Quelle certification ISACA vous convient le mieux ?

	Domaines clés	Étape de carrière	Postes typiques pour les titulaires de ces certifications	Expérience requise	Laboratoires inclus	Pré-requis recommandé	Se complète bien avec
CISA Certified Information Systems Auditor. An ISACA® Certification	• Processus d'audit des systèmes d'information • Gouvernance et gestion des TI • Acquisition, développement et mise en œuvre de systèmes d'information • Exploitation des systèmes et résilience operationnelle • Protection des actifs informationnels	• Intermédiaire	• Auditeur TI • Analyste en conformité • Analyste en gestion des risques • Consultant TI • Gestionnaire de programme	Cinq ans d'expérience professionnelle dans l'audit, l'environnement de contrôles ou la sécurité des systèmes d'information	Non	• IT Audit Fundamentals	• AAIA • CDPSE • Cybersecurity Fundamentals • Cloud Auditing
AAIA Advanced in AI Audit. An ISACA® Certification	• Gouvernance & risques liés à l'IA • Opérations basées sur l'IA • Outils et techniques d'audit de l'IA	• Intermédiaire • Avancé	• Auditeur TI Senior • Gestionnaire de risque • Gestionnaire de l'information • CISO/CRO	Aucune expérience supplémentaire requise. Détenir une certification CISA, CPA ou CIA et de satisfaire aux exigences associées	Non	Pré-requis: • CISA, CPA or CIA	• CDPSE
CISM Certified Information Security Manager. An ISACA® Certification	• Gouvernance de la SI • Gestion des risques de la SI • Programme de la SI • Gestion d'incident	• Intermédiaire • Avancé	• Conseiller en architecture TI • Analyste en sécurité • Responsable de la sécurité des données • Directeur de la sécurité et de la conformité • Vice-président / Vice-président adjoint – Sécurité de l'information • CIO/CISO/	Plus de cinq ans d'expérience en sécurité informatique technique et en cybersécurité	Non	• CISA • CRISC	• CGEIT
AAISM Advanced in AI Security Management. An ISACA® Certification	• Gouvernance & et gestion des programmes IA • Gestion des risques liés à l'IA • Technologies et contrôles de l'IA	• Intermédiaire • Avancé	• Responsable de la SI • Responsable cybersécurité • Responsable de la sécurité de l'IA • Responsable de la sécurité des données • Directeur en conformité et sécurité • VP - Sécurité de l'information • CIO/CISO/CTO	Aucune expérience supplémentaire requise. Détenir une certification CISM ou CISSP et de satisfaire aux exigences associées.	Non	Pré-requis: • CISM or CISSP	• CDPSE • Hands-on AI Courses
CRISC Certified in Risk and Information Systems Control. An ISACA® Certification	• Gouvernance d'entreprise des TI • Évaluation des risques TI • Réponse et signalement des risques • Technologies de l'information & sécurité	• Intermédiaire • Avancé	• Gestionnaires des risques et sécurité • Analyste d'affaires ou SI • Responsable de la SI • Responsable des opérations • CISO/CCO	Une à trois années d'expérience dans le domaine des risques informatiques et/ou de la sécurité et de l'audit	Non	Candidats en début de carrière: • IT Risk Fundamentals • CISA	• CISM • CGEIT
CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification	• Gouvernance d'entreprise des TI • Ressources TI • Réalisations des bénéfices • Optimisation des risques	• Profesionnel TI hautement expérimenté • Conseillers auprès de la haute direction et du conseil d'administration	• CIO/CTO/CISO • Auditeur TI Senior • Leader de pratique —Gouvernance TI, risque et conformité • Spécialiste de la gestion des risques et conformité • Gestionnaire de conformité SI • Consultant en gouvernance des risques	Plus de cinq ans d'expérience dans les domaines CGEIT: • Gouvernance TI • Ressources TI • Réalisation de bénéfices • Optimisation du risque	Non	• CISA • CRISC • CISM	• COBIT
CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification	• Gouvernance de la confidentialité • Gestion des risques liés à la protection de la vie privée et conformité • Gestionnaire du cycle de vie des données • Ingénierie de la confidentialité	• Intermédiaire • Expérience dans l'implnatation de contrôles liés à la confidentialité	• Analyste des données • Conseiller en ingénierie des données • Conseiller en architecture de solutions de protection des données • Responsable de la protection des données • Consultant TI	Expérience de trois à cinq ans dans au moins deux domaines: • Gouvernance de la protection des données • Architecture de protection des données • Cycle de vie des données	Non	• CISA • CRISC • Data Science Fundamentals	• ISACA Privacy Labs
CCOA Certified Cybersecurity Operations Analyst. An ISACA® Certification	• Principes technologiques • Détection & réponse aux incidents • Principes et risques liés à la sécurisation des actifs • Procédures, techniques et tactiques adverses	• Débutant • Intermédiaire	• Analyste cybersécurité • Analyste SOC • Analyste en gestion des vulnérabilités • Analyste en réponse aux incidents • Support SOC Niveau 1 & 2	Professionnels de la cybersécurité ayant 2 à 3 ans d'expérience	Oui: 13	• Cybersecurity Fundamentals	• CISM

isaca.org/credentialing

Crédits de formation professionnelle continue (CPE):

Les CPE (formation professionnelle continue) sont essentielles au maintien de votre certification.

Les CPE sont facultatifs la première année suivant la certification initiale.

Pour maintenir votre certification, à partir de la deuxième année, vous devez obtenir et déclarer les crédits suivants:

- Un minimum de 20 CPEs par année
- Un minimum de 120 CPEs sur une période de trois ans
- Respect du code de déontologie ISACA et de l'éthique profesionnel

Les politiques complètes de CPE sont disponibles sur isaca.org

ISACA®

©2026 ISACA. All Rights Reserved. 09-2026