Initiative Data Compétences
Un réseau CCI FRANCE

Référentiel de compétences et d'évaluation

Intitulé de la certification		
Référent cybersécurité en TPE/PME		
Description de la situation professionnelle et de l'activité		
Initialisation et pérennisation au sein de la TPE/PME de la démarche de prévention en matière de cybersécurité visant à préserver et protéger son patrimoine immatériel d'actes d'hostilité, dans le respect de la règlementation. Tâches exercées : • Identification et prise et compte des problématiques de cybersécurité de l'entreprise en lien avec l'environnement juridique et technologique • Evaluation des usages et du niveau de sécurité de l'entreprise • Elaboration, mise en œuvre et animation d'une démarche de prévention et d'amélioration des pratiques de cybersécurité au sein de l'entreprise		
COMPÉTENCES	**MODALITÉS D'ÉVALUATION**	**CRITÈRES D'ÉVALUATION**
C.1 Identifier les enjeux et problématiques d'intelligence économique et de cybersécurité touchant l'activité de l'entreprise, en repérant les institutions et organisations ressources dans le domaine (ANSSI, CNIL…) et en exploitant leurs publications et services, afin de prendre en compte les multiples aspects environnementaux de sécurité informatique au sein de l'organisation.	Les candidats doivent présenter les productions suivantes : **Un plan d'amélioration pour la mise en place d'une démarche de prévention des risques liés à la cybersécurité au sein de l'entreprise.** Le plan d'amélioration comporte 3 parties associées aux 3 tâches exercées et aux compétences mobilisées : • Identification de la problématique de cybersécurité propre à l'entreprise et tenant compte de son environnement juridique et technologique (compétences C.1, C.2, C.3).	- Les enjeux de cybersécurité et leur articulation avec ceux de sécurité et d'intelligence économiques propres à l'entreprise sont identifiés. - Les besoins spécifiques à l'entreprise en matière de cybersécurité sont définis. - Les métiers impactés par les enjeux de cybersécurité au sein de l'entreprise sont identifiés.
C.2 Identifier les risques et menaces présentant potentiellement un danger pour l'intégrité du système d'information de l'entreprise et de son patrimoine immatériel, en repérant les techniques de cyber-attaques et d'intrusion existantes et émergentes, en vue de la détermination ultérieure des solutions, outils et mesures d'hygiène informatiques permettant de protéger l'entreprise d'actes d'hostilité.		- Les techniques de cyber-attaques et d'intrusion existantes et émergentes sont repérées. - Les différents types de menaces technologiques potentielles sont identifiés. - les risques pour l'entreprise résultants des menaces potentielles sont identifiées.

C.3 Identifier les responsabilités juridiques de l'entreprise en matière de cybersécurité et protection des données, en tenant compte du cadre législatif et de ses évolutions, afin de déterminer les obligations qui en résultent pour l'entreprise en vue de la mise en conformité ultérieure des usages internes.	• Evaluation du niveau de sécurité de l'entreprise (compétences C.4, C.5, C.6). • Plan des actions à mettre en œuvre, comprenant la documentation et les outils de suivi associés (compétences C.7, C.8, C.9, C.10). *La production est accomplie individuellement par chaque candidat, sur la base d'une étude de cas réelle ou fictive*	- Le paysage et les acteurs institutionnels de la cybersécurité sont repérés. - Les dispositions légales et règlementaires ayant un impact sur la cybersécurité sont identifiées. - Les responsabilités juridiques et les obligations actuelles en résultant pour l'entreprise en matière de cybersécurité et protection des données sont identifiées.
C.4 Analyser l'organisation interne et le système d'information de l'entreprise, en identifiant les acteurs concernés par les problématiques de cybersécurité et en repérant les éléments digitalisés entrant dans sa chaîne de création de valeur, afin de définir le patrimoine immatériel de l'entreprise entrant dans les enjeux de la cybersécurité.		- Les éléments digitalisés porteurs de création de valeur et ayant une dimension stratégique pour l'entreprise sont identifiés. - Le patrimoine immatériel de l'entreprise est clairement identifié et défini. - Le périmètre couvert par l'évaluation est délimité et suffisant au regard de la problématique et des spécificités de l'entreprise.
C.5 Evaluer les vulnérabilités de l'entreprise et son niveau de sécurisation, en analysant ses solutions techniques, usages et pratiques informatiques au moyen, le cas échéant, de méthodes et d'outils de diagnostic préexistants, afin de définir et de qualifier les risques et menaces liés à l'utilisation de l'informatique et des réseaux (publics, privés et Internet) pesant sur l'organisation.		- Les méthodes et outils de diagnostic choisis sont adaptés au contexte et aux spécificités de l'entreprise ; le cas échéant, des outils préexistants sont mobilisés. - Les éventuelles vulnérabilités du système d'information sont détectées. - Les insuffisances d'usage et de respect des règles d'hygiène fondamentales de la part des utilisateurs sont repérées. - Les insuffisances au regard des obligations règlementaires de l'entreprise en matière de cybersécurité sont identifiées.
C.6 Etablir un état des lieux du niveau de sécurité de l'entreprise et du respect de ses obligations règlementaires, en identifiant les bonnes pratiques à capitaliser ainsi que les lacunes et insuffisances vectrices de risques, afin d'évaluer les besoins et conditions de mise en œuvre d'un futur plan d'amélioration.		- Les bonnes pratiques capitalisables sont identifiées. - Le niveau de sécurité de l'entreprise en matière de cybersécurité est qualifié. - Les menaces, risques et vulnérabilités avérées de l'entreprise sont qualifiées.

C.7 Déterminer les actions à mettre en œuvre et le type de supports à déployer, en identifiant les profils et spécificités des collaborateurs à cibler et impliquer et en décidant des choix d'infrastructures ou de sous-traitance à opérer, afin de mettre en place une démarche de prévention des risques liés à la cybersécurité au sein de l'entreprise.		- Les objectifs visés sont définis, qualifiés et quantifiés. - Les objectifs sont atteignables et leur atteinte est planifiée. - Le choix des actions est cohérent au regard de la problématique de l'entreprise et des constats tirés de l'évaluation des pratiques et du niveau de sécurité de l'entreprise. - Les actions sélectionnées sont complémentaires et correctement dimensionnées au regard des moyens et des enjeux de cybersécurité de l'entreprise. - Les actions sont planifiées et leur articulation dans le temps est cohérente. - Les spécificités des collaborateurs impliqués sont prises en compte et des adaptations sont identifiées pour garantir l'inclusivité de la démarche, notamment concernant le personnel en situation de handicap.
C.8 Diffuser les bonnes pratiques et règles d'hygiène fondamentales de la cybersécurité, en préconisant à ses collaborateurs les comportements adaptés et les précautions techniques et juridiques à appliquer et en les sensibilisant aux enjeux associés, afin d'infuser une culture de la cybersécurité au sein de l'entreprise.		- Les mesures d'hygiène préconisées sont adaptées à l'organisation du système d'information (SI) de l'entreprise et correctement dimensionnées au regard des enjeux que la cybersécurité revêt pour elle. Elles prévoient notamment : - la limitation des accès aux différentes ressources du SI et sa protection au moyen d'un système d'authentification, - la mise en place de protections des postes de travail (*firewall*, antivirus), des supports amovibles et des appareils nomades, - la sécurisation du réseau informatique de l'entreprise (segmentation, protection des accès Wi-Fi, séparation des usages, protection des messageries…), - la mise à jour régulière des logiciels et composants du système d'information.
C.9 Systématiser la mise en application des règles d'hygiène fondamentales de la cybersécurité pour l'organisation et les individus, en mettant en place les outils, la documentation et les méthodes favorisant l'appropriation et le respect des bonnes pratiques, afin d'optimiser la protection de l'entreprise et de son patrimoine immatériel.		- Les choix de sous-traitance et de supports documentaires sont en adéquation avec les besoins, les moyens et la problématique de l'entreprise. - Les supports documentaires choisis sont adaptés à leur cible d'utilisateurs.

C.10 Opérer le suivi des comportements et usages en matière de cybersécurité, en s'appuyant sur des outils de contrôle et d'évaluation et en identifiant les mesures correctives et ajustements à adopter, afin d'assurer la pérennité d'une démarche préservant l'entreprise et son patrimoine immatériel d'actes d'hostilité et d'attaques externes.		- Les critères de suivi et d'évaluation du plan d'action sont justes. - Les critères sont formalisés dans des outils de suivi et d'évaluation permettant le contrôle et l'amélioration continue de la démarche.