RÉFÉRENTIEL DE COMPÉTENCES ET D'ÉVALUATION RÉPERTOIRE SPÉCIFIQUE CYBERSÉCURITÉ

1 - Pilotage de la gouvernance de la cybersécurité
2 - Gestion des systèmes d'information sécurisés
3 - Gestion des risques et protection des systèmes
4 - Évaluation du niveau de sécurité
5 - Gestion des incidents de cybersécurité

REFERENTIEL D'ACTIVITES *Décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *Identifie les compétences transversales, qui découlent du référentiel d'activités*	**COMPÉTENCES ÉVALUÉES**	**REFERENTIEL D'EVALUATION** *Définit les critères et les modalités d'évaluation des acquis*	
			MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
1 - Pilotage de la gouvernance de la cybersécurité a - Définition de la stratégie de la cybersécurité b - Pilotage de la cybersécurité c - Définition de la stratégie de communication sur la cybersécurité d - Gestion des ressources humaines permettant la cybersécurité	a.1 - Prendre en compte la cybersécurité au plus haut niveau a.2 - Définir les orientations de cybersécurité a.3 - Définir les moyens alloués à la cybersécurité a.4 - Établir une cartographie fonctionnelle b.1 - Définir l'organisation et les responsabilités en matière de cybersécurité b.2 - Établir la documentation de cybersécurité b.3 - Intégrer la cybersécurité dans les projets	- Définir les orientations de cybersécurité - Définir les moyens alloués à la cybersécurité - Établir une cartographie fonctionnelle - Définir l'organisation et les responsabilités en matière de cybersécurité - Établir la documentation de cybersécurité - Intégrer la cybersécurité dans les projets	Présentation orale individuelle de 20 minutes, dans les locaux du centre certificateur, d'un rapport d'expérience professionnelle sur le pilotage d'une gouvernance de sécurité, suivie de 20 minutes de questions du jury Le rapport doit • contenir obligatoirement la stratégie de sécurité • obligatoirement prendre en compte les aspects non techniques de la sécurité : communication,	- Le cas présenté est structuré et répond aux compétences évaluées. - Les choix relatifs à la cybersécurité sont effectués en cohérence avec la stratégie de la structure et les risques auxquels elle est exposée. - La structure dispose des moyens financiers, techniques et humains nécessaires à la réalisation des objectifs de cybersécurité définis. - La chaîne de responsabilité cybersécurité est établie et l'organisation est adaptée pour répondre aux objectifs de cybersécurité.

e - Inclusion de la cybersécurité dans les contrats	b.4 - Définir et utiliser des indicateurs cybersécurité b.5 - S'inscrire dans une démarche d'amélioration continue c.1 - Communiquer en interne et sensibiliser le personnel c.2 - Communiquer vers l'extérieur lors des crises d.1 - Responsabiliser le personnel d.2 - Gérer les autorisations du personnel d.3 - Disposer des compétences de cybersécurité nécessaires dans la durée e.1 - Protéger les biens des clients et des partenaires e.2 - Gérer les achats e.3 - Choisir des prestataires de confiance e.4 - Gérer les interfaces e.5 - Effectuer une veille sur les obligations légales et réglementaire	- Définir et utiliser des indicateurs cybersécurité - Communiquer en interne et sensibiliser le personnel - Responsabiliser le personnel - Gérer les autorisations du personnel - Protéger les biens des clients et des partenaires - Gérer les achats - Choisir des prestataires de confiance - Gérer les interfaces	ressources humaines et aspects juridiques.	- La stratégie de communication est établie. - Les obligations légales et réglementaires ayant trait à la cybersécurité et la protection des données sont respectées.

2 - Gestion des systèmes d'information sécurisés a - Gestion des systèmes tout au long de leur cycle de vie b - Gestion des accès aux systèmes	a.1 - Cartographier ses systèmes a.2 - Disposer de la documentation de ses systèmes et composants a.3 - Sécuriser la manipulation des informations sensibles a.4 - Concevoir et développer des systèmes sûrs a.5 - Gérer ses chaînes d'approvisionnement a.6 - Valider la cybersécurité lors de la recette a.7 - Exploiter de manière sécurisée a.8 - Gérer la maintenance et le maintien en condition de sécurité a.9 - Encadrer l'évolution de ses systèmes a.10 - Garantir la sécurité lors du retrait de service c.1 - Définir les principes de maîtrise des droits d'accès c.2 - Définir les principes d'identification et d'authentification c.3 - Définir les rôles et les profils c.4 - Limiter l'accès selon des principes d'habilitation	- Cartographier les systèmes - Sécuriser la manipulation des informations sensibles - Concevoir et développer des systèmes sûrs - Gérer les chaînes d'approvisionnement - Valider la cybersécurité lors de la recette - Exploiter de manière sécurisée - Gérer la maintenance et le maintien en condition de sécurité - Encadrer l'évolution des systèmes - Garantir la sécurité lors du retrait de service - Définir les principes de maîtrise des droits d'accès - Définir les principes d'identification et d'authentification - Définir les rôles et les profils - Limiter l'accès selon des principes d'habilitation	Présentation orale individuelle de 20 minutes, dans les locaux du centre certificateur, d'un rapport d'expérience professionnelle sur la gestion d'un système d'information sécurisé, suivie de 20 minutes de questions du jury Le rapport doit contenir obligatoirement une cartographie du système d'information	- le système est cartographié - la manipulation des informations sensibles est sécurisée - l'exploitation du système d'information est sécurisée et conforme à la politique de sécurité de la structure - L'évolution du système d'information est encadré de manière à satisfaire les évolutions des besoins métiers tout en maintenant le niveau de sécurité attribué au système. - les droits d'accès sont contrôlés

	c.5 - Gérer les droits utilisateurs selon leur cycle de vie c.6 - Contrôler les droits d'accès	- Gérer les droits utilisateurs selon leur cycle de vie - Contrôler les droits d'accès		
3 - Gestion des risques et protection des systèmes a - Gestion des risques b - Utilisation des composants sécurisés c - Protection physique des systèmes d'information d - Protection logique des systèmes d'information	a.1 - Analyser les risques cyber relatifs aux systèmes a.2 - Homologuer les systèmes d'information b.1 - Confirmer le développement de confiance des composants b.2 - Utiliser des composants qualifiés b.3 - Configurer correctement ses composants b.4 - Utiliser des services cryptographiques à l'état de l'art et protéger ses clés b.5 - Garantir la robustesse des authentifiants et mots de passe c.1 - Garantir la disponibilité des servitudes c.2 - Résister aux événements naturels, incidents et attaques physiques c.3 - Protéger les accès physiques c.4 - Contrôler l'accès physique des personnes	- Analyser les risques cyber relatifs aux systèmes - Homologuer les systèmes d'information - Confirmer le développement de confiance des composants - Utiliser des composants qualifiés - Configurer correctement ses composants - Utiliser des services cryptographiques à l'état de l'art et protéger ses clés - Garantir la robustesse des authentifiants et mots de passe - Garantir la disponibilité des servitudes - Résister aux événements naturels, incidents et attaques physiques - Protéger les accès physiques - Contrôler l'accès physique des personnes	Présentation orale individuelle de 20 minutes, dans les locaux du centre certificateur, d'un rapport d'expérience professionnelle sur une évaluation des risques des systèmes d'information d'une structure et sur les actions de protection mises en place, suivie de 20 minutes de questions du jury	- Les risques sont évalués sur tous les systèmes d'information de la structure, afin de les sécuriser de manière adaptée aux risques et enjeux. - Les risques résiduels des systèmes d'information sont identifiés - Les composants utilisés dans les systèmes d'information sont configurés de manière à limiter leur exposition aux menaces - Les systèmes d'information sont protégés contre les accès physiques illégitimes, les agressions physiques et les événements naturels. - Les systèmes d'information sont protégés contre les applications malveillantes ; les réseaux, les équipements, les données et les supports de données sont sécurisés.

	c.5 - Se prémunir contre les risques électromagnétiques d.1 - Se prémunir contre les codes malveillants d.2 - Protéger les réseaux d.3 - Protéger les équipements d.4 - Protéger les données d.5 - Protéger les supports de données d.6 - Contrôler les accès logiques d.7 - Protéger l'administration des systèmes d.8 - Garantir la non-répudiation des actions d.9 - Renforcer la vigilance et la protection	- Se prémunir contre les risques électromagnétiques - Se prémunir contre les codes malveillants - Protéger les réseaux - Protéger les équipements - Protéger les données - Protéger les supports de données - Contrôler les accès logiques - Protéger l'administration des systèmes - Garantir la non-répudiation des actions - Renforcer la vigilance et la protection		

4- Évaluation du niveau de sécurité a - Audits et vérifications b - Organiser des exercices et des entraînements	a.1 - Identifier les écarts au référentiel a.2 - Évaluer par rapport à l'état de l'art a.3 - Rechercher des traces de compromission a.4 - Corriger les problèmes identifiés a.5 - Mener des audits de sites internationaux b.1 - Organiser des entraînements et des exercices à destination du personnel afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles b.2 - Organiser des entraînements et des exercices à destination des prestataires externes afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles	- Identifier les écarts au référentiel - Évaluer par rapport à l'état de l'art - Rechercher des traces de compromission - Corriger les problèmes identifiés - Organiser des entraînements et des exercices à destination du personnel afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles - Organiser des entraînements et des exercices à destination des prestataires externes afin de vérifier que des procédures adaptées aux crises sont correctement mises en place et opérationnelles	Présentation orale individuelle de 20 minutes, dans les locaux du centre certificateur, d'un rapport d'audit, suivie de 20 minutes de questions du jury	- l'audit détermine si le système comporte des vulnérabilités exploitables par un attaquant. - des traces de compromission du système ont été recherchés. - la vulnérabilité de la structure a été diminuée en corrigeant les problèmes de sécurité identifiés lors des vérifications et des audits. - Des exercices et des entrainements ont été organisés

5 - Gestion des incidents de cybersécurité a - Préparation du dispositif de gestion des incidents b - Analyse et qualification des incidents c - Réaction aux incidents d - Garantie de la continuité de service	a.1 - Disposer d'une chaîne opérationnelle de gestion des incidents a.1 - Collecter les événements de sécurité a.1 - Détecter les événements anormaux b.1 - Reconstituer le scénario des incidents, les vecteurs et leur étendue b.1 - Évaluer l'impact et le périmètre de l'incident sur l'activité c.1 - Organiser la réaction c.1 - Préparer des mesures de réaction c.1 - Conduire la réaction c.1 - Réaliser un retour d'expérience d.1 - Se préparer à un sinistre d.1 - Garantir la résilience de ses systèmes d.1 - Réagir face à un sinistre	- Disposer d'une chaîne opérationnelle de gestion des incidents - Collecter les événements de sécurité - Détecter les événements anormaux - Reconstituer le scénario des incidents, les vecteurs et leur étendue - Évaluer l'impact et le périmètre de l'incident sur l'activité - Organiser la réaction - Préparer des mesures de réaction - Conduire la réaction - Réaliser un retour d'expérience - Se préparer à un sinistre - Garantir la résilience de ses systèmes - Réagir face à un sinistre	Mise en situation professionnelle individuelle de 30 minutes, dans les locaux du centre certificateur, sur le thème de la gestion d'incident cybersécurité	- Les caractéristiques de l'incident sont déterminées (scénario, vecteur, périmètre). - La réaction a été organisée et conduite pour supprimer les causes de l'incident afin d'éviter qu'il ne se reproduise. - Les conséquences de l'incident ont été limitées. - La continuité de service des missions sensibles a été assurée ou les activités ont pu reprendre dans un délai défini.