ACG | Cybersecurity

Parcours GRC

Gouvernance, Risques et Conformité

Catégorie : Gouvernance, Risques et Conformité (GRC)
Durée : 20 Jours (140 heures de formation)
Certification : Parcours Certifiant GRC – Gouvernance, Risques et Conformité
Référence : ACGGRC

Connaissances préalables

- Nécessaires pour suivre le parcours GRC reposent principalement sur une compréhension générale des systèmes d'information et de leur rôle dans l'organisation. Des notions de base en cybersécurité et en gestion des risques sont recommandées. Une première expérience dans la conformité, la gouvernance ou la sécurité de l'information constitue un atout, mais elle n'est pas indispensable pour entreprendre la formation.

Profil des stagiaires

- Le profil des stagiaires attendu regroupe différents professionnels. Ce parcours s'adresse aux responsables et consultants en cybersécurité souhaitant se spécialiser dans la gouvernance, les risques et la conformité, aux auditeurs internes et externes, aux chefs de projets sécurité, ainsi qu'aux experts en conformité réglementaire (RGPD, NIS 2, DORA, etc.). Il concerne plus largement toute personne impliquée dans la mise en place, la gestion ou l'audit d'un SMSI ou d'un dispositif de gouvernance.

Objectifs

- Comprendre les fondamentaux de la gouvernance, de la gestion des risques et de la conformité.
- Acquérir une méthodologie structurée pour évaluer et gérer les risques.
- Savoir mettre en place et piloter un cadre de conformité (ISO 27001, NIS 2, DORA, etc.).
- Développer les compétences nécessaires pour accompagner une organisation dans sa stratégie GRC.

Certification préparée

- Le parcours prépare à plusieurs certifications reconnues, correspondant à chaque module inclus dans le programme. Selon le module choisi, les stagiaires peuvent se préparer aux examens ISO/IEC 27001 Lead Implementer, ISO/IEC 27001 Lead Auditor, CISM, NIS 2 ou DORA. La réussite à ces certifications atteste des compétences acquises et valorise l'expertise des participants dans le domaine de la GRC.

Méthodes pédagogiques

- Alternance d'apports théoriques et de mises en pratique.
- Études de cas concrets issus de situations professionnelles.
- Exercices et travaux dirigés pour ancrer les compétences.
- Utilisation de supports numériques et de documentation officielle.

Formateur

Consultant-formateur expert en Cybersécurité et en GRC

Méthodes d'évaluation des acquis

- Quiz et exercices pratiques tout au long de la formation.
- Études de cas en groupe ou individuelles.
- Simulation d'audit ou de mise en œuvre selon la certification.
- Examen final officiel de certification (QCM, étude de cas ou mise en situation selon le référentiel).

Contenu du cours

Module 1 : Fondements de la cybersécurité

Chapitre 1 : Introduction à la cybersécurité

- Concepts de base de la cybersécurité
- Types de menaces et d'attaques
- Rôles et responsabilités de l'Analyste SOC

Chapitre 2 : Surveillance et détection

- Surveillance en temps réel des journaux et des événements
- Détection d'anomalies
- Corrélation des événements

Module 2 : Analyse des menaces

Chapitre 3 : Analyse Des Menaces

- Évaluation des incidents de sécurité
- Collecte de données forensiques
- Analyse de malware

Chapitre 4 : Outils Et Technologies

- Utilisation d'outils SIEM (Security Information and Event Management)
- Analyse de paquets réseau avec Wireshark
- Utilisation d'outils d'analyse de vulnérabilités

Module 3 : Réponse aux incidents

Chapitre 5 : Gestion Des Incidents De Sécurité

- Planification de la réponse aux incidents
- Coordination des équipes d'intervention
- Communication en cas d'incident

Chapitre 6 : Contaminent et éradication

- Isolation des systèmes compromis
- Élimination des menaces
- Restauration du système

Module 4 : Prévention et amélioration continue

Chapitre 7 : Prévention des menaces

- Mise à jour des politiques de sécurité
- Configuration des systèmes sécurisés
- Sensibilisation à la sécurité

Chapitre 8 : amélioration continue

- Analyse post-incident
- Documentation des incidents
- Mise à jour des procédures et des politiques de sécurité

Exercices Pratiques Et Scénarios D'Entraînement

- Simulations d'incidents de sécurité
- Analyse de cas réels
- Rédaction de rapports d'incidents

Accessibilité de la formation :

ACG Cybersecurity s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap.

Notre réfèrent handicap se tient à votre disposition par mail à referent.handicap@acgcybersecurity.fr pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.