+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 03/10/2025

S'inscrire

Formation CGRC - Certified in Governance, Risk and Compliance

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Le Certified in Governance, Risk and Compliance (CGRC) est une certification internationale délivrée par ISC², destinée aux professionnels de la cybersécurité souhaitant renforcer leurs compétences en gouvernance, gestion des risques et conformité.

Cette formation couvre le NIST Risk Management Framework (RMF) et les obligations liées à des référentiels.

Notre formation CGRC vous permettra de traduire les exigences réglementaires en pratiques opérationnelles : sélection et évaluation des contrôles, autorisation des systèmes et surveillance continue.

Vous apprendrez à piloter la conformité au sein de votre organisation et à intégrer la GRC dans la stratégie de cybersécurité.

À l'issue, vous serez en mesure de gérer des projets de conformité de bout en bout, d'accompagner des audits internes/externes, de structurer la gouvernance autour des enjeux de sécurité et de vous préparer efficacement à la certification CGRC.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable des ressources officielles ISC² et privilégie une approche pratique et opérationnelle.

Objectifs

- Comprendre les fondamentaux gouvernance-risque-conformité.

- Mettre en œuvre le NIST RMF et autres cadres.
- Identifier, évaluer et mitiger les risques.
- Sélectionner, déployer et auditer les contrôles.
- Piloter la conformité réglementaire.
- Se préparer efficacement à la certification CGRC.

Public visé

- CISO/RSSI
- Auditeurs IT
- Risk managers
- Consultants GRC
- Chefs de projet sécurité

Pré-requis

- Notions de base en sécurité de l’information
- Familiarité avec la gestion des risques
- Une première expérience audit/conformité est recommandé

Programme de formation CGRC – Certified in Governance, Risk and Compliance

[Jour 1 - Matin]

Introduction à la gouvernance, au risque et à la conformité

- Définir la GRC et son rôle en cybersécurité
- Panorama des référentiels : ISO 27001, NIST RMF, COBIT, GDPR
- Chaîne Gouvernance - Risque - Conformité et impacts business
- Rôles des parties prenantes (Board, CISO/RSSI, DPO, métiers)
- Livrables attendus et périmètre formation
- Atelier pratique : Cartographier les parties prenantes d’un programme GRC.

[Jour 1 - Après-midi]

Cadres réglementaires et normatifs

- Lois vs normes vs référentiels : obligations et « due care »
- Réglementations clés : GDPR, HIPAA, PCI-DSS, eIDAS, DORA
- Choisir un cadre d’alignement adapté à son secteur
- Rôle des autorités et audits de conformité
- Stratégie d’alignement réglementaire et gouvernance

- Atelier pratique : Identifier les obligations applicables à un cas d’usage.

Gestion des risques en cybersécurité

- Concepts : menaces, vulnérabilités, risques, appétence
- Méthodes : ISO 27005, EBIOS RM, NIST SP 800-30
- Échelles probabilité × impact et critères d’acceptation
- Prioriser les actifs et scénarios critiques
- Traitements : réduction, acceptation, transfert, évitement
- Atelier pratique : Construire une matrice de risques.

[Jour 2 - Matin]

Cycle de vie du NIST RMF

- Étapes : Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor
- Correspondances avec ISO 27001 et gouvernance
- Définir la portée et les limites du système
- Intégration dans les processus SI
- Traçabilité des décisions de risque
- Atelier pratique : Modéliser un RMF sur un cas organisation.

[Jour 2 - Après-midi]

Gouvernance et responsabilités

- Redevabilité et ségrégation des rôles
- Rôles CISO/RSSI, DPO, métiers, comités
- Modèles d’organisation
- Politique sécurité, charte et processus
- Indicateurs GRC et pilotage
- Atelier pratique : Définir une gouvernance cible.

Sélection des contrôles de sécurité

- Contrôles préventifs, détectifs, correctifs
- Cartographie des risques - contrôles
- Cadres de contrôle
- Critères d’efficacité et coûts
- Équilibrer les contrôles pour éviter les excès ou les lacunes
- Atelier pratique : Sélectionner des contrôles pour un scénario.

[Jour 3 - Matin]

Mise en œuvre et documentation

- Plan d’implémentation et gestion du changement
- Évidences de conformité et « trace d’audit »
- Rédiger le SSP (System Security Plan)
- Procédures, normes et guides opérationnels
- Suivi d’avancement et de maturité
- Atelier pratique : Créer un mini-SSP.

[Jour 3 - Après-midi]

Évaluation et audit

- Objectifs d’audit et indépendance
- Méthodes : tests, interviews, revue documentaire
- Plan d’actions correctives (CAPA)
- Outils et checklists d’évaluation
- Rapports et restitution aux instances
- Atelier pratique : Simuler un audit interne.

Autorisation et acceptation du risque

- Rôle des autorités d’autorisation (AO/DAA)
- Dossier d’accréditation et preuves
- Conditions, limites et responsabilités
- Cas Cloud vs On-Prem
- Maintien de l’autorisation dans le temps
- Atelier pratique : Schéma de cycle d’autorisation.

[Jour 4 - Matin]

Surveillance continue

- Capteurs, indicateurs et KRI/KPI
- Automatisation et tableaux de bord
- Alignement PDCA et amélioration continue
- Gestion des dérogations et écarts
- Rôles opérationnels
- Atelier pratique : Construire un dashboard de conformité.

[Jour 4 - Après-midi]

Gestion des incidents et conformité

- Chaîne détection ? réponse ? rétablissement
- Exigences de notification (ex. RGPD)

- Post-mortem, RCA et actions correctives
- Interaction techniques, juridiques, communication
- Lien PCA/PRA et obligations
- Atelier pratique : Simuler une notification d’incident.

Gouvernance de la donnée et confidentialité

- Privacy by design/by default
- Base légale, registres et DPIA
- Transferts internationaux et clauses contractuelles
- Données sensibles et minimisation
- Gouvernance data et sécurité
- Atelier pratique : Cartographier un traitement sensible.

[Jour 5 - Matin]

Conformité organisationnelle et conduite du changement

- Comités, politiques et procédures
- Gestion documentaire et archivage
- Plan de formation et sensibilisation
- Mesure de maturité et roadmaps
- Alignement avec ISO / SOC 2
- Atelier pratique : Rédiger une politique sécurité.

[Jour 5 - Après-midi]

Intégration GRC dans les cycles projets/produits

- GRC et DevSecOps : « shift-left » conformité
- Contrôles dans les pipelines
- Critères d’acceptation sécurité
- Contrats, fournisseurs et tier risk
- FinOps et priorisation des contrôles
- Atelier pratique : Checklist GRC pour un produit.

Préparation à l’examen CGRC

- Structure de l’examen et domaines couverts
- Méthodologie de révision et gestion du temps
- QCM types : pièges et techniques d’élimination
- Plan de révision personnalisé
- Ressources officielles (ISC²)
- Atelier pratique : Passage de l'examen blanc + correction.

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.