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