

Mis à jour le 28/07/2026

S'inscrire

Formation Certification CDPSE

3 jours (21 heures)

Présentation

La certification CDPSE valide une expertise technique en privacy by design, en gouvernance de la vie privée, en gestion des risques et en privacy engineering. Elle s'adresse aux professionnels qui conçoivent, déploient et sécurisent des solutions de protection des données dans des environnements métiers et techniques exigeants.

Notre formation Certification CDPSE vous prépare de manière structurée à l'examen officiel et aux attendus du référentiel ISACA. Vous y consoliderez les notions clés du programme, avec une progression pensée pour un public de niveau intermédiaire.

Vous apprendrez à relier les principes de privacy governance, les démarches de privacy risk management and compliance, la maîtrise du data life cycle management et les pratiques de privacy engineering. L'objectif est de vous aider à raisonner comme un candidat prêt pour la certification et comme un praticien capable de sécuriser les traitements de données.

La formation met également l'accent sur la lecture du sujet d'examen, l'analyse des cas d'usage, la consolidation des connaissances transverses et l'entraînement sur des situations proches des questions de certification. Vous serez ainsi mieux armé pour identifier les bons réflexes, prioriser les contrôles et justifier vos choix techniques.

À l'issue de ce parcours, vous disposerez d'une vision claire des domaines évalués, d'une méthode de révision efficace et d'une base solide pour aborder l'examen CDPSE avec confiance.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le périmètre et la structure de l'examen CDPSE.
- Maîtriser les quatre domaines du référentiel ISACA et leurs attendus.
- Appliquer les principes de privacy by design aux architectures et aux processus.
- Identifier les risques, les contrôles et les preuves attendus dans une démarche de conformité.
- Préparer efficacement l'examen grâce à des exercices ciblés et des mises en situation.

Public visé

- Responsable conformité
- Auditeur cybersécurité
- Architecte sécurité
- Data Protection Officer
- Consultant gouvernance des données

Pré-requis

- Connaissances générales en cybersécurité et en gouvernance des données.
- Expérience préalable sur des sujets de privacy, de conformité ou de risque.
- Compréhension des notions de PIA, de data lifecycle et de contrôles de sécurité.
- Lecture courante de documents techniques et réglementaires en anglais.
- Pratique professionnelle dans un environnement impliquant la protection des données personnelles.

Pré-requis techniques

- Un ordinateur récent avec navigateur web à jour et au moins 8 Go de RAM.
- Une connexion Wi-Fi ou Ethernet stable pour les sessions à distance.
- Un micro et un casque fonctionnels pour les classes virtuelles.
- Un lecteur de documents PDF et un outil bureautique compatible Microsoft Office ou équivalent.
- Un compte utilisateur permettant d'accéder aux supports, quiz et exercices de la formation.

Programme de notre formation CDPSE

[Jour 1 - Matin]

Fondamentaux de la certification

- Comprendre le positionnement de CDPSE dans l'écosystème ISACA.
- Identifier les objectifs de l'examen, son format et ses attentes méthodologiques.
- Relier la certification aux enjeux de privacy, de gouvernance et de risque.
- Cartographier les quatre domaines du référentiel et leur poids relatif.
- Adopter une stratégie de préparation adaptée à un niveau intermédiaire.
- Atelier pratique : diagnostic initial des acquis et repérage des axes de progression.

[Jour 1 - Après-midi]

Privacy governance et organisation

- Analyser les principes de privacy governance et leur traduction opérationnelle.
- Étudier les notions de privacy by design, de transparence et de consentement.
- Structurer les rôles, responsabilités et circuits de décision autour de la vie privée.
- Intégrer la gestion des tiers, des sous-traitants et de la chaîne d'approvisionnement.
- Relier politique de confidentialité, documentation et pilotage de programme.
- Atelier pratique : lecture guidée d'un cas de gouvernance et identification des contrôles attendus.

[Jour 2 - Matin]

Risques et conformité

- Définir une démarche de privacy risk management structurée et traçable.
- Identifier les menaces, vulnérabilités et impacts liés aux traitements de données.
- Exploiter les PIA et les évaluations de risques comme outils de décision.
- Comprendre les exigences de conformité, d'auditabilité et de preuves.
- Mettre en place des indicateurs de suivi, de contrôle et de remédiation.
- Atelier pratique : construction d'une grille d'analyse des risques sur un scénario métier.

[Jour 2 - Après-midi]

Cycle de vie des données

- Maîtriser les étapes du data life cycle management depuis la collecte jusqu'à la destruction.
- Définir les règles de classification, d'inventaire et de cartographie des flux.
- Appliquer les principes de minimisation, de limitation d'usage et de qualité des données.
- Gérer la conservation, l'archivage, le partage et les transferts de données.
- Préparer les réponses attendues sur les cas d'usage liés à l'IA et à l'analytique.
- Atelier pratique : reconstitution d'un cycle de vie de données et identification des points de contrôle.

[Jour 3 - Matin]

Privacy engineering et contrôles techniques

- Relier les enjeux de privacy engineering aux architectures applicatives et cloud.
- Étudier les contrôles liés à l'IAM, au chiffrement, au hachage et à la journalisation.
- Comprendre les impacts des API, des services cloud-native et des terminaux.
- Intégrer les pratiques de durcissement, de gestion des correctifs et de supervision.
- Associer les technologies de protection à des cas d'usage concrets de conformité.
- Atelier pratique : analyse d'une architecture technique et repérage des contrôles de protection des données.

[Jour 3 - Après-midi]

Révision et préparation à l'examen

- Revoir les notions transverses des quatre domaines avec une logique de synthèse.
- Identifier les pièges récurrents des questions de certification.
- Travailler la méthode d'élimination et de justification des réponses.
- Consolider le vocabulaire clé et les relations entre concepts.
- Préparer un plan de révision personnel pour les dernières semaines avant l'examen.
- Atelier pratique : quiz de validation et correction commentée sur un mini-sujet type certification.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.