Identification du module

Numéro de module	662	
Titre	Assurer la sécurité TIC	
Compétence	Assurer la sécurité lors de la planification, le développement et dans le système productif global, soit l'intégrité, la confidentialité (y.c. la protection de données) ainsi que la disponibilité des informations/données et le système TIC de base y relatif.	
Objectifs opérationnels	1	Définir quelles normes nationales et internationales ainsi que règles externes dans le domaine du respect TIC concernent l'entreprise.
	2	Définir et formuler, en collaboration avec la direction d'entreprise, la ligne de conduite et les objectifs pour la sécurité des informations, et les mettre en œuvre à l'aide d'un cercle PDCA (planifier-développer-contrôler-ajuster).
	3	Etablir un système de gestion de la sécurité des informations et un cadre de conformité TIC.
	4	Mettre en œuvre ceux-ci en étroite collaboration avec la direction d'entreprise sur la base d'un processus de gestion de la sécurité des informations et assurer son respect.
	5	Etablir, pour la surveillance, le contrôle et l'optimisation des systèmes TIC, une gestion exhaustive des contrôles sur tous les processus commerciaux et infrastructures.
	6	Documenter le déroulement d'audits, la saisie, respectivement, l'évaluation des résultats de sorte que ceux-ci soient contrôlables et reproductibles.
	7	Exécuter régulièrement des audits d'informations et systèmes dans le cadre des TIC (disponibilité, confidentialité, intégrité, sécurité des informations, conservation et protection des données).
	8	Exploiter les résultats des audits et définir le cadre des processus pour l'implémentation et la gestion de mesures afin d'assurer les objectifs spécifiques de la sécurité des informations.
Domaine de compétence	Security/Risk Management	
Objet	Entreprise et/ou systèmes TIC avec les directives et conditions cadres suivantes:Directives juridiques nationales et internationales qui se limitent à la protection des données.Taux élevé de solutions standards dans l'environnement technique avec une complexité moyenne (par ex. en regard des technologies mises en œuvre, répartition des systèmes).Directives internes concernant la confidentialité, la disponibilité et l'intégrité, sans les domaines de haute sécurité (par ex. police criminelle, secret bancaire).Informations sur les clients, collaborateurs, et produits/prestations d'une entreprise.	
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	662
Titre	Assurer la sécurité TIC
Compétence	Assurer la sécurité lors de la planification, le développement et dans le système productif global, soit l'intégrité, la confidentialité (y.c. la protection de données) ainsi que la disponibilité des informations/données et le système TIC de base y relatif.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des normes nationales et internationales dans le domaine de la sécurité TIC (par ex. CobiT, BSI 100-x, ISO 2000, ITIL, ISO 2700x, IKS, etc.) et leurs relations.
	1.2	Connaître des règles externes et leur définition (par ex. loi et ordonnance sur la protection des données LPD).
2	2.1	Connaître les catégories d'objectifs de sécurité TIC (par ex. confidentialité, disponibilité, intégrité).
	2.2	Connaître les restrictions qui doivent être observées lors de la définition des objectifs de sécurité TIC (par ex. état des technologies, budget, connaissances).
	2.3	Connaître les étapes du cercle PDCA et pouvoir expliquer comment celles-ci contribuent à l'obtention de la sécurité TIC.
3	3.1	Connaître les éléments de définition d'un système de gestion de la sécurité des informations (par ex. selon ISO 27000).
	3.2	Connaître les éléments d'un cadre de conformité TIC en tant que partie intégrante d'un système de gestion de la sécurité des informations.
4	4.1	Connaître les enjeux spécifiques qui doivent être pris en considération dans le but d'une introduction et mise en œuvre durable d'un système de gestion de la sécurité des informations.
	4.2	Connaître les possibilités pour la définition de mécanismes de contrôle (par ex. questions de contrôle, catalogue de la protection de base).
5	5.1	Connaître les exigences pour un système de gestion des audits (par ex. des systèmes et composants de soutien, conformité de la certification).
	5.2	Connaître des formes, construction et contenu de mécanismes de surveillance et de contrôle en relation avec les directives de sécurité TIC (par ex. sous forme de règles IDS).
	5.3	Connaître les mesures préventives, lors de la définition et planification d'un audit, sur la profondeur, l'environnement et la force d'expression qui en résultent.
6	6.1	Connaître les données dans un rapport d'audit et pouvoir démontrer comment celles-ci influencent la reproductibilité et la force d'expression.

Connaissances opérationnelles nécessaires

7	7.1	Connaître des modèles de déroulement pour l'exécution d'un audit dans des systèmes TIC (par ex. importance, profondeur, connaissances préalables, état du savoir, interne/externe).
	7.2	Connaître des systèmes d'évaluation et leur force d'expression dans le domaine de la sécurité TIC (par ex. OSSTMM).
8	8.1	Connaître des dimensions d'évaluation pour l'exploitation de mécanismes de surveillance et de contrôle (par ex. potentiel de menaces).
	8.2	Connaître les méthodes et techniques fondamentales pour la planification et la surveillance de mesures de sécurité TIC (délégation, convention, rapport).

Version du module	1.0
Créé le	11.02.2021