

Mis à jour le 28/07/2026

S'inscrire

Formation Certification CRISC

4 jours (28 heures)

Présentation

La certification CRISC d'ISACA valide une expertise reconnue en gestion des risques IT, gouvernance et contrôles de sécurité. Elle s'adresse aux professionnels qui veulent structurer une démarche de risque robuste, alignée sur les attentes du terrain et de l'examen officiel.

Notre formation Certification CRISC vous prépare de manière ciblée à l'examen officiel, avec une progression pensée pour consolider les notions clés du référentiel et les appliquer à des cas concrets.

Vous apprendrez à analyser les risques métiers, à évaluer les menaces et vulnérabilités, à définir des réponses au risque et à piloter les indicateurs et les reportings attendus dans un contexte de gouvernance.

La formation met également l'accent sur la compréhension des quatre domaines CRISC, la logique de l'examen, les types de questions et les réflexes méthodologiques pour répondre avec précision et efficacité.

À l'issue de ce parcours, vous disposerez d'une vision structurée de la gouvernance des risques, des contrôles et des bonnes pratiques ISACA, afin d'aborder l'examen avec méthode et confiance.

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

Objectifs

- Comprendre le périmètre et les attentes de la certification CRISC.

- Maîtriser les quatre domaines du référentiel officiel et leur articulation.
- Analyser les risques, les impacts et les priorités de traitement.
- Choisir des réponses au risque adaptées aux enjeux de gouvernance et de conformité.
- Se préparer efficacement au format de l'examen avec des mises en situation ciblées.

Public visé

- Auditeur cybersécurité
- Risk manager
- Responsable SSI
- Consultant GRC
- Contrôleur interne

Pré-requis

- Connaissances de base en cybersécurité et en gestion des risques.
- Expérience professionnelle dans un environnement IT, audit ou sécurité.
- Compréhension des enjeux de gouvernance et de conformité.
- Pratique des notions de contrôle interne et de gestion des incidents.

Pré-requis techniques

- Un ordinateur récent avec navigateur à jour et affichage confortable pour les supports de cours.
- Une connexion Wi-Fi ou Ethernet stable pour les sessions à distance et les échanges en direct.
- Un micro et un casque ou des écouteurs pour garantir une bonne qualité audio en visioconférence.
- Un environnement bureautique standard avec PDF, Excel ou équivalent pour les exercices et les corrigés.
- Si la session est animée à distance, un second écran peut faciliter le suivi des supports et des ateliers.

Programme de notre formation CRISC

[Jour 1 - Matin]

Fondamentaux de la certification

- Présentation de la certification CRISC, de ses enjeux et de sa logique de valorisation professionnelle.
- Lecture du référentiel officiel, des quatre domaines et des compétences évaluées à l'examen.
- Positionnement de l'approche gouvernance, risque, contrôle et reporting.
- Cartographie des attentes de l'examen et des pièges de compréhension les plus fréquents.
- Organisation de la préparation sur quatre jours, avec méthode de révision et priorités d'apprentissage.
- Atelier pratique : diagnostic initial du niveau et repérage des domaines à renforcer.

[Jour 1 - Après-midi]

Gouvernance et contexte métier

- Comprendre la place de la gouvernance des risques dans l'organisation et ses liens avec la stratégie.
- Identifier les rôles, responsabilités et lignes de défense dans un dispositif de maîtrise des risques.
- Relier les objectifs métiers, les politiques internes et les exigences réglementaires.
- Analyser l'appétence au risque, la tolérance au risque et les critères de décision associés.
- Étudier les notions de cadre de contrôle, de priorisation et de pilotage.
- Atelier pratique : lecture guidée d'un cas d'entreprise et qualification des enjeux de gouvernance.

[Jour 2 - Matin]

Identification et évaluation des risques

- Maîtriser les étapes d'identification des actifs, menaces, vulnérabilités et scénarios de risque.
- Différencier les approches qualitatives et quantitatives de l'évaluation des risques.
- Apprécier l'impact, la vraisemblance et le niveau de criticité dans un contexte métier.
- Structurer une analyse de risque cohérente avec les objectifs de l'organisation.
- Comprendre les liens entre risque inhérent, risque résiduel et niveau acceptable.
- Atelier pratique : construction d'une matrice de risque à partir d'un scénario réaliste.

[Jour 2 - Après-midi]

Réponse au risque et traitement

- Comparer les stratégies de traitement du risque, accepter, réduire, transférer ou éviter.
- Définir des contrôles adaptés selon le coût, l'efficacité et le niveau de risque résiduel visé.
- Intégrer la notion de plan d'actions, de priorisation et de suivi dans le temps.
- Évaluer les effets attendus des mesures de sécurité et de gouvernance.
- Relier le traitement du risque aux exigences de continuité et de résilience.
- Atelier pratique : choix argumenté d'une stratégie de traitement pour plusieurs cas d'usage.

[Jour 3 - Matin]

Contrôles et surveillance

- Comprendre le rôle des contrôles dans la réduction et la maîtrise du risque.
- Identifier les contrôles préventifs, détectifs et correctifs dans un dispositif opérationnel.
- Relier les mécanismes de surveillance aux exigences de pilotage et d'alerte.
- Analyser les indicateurs de performance et de risque pour suivre l'efficacité des mesures.
- Étudier la documentation attendue, les preuves et la traçabilité des contrôles.
- Atelier pratique : lecture d'un dispositif de contrôle et repérage des écarts de couverture.

[Jour 3 - Après-midi]

Reporting et communication

- Structurer un reporting risque lisible, utile et adapté aux décideurs.
- Présenter les résultats d'analyse avec les bons niveaux de synthèse et de détail.
- Adapter le discours aux parties prenantes, direction, métiers, audit et sécurité.
- Comprendre la place des tableaux de bord, des alertes et des plans de remédiation.
- Réviser les notions de conformité, d'escalade et de communication de crise.
- Atelier pratique : rédaction d'une synthèse de risque destinée à un comité de pilotage.

[Jour 4 - Matin]

Préparation ciblée à l'examen

- Revoir les points clés des quatre domaines avec une logique de mémorisation active.
- Identifier les formulations récurrentes dans les questions CRISC et les bonnes pratiques de lecture.
- Travailler les arbitrages entre réponses proches et la justification du meilleur choix.
- Renforcer la gestion du temps et la méthode d'élimination des distracteurs.
- Consolider le vocabulaire ISACA et les notions fréquemment testées.
- Atelier pratique : série de questions d'entraînement corrigées et débriefées en groupe.

[Jour 4 - Après-midi]

Révision finale et examen blanc

- Effectuer une revue finale des notions prioritaires et des erreurs classiques.
- Réaliser un examen blanc dans des conditions proches de la certification.
- Analyser les réponses, les réflexes attendus et les points de vigilance par domaine.
- Construire une stratégie personnelle de révision jusqu'au passage de l'examen.
- Préparer les derniers ajustements méthodologiques et la gestion du stress.
- Atelier pratique : examen blanc complet suivi d'une correction commentée.

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.