Identification du module

No. module	661
Titre	Exécuter des analyses de sécurité TIC
Compétence	Exécuter régulièrement les analyses des processus d'entreprises, soutenu par les systèmes TIC, afin de déterminer les points faibles et les risques. Planifier, à l'aide de des résultats, les mesures de minimisation des risques économiquement appropriées.
Objectifs opérationnels	1. Enregistrer quels systèmes TIC supportent quels processus d'entreprise (tâches, fonctions). 2. Définir, en collaboration avec les responsables des processus d'entreprise, les exigences des systèmes TIC en regard de la disponibilité et de l'échéance.0 3. Identifier des points faibles des systèmes TIC en relation avec la sécurité des tâches et fonctions que ceux-ci supportent durant le déroulement des processus d'entreprise. 4. Etablir une analyse qui définit le potentiel de risques, respectivement des dangers, des points faibles sur les capacités commerciales et l'existence de l'entreprise. 5. Prendre des mesures, en accord avec l'analyse, pour l'élimination de points faibles dans les systèmes TIC et contribuer ainsi à la sécurisation des capacités commerciales et de la survie de l'entreprise. 6. Définir, en accord avec l'analyse, des mesures qui garantissent la continuité des capacités commerciales en cas de panne des systèmes TIC, respectivement de leur soutien par les processus commerciaux. 7. Etablir un concept pour la vérification régulière de l'efficacité des mesures prises et pour l'actualisation de l'analyse. 8. Mettre en œuvre les mesures visées en collaboration avec les responsables des processus d'entreprise sur la base de normes et de concepts de meilleure pratique.
Compétences personnelles	Etre conscient de la responsabilité que supporte le domaine des TIC par le biais du soutien aux fonctions commerciales d'une entreprise et mettre tout en œuvre pour la concrétiser par le biais de l'assurance d'une grande fiabilité et d'une grande disponibilité des prestations.
Domaine de compétence	Gestion des risques TIC
Objet	Systèmes et technologies établies; taux élevé de solutions standards dans l'environnement technique de complexité moyenne (par ex. en regard du nombre de technologies mises en œuvre, répartition des systèmes).
Test	Mini-Case comportant 2 à 3 tâches qui testent diverses actions et qui nécessitent globalement entre 45 et 60 minutes de durée de résolution.
Niveau e-CF	6
Prérequis	
Nb. Leçons (h)	40
Reconnaissance	ICT-Manager diplômé/-e
Module	V1.0
Plan modulaire	V5.1

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs nécessaires à l'exécution compétente des actions d'un module. Leur valeur est purement informative et leur définition non exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage incombent aux prestataires de formation.

No. module	661
Titre	Exécuter des analyses de sécurité TIC
Domaine de compétence	Gestion des risques TIC
Module	V1.0
Plan modulaire	V5.1

Objectifs opérationnels et connaissances opérationnelles nécessaires	1	1.1	Connaître les normes de la gestion de continuité opérationnelle (par ex. BS 25999, ISO 22399).
		1.2	Connaître le déroulement de la préparation, de l'exécution et de l'évaluation d'entretiens structurés.
		1.3	Connaître des techniques de représentation pour la définition de processus commerciaux par le biais de systèmes TIC (par ex. architecture des processus).
	2	2.1	Connaître les facteurs qu'il faut prendre en compte lors de la définition des exigences sur la durée de panne et la disponibilité des systèmes TIC (par ex. temps nécessaire au redémarrage, exigences de la reprise après sinistre).
		2.2	Connaître les effets de divers scénarios de pannes sur le respect de la disponibilité et la durée maximale de panne.
	3	3.1	Connaître des méthodes et des instruments que les fournisseurs et ONG mettent à disposition pour couvrir les points faibles et pouvoir les appliquer (par ex. scanner de vulnérabilité, base de connaissances).
	4	4.1	Connaître des méthodes et techniques pour l'exécution d'analyses qui permettent de quantifier les potentiels de risques des points faibles de systèmes TIC en regard des processus commerciaux (par ex. selon ISO 27005).
		4.2	Connaître les éléments d'un catalogue de risques et pouvoir expliquer dans quelles circonstances ceux-ci se côtoient et contribuent à la définition finale d'un risque.
	5	5.1	Connaître les catégories de mesures pour garantir la disponibilité définie et pour assurer une durée de panne minimale (par ex. infrastructure, organisation, personnel, matériel et logiciel).
	6	6.1	Connaître des catégories de mesures organisationnelles pour assurer des déroulements commerciaux sans interruption (par ex. les responsabilités).
		6.2	Connaître des catégories de mesures techniques pour assurer des déroulements commerciaux sans interruption (par ex. reprise après sinistre TIC).
		6.3	Connaître les conditions cadres et exigences qui doivent être pris en compte lors de l'établissement d'un plan de secours (par ex. les dépendances systèmes, les proportions, la couverture du processus).
	7	7.1	Connaître des possibilités de vérification de l'efficacité de concepts de secours (par ex. système de veille).
		7.2	Connaître des facteurs qui doivent être pris en compte lors de l'évaluation d'exercices de secours réguliers (par ex. répartition du travail, étapes du processus).
	8	8.1	Connaître des dispositions et directives qui doivent être respectées lors de la mise en œuvre de mesures pour la vérification de concepts de secours (par ex. catalogue de sécurité de base, InfoSurance).