Identification du module

Numéro de module	656	
Titre	Garantir la sécurité et la compliance	
Compétence	Évaluer les processus métiers et les projets ICT en termes de risques opérationnels, d'aspects pertinents de la sécurité de l'information et de la conformité et définir des mesures efficaces pour l'exploitation opérationnelle ICT.	
Objectifs opérationnels	1	Identifier, évaluer et prioriser, dans le cadre de la gestion des risques, les risques opérationnels dans les processus métiers ou les projets ICT et développer, en tenant compte des directives supérieures, des mesures appropriées pour le traitement des risques.
	2	Examiner les processus métiers et les projets ICT sous l'angle des aspects pertinents de la sécurité de l'information.
	3	Evaluer les processus métiers et les projets TIC sous l'angle de la sécurité des données et définir, si nécessaire, des mesures de sécurité appropriées.
	4	Analyser et évaluer les processus métiers et les projets ICT sous l'angle du respect de la protection des données et prendre, si nécessaire, des mesures correctives.
	5	Elaborer, dans le cadre du Business Continuity Management, des concepts pour la poursuite des processus métiers en cas d'urgence et de crise.
	6	Analyser et évaluer les processus métiers et les projets ICT sous l'angle du respect du droit des contrats et prendre, si nécessaire, des mesures correctives.
	7	Analyser et évaluer les processus métiers et les projets ICT sous l'angle du respect du droit de la propriété intellectuelle et prendre, si nécessaire, des mesures correctives.
	8	Assurer le retour d'informations dans les domaines de la sécurité et de la conformité dans le cadre de l'amélioration continue d'une organisation.
Domaine de compétence	Security/Risk Management	
Objet	Processus métiers ou projets ICT (projet, développement de produits ou de ser-vices) avec un environnement clair, une intégration prédéfinie dans l'architecture de l'entreprise et de l'informatique et des directives internes à l'organisation définies.	
Version du module	1.0	
Créé le	26.08.2021	

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	656
Titre	Garantir la sécurité et la compliance
Compétence	Évaluer les processus métiers et les projets ICT en termes de risques opérationnels, d'aspects pertinents de la sécurité de l'information et de la conformité et définir des mesures efficaces pour l'exploitation opérationnelle ICT.

Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	Connaître les étapes de base du processus de gestion des risques (p. ex. ISO 31000, ISO/IEC 27005) et les directives supérieures applicables dans une organisation (p. ex. stratégie IT et stratégie de sécurité de l'information, appétence au risque, tolérance au risque, inventaire et classification des valeurs/actifs).
	1.2	Connaître les méthodes et techniques d'identification des risques opérationnels (p. ex. enquêtes, table ronde d'experts, listes de contrôle, Brainstorming) et pouvoir en expliquer les avantages et les inconvénients.
	1.3	Connaître les méthodes d'évaluation et de représentation des risques (p. ex. matrice des risques, cartographie des risques).
	1.4	Connaître différentes stratégies de traitement des risques (p. ex. réduction, évitement, acceptation, externalisation) et pouvoir expliquer leurs caractéristiques.
	1.5	Connaître la structure et les contenus d'un rapport sur les risques et d'un plan structuré de traitement des risques.
2	2.1	Connaître les objectifs de protection de la sécurité de l'information (p. ex. confidentialité, disponibilité, intégrité, fiabilité, authenticité, imputabilité, résilience) et pouvoir expliquer leur rôle lors de la création, du traitement, du stockage et de la transmission de données.
	2.2	Connaître les sources d'information sur les menaces actuelles (p. ex. catalogues des menaces NCSC, BSI ; rapports de sécurité des fabricants, forums de sécurité) et pouvoir expliquer les menaces actuelles en fonction de leur point d'entrée (p. ex. application, réseau, infrastructure, personne) et de leur cible (p. ex. panne de système, abus de système, vol, fraude, chantage).
	2.3	Connaître les causes typiques et fréquentes des menaces (p. ex. points faibles, défaillance technique, erreur humaine, force majeure, acte intentionnel) et pouvoir expliquer leur signification pour la sécurité de l'information.
3	3.1	Connaître les objectifs de la sécurité des données et pouvoir en expliquer l'importance dans le contexte de la sécurité de l'information et de la protection des données.
	3.2	Connaître les phases typiques du cycle de vie des données (p. ex. production, stockage, utilisation, transmission, archivage, destruction) et pouvoir expliquer la signification de ces phases dans le contexte de la sécurité des données.

Connaissances opérationnelles nécessaires

	3.3	Connaître l'importance de la sauvegarde (Backup), de l'archivage et de la restauration (Restore) des données et pouvoir expliquer les stratégies et procédures appropriées pour leur mise en œuvre.
	3.4	Connaître les dispositions légales applicables dans le domaine de la sécurité des données (p. ex. conservation des données commerciales selon le CO et l'Olico, archivage fiscal, e-Billing, responsabilité du fait des produits).
	3.5	Connaître les normes et catalogues courants de mesures de sécurité (p. ex. ISO/CEI-27002, Compendium de protection IT de base BSI) et pouvoir expliquer les mesures de sécurité techniques et organisationnelles de base (p. ex. contrôle d'accès, cryptage, journalisation, gestion des correctifs, sauvegarde des données, sensibilisation).
4	4.1	Connaître les bases légales applicables dans le domaine de la protection des données (LPD, OLPD, RGPD de l'UE) et pouvoir expliquer l'importance de la sécurité des données comme condition préalable à la protection des données.
	4.2	Connaître les domaines typiques de la protection des données dans le domaine opérationnel des ICT (p. ex. collecte de données, journalisation, surveillance du comportement, transmission de données personnelles, demandes de renseignements, de rectification et d'effacement).
	4.3	Connaître les mesures visant à garantir la protection des données lors de l'utilisation de données personnelles (p. ex. mesures de sécurité des données, pseudonymisation, anonymisation, sensibilisation).
5	5.1	Connaître les objectifs du Business Continuity Management (BCM) et du Disaster Recovery (DR) et pouvoir expliquer leurs différences.
	5.2	Connaître l'objectif et les contenus essentiels d'une Business Impact Analysis (p. ex. Recovery Time Objective RTO, Recovery Point Objective RPO) et pouvoir en expliquer la signification pour le Business Continuity Management.
	5.3	Connaître les possibilités de prévention d'une panne des processus métiers basés sur l'ICT (p. ex. tolérances, redondances).
	5.4	Connaître des mesures proactives pour minimiser l'impact d'une panne des processus métiers basés sur les ICT (p. ex. plans d'urgence, cellule d'urgence ou de crise, exercices d''urgence, audits, réseau d'experts et de partenaires).
6	6.1	Connaître les caractéristiques et les différences des différents contrats selon le Code des obligations CO (vente, location, contrat d'entreprise, contrat simple, contrat de travail) et pouvoir en expliquer la signification dans le contexte des ICT.
	6.2	Connaître les caractéristiques et le contenu des contrats typiques dans l'environnement ICT (p. ex. contrat de service, contrat d'outsourcing, contrat de licence) et pouvoir en expliquer l'utilisation et les risques potentiels.
	6.3	Connaître les caractéristiques et le contenu des accords contractuels additionnels typiques dans l'environnement ICT (p. ex. CG, SLA, règlement d'utilisation, Non-Disclosure Agreement, déclaration d'intention) et pouvoir en expliquer l'utilisation et les risques potentiels.
7	7.1	Connaître les bases du droit suisse de la propriété intellectuelle en matière de droit d'auteur, de brevets, de marques et de design et pouvoir expliquer la différence entre les droits moraux (reconnaissance de la qualité d'auteur, première publication) et les droits patrimoniaux (p. ex. réalisation de copies, droit de location).

Connaissances opérationnelles nécessaires

	7.2	Connaître la classification des contrats de licence dans le droit des contrats et de la propriété intellectuelle.
	7.3	Connaître les différents modèles de licence propriétaires et ouverts (p. ex. achat, location, Open Source, Freeware, Creative Commons, Royalty Free) et les différentes formes de licence (p. ex. basée sur l'utilisateur, basée sur l'utilisation, basée sur la fonction, licence individuelle et licence en volume) et pouvoir expliquer leurs caractéristiques en termes d'utilisation, de prix et de facturation.
8	8.1	Connaître le principe du processus d'amélioration continue (PAC) et du cycle PDCA et pouvoir expliquer leur rôle pour la gestion de la qualité dans une organisation.
	8.2	Connaître le but et les exigences fondamentales d'un système de gestion de la sécurité de l'information (ISMS) selon ISO/CEI-2700x.

Version du module	1.0
Créé le	26.08.2021