EIT.swiss
Limmatstrasse 63
8005 Zürich
044 444 17 17
www.eitswiss.ch

Identification du module

Numéro du module	**232**
Titel	**Garantir la sécurité informatique et la protection des données de projets ACM**
Compétences	Identifie les menaces et les vulnérabilités dans les projets ACM. Sécurise les moyens matériels avec les mesures de protection nécessaires et selon l'état actuel de la technique.
Objectifs opérationnels	1. Développe des mesures basées sur les informations collectées pour la sécurité du système d'un projet ACM. 2. Développe des mesures de sécurité et de protection informatiques pour répondre aux exigences légales et opérationnelles. 3. Définit des mesures de protection proactives qui garantissent la poursuite des activités commerciales.
Champ de compétences	Security / Risk Management
Objet	Mesures visant à garantir la politique de confidentialité et la sécurité informatique pour un simple projet ACM.
Justificatif	
Année d'apprentissage	4
Niveau	
Conditions préalables	
Charge de travail/Leçons	40
Homologation	CFC
Compétences opérationnelles Informaticien/ne du bâtiment CFC	a2: Vérifier les exigences techniques, la sécurité informatique et la protection des données pour un projet ACM simple et les consigner dans un cahier des charges

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Connaissances opérationnelles requises

Les connaissances opérationnelles requises décrivent les connaissances qui soutiennent l'exécution compétente des opérations d'un module. Ces connaissances servent à l'orientation et ne sont pas définies de manière exhaustive. La concrétisation des objectifs de formation qui en résulte et la détermination du parcours de formation pour l'acquisition des compétences sont de la responsabilité des prestataires de formation.

Numéro du module			**232**
Titre			**Garantir la sécurité informatique et la protection des données de projets ACM**
Champ de compétences			Security / Risk Management
Objectifs opérationnels et connaissances opérationnelles requises	1	1.1	Connaît des moyens et des méthodes simples pour détecter les lacunes de sécurité et les défauts de configuration dans les systèmes (par ex. balayage de ports, outils de durcissement).
		1.2	Connaît l'importance d'une documentation complète en ce qui concerne la sécurité du système.
		1.3	Connaît les erreurs les plus courantes en matière de sécurité lors de la configuration de systèmes.
		1.4	Connaît des méthodes et leurs domaines d'application afin de pouvoir recueillir des informations sur des circonstances particulières de manière ciblée et efficace (par ex. atelier, analyse de processus, étude de documents).
	2	2.1	Connaît les principales sources dans lesquelles on peut trouver des descriptions et des documentations concernant les exigences opérationnelles et juridiques (par ex. descriptions de fonctions et de processus, directives, organigrammes).
		2.2	Connaît l'état actuel des techniques et des sources d'information (par ex. Centrale d'enregistrement et d'analyse pour la sûreté de l'information) afin de formuler des recommandations sur les améliorations ou les possibilités d'extension futures en matière de protection des données et de sécurité informatique.
		2.3	Connaît diverses mesures et leurs avantages et inconvénients (par ex. organisationnels, techniques), qui servent à assurer la sécurité des informations (par ex. autorisations d'accès, heures de fonctionnement, stockage des fichiers, protection du mot de passe).
	3	3.1	Connaît les techniques d'application permettant d'éviter la défaillance des processus soutenus par les TIC (par ex. tolérances, redondances).
		3.2	Connaît des mesures proactives pour minimiser l'impact en cas de défaillance d'un processus soutenu par les TIC (par ex. plans d'urgence, système d'alimentation électrique sans coupure).