REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC1 - Auditer et élaborer la politique de conformité et de gouvernance des données			
A1.1. Évaluation initiale de la conformité des traitements et mise à jour des registres des traitements - Identification des traitements de données existants auprès des services concernés, via des entretiens et un examen des documents existants. - Analyse des types de données traitées (ex. : données clients, RH, marketing) et de la conformité des traitements en précisant leur finalité, les bases légales, les catégories de données, les durées de conservation et les acteurs impliqués.. - Cartographie des flux de données internes et externes, en précisant les acteurs impliqués et les mesures de sécurité associées. - Évaluation des traitements impliquant des flux transfrontaliers, en identifiant les acteurs et les risques associés.	**C1.1** Cartographier l'ensemble des traitements de données personnelles et sensibles de l'organisation, en identifiant les flux et les acteurs impliqués, en appliquant des techniques de classification des données selon leur sensibilité et en analysant les enjeux de conformité réglementaires et sectoriels (ex. : santé, finance, e-commerce) afin d'établir un diagnostic détaillé des flux de données et des pratiques de traitement	**Etude de cas (épreuve écrite) :** À partir d'un dossier d'étude de cas présentant l'environnement RGPD d'une entreprise (registre des traitements, documentation contractuelle, flux de données internes et externes), le candidat devra : ▪ Examiner les documents fournis (registre des traitements, contrats de sous-traitance, documentation interne). ▪ Repérer les écarts de conformité et les risques associés en s'appuyant sur les exigences du RGPD et des réglementations sectorielles. ▪ Cartographier les flux de données internes et externes, en identifiant les flux transfrontaliers et les parties prenantes concernées. ▪ Analyser les clauses contractuelles des sous-traitants et partenaires pour vérifier leur conformité et proposer des ajustements si nécessaire. ▪ Rédiger un rapport structuré, incluant un diagnostic, une analyse des risques et des recommandations de mise en conformité adaptées à l'entreprise étudiée.	- Les traitements de données sont identifiés de manière exhaustive. - Chaque traitement décrit comporte bien 3 aspects : finalité, consentement et durée de conservation - Les acteurs concernés sont identifiés.
	C1.2 Évaluer la conformité des traitements existants, y compris ceux liés aux technologies émergentes, en analysant les écarts entre les pratiques actuelles et les obligations légales et sectorielles (ex. : santé, finance, e-commerce), afin d'auditer le niveau de conformité de l'organisation		- Les écarts entre la réglementation et les pratiques de l'entreprise sont clairement identifiés. - L'analyse des écarts entre les pratiques actuelles et les exigences légales est pertinente et justifiée par des références précises au RGPD et aux réglementations sectorielles (ex. : finalités, bases légales, durée de conservation, mesures de sécurité). - Les risques identifiés sont priorisés en fonction de leur impact sur la conformité et les enjeux métiers.
	C1.3 Produire un rapport de diagnostic détaillé, en hiérarchisant les risques identifiés (ex : risques juridiques,		- Le diagnostic présente des pistes de recommandation adaptées au contexte de

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC1 - Auditer et élaborer la politique de conformité et de gouvernance des données			
- Identification des écarts de conformité en analysant les finalités, bases légales, durées de conservation et mesures de protection en place. - Rédaction d'un rapport de diagnostic intégrant les écarts identifiés, les risques associés et les recommandations prioritaires. - Mise à jour des registres des traitements, en consolidant les informations issues de l'audit et en intégrant les mesures correctives identifiées.	opérationnels, réputationnels) et en formulant des recommandations spécifiques, pour guider la stratégie de mise en conformité de l'organisation.	**Compétences visées** : C1.1 à C1.6	l'entreprise (ex. : ressources, priorités stratégiques, obligations sectorielles). - Les recommandations sont argumentées sur la base des risques identifiés et permettent d'orienter la mise en conformité Les actions correctives proposées sont adaptées à la nature des écarts. - La hiérarchisation des risques est cohérente avec la criticité des non-conformités.
	C1.4 Créer ou mettre à jour les registres des traitements de données personnelles, en élaborant des fiches descriptives détaillées pour chaque traitement en collaboration avec les responsables métiers, en consolidant les informations requises par le RGPD (ex. : finalités, catégories de données, mesures de sécurité) et en intégrant les spécificités technologiques et métiers de l'organisation (ex. : algorithmes d'IA, protocoles IoT), afin d'assurer une traçabilité complète des activités de traitement et de garantir leur conformité aux exigences réglementaires.		- La mise à jour du registre est conforme aux exigences du RGPD (ex. : finalités, bases légales, durées de conservation, mesures de sécurité). - Les traitements sont décrits de manière exhaustive et sont appropriés au contexte. - La durée de conservation légale est appliquée. - Les responsables de chaque traitement sont identifiés. - La finalité du traitement est précise. - Les fiches descriptives des traitements sont détaillées et adaptées aux exigences réglementaires. - Les fiches descriptives des traitements intègrent les spécificités métiers et technologiques (ex. : IA, IoT).
A1.2. Encadrement des relations contractuelles et des transferts de données hors UE	**C1.5** Analyser les contrats en cours avec les sous-traitants et partenaires externes , en vérifiant les clauses liées à la protection des données		- Un inventaire des contrats avec les sous-traitants est réalisé et mis à jour. - Les clauses contractuelles liées aux traitements de données (ex. : responsabilités, garanties de

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC1 - Auditer et élaborer la politique de conformité et de gouvernance des données			
- Recensement et analyse des contrats en cours avec les sous-traitants et partenaires externes. - Audit de conformité des sous-traitants et suivi de leurs obligations réglementaires en collaboration avec les services juridiques et achats. - Vérification des clauses contractuelles spécifiques à la protection des données (ex. : responsabilités, garanties de sécurité, obligations réglementaires)	(ex. : traitement, stockage, partage) et aux engagements des parties prenantes, en mettant en œuvre des processus d'audit contractuel afin de garantir l'application des exigences réglementaires et de sécuriser les échanges de données avec les partenaires.		sécurité, modalités de sous-traitance) sont évaluées en fonction de leur conformité avec l'article 28 du RGPD. - Une liste des contrats non conformes est établie et priorisée selon les risques identifiés. - Un plan de progrès pour les contrats non conformes est proposé, incluant des recommandations concrètes et adaptées au contexte de l'entreprise. - Les recommandations d'ajustement des contrats en cas de non-conformité sont cohérentes avec les exigences du RGPD. - Un plan d'audit des sous-traitants est organisé pour contrôler l'application des clauses contractuelles.
- Évaluation des risques liés aux transferts de données hors UE, en tenant compte des législations locales et des recommandations des autorités de contrôle. - Application des outils juridiques adaptés (Clauses Contractuelles Types, Binding Corporate Rules) - Élaboration et mise à jour des standards contractuels conformes au RGPD et adaptés aux besoins spécifiques de l'organisation.	**C1.6** Gérer les transferts de données hors Union Européenne (UE), en mettant en œuvre les mécanismes juridiques appropriés (ex. : Clauses Contractuelles Types, Binding Corporate Rules) et en assurant le suivi des obligations réglementaires, afin de garantir la conformité et sécuriser les flux transfrontaliers.		- Les flux transfrontaliers sont identifiés de manière exhaustive, en précisant les pays concernés, les bases légales de transfert et les mesures de protection associées, conformément aux exigences du RGPD et aux recommandations des autorités de contrôle. - Les solutions proposées respectent les contraintes des transferts hors UE. - La justification des choix de mécanismes de transfert est fondée sur les obligations réglementaires. - Les mécanismes juridiques appropriés (ex. : Clauses Contractuelles Types, Binding Corporate Rules) sont correctement appliqués et justifiés au regard des dernières décisions et

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC1 - Auditer et élaborer la politique de conformité et de gouvernance des données			
- Mise à jour et suivi des contrats, en s'assurant de leur conformité continue avec les évolutions réglementaires			recommandations des autorités de contrôle (ex. : CJUE, CNIL).
A1.3. Élaboration et mise en œuvre des politiques de conformité RGPD et gestion des droits des personnes concernées - Définition des règles internes de conformité, en intégrant les exigences du RGPD et les spécificités sectorielles. - Rédaction et diffusion des documents cadres (politique de confidentialité, charte RGPD, procédures internes). - Mise en place des procédures de gestion des droits (accès, effacement, opposition), avec suivi des délais réglementaires. - Intégration d'outils automatisés pour le traitement des demandes et suivi des délais de réponse. - Suivi des indicateurs de gestion des droits et ajustement des processus en fonction des retours d'expérience et des évolutions réglementaires.	**C1.7** Concevoir une politique de gouvernance des données personnelles, incluant des documents opérationnels (ex. : politique de conservation des données, politique de confidentialité, charte RGPD) et des principes clés (ex. : licéité, minimisation, conservation limitée), en collaboration avec les départements métiers (ex. : juridique, IT, marketing) afin d'uniformiser les pratiques de gestion des données et de garantir la conformité au RGPD.	**Etude de cas (épreuve écrite)** À partir d'un dossier d'étude de cas détaillant les obligations de conformité RGPD d'une organisation, ainsi que ses politiques internes existantes, le candidat devra : ▪ Analyser le cadre existant et les obligations réglementaires spécifiques à l'entreprise présentée dans l'étude de cas. ▪ Rédiger une politique interne de protection des données, en tenant compte des enjeux liés à la conservation, à la minimisation des données et aux obligations de transparence. ▪ Définir une procédure opérationnelle détaillée de gestion des droits des personnes concernées, en décrivant les étapes de traitement des demandes, les outils à mobiliser et les responsabilités associées. ▪ Proposer des outils et mécanismes de suivi des demandes pour assurer la	- La politique de gouvernance est complète et adaptée aux réalités de l'entreprise. - Les principes clés du RGPD (ex. : licéité, minimisation, conservation limitée) sont intégrés dans la politique de gouvernance. - La politique élaborée est adaptée au secteur d'activité et prend en compte les spécificités métiers.
	C1.8 Concevoir des protocoles de gestion des consentements et des préférences, intégrant des mécanismes de preuve (ex : horodatage, journalisation) et de révocation (ex : interface utilisateur dédiée, processus automatisé de suppression), en veillant à leur accessibilité et leur compréhension par l'ensemble des publics concernés, y compris les personnes		- Les mesures proposées garantissent le respect des droits des personnes concernées tout au long du cycle de vie des données (ex. : collecte du consentement explicite, possibilité de révocation, conservation des preuves de consentement). - Les mécanismes de traçabilité et d'historisation des consentements sont conformes aux exigences réglementaires et permettent de justifier la validité du traitement (ex. : journalisation des actions, stockage sécurisé).

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC1 - Auditer et élaborer la politique de conformité et de gouvernance des données			
	en situation de handicap, afin de garantir le respect des choix des personnes concernées et leur traçabilité tout au long du cycle de vie des données.	traçabilité et le respect des délais réglementaires. ▪ Analyser la demande de la CNIL et identifier les documents et preuves de à fournir en fonction des traitements concernés. ▪ Structurer une réponse écrite argumentée à destination de la CNIL, en mettant en avant les éléments justificatifs et les mesures mises en place. **Compétences visées** : C1.7 à C1.10	- Les protocoles de gestion des consentements et des préférences sont conçus de manière à garantir leur accessibilité à tous les publics, y compris les personnes en situation de handicap (ex. : formats adaptés, clarté des informations, compatibilité avec les outils d'assistance).
	C1.9 Mettre en place un processus structuré de gestion des demandes d'exercice des droits des personnes concernées (ex. : droit d'accès, droit d'effacement, droit d'opposition), en intégrant des workflows automatisés (ex. : système de ticketing), en veillant à l'accessibilité des démarches pour tous les publics, notamment les personnes en situation de handicap, et en définissant des indicateurs clés de suivi (ex. : délais de réponse, taux de résolution), afin de garantir un traitement conforme et une traçabilité des demandes dans les délais réglementaires.		- La procédure de gestion des droits est complète, détaillant les différentes étapes (réception, traitement, validation, réponse) et les solutions mobilisées pour assurer la traçabilité et le respect des délais réglementaires (ex. : système de gestion des requêtes, plateforme de suivi des demandes, outils d'horodatage). - Les procédures de gestion des demandes d'exercice des droits sont accessibles à tous les publics, y compris les personnes en situation de handicap (ex. : mise à disposition de formats alternatifs, assistance dédiée, accessibilité numérique des démarches). - Les indicateurs de suivi définis (ex. : délais de réponse, taux de résolution) permettent un contrôle efficace du respect des délais réglementaires.
A1.4. Gestion des interactions avec les autorités de contrôle (CNIL) - Préparation des réponses aux demandes d'information ou de contrôle des autorités (ex. : CNIL), en collaboration avec les équipes internes.	**C1.10** Gérer les échanges avec la CNIL lors d'un contrôle ou d'une demande d'information, en rassemblant les éléments de conformité requis et en coordonnant la communication entre les parties prenantes internes et l'autorité de		- Les documents de conformité sont préparés de façon à anticiper les contrôles des autorités de régulation. - Les documents de conformité sont évalués de manière exhaustive, avec une identification pertinente des éventuelles lacunes (ex. : absence de justification des bases légales, registres

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC1 - Auditer et élaborer la politique de conformité et de gouvernance des données			
- Coordination des échanges avec la CNIL concernant les actions entreprises. - Gestion des demandes d'information ou de contrôle des autorités (ex. : CNIL)	contrôle, afin d'assurer une coopération efficace et démontrer la conformité de l'organisation.		incomplets, clauses contractuelles insuffisantes). - La réponse est structurée et argumentée, en intégrant des références aux exigences légales et aux politiques internes de conformité. - Les actions correctives proposées sont adaptées aux écarts identifiés et prennent en compte les risques de non-conformité.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC2 - Superviser la sécurité des données et des systèmes d'information			
A2.1. Mise en place d'un cadre de gouvernance pour la gestion des données - Identification des acteurs impliqués dans la gouvernance des données (DPO, RSSI, directions métiers, sous-traitants). - Définition des rôles et responsabilités des acteurs internes et externes. - Définition de mécanismes de gouvernance, incluant les modalités d'approbation et de reporting. - Intégration des principes de Privacy by Design et Privacy by Default dans les systèmes d'information et les processus métiers. - Validation des mécanismes de gouvernance et mise en œuvre des ajustements si nécessaire. - Suivi de l'application des mesures de gouvernance et ajustements en fonction des retours des parties prenantes.	**C2.1** Cartographier les acteurs internes et externes impliqués dans la gestion des données personnelles, en identifiant leurs rôles et responsabilités afin d'assurer une gouvernance alignée avec les objectifs de conformité.	**Étude de cas (épreuve écrite)** À partir d'une étude de cas présentant la gouvernance des données d'une entreprise et ses mécanismes de suivi de la sécurité (ex. : organigramme de gouvernance, tableaux de bord de suivi des incidents), le candidat devra : ▪ Analyser la gouvernance des données et la répartition des responsabilités (ex. : DPO, RSSI, directions métiers, sous-traitants). ▪ Évaluer l'intégration des principes de Privacy by Design et Privacy by Default dans les projets SI. ▪ Examiner les indicateurs de sécurité et les tableaux de bord existants, en identifiant les limites et les axes d'amélioration. ▪ Proposer un plan d'amélioration de la gouvernance et des indicateurs de suivi, pour renforcer la sécurité et la conformité. **Compétences visées** : C2.1 à C2.4	- Les acteurs internes et externes (DPO, RSSI, directions métiers, sous-traitants) sont clairement identifiés et leurs rôles sont correctement définis. - La répartition des responsabilités entre les parties prenantes (DPO, RSSI, équipes juridiques et métiers) est explicitée à travers des mécanismes concrets de gouvernance (ex. : processus d'approbation des traitements, reporting de conformité, comité de suivi RGPD).
	C2.2 Définir un cadre de gouvernance en collaboration avec les équipes IT et juridiques pour intégrer les principes de Privacy by Design et Privacy by Default dès la conception d'un projet impliquant des traitements de données (ex : déploiement d'un SIRH, développement d'une application métier, implémentation d'une solution d'IA)		- L'intégration des principes de Privacy by Design et Privacy by Default est clairement expliquée et justifiée. - Les recommandations tiennent compte des contraintes organisationnelles et techniques spécifiques (ex. : compatibilité avec l'architecture SI, exigences métiers, impacts opérationnels). - Les modalités de contrôle et d'application des principes RGPD sont explicitées (ex. : points de validation dans le cycle de développement, documentation des traitements).
A2.2. Suivi des indicateurs de gouvernance et de sécurité	**C2.3** Suivre les politiques de gouvernance et de sécurité à travers des		- Les indicateurs clés de performance (KPI) sont définis de manière précise et en adéquation avec

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC2 - Superviser la sécurité des données et des systèmes d'information			
- Définition des indicateurs de performance des politiques de gouvernance et de sécurité (ex. : vulnérabilités, tentatives de phishing, mails frauduleux, etc). - Mise en place de tableaux de bord pour le suivi des activités liées à la gestion des données et aux incidents de sécurité. - Mise en place d'un processus d'alerte en cas d'anomalie détectée sur les indicateurs de sécurité. - Analyse des résultats et identification des axes d'amélioration, en tenant compte des tendances observées sur les incidents et les écarts de conformité. - Planification des échéanciers pour le déploiement des actions correctives. - Communication des résultats aux parties prenantes internes et externes (COMEX, IT, juridique, partenaires).	indicateurs clés de performance (KPI) (ex. : taux de résilience aux cybermenaces, conformité des sous-traitants) et des tableaux de bord, en identifiant les écarts pour optimiser les pratiques de gestion des données et des systèmes de sécurité.		les objectifs de gouvernance et de sécurité des données. - L'analyse des indicateurs fournis dans l'étude de cas est précise et met en avant les écarts et axes d'amélioration. - Les propositions d'ajustement sont cohérentes et permettent une meilleure optimisation des pratiques de gestion des données et des systèmes de sécurité.
	C2.4 Présenter les résultats des KPI aux parties prenantes internes (ex. : IT, juridique, directions métiers) et externes (ex. : sous-traitants, partenaires, COMEX), en formulant des analyses stratégiques pour orienter les décisions et prioriser les investissements en sécurité.		- L'analyse des résultats des KPI met en évidence les tendances significatives liées à la conformité et à la sécurité des données, en identifiant les évolutions critiques (ex. : amélioration du taux de conformité, efficacité des actions correctives, fréquence des incidents de sécurité). - Les analyses fournies permettent d'orienter efficacement les décisions des parties prenantes en matière de sécurité et de gouvernance des données. - Les propositions d'investissement et d'amélioration de la sécurité sont justifiées par des données concrètes et adaptées aux besoins de l'organisation.
A2.3. Supervision et suivi des audits de cybersécurité et de conformité	**C2.5** Superviser un audit de sécurité et de conformité des systèmes d'information, en définissant le	**Étude de cas (épreuve écrite)** À partir d'une étude de cas décrivant un audit de sécurité réalisé au sein d'une	- Le périmètre d'évaluation de l'audit est défini de manière claire et prend en compte les exigences

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC2 - Superviser la sécurité des données et des systèmes d'information			
- Définition du périmètre et des objectifs des audits internes et externes sur la cybersécurité et la conformité RGPD, en collaboration avec les équipes métiers et techniques. - Identification des écarts liés à la sécurité des systèmes selon les standards de sécurité (ISO 27001, NIST, etc.) et à la conformité (RGPD, NIS I, NIS II, DORA, etc.) - Exploitation des résultats des audits, en analysant les vulnérabilités identifiées et en formulant des recommandations adaptées. - Vérification de la mise en œuvre des recommandations issues des audits techniques et organisationnels. - Suivi post-audit des actions correctives mises en œuvre	périmètre d'évaluation et les exigences réglementaires (ex. : RGPD, ISO 27001), afin d'identifier les failles de sécurité et les écarts de conformité impactant la protection des données personnelles. **C2.6** Exploiter les résultats d'un audit de sécurité et de conformité, en analysant les écarts identifiés et en veillant à la mise en œuvre des mesures correctives, afin d'améliorer la protection des données et d'assurer la conformité des dispositifs de sécurité.	organisation, incluant des constats sur la conformité RGPD, les vulnérabilités des systèmes d'information et la gestion des cybermenaces, le candidat devra : ▪ Analyser les résultats de l'audit fourni, et identifier les principaux écarts de conformité et les failles de sécurité du système d'information. ▪ Proposer un plan d'actions correctives adaptées, en précisant les priorités, les parties prenantes concernées (DPO, RSSI, métiers) et les échéances. ▪ Décrire les modalités de suivi et de contrôle de la mise en œuvre des correctifs. ▪ Produire une analyse sur l'état de la menace cybercriminelle pour identifier les acteurs malveillants susceptibles de porter atteinte aux données. ▪ Proposer une stratégie de surveillance des cybermenaces, en listant les indicateurs permettant d'anticiper les risques (ex. : détection d'anomalies, surveillance des failles, alertes d'intrusion) et en proposant un plan de prévention des incidents futurs. **Compétences visées** : C2.5 à C2.9	réglementaires applicables (ex. : RGPD, NIS I, NIS II, DORA, ISO 27001, NIST, etc.). - Les vulnérabilités et écarts de conformité sont identifiés en s'appuyant sur des méthodes d'évaluation structurées (ex. : tests de sécurité, audit de conformité, etc.) - L'analyse des écarts identifiés met en évidence les risques associés, en tenant compte de leur impact sur la protection des données et des obligations réglementaires applicables. - Les mesures correctives proposées sont adaptées à la criticité des vulnérabilités identifiées. - Le suivi des actions correctives inclut un plan d'exécution détaillé, précisant les priorités, les échéances et les parties prenantes responsables,
A2.4. Gestion de la sécurité des systèmes d'information liés aux données personnelles - Contrôle de l'application des mesures techniques renforcées en lien avec les recommandations de l'ANSSI	**C2.7** Superviser l'application des mesures techniques de sécurité (ex. : chiffrement, segmentation des accès, tests de vulnérabilité) en collaboration avec le RSSI et en s'appuyant sur les standards de cybersécurité (ISO 27001, ANSSI,		- L'application des mesures techniques de sécurité (ex. : chiffrement, segmentation des accès, tests de vulnérabilité) est contrôlée en fonction des recommandations des référentiels de cybersécurité (ex. : ANSSI, ISO 27001) et de leur efficacité sur la réduction des cybermenaces.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC2 - Superviser la sécurité des données et des systèmes d'information			
(ex. : chiffrement, gestion des accès, tests de vulnérabilité). - Mise en place et suivi des politiques de gestion des accès et des habilitations, en garantissant une séparation des droits selon les fonctions. - Identification et analyse des cybermenaces émergentes en collaboration avec le RSSI.	NIST), afin de garantir une protection efficace des données personnelles et une conformité réglementaire continue.		- Les solutions de protection contre les cybermenaces sont sélectionnées et justifiées en fonction de leur capacité à réduire les risques identifiés (ex. : déploiement de mécanismes de détection proactive, renforcement des contrôles d'accès, surveillance des tentatives d'intrusion). - Les actions mises en œuvre pour prévenir les cybermenaces sont alignées avec les stratégies de gestion des risques définies dans la gouvernance des données.
- Suivi des cyberattaques et incidents de sécurité signalés en coordination avec le RSSI, et application des plans d'actions correctifs - Veille technologique et réglementaire sur les innovations et menaces liées à la cybersécurité.	**C2.8** Surveiller l'évolution des cybermenaces en collaboration avec le RSSI, en mobilisant des outils de détection avancés (ex : SIEM, EDR) et en effectuant une veille active sur les menaces émergentes, afin d'anticiper et prévenir les risques de sécurité.		- Les outils de détection des cybermenaces (ex. : SIEM, EDR) sont sélectionnés et analysés en fonction des besoins de l'organisation, en tenant compte des menaces spécifiques. - L'analyse des tendances en matière de cybermenaces est argumentée et permet d'anticiper les nouvelles vulnérabilités. - Les actions de prévention proposées sont adaptées et permettent de limiter efficacement les risques identifiés.
	C2.9 Évaluer les incidents de sécurité signalés, en supervisant la mise en œuvre des plans de réponse et des mesures correctives, afin de limiter l'impact sur les données personnelles et de renforcer la capacité de l'organisation à prévenir les violations futures.		- L'évaluation des incidents de sécurité est précise et met en évidence les conséquences potentielles sur la protection des données. - La mise en œuvre des mesures correctives est suivie à l'aide d'un plan structuré incluant des jalons de validation, des tests de sécurité récurrents et un reporting auprès des instances de gouvernance,

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC2 - Superviser la sécurité des données et des systèmes d'information			
			- Les recommandations pour améliorer la capacité de prévention des violations futures sont détaillées et applicables à l'organisation.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC3 – Gérer les risques et les crises liés aux traitements de données			
A3.1. Réalisation d'analyses d'impact sur la vie privée (PIA) - Sélection des traitements nécessitant une analyse d'impact dédiée et approfondie en fonction de leur criticité (ex. : reconnaissance faciale, vidéosurveillance, systèmes d'IA, traitement de données de santé, etc.) et de leur finalité. - Mobilisation d'outils spécifiques pour la réalisation des analyses d'impact (ex. : logiciel PIA de la CNIL). - Analyse des traitements à risque selon les exigences réglementaires et les recommandations des autorités de contrôle (ex. : impact sur les droits des personnes, licéité des traitements). - Définition des mesures préventives et correctives spécifiques aux traitements à haut risque, incluant les protocoles techniques et organisationnels adaptés (ex. : pseudonymisation, minimisation des données,	**C3.1** Évaluer au préalable les potentiels impacts de causés par des traitements de données sensibles ou à risques pour les droits et libertés des personnes concernées afin d'évaluer le niveau de risques pour les classer par ordre de gravité	**Etude de cas (épreuve écrite)** À partir d'une étude de cas décrivant une organisation confrontée à divers risques liés à la gestion de données personnelles, le candidat devra : ▪ Analyser les traitements nécessitant une analyse d'impact, en justifiant leur criticité par rapport aux risques pour les droits et libertés des personnes concernées. ▪ Formuler un plan d'actions correctives, en justifiant les mesures proposées pour réduire les risques identifiés. ▪ Proposer une priorisation des actions, en indiquant quelles actions doivent être entreprises en priorité et pourquoi, en fonction des risques identifiés. ▪ Rédiger une note stratégique synthétisant les risques et les recommandations à destination d'un comité de direction. **Compétences visées** : C3.1 à C3.7	- Les traitements nécessitant une analyse d'impact sont identifiés en justifiant leur criticité par des critères précis (ex. : finalité, volume, nature des données, risques pour les droits des personnes). - L'évaluation des risques intègre les principes de minimisation et de proportionnalité, avec des références aux exigences du RGPD et aux recommandations de la CNIL.
	C3.2 Définir des mesures correctives adaptées aux analyses d'impact, en intégrant des solutions spécifiques (ex. : pseudonymisation, anonymisation, renforcement des contrôles d'accès) afin de réduire les risques identifiés et garantir la conformité des traitements.		- Les mesures correctives proposées sont alignées avec les recommandations des autorités de contrôle et adaptées à la nature des traitements (ex. : pseudonymisation, minimisation des données, contrôle des accès). - L'adéquation des mesures techniques et organisationnelles est argumentée et démontrée par une évaluation des effets attendus sur la protection des données.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC3 – Gérer les risques et les crises liés aux traitements de données			
mesures de sécurité renforcées). - Validation des PIA par un comité interne de gouvernance des données (DPO, RSSI, direction juridique). - Suivi de la mise en œuvre des actions correctives issues des PIA et ajustements si nécessaire.			
A3.2. Identification et analyse des risques de cybersécurité liés aux traitements de données - Cartographie des risques associées aux traitements de données selon le contexte de l'organisation. - Évaluation des vulnérabilités associées aux technologies utilisées (ex. : IA, IoT, API) et leurs impacts sur la protection des données personnelles. - Évaluation des risques liés aux cybermenaces susceptibles d'affecter la protection des données (ex. : détournement de bases de données clients,	**C3.3** Cartographier les risques selon leur typologie (financiers, juridiques, réputationnels, opérationnels, etc.) et leur origines (internes : erreurs humaines, falsification, pratiques non conformes, etc. ; et externes : extorsion de données, phishing, intrusion) associés aux traitements de données personnelles, afin d'identifier les priorités.		- Les sources de risques sont identifiés selon leur nature (interne, externe) - Les risques sont priorisés selon leur criticité et leurs conséquences potentielles sur la conformité et la sécurité des données - Les scénarios réalistes sont construits sur la base d'une analyse des sources de risques et des impacts.
	C3.4 Évaluer les vulnérabilités associées aux technologies utilisées dans les traitements (ex. : IA, IoT, API), en tenant compte des impacts potentiels sur les droits des personnes concernées, afin de sécuriser l'usage des données et garantir leur conformité.		- Les vulnérabilités identifiées tiennent compte des spécificités technologiques de l'organisation (ex. : API non sécurisées, données non chiffrées, absence de contrôle d'accès). - L'évaluation des vulnérabilités est argumentée à l'aide de scénarios concrets.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC3 – Gérer les risques et les crises liés aux traitements de données			
hameçonnage ciblé sur les données de santé). - Priorisation des risques identifiés en fonction de leur criticité et de leurs conséquences potentielles, en appliquant des méthodologies adaptées (ex. : Ebios Risk Manager, ISO 27005, etc.). - Mise en place d'un mécanisme de surveillance continue des risques et mise à jour régulière de la cartographie.	**C3.5** Prioriser les risques identifiés en fonction de leur criticité et des enjeux de conformité, en appliquant une méthodologie d'évaluation des risques (ex. : Ebios Risk Manager, ISO 27005, etc.), afin d'orienter les actions de remédiation et d'améliorer la maîtrise des traitements de données.		- La hiérarchisation des risques repose sur des critères objectifs (ex. : niveau de gravité, fréquence d'occurrence, capacité d'atténuation). - Les risques sont priorisés en fonction de leur impact sur la conformité réglementaire et la continuité des activités de l'organisation.
A3.3. Définition et supervision des mesures de réduction des risques - Définition des mesures organisationnelles et techniques adaptées aux risques identifiés (ex. : chiffrement, pseudonymisation, restriction des accès).	**C3.6** Définir un plan d'actions correctives, en définissant des mesures organisationnelles et techniques adaptées aux risques identifiés, afin d'assurer la sécurité des données et leur conformité ou afin d'atténuer les impacts sur les données personnelles et d'assurer leur mise en conformité avec les exigences réglementaires.		- Le plan d'actions est structuré et contient des mesures adaptées à la criticité des risques (ex. : mise en place d'un contrôle d'accès renforcé pour un traitement critique). - Les échéances et priorités définies dans le plan d'actions sont réalistes et conformes aux obligations réglementaires.
- Élaboration d'un plan d'actions correctives en fonction de la criticité des risques et des obligations réglementaires applicables. - Présentation et communication des résultats	**C3.7** Superviser la mise en œuvre des mesures correctives définies, en coordonnant leur application avec les équipes IT et métiers, en établissant des jalons et des échéanciers adaptés, afin de vérifier leur mise en œuvre, d'évaluer leur		- La coordination des actions avec les équipes IT et métiers est détaillée et intègre des jalons et des indicateurs de suivi clairs. - Les ajustements proposés en fonction des résultats obtenus sont cohérents avec une démarche d'amélioration continue.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC3 – Gérer les risques et les crises liés aux traitements de données			
de l'analyse aux parties prenantes internes et aux décideurs stratégiques (ex. : DSI, RSSI, responsables métiers). - Coordination avec les équipes IT et métiers pour la mise en œuvre des mesures validées. - Mise à jour régulière des mesures en fonction des évolutions réglementaires et des nouvelles menaces identifiées (ex. : veille technologique, retours d'audits internes). - Évaluation de l'efficacité des mesures mises en place et élaboration d'un bilan synthétique des actions entreprises et de leurs résultats.	efficacité et d'ajuster les actions en fonction des résultats observés.		
A3.4. Coordination des actions en cas de crise - Élaboration de protocoles de déclenchement de gestion des crises, incluant des niveaux d'alerte (ex. : piratage, perte de données sensibles). - Rédaction de procédures internes pour la gestion des	**C3.8** Concevoir des protocoles de gestion des crises, en définissant des niveaux d'alerte (ex. : niveau de compromission, sites touchés, données touchées, etc.), et en structurant les modalités de signalement et de communication interne et externe, en veillant à ce que les informations et procédures	**Mise en situation professionnelle + entretien avec le jury** Le candidat sera confronté à une situation de crise où il devra : ▪ Évaluer la situation initiale de crise (ex. : piratage de données, violation de la confidentialité) et décrire les premières actions à mener pour limiter l'impact	- Les protocoles de gestion des crises sont structurés, opérationnels et adaptés à différents scénarios (ex. : violation de données, cyberattaque). - Les niveaux d'alerte définis sont adaptés aux différents scénarios de crise (ex. : fuite massive de données, cyberattaque, erreur humaine). - Les protocoles intègrent une chaîne de responsabilité claire et des mécanismes de

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC3 – Gérer les risques et les crises liés aux traitements de données			
crises (ex. : modalités de signalement, listes d'interlocuteurs à prévenir). - Conception des outils de communication à destination des parties externes (ex. : notifications CNIL, informations aux personnes concernées).	de gestion de crise soient accessibles et compréhensibles pour tous, y compris les personnes en situation de handicap, afin de réduire l'impact des incidents sur l'organisation.	immédiat sur les données personnelles. ▪ Proposer un plan de communication pour la gestion de crise, en détaillant les informations à transmettre et les étapes de communication. ▪ Analyser la réponse aux incidents, en évaluant l'efficacité des actions prises et en proposant des améliorations pour mieux gérer les futures crises. ▪ Exposer ses propositions devant le jury et défendre ses choix concernant la gestion de la crise et des mesures correctives mises en place. **Compétences visées** : C3.8 à C3.10	communication efficaces avec les parties prenantes concernées (ex. : notification CNIL, communication aux clients). - Les procédures de gestion de crise et les documents associés sont accessibles et compréhensibles par tous, y compris les personnes en situation de handicap (ex. : langage simplifié, supports adaptés, versions audio ou visuelles des procédures).
- Rédaction des formulaires de notification des violations auprès de la CNIL. - Interface avec les autorités de régulation (ANSSI, CNIL) en cas de violation de données ou d'incident de sécurité majeur. - Coordination des actions correctives immédiates avec les équipes internes (juridique, IT, métier). - Suivi post-crise et intégration des retours d'expérience dans les procédures de gestion des incidents.	**C3.9** Coordonner les actions correctives en situation de crise, en collaborant avec les équipes internes (IT, juridique, métiers) et en assurant une communication adaptée avec les parties externes (ex. : CNIL, personnes concernées), et en prenant en compte les besoins spécifiques des personnes en situation de handicap ou en difficulté numérique (ex. : communication en langage simplifié, mise à disposition de supports adaptés), afin de limiter les impacts sur les données personnelles et rétablir la sécurité des systèmes.		- Les actions mises en œuvre en réponse à la crise sont adaptées à la situation et permettent de limiter immédiatement l'impact sur les données personnelles. - Les actions correctives et la communication en situation de crise prennent en compte la diversité des publics concernés, en intégrant des moyens de communication accessibles aux personnes en situation de handicap (ex. : transcription écrite, communication en langage simplifié). - Les décisions prises en réponse à la crise sont justifiées et démontrent une capacité d'adaptation face aux événements. - Les interactions avec les régulateurs (ex. : CNIL, ANSSI) respectent les obligations légales et incluent la transmission complète des informations requises (ex. : nature de l'incident, mesures correctives mises en œuvre)
	C3.10 Evaluer les réponses apportées lors d'une crise (ex. : piratage, perte de données), en analysant les		- L'analyse des actions entreprises met en évidence les réussites et les points d'amélioration.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC3 – Gérer les risques et les crises liés aux traitements de données			
	actions correctives mises en œuvre et en identifiant les améliorations nécessaires, afin d'améliorer les protocoles de gestion des crises et garantir une meilleure anticipation des incidents futurs.		- Les propositions d'optimisation des protocoles de gestion de crise sont adaptées aux retours d'expérience et aux nouvelles menaces identifiées. - Les retours d'expérience post-crise sont intégrés dans l'amélioration continue des procédures de gestion des incidents et des niveaux d'alerte.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC4 – Former et sensibiliser les parties prenantes aux enjeux de protection des données			
A4.1. Mobilisation et coordination des parties prenantes pour la mise en œuvre des actions RGPD - Identification des parties prenantes impliquées dans la mise en œuvre des actions RGPD. - Coordination des réunions interservices autour les priorités et des jalons des actions RGPD. - Mise en place d'outils de suivi des actions RGPD et définition d'indicateurs - Recueil et mutualisation des retours d'expérience des différents services.	**C4.1** Coordonner la mise en œuvre des actions RGPD en mobilisant les parties prenantes internes, en facilitant l'organisation des échanges interservices et en assurant le suivi des actions, afin d'optimiser l'engagement des acteurs et la progression des initiatives de conformité.	**Projet professionnel + soutenance orale devant un jury** À partir d'un cas fictif ou réel donné en amont, le candidat devra concevoir et mettre en œuvre un projet global de mise en conformité RGPD, intégrant la mobilisation des parties prenantes, la communication, la sensibilisation et la formation des équipes. L'évaluation se structure en deux parties : **Partie 1 : Réalisation du projet (en amont des épreuves de certification)** Le candidat prépare un projet détaillé et fournit les livrables suivants sous forme de documents écrits et supports pédagogiques : ▪ Présentation du projet, incluant les objectifs stratégiques, le public cible et les parties prenantes mobilisées. ▪ Élaboration d'un plan de mobilisation et de coordination des parties prenantes, détaillant les actions prévues pour structurer la mise en œuvre des actions RGPD. ▪ Conception d'un plan de communication structuré, précisant les messages clés, les canaux de diffusion et les supports utilisés (ex. : intranet, newsletters, affichages).	- Les parties prenantes internes sont identifiées et mobilisées en fonction de leur rôle et de leur contribution aux actions RGPD. - Les échanges inter services sont organisés de manière efficace, avec des modalités de coordination adaptées (ex. : réunions, outils collaboratifs, reporting structuré). - Les objectifs et priorités des actions RGPD sont définis et communiqués. - Le suivi des actions RGPD repose sur des indicateurs mesurables, permettant d'évaluer la progression des initiatives de conformité (ex. : taux d'avancement des plans d'action, respect des échéances, taux de correction des non-conformités).
	C4.2 Analyser les retours d'expérience sur les actions RGPD réalisées, en identifiant les bonnes pratiques et les points d'amélioration avec les départements métiers (ex. : IT, juridique, opérationnel), afin d'optimiser les processus internes et d'adapter les politiques de conformité aux enjeux opérationnels.		- Les retours d'expérience recueillis permettent d'identifier les bonnes pratiques et les difficultés rencontrées dans la mise en œuvre des actions RGPD. - Les enseignements tirés des retours d'expérience sont synthétisés et conduisent à des recommandations opérationnelles adaptées aux réalités des départements métiers. - Les propositions d'amélioration des actions RGPD sont argumentées, en tenant compte des retours des équipes métiers et des évolutions réglementaires et organisationnelles.
A4.2. Pilotage des actions de communication internes et externes sur les enjeux de protection des données	**C4.3** Élaborer une stratégie de communication sur les enjeux et les actions RGPD, en définissant des objectifs et des messages clés pour les publics internes et externes (ex. :		- L'analyse du contexte et des besoins en communication est détaillée, tenant compte des spécificités des publics cibles.

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC4 – Former et sensibiliser les parties prenantes aux enjeux de protection des données			
- Élaboration d'un plan de communication structuré sur les enjeux et les actions RGPD. - Conception de messages ciblés pour les parties prenantes internes (collaborateurs, direction) et externes (clients, partenaires).	collaborateurs, clients, partenaires), afin de renforcer la visibilité des actions de conformité.	▪ Développement d'un programme de sensibilisation, détaillant les supports et outils pédagogiques adaptés aux publics internes (ex. : affiches, vidéos, guides pratiques). ▪ Conception d'un module de formation, incluant les objectifs pédagogiques, les modalités d'animation et un support interactif (ex. : présentation PowerPoint, quiz, infographie) adapté aux besoins spécifiques des différents publics. ▪ Définition d'un plan d'évaluation de l'impact, intégrant les indicateurs de suivi des actions mises en place et les méthodes pour analyser les retours d'expérience. ▪ Une note explicative justifiant les choix pédagogiques, organisationnels et stratégiques en lien avec les enjeux de protection des données et les obligations réglementaires. **Partie 2 : Soutenance orale devant le jury** Lors de l'épreuve orale, le candidat devra : ▪ Présenter son projet de sensibilisation et de formation, en expliquant le contexte, les acteurs mobilisés et leur rôle, les objectifs pédagogiques, les	- Les objectifs de communication sont définis de manière claire et alignés avec les enjeux RGPD identifiés. - Les messages clés sont définis en fonction des enjeux RGPD et des spécificités des publics internes et externes (ex. : collaborateurs, clients, partenaires) et sont formulés de manière claire, pédagogique et engageante
- Coordination de la diffusion des messages via des canaux et formats variés (ex. : intranet, newsletters, webinars). - Réalisation de bilans réguliers sur l'efficacité des communications. - Adaptation des messages de communication en fonction des évolutions réglementaires et des retours des parties prenantes.	**C4.4** Superviser la diffusion des messages RGPD via des canaux adaptés (ex. : intranet, newsletters, plateformes collaboratives) et des formats variés (ex. : vidéos, webinars), en veillant à l'accessibilité des contenus pour tous les publics (ex. : sous-titrage, versions en langage simplifié, compatibilité avec les lecteurs d'écran), afin de maximiser leur impact et renforcer l'engagement des parties prenantes dans la démarche de conformité.		- Les canaux de diffusion proposés sont adaptés aux publics cibles (ex. : collaborateurs, clients, partenaires) et à leurs habitudes de communication. - Le plan de diffusion est structuré et prévoit une articulation cohérente des messages, garantissant une diffusion progressive et efficace. - Les formats de communication sélectionnés (ex. : newsletters, intranet, webinars) sont justifiés en fonction des objectifs et des contraintes de l'organisation. - Les supports de communication (vidéos, newsletters, plateformes collaboratives) respectent les principes d'accessibilité numérique et sont adaptés aux différents besoins des publics (ex. : sous-titrage, compatibilité avec les lecteurs d'écran, versions en langage simplifié).
	C4.5 Évaluer l'efficacité des actions de communication, en analysant les retours qualitatifs et quantitatifs (ex. : taux de participation, feedback), afin d'ajuster les stratégies et d'optimiser les campagnes futures.		- Les indicateurs de suivi définis sont pertinents et permettent d'évaluer l'efficacité des actions mises en œuvre (ex. : taux de participation aux sessions de sensibilisation, nombre de vues des supports pédagogiques, feedback des participants).

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC4 – Former et sensibiliser les parties prenantes aux enjeux de protection des données			
		choix méthodologiques et les supports développés. ▪ Animer un extrait du module de formation ou de sensibilisation devant le jury, en précisant le public ciblé et les objectifs visés. **Compétences visées** : C4.1 à C4.10	- L'analyse des résultats met en évidence les tendances clés, permettant d'identifier les points forts et les axes d'amélioration. - Les recommandations pour ajuster les futures campagnes sont argumentées, en tenant compte des contraintes organisationnelles et des retours des parties prenantes. - Le plan d'évaluation inclut des actions concrètes pour optimiser la communication sur la protection des données, en proposant des ajustements basés sur les données collectées.
A4.3. Déploiement d'actions de sensibilisation auprès des équipes internes sur la protection des données - Diffusion d'informations visant à attirer l'attention sur les enjeux de la protection des données et à promouvoir les bonnes pratiques. - Élaboration et mise en place de campagnes de sensibilisation sur les cybermenaces et les nouvelles technologies (ex. : phishing, IA).	**C4.6** Concevoir des supports et outils de sensibilisation sur les enjeux de protection des données et les cybermenaces, en adaptant les messages et formats (ex. : affiches, vidéos, guides pratiques) aux différents publics internes (ex. : équipes RH, marketing, IT), y compris les personnes en situation de handicap, afin d'informer et attirer l'attention sur les bonnes pratiques en matière de protection des données.		- Les supports de sensibilisation (ex. : affiches, guides, vidéos) sont adaptés aux besoins des différents publics internes, y compris les personnes en situation de handicap - Les contenus sont clairs, accessibles et intègrent des formats inclusifs et interactifs. - Les messages sont adaptés aux enjeux de cybersécurité et RGPD, avec des exemples concrets liés aux métiers concernés (ex. : cas pratiques pour le service marketing, IT, RH). - Les supports sont conçus pour capter l'intérêt du public cible et favoriser l'appropriation des messages clés.
- Conception de supports de sensibilisation adaptés aux différents publics internes, incluant des formats accessibles et inclusifs (ex. : affiches, guides pratiques, vidéos sous-titrées)	**C4.7** Coordonner le déploiement des campagnes de sensibilisation internes sur les enjeux RGPD et la sécurité des données, en utilisant des canaux adaptés (intranet, newsletters, événements), en veillant à ce que ces supports soient		- La stratégie de sensibilisation est structurée et cohérente, avec un calendrier détaillé des actions de sensibilisation. précisant les fréquences et canaux utilisés (ex. : newsletters, intranet, sessions de formation). - Les campagnes de sensibilisation intègrent des formats accessibles et incluent des moyens

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC4 – Former et sensibiliser les parties prenantes aux enjeux de protection des données			
- Organisation de campagnes de sensibilisation régulières via des canaux internes (intranet, newsletters). - Adaptation des messages de sensibilisation en fonction des besoins spécifiques des départements métiers (ex. : marketing, RH, IT). - Analyse des résultats des actions de sensibilisation à l'aide d'indicateurs de diffusion et d'engagement (ex. : nombre de vues des supports, taux d'ouverture des communications, interactions des collaborateurs) et ajustement des campagnes en fonction des retours et des évolutions réglementaires	accessibles à tous les publics, y compris les personnes en situation de handicap, et en évaluant leur impact à travers des indicateurs de diffusion et d'engagement, afin de maximiser leur portée et renforcer la culture de la protection des données.		permettant à tous les publics d'y accéder (ex. : formats alternatifs, adaptation aux besoins spécifiques de certains collaborateurs). - Les supports et canaux de diffusion sont variés et adaptés aux différents départements (ex. : guides interactifs pour IT, vidéos pédagogiques pour RH, quiz pour les équipes opérationnelles). - Les indicateurs d'impact des campagnes sont définis et expliqués pour mesurer la diffusion et l'engagement des collaborateurs (ex. : nombre de vues des supports, taux d'ouverture des newsletters, interactions sur l'intranet). - Les ajustements des campagnes sont réalisés en fonction des retours des collaborateurs et des évolutions réglementaires.
A4.4. Formation des équipes ou collaborateurs aux principes et procédures RGPD - Identification des besoins de formation spécifiques à chaque métier ou département (juridique, technique, opérationnel). - Conception de modules de formation adaptés aux niveaux des collaborateurs (initiation, perfectionnement, expertise).	**C4.8** Analyser les besoins de formation en matière de protection des données, en identifiant les compétences à développer pour chaque métier ou département (ex. : juridique, technique, opérationnel), afin de garantir une montée en compétence ciblée.		- L'identification des besoins s'appuie sur une analyse détaillée des enjeux spécifiques à chaque département (ex. : risques liés à la gestion des données clients en marketing, conformité des contrats en juridique). - Les méthodes de formation sont adaptées aux niveaux de compétence des publics cibles, en proposant des parcours progressifs (ex. : initiation, perfectionnement, expertise).
	C4.9 Concevoir des modules de formation adaptés aux niveaux des collaborateurs (initiation,		- Les supports de formation sont structurés et adaptés aux niveaux des collaborateurs (initiation, perfectionnement, expertise).

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BC4 – Former et sensibiliser les parties prenantes aux enjeux de protection des données			
- Animation de sessions interactives avec des études de cas concrets et des exemples métiers. - Suivi des acquis via des évaluations régulières (tests, certifications internes). - Analyse de l'impact des formations sur la mise en conformité des équipes et ajustements des programmes de formation en fonction des évolutions réglementaires et des retours des participants	perfectionnement, expertise), y compris les personnes en situation de handicap, en intégrant des études de cas concrets, afin de faciliter l'apprentissage et l'application des principes RGPD dans les pratiques métiers.		- Les contenus sont contextualisés et illustrés par des cas concrets et des exemples métiers. - L'ensemble des supports de formation respecte les principes de pédagogie active, favorisant l'engagement et l'apprentissage des participants. - Les modules de formation sont conçus en tenant compte des besoins spécifiques des personnes en situation de handicap (ex. : sous-titrage, formats interactifs accessibles, transcription textuelle).
	C4.10 Animer des sessions de formation sur la protection des données, en mobilisant des méthodes pédagogiques adaptées et inclusives (ex. : ateliers pratiques, quiz, jeux de rôle), afin d'assurer l'acquisition des connaissances et des savoir-faire liés aux enjeux RGPD.		- Les sessions de formation sont animées en mobilisant des méthodes pédagogiques accessibles et inclusives, permettant la participation de tous les collaborateurs, y compris ceux en situation de handicap (ex. : supports visuels accessibles, scénarios adaptés, formats interactifs variés, assistance en cas de besoin). - Les méthodes pédagogiques sont adaptées au public (ex. : jeux de rôle, quiz, démonstrations pratiques). - Les exemples et mises en situation proposés facilitent la compréhension des principes RGPD et de leur application opérationnelle. - Les mécanismes d'évaluation des acquis sont définis, permettant de mesurer la compréhension des apprenants (ex. : tests de fin de formation, mises en situation).

Pour obtenir la certification professionnelle, le candidat devra valider les quatre blocs de compétences et réaliser un mémoire professionnel basé sur une expérience en entreprise d'au moins 3 mois.

Le mémoire doit **analyser une problématique liée à la protection des données**, en intégrant les dimensions **juridique, technique et organisationnelle** du métier de DPO.

Le mémoire devra :

- ✓ Présenter une problématique concrète liée à la protection des données personnelles dans une organisation
- ✓ Évaluer les enjeux de conformité et les risques,
- ✓ Proposer des solutions adaptées et argumentées,
- ✓ Évaluer la mise en œuvre et les impacts des actions préconisées.

Le mémoire devra refléter une vision stratégique du rôle du DPO et démontrer une capacité à structurer une approche complète de mise en conformité et de gouvernance des données.

Le mémoire fera l'objet d'une soutenance orale de 1 heure devant un jury composé de professionnels et d'experts du domaine. L'évaluation portera sur :

- ✓ La pertinence de l'analyse et des recommandations,
- ✓ La maîtrise des enjeux et des exigences du RGPD,
- ✓ La capacité à défendre ses choix et à répondre aux questions du jury.

Cette épreuve permet de vérifier que le candidat est en mesure d'exercer les fonctions de DPO avec autonomie, en apportant des solutions adaptées aux exigences réglementaires et aux contraintes métier de son organisation.

Critères de validation

- Note minimale de 10/20 pour le mémoire écrit
- Note minimale de 10/20 pour la soutenance orale