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