d'audit concernant la compliance - d'effectuer des activités de conseil pour des projets d'autres domaines concernant la sécurité de l'information - d'analyser, d'évaluer des projets d'autres domaines concernant la sécurité de l'information et de communiquer les résultats - de définir et de procéder au sign-off de sécurité dans des projets d'autres domaines - de déduire des exigences en termes de sécurité concernant un produit à partir des exigences commerciales fonctionnelles - de fixer une intégration minimale d'un produit dans l'architecture de sécurité existante pour l'étude de faisabilité (Proofs of Concept) - de contrôler le rapport de test lors de l'élaboration du plan de contrôle de sécurité et du contrôle de l'étude de faisabilité (Proofs of Concept) - de convenir et de contrôler les contrats de prestation avec les clients et les fournisseurs en termes de sécurité de l'information
D2 – Conseil spécialisé des parties prenantes	Gouvernance et processus dans l'entreprise ISO 2700x	
D3 – Exigence du respect des directives de sécurité de l'information	Lois Réglementations Directives / processus internes Principe TCR	
D4 – Accompagnement des projets	Internet des objets AI Robotique Industrial Control Systems	
D5 – Fixer des aspects concernant la sécurité dans les études de faisabilité (Proofs of Concept)	Service Level Agreement	

E) Création d'une prise de conscience

Description du domaine de compétences opérationnelles:
Les ICT Security Experts sensibilisent les collaborateurs, la direction et le Conseil d'administration aux aspects de la sécurité ICT. Ils planifient des campagnes de sensibilisation internes, les coordonnent avec les programmes existants et les analysent. Ce sont les groupes cibles qui décident des contenus et des canaux de communication. Les ICT Security Experts formulent les contenus et les préparent de façon didactique. Ils vérifient la participation des collaborateurs aux formations. Ils analysent les formations et informent les mandants sur le résultat des formations.

Ils informent de façon interne et externe sur les aspects de la sécurité par le biais de médias comme les newsletterset les publications en ligne.

Contexte:
La création d'une prise de conscience constitue une tâche centrale des ICT Security Expert.
Un rôle clé est la sensibilisation de la direction et du Conseil d'administration, car ce sont eux qui décident des risques que comprend la stratégie de sécurité et du niveau auquel elle doit être menée. La sensibilisation des collaborateurs permet de mettre en place le système de gestion de la sécurité de l'information (ISMS) et de diriger le programme de sécurité.

La sensibilisation doit être atteinte auprès de tous les collaborateurs. Ce processus n'est jamais terminé et nécessite toujours de nouveaux efforts sur le plan de la communication. La sensibilisation ne doit pas se traduire uniquement dans des connaissances, mais aussi dans la mise en œuvre par les collaborateurs au quotidien.

Le domaine de compétences opérationnelles E est en relation avec les domaines de compétences opérationnelles A – Ancrage de la stratégie en matière de sécurité de l'information, B – Mise en place du système de gestion de la sécurité de l'information (ISMS) et C – Direction du programme de sécurité. Dans tous ces domaines de compétences opérationnelles, la sensibilisation joue un rôle primordial.

E) Création d'une prise de conscience (aperçu)

Compétences opérationnelles professionnelles	**Thèmes importants / Contenus**	**Critères de performance**
E1 – Réalisation de campagnes de prise de conscience	Didactique Communication	Les ICT Security Experts sont en mesure: - de définir des campagnes de sensibilisation et de communication de sécurité avec le mandant - de coordonner les campagnes de sensibilisation avec un programme de sensibilisation existant - de fixer les thèmes, le public cible, la période, les outils, la valeur de référence et le canal de communication - de présenter sous forme didactique les contenus pour les campagnes de sensibilisation et de les préparer en conséquence pour le canal de communication sélectionné de façon adaptée aux groupes cibles - de planifier et de réaliser des formations auprès des groupes cibles - d'analyser les résultats des formations et d'en rendre compte auprès du mandant - d'identifier des améliorations pour la formation à la sensibilisation à partir des évaluations des formations
E2 – Assurance de la communication sur la sécurité en interne et en externe	Communication avec les médias	

F) Maîtrise d'événements

Description du domaine de compétences opérationnelles:
Les ICT Security Experts analysent la situation générale de la sécurité en se concentrant sur la propre organisation.
Dans le cas d'un événement de sécurité, ils déterminent, analysent et documentent l'impact sur l'organisation. Ils engagent des mesures afin d'en réduire les conséquences. Ils informent les parties prenantes et les responsables de processus commerciaux sur les répercussions correspondantes.

Ils conseillent et soutiennent le comité de crise dans la prise de décision en vue de maîtriser l'événement de sécurité. Suite à un événement de sécurité, ils évaluent la maîtrise de celui-ci et évaluent les dommages provoqués. Ils identifient des possibilités d'optimisation dans l'organisation de sécurité, les processus de sécurité ou l'architecture de sécurité.
Ils mettent en œuvre ces possibilités d'optimisation en coopération avec les personnes correspondantes.

Par ailleurs, ils assurent l'intégration des aspects concernant la sécurité dans le Business Continuity Management (BCM).

Contexte:
L'efficacité de la maîtrise d'un événement de sécurité est déterminante sur l'étendue des dommages.
Toutes les mesures doivent être coordonnées. Dans ce cadre, les ICT Security Experts ont la fonction de service de coordination et de contact pour la direction, le Conseil d'administration et les collaborateurs.

Le domaine de compétences opérationnelles F est en relation avec tous les autres domaines de compétences opérationnelles, car la maîtrise d'un événement de sécurité se fonde sur les autres domaines de compétences opérationnelles.

F) Maîtrise d'événements (aperçu)

Compétences opérationnelles professionnelles	Thèmes importants / Contenus	Critères de performance
F1 – Assurance de la Business Impact Analyse		Les ICT Security Experts sont en mesure: - d'établir et de mettre à jour des bilans de la situation sur les menaces de processus, produits, infrastructures etc. importants (BIA) - d'identifier des points faibles dans des processus, produits et infrastructures importants - d'évaluer les dépendances aux risques sur la base d'un BIA - de déduire un besoin en action pour l'organisation de la sécurité - d'analyser la situation générale de sécurité en se concentrant sur le potentiel de dangers pour la propre organisation et d'élaborer des mesures immédiates - de déterminer, d'analyser et de documenter la conséquence d'une panne des services d'information - de déduire des mesures à partir de la conséquence (dommage) et de les classer par priorité - d'informer les parties prenantes et les responsables de processus commerciaux sur les interdépendances pertinentes dans le processus commercial - de conseiller le comité de crise et de le soutenir dans la prise de décision - de fixer la solution d'un événement de sécurité et d'évaluer le dommage provoqué - d'identifier une optimisation pour d'autres événements de sécurité possibles et de procéder à des améliorations dans l'organisation de la sécurité, des processus de sécurité et/ou dans l'architecture de sécurité - de contrôler si les aspects portant sur la sécurité sont pris en compte dans le BCM
F2 – Assurance d'une organisation d'urgence pour les événements de sécurité	Prestataires de sécurité, blogs sur la sécurité et autorités pour la sécurité, p. ex. MELANI	
F3 – Gestion des événements de sécurité	Criminologie / justice Médecine légale Collaboration lors d'enquêtes et de poursuites pénales	
F4 – Assurance de l'intégration d'aspects relevant de la sécurité de l'information dans le Business Continuity Management	Processus BCM ISO2700x	

G) Garantie de la fourniture d'informations

Description du domaine de compétences opérationnelles:
Les ICT Security Expert définissent le règlement visant à la classification des données en concertation avec les propriétaires des données.
Ils établissent la gestion de gestion des données sur cette base. Dans ce concept, les aspects de la télétransmission des données, de la sauvegarde des données et des accès aux données sont définis. Les bases légales concernant la protection des données et les directives régulatoires spécifiques à un secteur sont prises en compte dans ce cadre.

Contexte:
La quantité de données et d'informations est quasiment illimitée en raison de l'augmentation des interconnexions des systèmes informatique et de la modification des chaînes de création de valeur. Ces données et informations se produisent de façon locale, décentralisée ainsi que dans des solutions cloud de tiers, où elles sont enregistrées.

Pour une organisation, des données et informations générées aussi bien en interne qu'en externe sont importantes. Cela provoque des interfaces qui nécessitent une solution technique (transfert, sauvegarde). Par ailleurs, les données doivent être classifiées en termes de disponibilité, fiabilité et confidentialité. Pour ce faire, il convient de suivre les directives légales des pays impliqués.

Le domaine de compétences opérationnelles G est contenu dans tous les autres domaines de compétences opérationnelles, notamment dans le domaine de compétences opérationnelles B.

G) Garantie de la fourniture d'informations (aperçu)

Compétences opérationnelles professionnelles	**Thèmes importants / Contenus**	**Critères de performance**
G1 – Assurance de la classification des informations		Les ICT Security Experts sont en mesure: - de formuler des directives pour la gestion des données - d'assurer les bases légales pour l'administration des données et des informations - de contrôler la disponibilité, l'authenticité, la fiabilité et la confidentialité des données et des informations d'un concept de gestion des données - d'établir un concept de classification - d'assurer le respect des directives pour la gestion des données - d'ordonner la technique de cryptage et son utilisation selon la situation - de contrôler les aspects de sécurité de la sauvegarde, des technologies d'archivage et de la classification
G2 – Assurance de la sécurité des données lors du transfert	Dispositions de protection des données Cryptage	
G3 – Assurance de la sécurité des données lors de la sauvegarde et de l'archivage		

– Attitudes

Attitudes	Critère de prestation	A	B	C	D	E	F	G
Autonomie	DCO A et B tous les critères de prestation DCO D: - de documenter et de rendre compte des résultats d'audit concernant la compliance - Analyser, évaluer des projets d'autres domaines concernant la sécurité de l'information et communiquer les résultats	x	x		x			
A	DCO A: - Effectuer des présentations de façon adaptée aux destinataires - Elaborer une stratégie en matière de sécurité de l'information sur la base de la disposition à prendre des risques de la direction et du Conseil d'administration - de déterminer le degré de maturité de la sécurité dans l'organisation - de transmettre à leur équipe le contenu des publications sur la sécurité - de soutenir les collaborateurs subordonnés sur le plan spécialisé - Mettre en place une communauté de spécialistes en sécurité de l'information et garantir l'échange permanent d'expériences et de connaissances DCO B: - Définir et introduire des processus - Définir des exigences concernant les processus, les coordonner et les finaliser avec le responsable des processus DCO C: - de définir des mesures de protection à partir des écarts par rapport aux exigences techniques - de déduire des solutions de protection techniques coordonnées avec les parties prenantes	x	x	x	x	x	x	

Attitudes	Critère de prestation	A	B	C	D	E	F	G
	DCO D: - Mettre en place et entretenir un réseau de relation dans le domaine de la sécurité de l'information - Effectuer des activités de conseil pour des projets d'autres domaines concernant la sécurité de l'information DCO E: - Présenter sous forme didactique les contenus pour les campagnes de sensibilisation et les préparer en conséquence pour le canal de communication sélectionné de façon adaptée aux groupes cibles - Planifier et réaliser des formations auprès des groupes cibles DCO F: - Déterminer, analyser et documenter la conséquence d'une panne des services d'information - Informer les parties prenantes et les responsables de processus commerciaux sur les interdépendances pertinentes dans le processus commercial - Conseiller le comité de crise et le soutenir dans la prise de décision							
Loyauté	DCO A et B tous les critères de prestation	x	x					
Capacité de jugement	DCO A: - Définir les scénarios de menace ayant une pertinence pour l'organisation - Analyser les risques DCO B tous les critères de prestations DCO C: - Planifier, réaliser et évaluer les projets dans le domaine de la sécurité de l'information	x	x	x	x		x	

Attitudes	Critère de prestation	A	B	C	D	E	F	G
	DCO D: - Enregistrer des questions de parties prenantes et y répondre de façon adaptée aux groupes cibles - Déduire des exigences en termes de sécurité concernant un produit à partir des exigences commerciales fonctionnelles DCO F: - Analyser la situation générale de sécurité en se concentrant sur le potentiel de dangers pour la propre organisation et élaborer des mesures immédiates - Déterminer, analyser et documenter la conséquence d'une panne des services d'information - Fixer la solution d'un événement de sécurité et évaluer le dommage provoqué - Contrôler si les aspects portant sur la sécurité sont pris en compte dans le BCM - Déduire des mesures de la conséquence d'un événement et les classer par priorité							
Réflexion tournée vers l'avenir	DCO A: - Connaître son propre besoin en formation ainsi que celui de l'équipe et mettre en œuvre des mesures DCO B: - S'informer en continu sur les thèmes relevant de la sécurité comme les nouvelles technologies, les scénarios d'attaques et les concurrents, et faire intégrer les nouveaux enseignements dans les règlements internes et dans la gestion des risques DCO C: - Esquisser des exigences concernant le modèle technique planifié dans les domaines du panorama des systèmes et des applications informatiques	x	x	x				x

Attitudes	**Critère de prestation**	**A**	**B**	**C**	**D**	**E**	**F**	**G**
	DCO G: - Ordonner la technique de cryptage et son utilisation selon la situation - Contrôler les aspects de sécurité de la sauvegarde, des technologies d'archivage et de la classification							
Aptitude à s'imposer	DCO A et B tous les critères de prestation DCO E: - Fixer les thèmes, le public cible, la période, les outils, la valeur de référence et le canal de communication DCO F: - Déduire des mesures de la conséquence d'un événement et les classer par priorité - Informer les parties prenantes et les responsables de processus commerciaux sur les interdépendances pertinentes dans le processus commercial	x	x			x	x	
Intégrité	DCO A et B tous les critères de prestation DCO D: - de convenir et de contrôler les contrats de prestation avec les clients et les fournisseurs en termes de sécurité de l'information DCO G: - Contrôler les aspects de sécurité de la sauvegarde, des technologies d'archivage et de la classification - Etablir un concept de classification	x	x		x			x
Capacité d'innover	DCO A: - Connaître son propre besoin en formation ainsi que celui de l'équipe et mettre en œuvre des mesures	x	x					

Attitudes	**Critère de prestation**	**A**	**B**	**C**	**D**	**E**	**F**	**G**
	DCO B: - S'informer en continu sur les thèmes relevant de la sécurité comme les nouvelles technologies, les scénarios d'attaques et les concurrents, et faire intégrer les nouveaux enseignements dans les règlements internes et dans la gestion des risques							
Aptitude au travail en équipe	DCO A et B tous les critères de prestation DCO C: - Planifier, réaliser et évaluer les projets dans le domaine de la sécurité de l'information DCO D: - Mettre en place et entretenir un réseau de relation dans le domaine de la sécurité de l'information DCO F: - Conseiller le comité de crise et le soutenir dans la prise de décision	x	x	x	x		x	
Réflexion pluridisciplinaire	DCO A et B tous les critères de prestation DCO C: - Analyser la situation actuelle du panorama de systèmes et d'applications informatiques et constater les implications sur les menaces intérieures et extérieures - Esquisser des exigences concernant le modèle technique planifié dans les domaines du panorama des systèmes et des applications informatiques DCO D: - Fixer une intégration minimale d'un produit dans l'architecture de sécurité existante pour la démonstration de faisabilité (Proof of concept)	x	x	x	x			

Attitudes	Critère de prestation	A	B	C	D	E	F	G
	- Participer à l'élaboration du plan de contrôle de la sécurité et au contrôle de la démonstration de faisabilité (Proof of concept) et contrôler le rapport de test							
Pensée systémique	DCO B: - d'élaborer un ISMS. Cela comprend la définition du volume de l'ISMS, la réalisation d'une analyse du risque, l'élaboration d'un plan de traitement du risque, la définition d'un système de contrôle des mesures ainsi que l'implémentation de mesures de sécurité et de processus - de piloter, de contrôler et de maintenir le fonctionnement d'un ISMS, de contrôler et si nécessaire, de modifier l'efficacité des mesures et des processus - d'assurer l'amélioration permanente de l'ISMS - S'informer en continu sur les thèmes relevant de la sécurité comme les nouvelles technologies, les scénarios d'attaques et les concurrents, et faire intégrer les nouveaux enseignements dans les règlements internes et dans la gestion des risques DCO C: - Analyser la situation actuelle du panorama de systèmes et d'applications informatiques et constater les implications sur les menaces intérieures et extérieures DCO F: - Analyser la situation générale de sécurité en se concentrant sur le potentiel de dangers pour la propre organisation et élaborer des mesures immédiates - Déterminer, analyser et documenter la conséquence d'une panne des services d'information - Fixer la solution d'un événement de sécurité et évaluer le dommage provoqué - Contrôler si les aspects portant sur la sécurité sont pris en compte dans le BCM		x	x			x	x

Attitudes	Critère de prestation	A	B	C	D	E	F	G
	- Déduire des mesures de la conséquence d'un événement et les classer par priorité DCO G: - Etablir un concept de classification - Formuler des directives pour la gestion des données							
Capacité d'apprentissage	DCO A et B tous les critères de prestation	x	x					
Sens des responsabilités	DCO A et B tous les critères de prestation DCO C: - Analyser la situation actuelle du panorama des systèmes et des applications informatiques et consigner les implications sur les menaces intérieures et extérieures, - Esquisser des exigences concernant le modèle technique planifié dans les domaines du panorama des systèmes et des applications informatiques - d'élaborer une analyse des écarts entre l'état effectif et l'état visé et de la coordonner avec les parties prenantes correspondantes - de définir des mesures de protection à partir des écarts par rapport aux exigences techniques DCO F: - Etablir la situation générale de sécurité en se concentrant sur le potentiel de dangers pour la propre organisation - Déduire des mesures de la conséquence d'un événement et les classer par priorité DCO G: - Etablir un concept de classification - Contrôler les aspects de sécurité de la sauvegarde, des technologies d'archivage et de la classification	x	x	x			x	x

Identification du module

Numéro de module	249	
Titre	Planifier et superviser des projets	
Compétence	Planifier, superviser et piloter un projet conformément au mandat de projet	
Objectifs opérationnels	1	Analyser un mandat de projet, le vérifier le cas échéant avec le mandant, le préciser si nécessaire et établir une planification générale de projet.
	2	Décomposer les livrables du projet en sous-projets et lots de travaux. Formuler les mandats de travail correspondants en les assortissant d'objectifs techniques, économiques et de délais.
	3	Planifier sur la base des objectifs techniques, économiques et des délais le suivi des sous-projets et lots de travaux.
	4	Planifier la communication de projet conformément aux consignes figurant dans le mandat de projet et aux parties prenantes définies dans l'organisation de projet.
	5	Choisir des exécutants compétents pour la réalisation des sous-projets et des lots de travaux et leur attribuer des missions.
	6	Identifier et analyser les risques liés au projet et proposer des mesures propres à les maîtriser.
	7	Assurer le suivi permanent de l'avancement du projet, mettre en œuvre les mesures de pilotage adéquates et les coordonner si nécessaire avec le mandant.
	8	Planifier le processus de traitement des demandes de modification concernant le projet, le mettre en place et traiter les demandes de modification en conséquence.
	9	Rédiger des rapports d'avancement de projet et de phase à l'intention du mandant et les présenter à l'occasion des réunions du comité de projet.
Domaine de compétence	Project Management	
Objet	Projets assortis d'un mandat.	
Version du module	3.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	249
Titre	Planifier et superviser des projets
Compétence	Planifier, superviser et piloter un projet conformément au mandat de projet

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les rôles d'un projet et savoir quelles sont leurs tâches, compétences et responsabilités au sein de l'organisation de projet.
	1.2	Connaître les caractéristiques que doit présenter un objectif pour être complet. Savoir comment elles permettent d'aboutir à un accord précis entre mandant et mandaté et comment elles aident le mandaté à réaliser les objectifs convenus.
	1.3	Connaître les facteurs relatifs au contenu, aux délais et au budget qui influencent le déroulement du projet et pouvoir expliquer comment en tenir compte dans l'élaboration d'une planification de projet.
	1.4	Connaître les méthodes de planification permettant d'atteindre les objectifs de délai, de qualité et de contenu (GANTT, plan PERT, organigramme de tâches, etc.).
	1.5	Connaître les principes fondamentaux du déroulement structuré d'un projet.
	1.6	Connaître les différents modèles de démarche (chute d'eau, Scrum, HERMES, modèle du cycle en V, etc.) et leurs différences.
	1.7	Connaître différentes formes d'organisation de projet (task force, coordination de projet, matrice, etc.).
2	2.1	Savoir comment les livrables du projet sont représentés et documentés dans un organigramme de tâches.
	2.2	Connaître les critères à prendre en compte dans la constitution de lots de travaux et pouvoir expliquer comment ils contribuent à une répartition judicieuse du travail et au déroulement efficace d'un projet.
	2.3	Connaître les exigences que doit remplir un mandat de travail pour être ciblé et adapté à son destinataire (cohérence, délimitation précise ou coïncidence avec les objectifs du projet, etc.).
	2.4	Connaître les critères utilisés pour définir des sous-projets.
3	3.1	Connaître les outils et méthodes de suivi d'un projet et pouvoir expliquer comment ils contribuent à la réalisation optimale des objectifs.
	3.2	Connaître la signification des facteurs d'influence environnementaux et savoir comment ils influent la réalisation des objectifs, autrement dit comment ils doivent être pris en compte.
4	4.1	Savoir quels sont les besoins d'information découlant des exigences formulées dans le mandat de projet et du suivi du projet.
	4.2	Savoir comment concrétiser ces exigences dans un plan de communication de projet.

Connaissances opérationnelles nécessaires

5	5.1	Connaître les critères qualitatifs et personnels à remplir pour réaliser des lots de travaux.
	5.2	Connaître les caractéristiques que doit présenter un mandat de travail pour être complet.
	5.3	Connaître les exigences de délai, qualitatives, environnementales et économiques que doit satisfaire l'attribution de sous-projets.
	5.4	Connaître les éléments que doit contenir un mandat de sous-projet. Connaître les directives internes relatives à l'attribution de sous-projets.
6	6.1	Pouvoir décrire la démarche systématique d'analyse des risques et la contribution de chacune de ses étapes à l'identification, à l'évaluation et à la maîtrise des risques des projets.
	6.2	Pouvoir indiquer des mesures adéquates de maîtrise des risques, expliquer leur efficacité. Savoir comment elles s'intègrent dans le processus de planification.
7	7.1	Connaître des méthodes de suivi permanent de l'avancement d'un projet, de sous-projets et de lots de travaux (rapports de travail, rapports d'avancement, rapports concernant les livrables, revues, etc.).
	7.2	Connaître des mesures de pilotage de projets qui peuvent être prises suite à l'identification d'écarts de planification lors du contrôle d'avancement. Savoir comment elles s'intègrent dans le processus de planification.
	7.3	Connaître les caractéristiques des mesures de pilotage prises en cas d'écart de planification qui définissent l'instance qui décide de leur réalisation. Pouvoir indiquer pourquoi leur prise en compte permet d'impliquer les décideurs en fonction de leur compétence.
8	8.1	Connaître les causes possibles d'une modification des conditions générales et des objectifs d'un projet.
	8.2	Savoir comment définir un processus de changement adapté au projet.
	8.3	Savoir quelles informations concernant la gestion du changement doivent être intégrées dans la documentation de projet.
9	9.1	Connaître les caractéristiques d'un rapport de projet (rapports de jalon, rapports de projet, rapports de phase, demandes d'autorisation de phase, etc.) et savoir comment les préparer à l'intention des décideurs.
	9.2	Savoir comment préparer une présentation concernant l'avancement d'un projet et pouvoir expliquer quels sont les critères qui en conditionnent la réussite.

Version du module	3.0
Créé le	11.02.2021

Identification du module

Numéro de module	665	
Titre	Développer une stratégie de sécurité de l'information	
Compétence	Etablir les objectifs stratégiques relatifs à la sécurité de l'information d'une organisation en tenant compte des facteurs d'influence déterminants et assurer l'intégration de la stratégie de sécurité de l'information dans la stratégie globale de l'entreprise.	
Objectifs opérationnels	1	Examiner les processus métier d'une organisation quant à la création de valeur et identifier les processus essentiels qui sont sensibles au niveau de la sécurité de l'information.
	2	Examiner l'environnement d'une organisation et identifier les parties prenantes concernées par la sécurité de l'information et leurs intérêts.
	3	Analyser la stratégie de l'entreprise et identifier les menaces pesant sur la sécurité de l'information.
	4	Déduire les objectifs stratégiques en matière de sécurité de l'information à partir des menaces et en tenant compte de l'appétence au risque de la direction.
	5	Sensibiliser la direction à la sécurité de l'information et assurer l'intégration de la stratégie de sécurité de l'information dans la stratégie globale de l'entreprise.
Domaine de compétence	Security/Risk Management	
Objet	Moyennes et grandes entreprises avec des processus métiers et une stratégie d'entreprise définis.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	665
Titre	Développer une stratégie de sécurité de l'information
Compétence	Etablir les objectifs stratégiques relatifs à la sécurité de l'information d'une organisation en tenant compte des facteurs d'influence déterminants et assurer l'intégration de la stratégie de sécurité de l'information dans la stratégie globale de l'entreprise.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les termes «processus de base», «processus de support» et «processus de management» ainsi que leur importance dans la chaîne de création de valeur d'une organisation.
	1.2	Connaître les objectifs généraux de protection de la sécurité de l'information (confidentialité, intégrité, disponibilité).
2	2.1	Connaître les facteurs d'influence déterminants (p.ex. économie, société, technologie, nature) et les parties prenantes (p.ex. clients, fournisseurs) dans le contexte de l'organisation.
	2.2	Connaître des méthodes et techniques pour analyser et représenter le cadre de référence d'une organisation (p. ex. modèle de management de l'Université de Saint-Gall, analyse de l'environnement, analyse des parties prenantes).
3	3.1	Connaître les éléments essentiels d'une stratégie d'entreprise (charte, mission, vision, valeurs, objectifs stratégiques).
	3.2	Connaître des méthodes et techniques de planification stratégique (p.ex. analyse SWOT, analyse de la chaîne de valeur, Balanced Scorecard ou tableau de bord prospectif/équilibré) et d'analyse des écarts stratégiques (p.ex. analyse GAP).
	3.3	Connaître les sources et catalogues courants recensant les menaces (p.ex. MELANI, catalogues des menaces de l'Office fédéral allemand de la sécurité des technologies de l'information [BSI]).
4	4.1	Connaître les termes «appétence au risque» et «tolérance au risque» et pouvoir expliquer leurs différences.
	4.2	Connaître les aspects essentiels en matière de formulation des objectifs stratégiques (Expectation Management ou gestion des attentes, mandat, horizon de planification, performances, organisation, financement).
5	5.1	Connaître l'importance et les raisons qui sous-tendent l'ancrage de la stratégie de sécurité de l'information au niveau de la direction.
	5.2	Connaître des attitudes contribuant à sensibiliser la direction (p.ex. capacité à communiquer, loyauté, intégrité).

Version du module	1.0

Connaissances opérationnelles nécessaires

Créé le	11.02.2021

Identification du module

Numéro de module	666	
Titre	Définir et ancrer une gouvernance relative à la stratégie de sécurité de l'information	
Compétence	Sur la base de la stratégie de sécurité de l'information, définir une organisation de sécurité appropriée et élaborer la directive de sécurité et ancrer celles-ci dans l'organisation en collaboration avec la direction.	
Objectifs opérationnels	1	Définir les rôles requis par l'organisation de sécurité, leurs responsabilités et la délimitation des tâches entre les différents rôles.
	2	Définir les processus et les mesures organisationnelles permettant de prendre en compte et d'ancrer la sécurité de l'information dans toutes les activités ICT et activités de l'entreprise concernées.
	3	Mettre en place un solide réseau de relations avec les autorités, les organes et services compétents dans le domaine de la sécurité de l'information et assurer l'échange régulier de connaissances et d'expériences.
	4	Elaborer une directive de sécurité applicable à toute l'organisation qui reflète la politique de sécurité de l'information et la rend transparente.
	5	Soumettre la directive pour acceptation à la direction et organiser sa communication auprès des parties prenantes concernées.
Domaine de compétence	Security/Risk Management	
Objet	Moyennes et grandes entreprises avec une stratégie d'entreprise et une stratégie de sécurité de l'information définies.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	666
Titre	Définir et ancrer une gouvernance relative à la stratégie de sécurité de l'information
Compétence	Sur la base de la stratégie de sécurité de l'information, définir une organisation de sécurité appropriée et élaborer la directive de sécurité et ancrer celles-ci dans l'organisation en collaboration avec la direction.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les rôles déterminants en vue de garantir la sécurité de l'information au sein de l'organisation.
	1.2	Connaître des techniques permettant de décrire et de définir les rôles et les responsabilités (p.ex. description des postes et des fonctions, matrice RACI, principe TCR [tâches, compétences et responsabilités]).
	1.3	Connaître des techniques de représentation des structures organisationnelles (p.ex. organigramme, diagrammes des fonctions).
2	2.1	Connaître les interfaces avec les domaines spécialisés d'une organisation (p.ex. Management, ICT, Facility Management et service technique interne, Département juridique, Ressources Humaines, direction de projet) et pouvoir en expliquer l'importance pour la sécurité de l'information.
	2.2	Connaître des techniques de modélisation des processus métier (p.ex. Business Process Model and Notation [BPMN] ou modèle de procédé d'affaire et notation, Event Driven Process Chain ou chaîne de processus événementielle, UML).
3	3.1	Connaître les autorités compétentes dans le domaine de la sécurité de l'information (p.ex. MELANI, Office fédéral de la police [fedpol], autres autorités en charge de la sécurité et de poursuite pénale).
	3.2	Connaître les organes et services externes compétents dans le domaine de la sécurité de l'information (p.ex. associations professionnelles, ISACA, forums d'experts, services de consultation).
4	4.1	Connaître les éléments d'une directive de sécurité (p.ex. but, engagement et obligations de la direction, organisation de la sécurité et compétences) et pouvoir en expliquer leur finalité.
5	5.1	Connaître l'importance et les raisons de l'engagement de la direction envers la sécurité de l'information.
	5.2	Connaître des formes appropriées d'intégration et de communication de la directive de sécurité auprès des différentes parties prenantes.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	667	
Titre	Mettre en place un système de gestion de la sécurité de l'information	
Compétence	Définir le domaine d'application ainsi que les processus et procédures nécessaires pour un système de gestion de la sécurité de l'information (ISMS) en tenant compte des besoins spécifiques d'une organisation et des normes déterminantes en la matière.	
Objectifs opérationnels	1	Définir, en tenant compte de la stratégie de sécurité de l'information propre à une organisation, les objectifs et le domaine d'application d'un système de gestion de la sécurité de l'information (ISMS).
	2	Identifier, inventorier et classifier les valeurs déterminantes (assets) et définir les responsabilités en vue de les protéger tout au long du cycle de vie de l'information.
	3	Définir le processus de gestion des risques au sein d'une organisation, effectuer une analyse des risques et établir un plan de gestion des risques pour l'ISMS.
	4	Définir la pertinence et l'applicabilité des mesures de sécurité au sein de l'organisation dans une Déclaration d'Applicabilité (Statement of Applicability [SoA]).
	5	Définir les procédures et les ressources nécessaires pour l'ISMS.
	6	Définir un système de contrôle et les chiffres clés permettant de mesurer la performance et l'efficacité de l'ISMS.
Domaine de compétence	Security/Risk Management	
Objet	Organisation souhaitant introduire un système de gestion de la sécurité de l'information (ISMS) conforme aux normes et adapté à ses besoins.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	667
Titre	Mettre en place un système de gestion de la sécurité de l'information
Compétence	Définir le domaine d'application ainsi que les processus et procédures nécessaires pour un système de gestion de la sécurité de l'information (ISMS) en tenant compte des besoins spécifiques d'une organisation et des normes déterminantes en la matière.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître la structure et les dispositions déterminantes de la norme ISO/IEC 2700x pour l'établissement, l'implémentation, le maintien et l'amélioration continue d'un ISMS.
	1.2	Connaître le cycle PDCA (roue de Deming) et pouvoir en expliquer les différentes phases.
	1.3	Connaître les facteurs d'influence déterminants sur un ISMS dans le contexte d'une organisation.
	1.4	Connaître les facteurs de succès critiques (FCS) ou critical success factors (CSF) lors de l'introduction d'un ISMS.
2	2.1	Connaître le terme «valeur» (asset) et son utilisation en relation avec un ISMS.
	2.2	Connaître les phases typiques du cycle de vie de l'information (création, traitement, sauvegarde, transmission, suppression, destruction).
	2.3	Connaître des schémas appropriés de classification des valeurs en termes de confidentialité (p.ex. secret, confidentiel, restreint, interne et public), d'intégrité (p.ex. vital, important, normal) et de disponibilité (p.ex. en fonction du temps de réparation maximal estimé en cas de panne).
	2.4	Connaître le rapport existant entre la classification des valeurs et les exigences de sécurité correspondantes et pouvoir expliquer les procédures appropriées permettant de garantir la sécurité de l'information.
3	3.1	Connaître les normes déterminantes en matière de gestion des risques (ISO 31000, ISO/IEC 27005).
	3.2	Connaître des méthodes et techniques d'identification des risques (p.ex. enquête, analyse de documents, analyse de la chaîne de valeur, méthode Delphi, Business Impact Analysis [BIA], analyse de scénarios) et pouvoir en expliquer les avantages et les inconvénients.
	3.3	Connaître des méthodes d'évaluation et de représentation des risques (p.ex. matrice des risques, carte des risques).
	3.4	Connaître les différentes options de traitement du risque (réduction, refus/évitement, acceptation/maintien, transfert) et pouvoir en expliquer les caractéristiques.

Connaissances opérationnelles nécessaires

	3.5	Connaître les éléments d'un plan de gestion des risques (p.ex. mesure de sécurité, responsabilité, délai).Définir la pertinence et l'applicabilité des mesures de sécurité au sein de l'organisation dans une Déclaration d'Applicabilité (Statement of Applicability [SoA]).
4	4.1	Connaître la signification et le but d'une Déclaration d'Applicabilité.
	4.2	Connaître la structure et le contenu de l'annexe A de la norme ISO/IEC 27001 comme référence pour les mesures de sécurité.
5	5.1	Connaître les procédures centrales pour un ISMS (p.ex. procédure de contrôle des documents, audits, mesures préventives et correctives) et les exigences relatives à leur documentation.
	5.2	Connaître les principales ressources de soutien d'un ISMS (p.ex. compétences, prise de conscience, communication et gestion des documents) et pouvoir en expliquer leur influence.
6	6.1	Connaître la structure et le contenu de la norme ISO/IEC 27004 comme base pour la surveillance, la mesure, l'analyse et l'évaluation de l'ISMS
	6.2	Définir un système de contrôle et les chiffres clés permettant de mesurer la performance et l'efficacité de l'ISMS.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	668	
Titre	Exploiter et améliorer un système de gestion de la sécurité de l'information	
Compétence	Gérer et piloter, sur la base des normes applicables en la matière, l'exploitation d'un système de gestion de la sécurité de l'information (ISMS) au sein d'une organisation et garantir son amélioration continue.	
Objectifs opérationnels	1	Contrôler et évaluer périodiquement les risques de sécurité dans le cadre de la gestion des risques et adapter, si nécessaire, les mesures de sécurité de l'ISMS.
	2	Contrôler et évaluer périodiquement la performance et l'efficacité de l'ISMS et adapter, si nécessaire, les mesures de sécurité de l'ISMS ou le système de contrôle.
	3	Planifier et organiser des audits périodiques internes ou externes en vue de contrôler l'ISMS et garantir la documentation des résultats.
	4	Vérifier le respect de la sécurité de l'information dans le cadre des relations d'affaires avec les fournisseurs et les prestataires de services externes et rendre compte des résultats aux services ou organes compétents en matière de conformité.
	5	Examiner, en cas de non-conformité, les causes d'une erreur, engager des mesures correctives et, si nécessaire, procéder aux adaptations de l'ISMS.
	6	Evaluer les informations pertinentes relevant de l'exploitation de l'ISMS, traiter et présenter les résultats de façon concluante et organiser l'évaluation périodique de l'ISMS par la direction.
	7	Adopter les approches et attitudes qui favorisent et soutiennent l'apprentissage en continu au sein de l'organisation.
Domaine de compétence	Security/Risk Management	
Objet	Organisation avec un système de gestion de la sécurité de l'information (ISMS) établi et conforme aux normes.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	668
Titre	Exploiter et améliorer un système de gestion de la sécurité de l'information
Compétence	Gérer et piloter, sur la base des normes applicables en la matière, l'exploitation d'un système de gestion de la sécurité de l'information (ISMS) au sein d'une organisation et garantir son amélioration continue.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les critères déterminants pour procéder à des évaluations périodiques des risques de sécurité de l'information.
	1.2	Connaître les étapes essentielles du processus de gestion des risques au sein d'une organisation (p. ex. identification, évaluation et traitement des risques) et pouvoir en expliquer le but.
	1.3	Connaître les éléments d'un plan de traitement du risque (p.ex. mesure de sécurité, responsabilité, délai).
	1.4	Connaître les critères d'acceptation des risques dans le contexte d'une organisation.
2	2.1	Connaître les objectifs de la sécurité de l'information d'une organisation et les bases de planification permettant d'atteindre les objectifs visés.
	2.2	Connaître les indicateurs clés de performance (ICP) d'une organisation servant à mesurer la performance et l'efficacité de l'ISMS.
	2.3	Connaître des méthodes de contrôle de la plausibilité et de comparaison des valeurs de mesure (p.ex. règles de plausibilité, comparaison état actuel/visé, comparaison par rapport à la période précédente, extrapolation de tendance).
3	3.1	Connaître différents types d'audit (p.ex. audit de système, audit de processus, audit de conformité, audit de performance, audit financier) et pouvoir expliquer le caractère distinctif de l'objet de l'audit.
	3.2	Connaître les exigences relatives à la planification d'un audit (p.ex. fréquence, méthode, étendue, objectivité, impartialité, rapport) et pouvoir expliquer la différence entre un audit interne et un audit externe.
	3.3	Connaître différents audits en relation avec la certification d'un ISMS (p.ex. audit préalable, audit de certification, audit de surveillance) et pouvoir expliquer le caractère distinctif du but de l'audit.
4	4.1	Connaître les aspects liés à la sécurité dans le cadre d'un processus de gestion des services avec les fournisseurs et les prestataires de services externes (p.ex. surveillance du respect des niveaux de service convenus, contrôle des rapports de niveau de service, réalisation d'audits fournisseurs, communication et fourniture d'informations en cas d'incidents de sécurité de l'information).
5	5.1	Connaître les sources possibles permettant d'identifier les non-conformités (p.ex. gestion des incidents de sécurité de l'information, contrôle périodi-

Connaissances opérationnelles nécessaires

		que de la performance et de l'efficacité d'un ISMS, rapport d'audit, rapport de management, gestion périodique des risques, processus d'amélioration continu).
	5.2	Connaître des méthodes et techniques de résolution de problèmes et d'analyse structurée de leurs causes (p.ex. analyse des causes profondes, analyse ABC selon Pareto, méthode des 5 pourquoi [the 5 Whys], diagramme de cause à effet selon Ishikawa).
6	6.1	Connaître les aspects déterminants pour procéder à un examen périodique (management review) de l'ISMS.
	6.2	Connaître des techniques de représentation appropriées visant à synthétiser les informations dans un rapport de management (p.ex. histogramme, diagramme de corrélation, analyse de tendance).
7	7.1	Connaître les principes de conduite qui favorisent l'apprentissage en continu et la capacité à s'améliorer (p.ex. culture de l'erreur, faculté à apprendre, participation, droit d'intervenir dans les discussions et décisions).
	7.2	Connaître le concept d'apprentissage en simple boucle et en double boucle ou single and double loop learning au sein des organisations.
	7.3	Connaître le concept de l'organisation apprenante selon P. M. Senge et pouvoir expliquer les disciplines fondamentales (maîtrise personnelle, modèles mentaux, visions partagées, apprenance en équipe et pensée systémique).
	7.4	Connaître des concepts (p.ex. le modèle SECI selon Nonaka et Takeuchi), des méthodes (p. ex. communautés de pratique, storytelling, lessons learned) et des techniques (p.ex. collecticiel ou groupware, médias sociaux, wiki d'entreprise, systèmes experts, intelligence artificielle) relevant de la gestion des connaissances au sein des organisations.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	669	
Titre	Assurer le traitement des incidents de sécurité de l'information	
Compétence	Mettre en place, surveiller et gérer au sein d'une organisation des structures, des processus et des procédures permettant d'identifier et de traiter les incidents de sécurité de l'information sur tout leur cycle de vie.	
Objectifs opérationnels	1	Surveiller en continu la situation des menaces actuelles, identifier les dangers potentiels pour la propre organisation et, si nécessaire, engager des mesures préventives.
	2	Analyser et évaluer les processus, procédures et outils servant à signaler et à traiter les incidents de sécurité de l'information et, si nécessaire, adapter ceux-ci aux nouvelles menaces et exigences.
	3	Evaluer les incidents de sécurité de l'information, engager des mesures immédiates si nécessaire et définir des mesures réactives en vue de réduire les répercussions d'un incident de sécurité de l'information.
	4	Informer les parties prenantes concernées des incidents de sécurité de l'information et de la marche à suivre.
	5	Examiner et documenter un incident de sécurité de l'information et en évaluer les dommages.
	6	Evaluer l'incident de sécurité de l'information et identifier avec les services et organes compétents les mesures d'amélioration en vue de réduire la probabilité de survenance de futurs incidents et leurs répercussions.
Domaine de compétence	Service Management	
Objet	Incidents de sécurité de l'information survenant dans le fonctionnement opérationnel normal d'une organisation (p. ex. violation des directives internes, vol ou perte de terminaux mobiles, attaque de virus).	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	669
Titre	Assurer le traitement des incidents de sécurité de l'information
Compétence	Mettre en place, surveiller et gérer au sein d'une organisation des structures, des processus et des procédures permettant d'identifier et de traiter les incidents de sécurité de l'information sur tout leur cycle de vie.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les termes «menace» (threat), «vulnérabilité» (vulnerability) et «applied threat» et pouvoir expliquer leur signification du point de vue de l'organisation.
	1.2	Connaître des sources d'information internes et externes sur les menaces actuelles ainsi que les catalogues de menaces (p. ex. catalogues MELANI ou BSI, rapports de sécurité actuels provenant de fabricants, forums, échanges d'expériences au sein du réseau de relations).
2	2.1	Connaître les exigences relatives au traitement des incidents de sécurité de l'information prévues par la norme ISO/IEC 27001.
	2.2	Connaître des processus semblables ou apparentés en vue de traiter les incidents ou problèmes (p. ex. gestion des incidents ou des problèmes ITIL).
	2.3	Connaître des outils permettant d'administrer les incidents de sécurité de l'information (p.ex. Security Incident Management System ou système de gestion des incidents de la sécurité, Issue Tracking System ou système de suivi de problèmes, banque de données répertoriant les problèmes).
3	3.1	Connaître des concepts de priorisation et de catégorisation des incidents de sécurité de l'information.
	3.2	Connaître le but d'une stratégie d'escalade et la différence entre une escalade hiérarchique et une escalade fonctionnelle.
	3.3	Connaître des mesures immédiates permettant de maintenir la sécurité de l'information et d'apporter des clarifications ultérieures (p. ex. désactivation des comptes ou des services, préservation des éléments de preuve, copies forensiques des disques durs et forensique informatique).
4	4.1	Connaître les parties prenantes concernées au sein de l'organisation (p.ex. direction, département Compliance, Ressources humaines) et les autorités externes (p.ex. autorités d'enquêtes et de poursuites pénales).
	4.2	Connaître différents moyens de communication (p.ex. concertation personnelle, rapport écrit, e-mail, téléphone, envoi d'un coursier) et pouvoir expliquer leurs différences en terme de temps, du caractère contraignant (non-répudiation) et d'imputabilité.
5	5.1	Connaître les éléments essentiels d'une documentation claire et cohérente relative aux incidents de sécurité de l'information (incident record ou rapport d'incident).
	5.2	Connaître des méthodes et techniques de résolution de problèmes et d'analyse structurée de leurs causes (p.ex. analyse des causes profondes,

Connaissances opérationnelles nécessaires

		analyse ABC selon Pareto, méthode des 5 pourquoi [the 5 Whys], diagramme de cause à effet selon Ishikawa).
	5.3	Connaître les facteurs potentiels permettant d'évaluer et de mesurer les dommages (p.ex. dégâts matériels, durée d'indisponibilité, responsabilité, préjudice de réputation).
6	6.1	Connaître les parties prenantes concernées au sein de l'organisation (p.ex. Management, ICT, Service technique, Département juridique, Ressources humaines, direction de projet) et pouvoir en expliquer la pertinence ou l'implication quant à la sécurité de l'information.
	6.2	Connaître des méthodes de résolution et des solutions potentielles en vue de garantir la sécurité de l'information.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	670	
Titre	Garantir la sécurité de l'information dans le Business Continuity Management	
Compétence	Garantir l'intégration de la sécurité de l'information dans le Business Continuity Management (BCM) d'une organisation et soutenir la direction dans la maîtrise des crises et des situations d'urgence.	
Objectifs opérationnels	1	Soutenir et conseiller la direction dans l'élaboration de la Business Impact Analysis (BIA) dans les domaines ayant trait à la sécurité de l'information.
	2	Analyser l'organisation d'urgence et de crise du Business Continuity Management et s'assurer que l'organisation de sécurité est représentée de façon adéquate.
	3	Evaluer les processus et procédures du Business Continuity Management et garantir la prise en compte et le respect des exigences relatives à la sécurité de l'information.
	4	Garantir le contrôle périodique de l'efficacité de l'organisation d'urgence et de crise ainsi que des processus et des procédures du Business Continuity Management.
	5	Soutenir et conseiller l'organisation d'urgence et de crise dans la maîtrise d'une situation d'urgence ou d'une crise.
Domaine de compétence	Security/Risk Management	
Objet	Organisations dotées d'un Business Continuity Management et d'une gestion correspondante des cas d'urgence et des crises.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	670
Titre	Garantir la sécurité de l'information dans le Business Continuity Management
Compétence	Garantir l'intégration de la sécurité de l'information dans le Business Continuity Management (BCM) d'une organisation et soutenir la direction dans la maîtrise des crises et des situations d'urgence.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître le but et le contenu d'une BIA (estimation des dommages consécutifs).
	1.2	Connaître les termes «dérangement», «urgence», «crise» et «catastrophe» et pouvoir en expliquer les différences du point de vue de l'organisation.
	1.3	Connaître des scénarios possibles de crises et de situations d'urgence pouvant entraîner des interruptions des processus ICT (p.ex. pannes des systèmes, interruptions affectant les bâtiments, le personnel ou les fournisseurs).
2	2.1	Connaître les exigences relatives à la sécurité de l'information dans le cadre du Business Continuity Management issues de la norme ISO/IEC 27001 et des normes connexes (p.ex. ISO/IEC 22301, BS 25999).
	2.2	Connaître le but du Business Continuity Management et pouvoir expliquer ce qui le différencie du Disaster Recovery (reprise après sinistre).
	2.3	Connaître les autorités compétentes et les instances externes pour la maîtrise des crises et des situations d'urgence (p.ex. MELANI, autorités d'enquêtes et de poursuites pénales).
	2.4	Connaître la composition d'un comité de crise ou d'urgence et pouvoir expliquer les activités liées aux différentes fonctions de l'état-major de crise et celles des conseillers spécialisés.
3	3.1	Connaître des moyens techniques pour prévenir les interruptions des processus ICT (p.ex. tolérances, redondances).
	3.2	Connaître des mesures organisationnelles pour réduire de façon proactive les répercussions d'une interruption des processus ICT (p.ex. plans d'urgence, audits, recours à des expertises externes).
4	4.1	Connaître des mesures appropriées pour contrôler l'efficacité (p.ex. exercices d'urgence périodiques, audits).
5	5.1	Connaître des modèles de déroulement d'une crise et leurs phases typiques (p.ex. modèles de crise selon Kast, Caplan ou Cullberg).
	5.2	Connaître les principes de base de la communication de crise (rapidité, véracité, langage compréhensible, cohérence) et les différents groupes cibles (p.ex. personnes concernées, autorités, médias, parties impliquées) et pouvoir expliquer l'importance d'une communication adaptée au public cible.

Connaissances opérationnelles nécessaires

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	671	
Titre	Garantir la conformité de la sécurité de l'information	
Compétence	Garantir la mise en conformité (compliance) et le respect des dispositions légales, contractuelles et réglementaires relatives à la sécurité de l'information au sein d'une organisation et dans le cadre des relations d'affaires de celle-ci avec des tiers.	
Objectifs opérationnels	1	Identifier, dans le cadre d'une activité ICT, les aspects juridiquement pertinents relevant de la sécurité de l'information, définir les points contractuels essentiels et les soumettre aux parties négociatrices.
	2	Examiner et évaluer les contrats, les processus et les projets ICT quant au respect de la protection des données et engager, si nécessaire, des mesures correctives.
	3	Examiner et évaluer les contrats, les processus, les activités ICT et les incidents de sécurité de l'information en vue de déterminer s'ils relèvent du domaine pénal et, si nécessaire, engager des mesures correctives.
	4	Examiner et évaluer les contrats, les processus et les activités ICT quant au respect des aspects pertinents du droit de la propriété intellectuelle et, si nécessaire, engager des mesures correctives.
	5	Définir les procédures de contrôles de sécurité relatifs aux personnes (CSP) et garantir leur mise en œuvre au sein de l'organisation.
	6	Garantir le contrôle de sécurité dans le cadre des relations d'affaires avec des fournisseurs et des prestataires externes, en évaluer les résultats et, si nécessaire, engager des mesures correctives.
	7	Vérifier périodiquement les consignes et directives internes en relation avec la sécurité de l'information quant à leur adéquation, leur actualité et leur conformité légale.
Domaine de compétence	Business Management	
Objet	Moyennes et grandes entreprises dotées de structures et de processus définis et entretenant des relations d'affaires avec des tiers tels que clients, fournisseurs et prestataires.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	671
Titre	Garantir la conformité de la sécurité de l'information
Compétence	Garantir la mise en conformité (compliance) et le respect des dispositions légales, contractuelles et réglementaires relatives à la sécurité de l'information au sein d'une organisation et dans le cadre des relations d'affaires de celle-ci avec des tiers.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître l'objet et les principales caractéristiques des contrats régis par le Code des obligations (CO) (vente, bail à loyer, contrat d'entreprise, mandat proprement dit, contrat de travail).
	1.2	Connaître l'objet, les principales caractéristiques et les risques potentiels des contrats usuels relevant du domaine ICT (p.ex. contrat de services, contrat d'externalisation, contrat de licence).
	1.3	Connaître l'objet, les principales caractéristiques et les risques potentiels des contrats complémentaires relevant du domaine ICT (p.ex. accord de niveau de service [SLA], accord de confidentialité ou de non-divulgation, déclaration ou lettre d'intention).
2	2.1	Connaître les lois et les ordonnances relatives à la protection des données (p. ex. loi fédérale sur la protection des données [LPD]) et le Règlement général sur la protection des données de l'UE (RGPD).
3	3.1	Connaître les infractions du Code pénal suisse (CPS) relevant du domaine ICT.
	3.2	Connaître les infractions pertinentes (p.ex. pourriels) de la loi fédérale contre la concurrence déloyale (LCD).
4	4.1	Connaître les fondements du droit de la propriété intellectuelle de la Suisse et de l'Union européenne en ce qui concerne le droit d'auteur, le droit des brevets, le droit des marques et le droit des designs ou droit des dessins et modèles et pouvoir expliquer les voies de droit possibles (p.ex. action en dommages-intérêts) en cas d'infraction.
	4.2	Connaître la différence entre les droits moraux (droit de faire reconnaître sa qualité d'auteur, première publication) et les droits patrimoniaux (p.ex. production de copies, droit de location) régis par le droit d'auteur et leur signification en ce qui concerne le transfert des droits.
	4.3	Connaître d'autres modèles des droits d'auteur et de licence dans le cadre de la propriété intellectuelle (p.ex. licences Creative Commons, Open Source).
5	5.1	Connaître les bases légales des contrôles de sécurité relatifs aux personnes (loi fédérale instituant des mesures visant au maintien de la sûreté intérieure [LMSI], ordonnance sur les contrôles de sécurité relatifs aux personnes [OCSP]).

Connaissances opérationnelles nécessaires

	5.2	Connaître différents degrés de contrôle et de sécurité et pouvoir en expliquer les différences en tenant compte du champ d'action des personnes.
	5.3	Connaître les services internes impliqués dans les contrôles de sécurité relatifs aux personnes (p.ex. départements Ressources humaines et Compliance) et pouvoir expliquer leur fonction dans le cadre du CSP.
6	6.1	Connaître les contenus fondamentaux d'un accord de niveau de service (SLA).
	6.2	Connaître les outils servant au contrôle de sécurité de tiers (p.ex. audit des fournisseurs, rapport de niveau de service).
	6.3	Connaître les aspects pertinents quant à la conformité des processus de gestion des services avec les fournisseurs et les prestataires externes (p.ex. modifications des niveaux de service convenus, technologies ou sites des établissements et des infrastructures de services, sous-traitance avec d'autres fournisseurs).
7	7.1	Connaître les documents internes relatifs à la sécurité (p.ex. directive de sécurité, règlement d'utilisation ICT, concept de sauvegarde des données) et pouvoir en expliquer la pertinence juridique.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	672	
Titre	Evaluer et introduire des solutions de sécurité de l'information	
Compétence	Recueillir les exigences relatives aux nouvelles solutions de sécurité de l'information, apporter les preuves de leur rentabilité, soutenir leurs processus d'évaluation et d'acquisition et garantir leur intégration dans l'organisation.	
Objectifs opérationnels	1	Identifier en continu les nouvelles technologies et innovations, les évaluer quant à leur intérêt pour la sécurité de l'information au sein de l'organisation.
	2	Recueillir et documenter les exigences relatives à une nouvelle solution de sécurité de l'information en coopération avec les départements spécialisés.
	3	Identifier et évaluer les implications possibles engendrées par l'intégration d'une nouvelle solution de sécurité de l'information dans l'architecture existante d'une organisation et, si nécessaire, engager des mesures en vue de réduire les risques ou de valider les exigences critiques.
	4	Calculer la rentabilité des nouvelles solutions de sécurité de l'information et, sur la base des résultats obtenus, établir une recommandation servant à la prise de décision du point de vue financier.
	5	Définir le catalogue des critères servant à évaluer une solution de sécurité de l'information en tenant compte des exigences et du calcul de rentabilité.
	6	Comparer différentes offres à l'aune du catalogue de critères et, sur cette base, établir une recommandation pour l'acquisition d'une solution de sécurité de l'information.
	7	Soutenir les organes et départements compétents dans l'acquisition et l'introduction d'une nouvelle solution de sécurité de l'information.
Domaine de compétence	Service Management	
Objet	Organisation dotée de plusieurs sites et d'une architecture ICT complexe dont le bon fonctionnement doit être garanti par des solutions actuelles de sécurité de l'information.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	672
Titre	Evaluer et introduire des solutions de sécurité de l'information
Compétence	Recueillir les exigences relatives aux nouvelles solutions de sécurité de l'information, apporter les preuves de leur rentabilité, soutenir leurs processus d'évaluation et d'acquisition et garantir leur intégration dans l'organisation.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître le modèle des courbes en S en gestion de l'innovation, classifier les technologies (technologies émergentes, technologies en développement, technologies matures et technologies obsolètes) et pouvoir expliquer leurs caractéristiques, les opportunités et les risques y afférents.
	1.2	Connaître des sources d'informations actuelles sur les tendances et innovations ICT (p.ex. Hype Cycle de Gartner, conférences pertinentes sur la sécurité de l'information, études).
	1.3	Connaître le modèle économique fondamental du cycle de vie d'un produit avec les phases introduction, croissance, maturité, saturation, déclin et fin de vie.
	1.4	Connaître des modèles et outils de gestion stratégique des technologies et des produits (courbe S, matrice d'analyse du portefeuille BCG, matrice McKinsey, matrice ADL).
2	2.1	Connaître le but et le contenu du cahier des charges et ceux du cahier des charges avec spécification des exigences.
	2.2	Connaître la différence entre des exigences fonctionnelles, techniques, économiques, organisationnelles et écologiques et pouvoir expliquer la signification de la mesure des exigences.
	2.3	Connaître la structure fondamentale d'un catalogue d'exigences.
	2.4	Connaître des méthodes et techniques de recensement des exigences (p.ex. étude de documents, interviews, sondages, workshops, observation, analyse de processus) et pouvoir expliquer leurs avantages et inconvénients.
3	3.1	Connaître des méthodes et techniques visant à vérifier la faisabilité (p.ex. études de faisabilité, preuve de concept, prototypage, projets pilotes).
4	4.1	Connaître le but d'un compte d'investissement et de ses paramètres déterminants (capital investi, cashflow, durée d'utilisation, produit de liquidation et taux d'intérêt).
	4.2	Connaître des méthodes statiques relatives au compte d'investissement (calcul comparatif des coûts, calcul comparatif des bénéfices, calcul de rentabilité [retour sur investissement ou ROI], calcul du délai de récupération [méthode payback] et leurs applications respectives.
	4.3	Connaître des méthodes dynamiques relatives au compte d'investissement (méthode de la valeur actuelle nette [VAN], calcul du délai de récupération) et leurs applications respectives.

Connaissances opérationnelles nécessaires

	4.4	Connaître différents modèles de financement (p.ex. achat, location) et formes de financement (autofinancement et financement externe) et pouvoir expliquer leur influence sur le bilan et le compte de résultat de l'organisation (p.ex. effet de levier).
5	5.1	Connaître différents types de critères (p.ex. critères qualitatifs et quantitatifs, critères d'exclusion) et la structure fondamentale d'un catalogue de critères servant de base à une évaluation compréhensible et transparente.
	5.2	Connaître les exigences de base d'une procédure d'appel d'offres et d'adjudication (p.ex. clarté, transparence) et pouvoir expliquer les différences entre les procédures courantes (p.ex. procédure publique, procédure sur invitation, procédure privée).
6	6.1	Connaître des méthodes et techniques d'évaluation et de comparaison des variantes (p.ex. pondération par paire de facteurs, matrice préférentielle, job ranking ou méthode de classement hiérarchique, analyse de la valeur utile).
7	7.1	Connaître les phases typiques d'un processus d'acquisition et pouvoir en expliquer les éléments déterminants portant sur la sécurité de l'information (p.ex. conformité des contrats, exploitation et maintenance).
	7.2	Connaître des mesures visant à garantir la sécurité de l'information après l'introduction d'une nouvelle solution (p.ex. actualiser les procédures et les processus existants, mesurer l'efficacité).

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	673	
Titre	Créer et favoriser une prise de conscience quant à la sécurité de l'information	
Compétence	Identifier et mettre en œuvre les mesures de communication et de formation adaptées aux besoins et aux groupes cibles permettant de créer et de favoriser une prise de conscience en matière de sécurité de l'information.	
Objectifs opérationnels	1	Constituer un solide réseau de relations avec les parties prenantes et les médias concernés et garantir l'échange régulier de connaissances et d'expériences dans le domaine de la sécurité de l'information.
	2	Recueillir les besoins et les questions des parties prenantes et les conseiller avec compétence en fonction de leur groupe cible dans le domaine de la sécurité de l'information.
	3	Analyser les informations de sécurité relatives au fonctionnement opérationnel de l'organisation et identifier les besoins en termes de mesures de communication ou de formation.
	4	Choisir, en tenant compte des conditions cadres, une méthode appropriée pour réaliser une mesure de communication ou de formation et définir les canaux de communication.
	5	Planifier une mesure de communication et préparer les contenus en adéquation avec les groupes cibles et les médias.
	6	Planifier une formation et préparer les contenus de façon didactique.
	7	Mettre en œuvre une mesure de communication ou de formation, évaluer les résultats obtenus et identifier les améliorations possibles.
Domaine de compétence	Service Management	
Objet	Organisation devant créer une prise de conscience auprès de différentes parties prenantes internes et externes.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	673
Titre	Créer et favoriser une prise de conscience quant à la sécurité de l'information
Compétence	Identifier et mettre en œuvre les mesures de communication et de formation adaptées aux besoins et aux groupes cibles permettant de créer et de favoriser une prise de conscience en matière de sécurité de l'information.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les organes externes déterminants dans le domaine de la sécurité de l'information (p.ex. associations professionnelles, ISACA, forums d'experts, centres de consultation).
	1.2	Connaître les médias pertinents dans le contexte d'une organisation et les facteurs permettant de garantir un travail de presse efficace.
2	2.1	Connaître des méthodes d'écoute (p. ex. Rogers, Steil) et pouvoir expliquer en quoi celles-ci contribuent à prévenir les malentendus.
	2.2	Connaître les principes de la consultation systémique orientée solutions (p.ex. orientation des ressources, approche multiperspective, technique de questionnement orientée solutions, technique de recadrage).
3	3.1	Connaître le processus de traitement des incidents de sécurité de l'information au sein de l'organisation (p.ex. priorités, catégories, processus d'escalade) et pouvoir expliquer les causes fondamentales des incidents et des non-conformités.
	3.2	Connaître les valeurs statistiques et les indicateurs clés de performance (ICP) d'une organisation en matière de sécurité.
	3.3	Connaître des méthodes et des techniques appropriées pour synthétiser les informations relatives au fonctionnement opérationnel de l'organisation (p.ex. histogramme, diagramme de corrélation, analyse des tendances).
4	4.1	Connaître les grandeurs d'influence déterminantes pour les mesures de communication et de formation (p.ex. groupe cible, coûts, temps, qualité).
	4.2	Connaître des méthodes de sensibilisation des parties prenantes (p.ex. campagne d'information, formation, démonstrations en direct, consultation) et pouvoir expliquer leur adéquation, leurs avantages et inconvénients.
	4.3	Connaître divers canaux de communication (p.ex. face-à-face, médias imprimés, médias sociaux, forums, webinaire, télévision, radio) et pouvoir expliquer leurs différences en termes d'impact ainsi que leurs avantages et inconvénients.
5	5.1	Connaître les différences fondamentales entre communication interne et communication externe.
	5.2	Connaître différents formats de médias (p.ex. texte, son, image, vidéo) et pouvoir expliquer leurs avantages et inconvénients.

Connaissances opérationnelles nécessaires

	5.3	Connaître les outils fondamentaux du travail médiatique (p.ex. communiqué de presse, conférence de presse, dossier de presse, embargo).
6	6.1	Connaître le concept de l'éducation complète «tête, cœur et mains».
	6.2	Connaître divers concepts de formation (p.ex. formation en classe, e-learning, apprentissage mixte ou blended learning, auto-apprentissage) et leurs différences en termes de didactique, de forme sociale et de forme de travail.
	6.3	Connaître différentes méthodes de formation (p.ex. exposé, démonstration en direct, jeux, jeux de rôle, discussions) et pouvoir expliquer leurs avantages et inconvénients.
	6.4	Connaître les facteurs essentiels de planification d'une formation (p.ex. sujet, public cible, temps, diversité des méthodes).
7	7.1	Connaître des méthodes et techniques pour mesurer les effets d'une mesure de communication (p.ex. webtracking, media clipping, sondage).
	7.2	Connaître les aspects déterminants permettant d'évaluer une formation (p.ex. degré de satisfaction des participants, succès de l'apprentissage, transfert dans la pratique, intérêt).
	7.3	Connaître des méthodes d'évaluation des formations (p.ex. questionnaire, tests) et pouvoir expliquer leurs avantages et inconvénients.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	674	
Titre	Diriger et soutenir une équipe	
Compétence	Diriger et soutenir une équipe sur le plan professionnel et social en adoptant un comportement de conduite et de communication adapté à la situation.	
Objectifs opérationnels	1	Mener une réflexion sur son propre comportement en vue de conduire une équipe de manière efficace et efficiente.
	2	Définir son propre comportement de conduite de manière consciente et l'adapter en fonction du contexte.
	3	Définir son propre comportement de communication de manière consciente et en fonction de la situation et instaurer au sein de l'équipe une culture de communication basée sur l'estime.
	4	Promouvoir activement le développement de l'esprit d'équipe et clarifier les rôles au sein de l'équipe.
	5	Créer les conditions cadres pour qu'une équipe puisse travailler avec motivation.
	6	Identifier les potentiels de conflit et les conflits au sein de l'équipe et prendre des mesures appropriées pour les éviter, les désamorcer ou les résoudre.
	7	Planifier des processus de changement et soutenir les personnes concernées lors du règlement de différends et de la gestion du changement.
	8	Identifier le besoin de formation continue au sein de l'équipe, développer avec les collaborateurs des objectifs de développement individuels et planifier des mesures correspondantes de formation continue ou de soutien.
Domaine de compétence	Project Management	
Objet	Responsabilité de conduite d'équipes de projet ou d'unités organisationnelles avec des spécialistes et 10 à 12 collaborateurs au maximum.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	674
Titre	Diriger et soutenir une équipe
Compétence	Diriger et soutenir une équipe sur le plan professionnel et social en adoptant un comportement de conduite et de communication adapté à la situation.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des modèles simples de perception des traits de la personnalité et des caractéristiques comportementales (p.ex. fenêtre de Johari, modèle de l'iceberg) et pouvoir expliquer les différences entre la perception de soi et la perception d'autrui.
	1.2	Connaître des modèles fondamentaux de la gestion du temps et de soi (p.ex. principe d'Eisenhower, principe de Pareto).
	1.3	Connaître l'importance du devoir d'exemplarité dans la conduite.
2	2.1	Connaître les différents styles de conduite et leurs caractéristiques et pouvoir expliquer l'adéquation d'un style en fonction de la situation.
	2.2	Connaître les différentes formes d'organisation et leurs caractéristiques (p.ex. organisation hiérarchique et organisation fonctionnelle, organisation hiérarchique avec état-major, organisation matricielle, organisation de projet pure avec Task Force) et pouvoir expliquer l'adéquation d'une forme d'organisation en fonction de la situation.
3	3.1	Connaître des modèles de communication fondamentaux (p.ex. le modèle des quatre oreilles de Schultz von Thun, la communication non violente selon B. Rosenberg) et pouvoir expliquer leur importance par rapport à son propre comportement de communication.
	3.2	Connaître les règles pour la transmission et la réception de feedbacks.
4	4.1	Connaître la différence entre un groupe et une équipe.
	4.2	Connaître les cinq étapes du développement de l'esprit d'équipe selon Tuckman (Forming, Storming, Norming, Performing et Adjourning) et pouvoir expliquer les caractéristiques de chaque étape.
	4.3	Connaître des modèles de rôles au sein d'une équipe (p.ex. rôles en équipe selon Belbin), connaître la différence entre la construction d'un rôle (role making) et la prise active d'un rôle (role taking) et pouvoir expliquer l'importance de la composition des rôles pour les performance au sein d'une équipe.
5	5.1	Connaître des modèles fondamentaux de la théorie de la motivation (p.ex. Maslow, Herzberg) et pouvoir expliquer leur importance dans la pratique.
	5.2	Connaître la différence entre la motivation intrinsèque et la motivation extrinsèque.
6	6.1	Connaître les caractéristiques et la dynamique des conflits.
	6.2	Connaître des mesures pour éviter et résoudre des conflits.

Connaissances opérationnelles nécessaires

7	7.1	Connaître les phases typiques des processus de changement et pouvoir expliquer les caractéristiques des différentes phases.
	7.2	Connaître les facteurs de succès (p.ex. perception de l'urgence, succès rapides, communication) et les risques liés aux processus de changement.
	7.3	Connaître les signes typiques des peurs et des oppositions et pouvoir expliquer des procédures adaptées pour les gérer.
8	8.1	Connaître des mesures de soutien (p.ex. formation, coaching, développement de l'équipe) et pouvoir expliquer leurs caractéristiques et leur adéquation en fonction de la situation.
	8.2	Connaître les exigences à remplir pour de bonnes conventions d'objectifs et des entretiens constructifs basés sur l'estime en vue d'une convention d'objectifs communs.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	675	
Titre	Examiner et évaluer la sécurité des réseaux	
Compétence	Examiner l'infrastructure réseau d'une organisation sur les couches de transfert, de transmission et de transport (couches OSI 1 à 4), évaluer leur degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer la sécurité réseau.	
Objectifs opérationnels	1	Faire l'état des lieux de l'infrastructure réseau d'une organisation et documenter l'architecture réseau sous une forme appropriée.
	2	Vérifier la sécurité de tout ou partie de l'architecture réseau au moyen de méthodes appropriées.
	3	Evaluer la sécurité de l'architecture réseau sous l'angle des processus et identifier les améliorations potentielles.
	4	Evaluer la sécurité de l'architecture réseau d'un point de vue technique et identifier les améliorations potentielles.
	5	Evaluer l'architecture réseau en regard de l'utilisation des mesures cryptographiques et identifier les améliorations potentielles.
	6	Elaborer, sur la base des points faibles identifiés, un catalogue de mesures permettant d'améliorer la sécurité réseau, formuler une recommandation et la présenter aux décideurs.
Domaine de compétence	Network Management	
Objet	Infrastructure réseau ICT complexe, physique ou virtualisée avec plusieurs sites et avec focalisation sur les couches de transfert, de transmission et de transport (couches OSI 1 à 4).	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	675
Titre	Examiner et évaluer la sécurité des réseaux
Compétence	Examiner l'infrastructure réseau d'une organisation sur les couches de transfert, de transmission et de transport (couches OSI 1 à 4), évaluer leur degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer la sécurité réseau.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les standards réseau usuels (IEEE 802) pour les réseaux locaux (LAN), les réseaux sans fil (WLAN), les réseaux personnels avec ou sans fil (PAN, WPAN) et pouvoir expliquer leurs caractéristiques et leurs points faibles potentiels au niveau de la sécurité de l'information.
	1.2	Connaître différents concepts permettant de relier plusieurs sites (p.ex. ligne directe, réseaux privés virtuels [VPN]) et pouvoir expliquer leurs caractéristiques en termes de sécurité (p.ex. utilisation partagée ou dédiée, performance, disponibilité et confidentialité).
	1.3	Connaître les différents composants réseau jusqu'à la couche OSI 4 (p.ex. pont, concentrateur, commutateur, routeur, pare-feu) et pouvoir expliquer leur fonction.
	1.4	Connaître les concepts de séparation physique ou logique de réseaux en segments (p.ex. spanning tree STP, switching des couches 2 et 3, subnetting, VLAN, pare-feu, DMZ).
	1.5	Connaître des formes de représentation de la documentation relative à l'architecture réseau (p.ex. diagrammes de réseaux physiques et logiques, plans de câblage, listes d'inventaire des équipements réseau).
2	2.1	Connaître les recommandations relatives à la sécurité réseau issues du standard de facto de l'Open Source Security Testing Methodology Manual (OSSTMM).
	2.2	Connaître des menaces et des vecteurs d'attaques de réseaux (p.ex. attaques DDoS, sniffing, man in the middle, MAC et IP spoofing, attaques DNS).
	2.3	Connaître la charge d'utilisation des réseaux et leurs évolution future et pouvoir citer des méthodes et des outils couramment utilisés pour vérifier la sécurité réseau (p.ex. scanneur de ports, tests de pénétration, analyseur de protocoles, sniffer, lignes de commandes pertinentes).
3	3.1	Connaître les exigences des processus de sécurité relatives à l'administration réseau (p.ex. contrôle de l'accès et gestion des clés), traitement des exceptions et des modifications, gestion des licences, actualité de la documentation).
	3.2	Connaître les exigences de sécurité déterminantes relatives à la surveillance des réseaux ainsi que les dispositions légales ou réglementaires pertinentes (p.ex. enregistrement d'événements, protection des données pour l'enre-

Connaissances opérationnelles nécessaires

		gistrement de données sensibles, proportionnalité, durée de conservation des données enregistrées).
	3.3	Connaître les exigences de sécurité déterminantes relatives à la gestion des versions, des mises à jour et de fin de vie des composants réseau.
4	4.1	Connaître les domaines d'application, les conditions et les limites des mesures techniques visant à séparer des réseaux et à augmenter la disponibilité.
	4.2	Connaître des mesures techniques pour le pilotage de services réseau IP (Quality of Service QoS) au moyen d'une bande passante réservée ou de la priorisation.
	4.3	Connaître des mesures techniques pour contrôler l'accès aux réseaux (p.ex. filtres MAC et IP, authentification WLAN).
	4.4	Connaître différents systèmes pour le contrôle de l'accès physique aux zones de réseau et à leur câblage (p.ex. clé, badge, systèmes biométriques).
5	5.1	Connaître les principes du chiffrement symétrique, asymétrique et hybride et pouvoir expliquer leurs différences.
	5.2	Connaître les procédures cryptographiques usuelles (p.ex. RSA, ECDHE, ECDSA, SHA, 3DES, AES) et pouvoir expliquer leurs fonctions (échange de clés, authentification, fonction de compression Hash et cryptage).
	5.3	Connaître les protocoles de réseau et de transport usuels pour le cryptage (p.ex. IPSec, TLS).
6	6.1	Connaître le contenu et la structure d'un catalogue de mesures (p.ex. mesure, temps nécessaire, responsabilité, valeur ajoutée, estimation des coûts).
	6.2	Connaître le contenu et la structure d'une bonne présentation et pouvoir expliquer l'influence des comportements déterminants sur le travail de persuasion.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	676	
Titre	Examiner et évaluer la sécurité des applications et des services de serveurs	
Compétence	Examiner les applications et les services de serveurs dans les environnements de développement, de test et d'exploitation d'une organisation, évaluer leur degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer la sécurité des applications et des serveurs.	
Objectifs opérationnels	1	Faire l'état des lieux de l'environnement serveurs et applications d'une organisation et documenter l'architecture sous une forme appropriée.
	2	Vérifier la sécurité de tout ou partie de l'environnement serveurs et applications au moyen de méthodes appropriées.
	3	Evaluer la sécurité de l'environnement serveurs et applications sous l'angle des processus et identifier les améliorations potentielles.
	4	Evaluer la sécurité de l'environnement serveurs et applications d'un point de vue technique et identifier les améliorations potentielles.
	5	Evaluer l'environnement serveurs et applications en regard de l'utilisation des mesures cryptographiques et identifier les améliorations potentielles.
	6	Elaborer, sur la base des points faibles identifiés, un catalogue de mesures permettant d'améliorer la sécurité des serveurs et des applications, formuler une recommandation et la présenter aux décideurs.
Domaine de compétence	System Management	
Objet	Environnement complexe de serveurs physiques ou virtualisés avec différentes applications et avec focalisation sur les couches session, présentation et application (couches OSI 5 à 7).	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	676
Titre	Examiner et évaluer la sécurité des applications et des services de serveurs
Compétence	Examiner les applications et les services de serveurs dans les environnements de développement, de test et d'exploitation d'une organisation, évaluer leur degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer la sécurité des applications et des serveurs.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les protocoles d'applications usuels dans les réseaux TCP/IP (p.ex. HTTP, protocoles de messagerie électronique, DHCP, DNS, services d'annuaires, protocoles de transfert des données, protocoles de gestion des réseaux).
	1.2	Connaître les concepts d'architecture fondamentaux des réseaux (client-serveur, peer to peer, machine to machine) et pouvoir expliquer leurs caractéristiques et leur pertinence en termes de sécurité de l'information.
	1.3	Connaître différentes solutions de clouds (p.ex. cloud privé, public, hybride, communautaire) et divers modèles de services (IaaS, PaaS, SaaS) et pouvoir expliquer leurs caractéristiques et différences en termes de sécurité de l'information.
	1.4	Connaître des formes de représentation de la documentation relative aux architectures serveurs et applications (p. ex. modèle par couches, schéma fonctionnel ou schéma-bloc, diagrammes structurels UML pertinents).
2	2.1	Connaître les recommandations relatives à la sécurité et aux tests des applications Web issues du standard de facto de l'Open Web Application Security Project (OWASP) et de l'Open Source Security Testing Methodology Manual (OSSTMM).
	2.2	Connaître des menaces et des vecteurs d'attaques déterminants pour la sécurité des serveurs et des applications (p.ex. maliciels, mauvaise configuration, attaques DDoS, attaque XSS ou cross-site scripting, injection de script, vol de session ou session hijacking, attaques DNS).
	2.3	Connaître la différence entre un scan de vulnérabilité et un test de pénétration et pouvoir citer des méthodes et des outils couramment utilisés pour vérifier la sécurité des serveurs et des applications.
3	3.1	Connaître les exigences de sécurité déterminantes relatives à la séparation des environnements de développement, de test et d'exploitation.
	3.2	Connaître les exigences de sécurité déterminantes relatives à l'administration des services de serveurs et des applications ainsi que le traitement du code source dans les environnements de développement (p.ex. contrôle de l'accès et gestion des clés).
	3.3	Connaître les exigences de sécurité déterminantes relatives à la surveillance des services de serveurs et des applications ainsi que les dispositions légales

Connaissances opérationnelles nécessaires

		et réglementaires pertinentes (p.ex. enregistrement d'événements, protection des données pour l'enregistrement de données sensibles, proportionnalité, durée de conservation des données enregistrées).
	3.4	Connaître les exigences de sécurité déterminantes relatives à la gestion des versions, des mises à jour et de fin de vie des services de serveurs et des applications.
4	4.1	Connaître des mesures techniques contre les maliciels (p. ex. analyseur de virus, solutions anti-maliciels), contre les pourriels ou les maliciels contenus dans les e-mails (p.ex. liste blanche, grise ou noire sur les serveurs de messagerie, serveurs relais, restrictions relatives aux pièces jointes des e-mails, blocage de macros dans les documents Office).
	4.2	Connaître les domaines d'application, les conditions préalables et les limites des solutions techniques (appliance) visant à détecter des attaques (p. ex. pare-feu WAF, système de détection d'intrusion IDS, système de prévention d'intrusion IPS, honeypot, menaces persistantes avancées ATP) ainsi que ceux de la gestion des événements et des informations de sécurité (SIEM).
	4.3	Connaître des mesures techniques pour le contrôle de l'accès aux services des serveurs, aux applications et aux environnements de développement (p.ex. liste de contrôle d'accès ACL, authentification des utilisateurs, authentification multifactorielle).
	4.4	Connaître différents systèmes pour le contrôle de l'accès physique aux infrastructures serveur (p.ex. clé, badge, systèmes biométriques).
5	5.1	Connaître les principes du chiffrement symétrique, asymétrique et hybride et pouvoir expliquer leurs différences.
	5.2	Connaître les procédures cryptographiques usuelles (p.ex. RSA, ECDHE, ECDSA, SHA, 3DES, AES) et leurs domaines d'utilisation applicative courants (p. ex. cryptage des fichiers et des bases de données).
	5.3	Connaître le protocole de chiffrement TLS pour sécuriser la transmission des données et ses domaines d'utilisation courants (p.ex. HTTPS, SMTPS, SIPS, FTPS, SFTP, LDAPS).
	5.4	Connaître le but des suites cryptographiques pour établir des connexions sécurisées et leurs domaines d'application typiques (p.ex. HTTPS, SMTPS).
	5.5	Connaître les standards usuels du chiffrement de bout en bout (E2EE) des messages électroniques (p.ex. PGP, GPG S/MIME).
6	6.1	Connaître le contenu et la structure d'un catalogue de mesures (p.ex. mesure, temps nécessaire, responsabilité, valeur ajoutée, estimation des coûts).
	6.2	Connaître le contenu et la structure d'une bonne présentation et pouvoir expliquer l'influence des comportements déterminants sur le travail de persuasion.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	677	
Titre	Examiner et évaluer la sécurité des solutions de stockage	
Compétence	Examiner les solutions de stockage d'une organisation, évaluer leur degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer leur sécurité.	
Objectifs opérationnels	1	Faire l'état des lieux des solutions de stockage d'une organisation et documenter l'architecture sous une forme appropriée.
	2	Définir, sur la base des dispositions légales et des directives de l'entreprise pertinentes, les exigences en termes de sécurité et de protection des données des solutions de stockage.
	3	Evaluer la sécurité des solutions de stockage au niveau des processus et identifier les améliorations potentielles.
	4	Evaluer la sécurité des solutions de stockage d'un point de vue technique et identifier les améliorations potentielles.
	5	Evaluer des solutions de stockage en regard de l'utilisation de mesures cryptographiques et identifier les améliorations potentielles.
	6	Elaborer, sur la base des points faibles identifiés, un catalogue de mesures visant à améliorer la sécurité des solutions de stockage, formuler une recommandation et la présenter aux décideurs.
Domaine de compétence	System Management	
Objet	Solutions complexes de stockage physique ou virtualisé avec plusieurs sites et des technologies différentes.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	677
Titre	Examiner et évaluer la sécurité des solutions de stockage
Compétence	Examiner les solutions de stockage d'une organisation, évaluer leur degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer leur sécurité.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les architectures de stockage (DAS, NAS, SAN et stockage objet) et leurs caractéristiques de connectivité (p.ex. SCSI, FC, Ethernet), les modes d'accès (bloc, fichier et objet) ainsi que les protocoles (p.ex. iSCSI, SAS, NFS, CIFS/SMB, HTTP).
	1.2	Connaître les médias de stockage électroniques, magnétiques et optiques usuels ainsi que leurs caractéristiques quant à leur performance, capacité de stockage, prix et durée de vie (longévité).
	1.3	Connaître les technologies et procédures usuelles pour relier et organiser des stockages de masse (p.ex. baies de stockage ou disk arrays, JBOD, RAID, bibliothèque de bandes ou Tape Library).
	1.4	Connaître le concept de virtualisation de stockage et les différentes technologies de virtualisation de stockage (p.ex. au niveau réseau: en bande, hors bande ou split-path; au niveau hôte; au niveau contrôleur, VTL).
	1.5	Connaître les différentes solutions de cloud (p.ex. cloud privé, cloud public, cloud hybride, cloud communautaire) et pouvoir expliquer leurs caractéristiques et leurs différences en termes de sécurité des solutions de stockage.
	1.6	Connaître des formes de représentation de la documentation relative aux solutions de stockage (p.ex. diagrammes de réseaux physiques et logiques, modèles par couches, diagrammes de blocs).
2	2.1	Connaître l'importance de la classification des informations en regard de la confidentialité, de l'intégrité et de la disponibilité, et pouvoir expliquer les exigences relatives à un concept de classification et les procédures appropriées pour la mise en œuvre.
	2.2	Connaître le but et l'importance de la sauvegarde, de l'archivage et de la restauration des données et pouvoir expliquer les exigences relatives à un concept de sauvegarde des données ainsi que les stratégies et procédures appropriées pour la mise en œuvre.
	2.3	Connaître les dispositions légales pertinentes applicables au stockage, au traitement et à l'archivage des données, (p.ex. délais de conservation selon l'ordonnance concernant la tenue et la conservation des livres de comptes [Olico], réglementation du Bouclier de protection des données UE-Etats-Unis [EU-US Privacy Shield]) et à la protection des données sensibles (p.ex. loi fédérale sur la protection des données [LPD], Règlement général sur la protection des données de l'UE [RGPD].

Connaissances opérationnelles nécessaires

3	3.1	Connaître les exigences des processus de sécurité relatives à l'administration et à l'exploitation des solutions de stockage (p.ex. contrôle d'accès et gestion des clés, conservation des supports de données, contrôle périodique de la restauration des données).
	3.2	Connaître les exigences de sécurité quant à la surveillance des solutions de stockage ainsi que les dispositions légales et réglementaires applicables en la matière (p.ex. enregistrement d'événements, protection des données pour l'enregistrement de données sensibles, proportionnalité, durée de conservation des données enregistrées).
	3.3	Connaître les exigences de sécurité déterminantes relatives à la gestion des versions, des mises à jour et de fin de vie des composants et des logiciels des solutions de stockage.
4	4.1	Connaître le degré d'adéquation et les domaines d'application typiques des différents médias de stockage et des technologies.
	4.2	Connaître des mesures techniques pour accroître la sécurité contre les pannes et la disponibilité (p.ex. RAID, cluster de basculement ou failover cluster, systèmes à haute disponibilité, mise en miroir et réplication des systèmes, géoredondance).
	4.3	Connaître des méthodes de stockage à plusieurs niveaux de différentes données sur divers médias de stockage (p.ex. tiered storage, gestion de stockage hiérarchique).
	4.4	Connaître des méthodes d'optimisation de la capacité et de la performance des solutions de stockage (p.ex. compression, déduplication).
5	5.1	Connaître les procédures cryptographiques usuelles pour le chiffrement matériel des supports de données (p.ex. standard de chiffrement avancé AES, hachage cryptographique SHA).
	5.2	Connaître les exigences étendues relatives au chiffrement des solutions de stockage réseau et pouvoir expliquer les procédures usuelles pour un transfert crypté des données.
6	6.1	Connaître le contenu et la structure d'un catalogue de mesures (p.ex. mesure, temps nécessaire, responsabilité, valeur ajoutée, estimation des coûts).
	6.2	Connaître le contenu et la structure d'une bonne présentation et pouvoir expliquer l'influence des comportements déterminants sur le travail de persuasion.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	678	
Titre	Examiner et évaluer la sécurité des terminaux et périphériques	
Compétence	Examiner l'utilisation et l'intégration des terminaux et périphériques fixes et mobiles d'une organisation, évaluer le degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer leur sécurité.	
Objectifs opérationnels	1	Implémenter la sécurité système (182); Implémenter la sécurité réseau (184)Faire l'état des lieux des terminaux et périphériques fixes et mobiles au sein d'une organisation et documenter leur intégration dans l'infrastructure ICT existante sous une forme appropriée.
	2	Vérifier au moyen de méthodes appropriées la sécurité en matière d'utilisation et d'intégration des terminaux et périphériques.
	3	Evaluer la sécurité des terminaux et périphériques au niveau des processus et identifier les améliorations potentielles.
	4	Evaluer la sécurité des terminaux et périphériques du point de vue technique et identifier les améliorations potentielles.
	5	Evaluer les terminaux et périphériques en regard de l'utilisation de mesures cryptographiques et identifier les améliorations potentielles.
	6	Elaborer, sur la base des points faibles identifiés, un catalogue de mesures permettant d'améliorer la sécurité des terminaux et périphériques, formuler une recommandation et la présenter aux décideurs.
Domaine de compétence	System Management	
Objet	Différents terminaux et périphériques fixes ou mobiles dans l'infrastructure ICT complexe d'une organisation avec plusieurs sites.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	678
Titre	Examiner et évaluer la sécurité des terminaux et périphériques
Compétence	Examiner l'utilisation et l'intégration des terminaux et périphériques fixes et mobiles d'une organisation, évaluer le degré de maturité quant à la sécurité de l'information et recommander des mesures en vue d'améliorer leur sécurité.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les différents terminaux et périphériques fixes et mobiles, capteurs et actionneurs (p.ex. client léger ou thin client, client lourd ou fat client et client mobile, imprimante, scanner, smart watches, solutions smart home) et leurs domaines d'application typiques.
	1.2	Connaître les différents standards réseau pour l'intégration et la communication des terminaux et périphériques dans LAN, WLAN, PAN et WPAN (p. ex. IEEE 802.3, IEEE 802.11, Bluetooth, infrarouge, RFID, Z-Wave) et pouvoir expliquer leurs caractéristiques et points faibles potentiels en termes de sécurité de l'information.
	1.3	Connaître les différents types d'accès à distance des terminaux au réseau de l'entreprise (p. ex. VPN client à site, VPN site à site, VPN mobile) et pouvoir expliquer leurs différences.
	1.4	Connaître les fonctions de sécurité des systèmes d'exploitation usuels des terminaux (p.ex. Windows, Linux, iOS, Android).
	1.5	Connaître le concept d'infrastructure de bureau virtuel (VDI) et pouvoir expliquer les avantages et inconvénients de telles solutions.
	1.6	Connaître des formes de représentation de la documentation relative aux terminaux et aux périphériques ainsi qu'à leur intégration dans l'infrastructure ICT (p.ex. diagramme de blocs, diagrammes de réseau, liste des appareils et inventaires).
2	2.1	Connaître les recommandations relatives aux terminaux et aux périphériques fixes et mobiles issues du standard de facto de l'Open Source Security Testing Methodology Manual (OSSTMM).
	2.2	Connaître des menaces et des vecteurs d'attaques des terminaux et périphériques (p.ex. maliciels, vol, mauvaise configuration, points faibles techniques, phishing, spoofing, snarfing, bluejacking).
	2.3	Connaître les exigences et les risques spécifiques à un environnement «Bring Your Own Device» (BYOD).
	2.4	Connaître les outils usuels permettant de détecter les points faibles sur les terminaux et périphériques (p.ex. scan de vulnérabilité, logiciels antivirus).
3	3.1	Connaître les exigences des processus de sécurité relatives à l'administration et à l'utilisation des terminaux et périphériques (p.ex. mesures contre la perte ou le vol, contrôle d'accès et gestion des clés).

Connaissances opérationnelles nécessaires

	3.2	Connaître les exigences de sécurité quant à la surveillance des terminaux et périphériques ainsi que les dispositions légales et réglementaires applicables en la matière (p.ex. protection des données dans un environnement BYOD et pour l'enregistrement de données sensibles, proportionnalité, durée de conservation des données enregistrées).
	3.3	Connaître les exigences de sécurité déterminantes relatives à la gestion des versions, des mises à jour et de fin de vie des terminaux et périphériques.
4	4.1	Connaître des mesures techniques contre les maliciels sur les terminaux et périphériques (p.ex. analyseur de virus, solutions contre les maliciels).
	4.2	Connaître des mesures techniques de contrôle d'accès aux terminaux et aux périphériques (p.ex. liste de contrôle d'accès ACL, authentification des utilisateurs, authentification multifactorielle).
	4.3	Connaître les possibilités, les fonctions et les limites des solutions de tout ou partie de l'Enterprise Mobility Management (EMM) (p.ex. MDM, MAM).
	4.4	Connaître les exigences, les possibilités et les limites de la gestion des événements et des informations de sécurité (SIEM) et leur importance pour la forensique.
5	5.1	Connaître les possibilités de chiffrement de données sur les terminaux et périphériques (p.ex. chiffrement logiciel du disque dur ou de la mémoire de l'appareil).
	5.2	Connaître les possibilités de sécurisation de la téléphonie (p.ex. SRTP pour VoIP, cryptage vocal pour les terminaux mobiles).
	5.3	Connaître le concept de Trusted Computing Platform (TC) et les domaines d'application des puces Trusted Platform Module (TPM).
6	6.1	Connaître le contenu et la structure d'un catalogue de mesures (p.ex. mesure, temps nécessaire, responsabilité, valeur ajoutée, estimation des coûts).
	6.2	Connaître le contenu et la structure d'une bonne présentation et pouvoir expliquer l'influence des comportements déterminants sur le travail de persuasion.

Version du module	1.0
Créé le	11.02.2021