iapp

CORPUS DE CONNAISSANCES ET PLAN D'EXAMEN POUR LE PROGRAMME CIPM

VERSION 4.0.0

DATE DE PRISE D'EFFET : 02/10/2023

CORPUS DE CONNAISSANCES POUR LE PROGRAMME CIPM DE L'IAPP

COMPRENDRE LE CORPUS DE CONNAISSANCES DE L'IAPP

L'objectif principal du corpus de connaissances est de documenter les connaissances et compétences qui seront évaluées lors de l'examen de certification. Les thèmes reflètent ce que le professionnel de la protection des données personnelles devrait savoir et être en mesure d'accomplir pour démontrer ses compétences dans ce domaine.

Le corpus de connaissances comprend également les nombres du plan d'examen, indiquant le nombre minimum et maximum de questions prévues dans chacun des thèmes lors de l'examen.

Le corpus de connaissances est établi et tenu à jour par les experts en la matière constituant le comité d'élaboration des examens et le comité du projet de chaque certification. Le corpus de connaissances est examiné (et, le cas échéant, mis à jour) chaque année ; les modifications figurent dans les mises à jour annuelles de l'examen et sont communiquées aux candidats au moins 90 jours avant que le nouveau contenu apparaisse dans l'examen.

COMPÉTENCES ET INDICATEURS DE PERFORMANCE

Le contenu de nos corpus de connaissances est désormais présenté sous la forme d'une série de compétences et d'indicateurs de performance, et non plus sous forme d'aperçu, comme c'était le cas auparavant.

Les compétences regroupent des tâches et aptitudes connexes qui constituent un vaste domaine de connaissances.

Les indicateurs de performance désignent les tâches et les aptitudes distinctes qui constituent le groupe de compétences le plus large. Les questions d'examen évaluent la compétence d'un professionnel de la protection des données personnelles en fonction des indicateurs de performance.

QUELS TYPES DE QUESTIONS SERONT INCLUSES DANS L'EXAMEN ?

Pour le candidat à la certification, les indicateurs de performance constituent des guides permettant d'approfondir les connaissances requises en vue de démontrer ses compétences. Les verbes apparaissant au début de chaque énoncé de compétence et de tâche (identifier, évaluer, mettre en œuvre et définir) indiquent le niveau de complexité des questions à l'examen et leurs corollaires figurent dans la Taxonomie de Bloom (voir page suivante).

ACCRÉDITATION ANAB

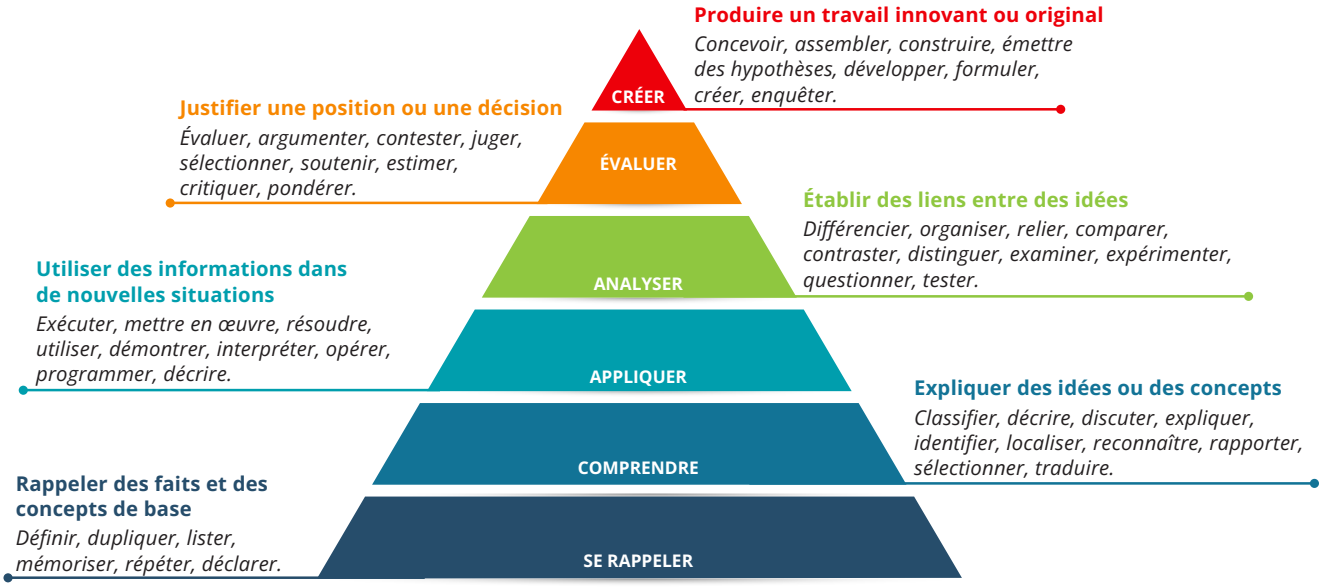
Les certifications CIPM, CIPP/E, CIPP/US et CIPT de l'IAPP sont agréées par le **National Accreditation Board (ANAB) de l'ANSI en vertu de la norme 17024:2012 de l'Organisation internationale de normalisation (ISO)** .

L'ANAB est un organisme d'accréditation reconnu à l'échelle internationale qui évalue et accrédite des programmes de certification répondant à des normes rigoureuses.

L'obtention d'une accréditation est une formidable reconnaissance de la qualité et de l'intégrité des programmes de certification de l'IAPP, qui :

- Prouve que les accréditations de l'IAPP sont conformes à un benchmark global reconnu par l'industrie.
- Garantit la cohérence, la comparabilité et la fiabilité des accréditations IAPP à travers le monde.
- Protège l'intégrité et garantit la validité du programme de certification IAPP.
- Assure aux employeurs, aux collègues, aux clients et aux fournisseurs que les professionnels certifiés IAPP disposent des connaissances, compétences et capacités nécessaires pour accomplir leur travail n'importe où dans le monde.

CORPUS DE CONNAISSANCES POUR LE PROGRAMME CIPM DE L'IAPP



Exemples de questions Se rappeler/ Comprendre supprimées issues de différentes catégories :

- Parmi les propositions suivantes, laquelle est la bonne définition des technologies renforçant la protection des données personnelles ?
- À quel type d'activité la Charte canadienne des droits s'applique-t-elle ?
- Quelle institution de l'Union européenne est compétente pour proposer une législation sur la protection des données personnelles ?
- Qui dispose d'un pouvoir de réglementation concernant le Fair Credit Reporting Act (FCRA) et le Fair and Accurate Credit Transactions Act (FACTA) ?

Les réponses à ces questions sont factuelles et ne peuvent pas être contestées.

Exemples de questions Appliquer/Analyser supprimées issues de différentes catégories :

- Parmi les propositions suivantes, laquelle constitue **la plus grande** difficulté pour un responsable du traitement des données de l'Union européenne en l'absence de dispositions contractuelles clairement définies ?
- Parmi les exemples suivants, lequel constituerait une violation de la protection des données personnelles au niveau territorial ?
- Quel est le **meilleur** moyen de s'assurer que tous les parties prenantes possèdent les mêmes connaissances de base sur les questions liées à la protection des données personnelles auxquelles une entreprise est confrontée ?
- Si les ingénieurs du service informatique avaient initialement paramétré par défaut les informations relatives à la carte de crédit du client sur « Ne pas sauvegarder », à quel concept cette action aurait-elle été conforme ?

La réponse à cette question sera basée sur les connaissances factuelles et une compréhension permettant d'appliquer, d'analyser et/ou d'évaluer les options fournies pour choisir la meilleure réponse.

MIN.	MAX.	Thème I : Programme de protection des données personnelles : Développement d'un cadre	
14	18	**Le Thème I – Programme de protection des données personnelles : Développement d'un cadre** documente les tâches préliminaires requises pour établir une base solide du programme de protection des données personnelles, les objectifs du programme et la personne responsable du programme. Il se concentre sur l'établissement du modèle de gouvernance du programme de protection des données personnelles dans le cadre de la stratégie de protection des données personnelles d'une organisation. Comme chaque entreprise peut avoir ses propres besoins, le modèle peut varier en fonction des entreprises.	
		Compétences	**Indicateurs de performance**
4	6	I.A Définir le champ d'application du programme et développer une stratégie de protection des données personnelles.	Choisir un modèle de gouvernance applicable.
			Identifier la source, les types et les utilisations d'informations personnelles au sein de l'organisation.
			Structurer l'équipe chargée de la protection des données personnelles.
			Identifier les parties prenantes et les soutiens internes.
4	6	I.B Communiquer la vision et l'énoncé de mission de l'organisation.	Sensibiliser au programme de protection des données personnelles de l'organisation au niveau interne et externe.
			Veiller à ce que les employés aient accès aux politiques et procédures ainsi qu'aux modifications en relation avec leur(s) fonction(s).
			Adopter le vocabulaire du programme de protection des données personnelles (par exemple, incident et violation).
5	7	I.C Indiquer les lois, les réglementations et les normes en vigueur applicables au programme.	Comprendre les réglementations et/ou lois territoriales, sectorielles et industrielles.
			Comprendre les sanctions en cas de non-conformité.
			Comprendre la portée et les pouvoirs des organismes de surveillance.
			Comprendre les implications en matière de protection de la vie privée du commerce ou en basant des opérations dans des pays possédant des lois sur la protection des données personnelles inadéquates.

MIN.	MAX.	Thème II : Programme de protection des données personnelles : Établissement d'une gouvernance de programme
12	16	**Le Thème II – Programme de protection des données personnelles : Établissement d'une gouvernance de programme** identifie la manière dont les exigences en matière de protection des données personnelles seront mises en œuvre dans l'ensemble l'organisation à chaque étape du cycle de vie de la protection des données personnelles. Ce thème cible les rôles, responsabilités et exigences en matière de formation des différentes parties prenantes, ainsi que les politiques et procédures qui seront appliquées pour garantir une conformité constante.

			Compétences	Indicateurs de performance
6	8	II.A	Créer les politiques et processus à appliquer à chaque étape du cycle de vie du programme de protection des données personnelles.	Définir le modèle d'organisation, les responsabilités et la structure hiérarchique appropriés à la taille de l'organisation.
				Définir des politiques efficaces relatives au traitement des données détenues et partagées par l'organisation, en tenant compte des exigences légales et éthiques.
				Identifier les points de collecte en prenant en compte les limites en matière de transparence et d'intégrité de la collecte de données.
				Établir un plan de gestion des violations.
				Établir un plan pour les procédures de gestion des réclamations.
1	3	II.B	Expliquer les rôles et responsabilités.	Définir les fonctions et responsabilités en matière de gestion du partage et de la divulgation des données pour un usage interne et externe.
				Définir les rôles et responsabilités en matière de réaction en cas de violation par fonction, y compris les parties prenantes et leur accountability envers les régulateurs, en coordonnant les équipes de détection (par exemple, service informatique, sécurité physique, RH, équipes d'investigation, fournisseurs) et en constituant des équipes de supervision.
2	4	II.C	Définir les indicateurs de la protection des données personnelles à des fins de supervision et de gouvernance.	Créer des indicateurs par public et/ou identifier le public visé par les indicateurs avec des processus clairs décrivant l'objectif, la valeur et la communication des indicateurs.
				Comprendre les objectifs, les types et les cycles de vie des audits en évaluant l'efficacité des contrôles dans l'ensemble des opérations, systèmes et processus de l'organisation.
				Établir des systèmes de surveillance et de mise en œuvre pour suivre l'évolution des lois sur la protection des données personnelles dans différentes juridictions afin de garantir un alignement constant.
1	3	II.D	Établir des formations et des activités de sensibilisation.	Développer des formations ciblées des employés, de la direction et des sous-traitants à chaque étape du cycle de vie de la protection des données personnelles.
				Créer des activités continues du programme de protection des données personnelles (par exemple, formation et sensibilisation, surveillance de la conformité interne, garantie de programme, y compris les audits et les procédures de gestion des réclamations).

MIN.	MAX.	Thème III : Cycle de vie opérationnel du programme de protection des données personnelles : Évaluation des données
12	16	**Le Thème III – Cycle de vie opérationnel du programme de protection des données personnelles : Évaluation des données** explique comment identifier et minimiser les risques en matière de protection des données personnelles et évaluer les impacts sur la protection des données personnelles associés aux systèmes, processus et produits d'une organisation. Aborder les problèmes potentiels dès le début permet par la suite d'établir un programme de protection des données personnelles plus fiable.

			Compétences	Indicateurs de performance
3	5	III.A	Documenter les systèmes de gouvernance des données.	Cartographier les inventaires de données, les flux de données, les cycles de vie et les intégrations de systèmes.
				Évaluer la conformité des politiques par rapport aux exigences internes et externes.
				Déterminer un état désiré et réaliser un gap analysis par rapport à la norme acceptée ou par rapport à la loi.
1	3	III.B	Évaluer les sous-traitants et fournisseurs tiers.	Identifier les risques liés à l'internalisation et l'externalisation des données, y compris les exigences contractuelles et les règles en matière de transfert international des données.
				Effectuer des évaluations au niveau fonctionnel le plus adéquat au sein de l'organisation (par exemple, achats, audit interne, sécurité des informations, sécurité physique et autorité de protection des données).
0	2	III.C	Évaluer les contrôles physiques et environnementaux.	Identifier les risques opérationnels des lieux physiques (par exemple, data centers et bureaux) et les contrôles physiques (par exemple, la conservation des documents, le nettoyage et la mise au rebut des supports, criminalistique des appareils et sécurité des appareils).
3	5	III.D	Évaluer les contrôles techniques.	Identifier les risques opérationnels du traitement numérique (par exemple, serveurs, stockage, infrastructure et cloud).
				Examiner et fixer les limites à l'utilisation des informations personnelles (par exemple, accès en fonction du rôle).
				Examiner et fixer les limites à la conservation des enregistrements.
				Déterminer la localisation des données, y compris les flux de données transfrontaliers.
2	4	III.E	Évaluer les risques associés aux données partagées dans le cadre de fusions, acquisitions et cessions.	Appliquer les procédures de due diligence.
				Évaluer les obligations contractuelles et les obligations de partage des données, y compris les lois, réglementations et normes.
				Alignement des risques et des contrôles de conduite.

MIN.	MAX.	Thème IV : Cycle de vie opérationnel du programme de protection des données personnelles : Protection des données personnelles		
9	13	**Le Thème IV – Cycle de vie opérationnel du programme de protection des données personnelles : Protection des données personnelles** explique comment protéger les actifs de données lors de l'utilisation avec l'implémentation de contrôles de sécurité et technologies du secteur en matière de protection des données personnelles et de sécurité. Indépendamment de la taille, de la zone géographique ou du secteur, les données doivent être protégées physiquement et virtuellement à tous les niveaux de l'organisation.		
			Compétences	**Indicateurs de performance**
4	6	IV.A	Appliquer les pratiques et politiques en matière de sécurité des informations.	Classer les données en fonction du système de classification applicable (par exemple, publiques, confidentielles, restreintes).
				Comprendre les objectifs et limitations des différents contrôles.
				Identifier les risques et mettre en œuvre les contrôles d'accès applicables.
				Utiliser des mesures organisationnelles adéquates pour atténuer les risques résiduels.
1	3	IV.B	Intégrer les principes de la protection des données dès la conception (Privacy by Design, PbD).	Intégrer la protection des données personnelles dans le cycle de vie de développement du système (System Development Life Cycle, SDLC).
				Intégrer la protection des données personnelles dans le processus opérationnel.
3	5	IV.C	Appliquer les lignes directrices d'entreprise concernant l'utilisation des données et s'assurer que les contrôles techniques sont appliqués.	Vérifier que les lignes directrices concernant les utilisations secondaires des données sont suivies.
				Vérifier que les garanties administratives appropriées, notamment les politiques, procédures et contrats relatifs aux fournisseurs et aux politiques des RH sont appliquées.
				S'assurer que les employés ont accès aux contrôles et classifications des données.
				Collaborer avec les technologues de la protection des données personnelles pour activer les contrôles techniques obfuscation, la minimisation des données, la sécurité et les autres technologies améliorant la protection des données personnelles.

MIN.	MAX.	Thème V : Cycle de vie opérationnel du programme de protection des données personnelles : Pour une performance de programme durable		
7	9	**Le Thème V – Cycle de vie opérationnel du programme de protection des données personnelles : Pour une performance de programme durable** explique comment le programme de protection des données personnelles est maintenu à l'aide des indicateurs et des procédures d'audit pertinents. À mesure qu'une organisation avance dans les cycles de gestion de leur programme de protection des données personnelles, il est important de s'assurer que l'ensemble des processus et procédures fonctionnent efficacement et peuvent être dupliqués à l'avenir.		
			Compétences	**Indicateurs de performance**
1	3	V.A	Utiliser des indicateurs pour mesurer la performance du programme de protection des données personnelles.	Déterminer les indicateurs adéquats concernant les différents objectifs et analyser les données collectées par le biais des indicateurs (par exemple, tendances, retour sur investissement, résilience commerciale, modèle de maturité relatif à la protection des données personnelles).
				Collecter les indicateurs afin de lier les activités de formation et de sensibilisation aux réductions des événements de protection des données personnelles et améliorer constamment le programme de protection des données personnelles en fonction des indicateurs collectés.
1	3	V.B	Auditer le programme de protection des données personnelles.	Comprendre les types, les objectifs et les cycles de vie des audits en évaluant l'efficacité des contrôles dans l'ensemble des opérations, systèmes et processus de l'organisation.
				Sélectionner les formes de surveillance applicables en fonction des objectifs du programme (par exemple, audits, contrôles, sous-traitants) et surveiller la conformité en auditant les politiques, les contrôles et les normes en matière de protection des données personnelles, notamment par rapport aux normes industrielles et aux modifications réglementaires et/ou législatives.
3	5	V.C	Gérer l'évaluation continue du programme de protection des données personnelles.	Mener des évaluations des risques des systèmes, applications, processus et activités.
				Comprendre l'objectif et le cycle de vie de chaque type d'évaluation (par exemple, PIA, AIPD, TIA, LIA, PTA).
				Mettre en œuvre une atténuation des risques et communiquer avec les parties prenantes internes et externes après des fusions, acquisitions et cessions.
				S'assurer que l'utilisation de l'IA est éthique, impartiale et conforme aux attentes en matière de minimisation des données et de limitation des finalités et est conforme aux réglementations et/ou aux lois sur la protection des données personnelles.

MIN.	MAX.	Thème VI : Cycle de vie opérationnel du programme de protection des données personnelles : Réponse aux demandes et incidents		
10	14	**Le Thème VI – Cycle de vie opérationnel du programme de protection des données personnelles : Réponse aux demandes et incidents** documente les activités impliquées pour réagir aux incidents de protection des données personnelles ainsi que les droits des personnes concernées. Sur la base des lois et réglementations territoriales, sectorielles et industrielles applicables, les organisations doivent garantir des processus adéquats concernant les demandes d'informations, les droits relatifs à la protection des données personnelles et les réponses aux incidents.		
		Compétences		**Indicateurs de performance**
5	7	VI.A	Répondre aux demandes d'accès des personnes concernées et aux droits relatifs à la protection des données personnelles.	S'assurer que les notices d'information relatives aux données à caractère personnel et politiques de confidentialité sont transparentes et expliquent clairement les droits des personnes concernées.
				Se conformer aux politiques de confidentialité l'organisation concernant le consentement (par exemple, les retraits de consentement, des demandes de rectification, les objections au traitement, l'accès aux données et les réclamations).
				Comprendre et se conformer aux législations établies au niveau international, fédéral et national concernant les droits des personnes concernées de contrôler leurs informations personnelles (par exemple, RGPD, HIPAA, CAN-SPAM, FOIA, CCPA/CPRA).
3	5	VI.B	Appliquer les procédures de l'organisation en matière de gestion et de réponse aux incidents.	Mener une évaluation des risques concernant l'incident.
				Mettre en œuvre des activités de confinement.
				Identifier et mettre en œuvre des mesures correctives.
				Communiquer avec les parties prenantes conformément aux exigences juridictionnelles, globales et commerciales.
				Impliquer l'équipe chargée de la protection des données personnelles afin de passer en revue les faits, de déterminer les actions et d'exécuter des plans.
				Tenir un registre des incidents et des documents en rapport avec l'incident.
1	3	VI.C	Évaluer et modifier le plan actuel de gestion des incidents.	Procéder à des évaluations postérieure à l'incident pour améliorer l'efficacité du plan.
				Mettre en œuvre des modifications pour réduire le risque de nouvelles violations.