Le Campus Numérique in the Alps

Formation Responsable Gouvernance, Risques et Conformité (GRC)

Formation déployée en partenariat avec CSB School, spécialiste de la cybersécurité

Objectifs de la formation

La formation « Responsable Gouvernance, Risques et Conformité (GRC) » vise à former des professionnels capables d'anticiper et d'encadrer les exigences réglementaires, les enjeux de conformité et les risques opérationnels dans un contexte numérique et stratégique en constante évolution.

Les objectifs professionnels visés sont les suivants :

- **Élaborer une cartographie des risques** en identifiant les menaces juridiques, opérationnelles et numériques, en structurant une démarche de gestion des risques adaptée à l'organisation.
- **Mettre en œuvre un dispositif de conformité réglementaire robuste,** en intégrant les cadres normatifs (RGPD, Sapin II, ISO 27001, NIS2…) dans les processus opérationnels et décisionnels.
- **Piloter la gouvernance des systèmes d'information,** en consolidant les politiques de sécurité, les rôles de responsabilité et les indicateurs de suivi dans une logique d'amélioration continue.
- **Conduire des audits GRC et des contrôles internes,** en produisant des analyses argumentées et des recommandations stratégiques à destination des directions métiers.
- **Accompagner les projets de transformation numérique,** en garantissant leur alignement avec les exigences de conformité, d'éthique, de souveraineté et de durabilité.
- **Animer des démarches de sensibilisation et de formation interne,** en favorisant la culture du risque, la responsabilisation des acteurs et la veille réglementaire partagée.

D'une durée de 10 mois, cette formation professionnalisante de niveau Bac+5 permet d'acquérir une posture d'expert GRC en entreprise, en combinant analyse, pilotage stratégique et mise en œuvre de dispositifs concrets.

Compétences développées

Le programme forme des professionnels capables d'anticiper, détecter, analyser et répondre efficacement aux risques et aux exigences de conformité. Il couvre l'ensemble des méthodes et technologies de gouvernance, de gestion des risques et de conformité, en intégrant les bonnes pratiques de veille, d'audit et de gestion des risques.

Les apprenants développent également des compétences en conception, déploiement et maintien en condition opérationnelle de solutions de gouvernance et de conformité, ainsi qu'en mise en œuvre de plans de remédiation. Une attention particulière est portée à l'analyse des événements de conformité et à la réponse aux incidents dans un environnement de type GRC (Governance, Risk, and Compliance).

En complément, la formation cultive les compétences transversales indispensables en entreprise, telles que la communication en environnement professionnel, le travail en équipe, l'adaptabilité, et la capacité à se former tout au long de la vie grâce à des méthodes d'apprentissage actives orientées vers l'autonomie et la montée en compétences continue.

Compétences développées à l'issue de la formation :

1. Cartographier les risques d'une organisation et piloter des plans de remédiation ;
2. Mettre en œuvre un programme de conformité réglementaire (RGPD, Sapin II, ISO 27001, NIS2...) ;
3. Animer des dispositifs de contrôle interne et produire des reportings pour la direction générale ;
4. Élaborer une stratégie de gouvernance intégrée, incluant la gestion des données, des processus et des parties prenantes ;
5. Accompagner les transformations numériques en garantissant leur conformité éthique, juridique et environnementale.

Méthodes pédagogiques

Le Campus adopte une approche par compétences, les modules de formation étant construits sur la base de compétences à acquérir : savoirs, savoir-faire, savoir-être, outils, méthodologies… Cette approche permet d'assurer une formation professionnalisante avec le développement de compétences opérationnelles correspondant aux exigences des métiers visés.

Le modèle de pédagogie par projet mis en place dans les modules de formation permet de rendre les stagiaires acteurs de la formation et de l'apprentissage. L'autonomie développée dans les modules (e-learning et classes inversées), la transversalité marquée des enseignements et une pratique pédagogique hautement professionnalisante sont au cœur du projet pédagogique.

Modalités d'évaluation et diplôme visé

Formation professionnalisante. La validation de la formation donne lieu à une attestation de compétences de CSB School et du Campus Numérique in the Alps.

La formation vous préparer au passage de la certification ISO 27001 Lead Implementer.

Modalités d'évaluation :

- **Réalisation de livrables professionnels (analyses de risques, plans de conformité, tableaux de bord GRC…) ;**

- **Validation de l'ensemble des compétences vues pendant la formation lors d'une session d'examen sur table**
- **Soutenance d'un mémoire de fin de parcours devant un jury de professionnels ;**
- **Évaluations formatives et mises en situation encadrées par les formateurs.**

Durée de la formation

La formation se décompose en deux phases :

- **6 mois de formation intensive au Campus (805 heures) permettant d'acquérir le socle de compétences techniques et de travail en équipe ;**
- **Mission professionnelle de 4 mois (stage) afin d'élargir et d'approfondir les compétences techniques et les soft skills développées.**

Modalités d'accès et prérequis

Être titulaire d'un diplôme de niveau 6 (Bac+3) ou justifier d'une expérience professionnelle significative dans les domaines de la gestion, du droit, du numérique ou de la cybersécurité.

Les critères de sélection sont basés sur :

- **La motivation et le projet professionnel défini ;**
- **La capacité à travailler en équipe et la bienveillance ;**
- **La maîtrise des fondamentaux du développement informatique ;**
- **La curiosité, l'autonomie et la créativité.**

Processus de sélection :

- **Participation à une réunion d'informations collectives**
- **Envoi d'une lettre de motivation, d'un CV et d'une vidéo pitch**
- **Entretiens de motivation et tests techniques.**

Délais d'accès : la formation débute en moyenne deux mois après l'ouverture des candidatures.

Prix de la formation

Sans reste à charge grâce aux partenaires financeurs de la formation et les fonds de financement de la formation.

Lieux de formation

Campus de Grenoble

Le Totem, 3ème étage

16 boulevard Maréchal Lyautey, 38000 Grenoble

07 50 66 51 51 / audrey.graffagnino@le-campus-numerique.fr

Accessibilité aux personnes en situation de handicap

La formation est accessible aux personnes en situation de handicap, avec une adaptation possible des modalités pédagogiques et d'évaluation. Le Campus Numérique est engagé dans la démarche H+ Formation de la Région Auvergne Rhône-Alpes.

Référentes handicap : Audrey Graffagnino (audrey.graffagnino@le-campus-numerique.fr) / Pauline Lacour (pauline.lacour@le-campus-numerique.fr)

Suites de parcours

La formation, conçue dans une logique de professionnalisation, permet une insertion rapide sur le marché du travail dans les domaines de la cybersécurité, des réseaux et de l'administration des systèmes.

À l'issue du parcours, vous serez en mesure d'occuper des postes tels que :

- Responsable GRC
- Risk Manager / Compliance Officer
- Consultant en gouvernance et conformité
- Responsable audit interne
- Chief Information Security Officer (CISO) junior

Ces fonctions s'exercent dans tous types de structures : grandes entreprises, cabinets de conseil, collectivités, banques, assurances, industries réglementées…

Contenus Pédagogiques

Pour cette formation, un accent fort sera mis sur la différenciation pédagogique. A partir des compétences antérieures des stagiaires et des missions en entreprise, les compétences à développer et les volumes horaires associés seront adaptées.

805 heures de formation		
Positionnement	Bilan, diagnostic et définition du parcours individualisé de formation	**7 heures**
Bloc 1 – Gouvernance et gestion des risques		
Gestion de projet informatique	Spécificités d'un projet informatique, application d'une méthodologie rigoureuse (cycle en V, Agile, DevSecOps) adaptée à la cybersécurité, bonnes pratiques de planification, pilotage et suivi avec des outils de gestion de projet (Gantt, RACI).	**35 heures**

Impact de l'IA sur la cybersécurité	Les enjeux et opportunités que présente l'Intelligence artificielle pour les praticiens de la cybersécurité.	**14 heures**
RGPD et Introduction générale au droit	Fondements et objectifs du RGPD, obligations des organisations, et exercice des droits. Sources du droit, hiérarchie des normes et rôle des institutions de régulation. Cadre juridique des technologies numériques, contrats, propriété intellectuelle, et structures juridiques des entreprises.	**63 heures**
Gestion de la chaine d'approvisionnement en cybersécurité	Assurer la sécurité de sa chaine d'approvisionnement en cybersécurité, les négociations contractuelles, l'évaluation des fournisseurs, la définition et négociation des accords de niveaux de service	**14 heures**
Bloc 2 –infrastructures & architecture		
Introduction aux systèmes d'information et au management des SI	Comprendre l'architecture et le fonctionnement d'un SI. Introduction aux rôles de la DSI, gouvernance IT, bonnes pratiques ITIL, management des risques et cartographie des processus.	**49 heures**
Architecture et sécurité des environnements industriels	Spécificités des environnements industriels (OT), présentation des infrastructures SCADA/DCS, automatisme, programmation des automates, supervision, sécurité des processus critiques.	**42 heures**
Fondamentaux des réseaux et télécommunications	Les réseaux de télécommunications, composants (câblage, équipements), catégories (LAN, WAN, etc.) et topologies. Protocole TCP/IP, modèle OSI, adressage IP, segmentation de réseau, switching, VLAN, routage et algorithmes (Bellman-Ford, Dijkstra). Protection des réseaux.	**63 heures**
Sécurisation des infrastructures Cloud	Risques et bonnes pratiques dans les environnements Cloud (AWS, Azure, GCP) : contrôle des accès, politiques de sécurité, journalisation, conformité et audits.	**21 heures**
Bloc 3 – Sécuriser d'un système d'information		
Stratégie et gouvernance des systèmes d'information	Normes de gouvernance (ISO, ITIL, COBIT). Sécurité des SI : acteurs, cadres de référence, outils de gouvernance et résilience en cybersécurité. Support informatique : gestion des incidents, bonnes pratiques, qualité de service et communication.	**46 heures**

Fondamentaux en cryptographie et sécurité des mails	Cryptographie, stéganographie. Clé de chiffrement, Hardware Secure Module et Key Management System. Cycle de vie des données, protection des données sensibles/critiques, mesures de protection, Data Masking, contrôle d'accès, et Data Loss Prevention.	**28 heures**
SOC - Enjeux et objectifs	Principe d'un SOC. Cartographie des assets, inventaire opérationnel, protection (IT, OT) via des mesures physiques et logiques (antivirus, EDR, licences, sauvegarde, mise à jour). Authentification, gestion des identités et accès (IAM), sécurisation.	**42 heures**
Bloc 4 – Gouvernance et gestion des risques		
Gestion Intégrée des Playbooks SOC et des Risques Cyber	Création et gestion des playbooks de sécurité, définition des rôles, tests et mises à jour, intégration des sources et règles de sécurité. Management des risques cyber, audit et contrôle interne, méthodologies de gestion des risques, sécurité.	**49 heures**
Gestion organisationnelle et financière en cybersécurité	Principes de comptabilité, gestion de budget, ventilation des coûts et impacts financiers de la cybersécurité. Diagnostic organisationnel en cybersécurité, implémentation de politiques, procédures et standards de sécurité.	**70 heures**
Mise en œuvre de la conformité normative en cybersécurité	Utilisation et mise en conformité d'une organisation aux normes et standards de sécurité (ISO, NIST, etc.)	**42 heures**
Mise en œuvre de la conformité réglementaire en cybersécurité	Mise en conformité d'une organisation des lois et réglementations en cybersécurité : RGPD, NIS2, DORA, CRA, export, HDS, etc. Principe de conformité dans la conception "compliance by design".	**63 heures**
Assurer la résilience d'une organisation	Mise en place d'un Plan de Continuité d'Activité (PCA), d'un Plan de Reprise d'Activité (PRA), d'un Plan de Réponse à Incident de Sécurité (PRIS), plan de formation en cybersécurité, sensibilisation en cybersécurité.	**28 heures**
Modules Transversaux		

Numérique responsable et impact de l'IA frugale	Impacts environnementaux et sociétaux du numérique, leviers de réduction de l'empreinte carbone des projets et principes de l'IA frugale pour optimiser la consommation énergétique et réutiliser les algorithmes.	**15 heures**
Relations client / usager	Étude de cas - Maîtriser les étapes et les techniques de la communication client/usager. Identifier les besoins, construire un cahier des charges à partir des demandes client/usager et traduire des résultats d'analyse en recommandations.	**14 heures**
Laïcité, citoyenneté et valeurs de la République	Comprendre les principes de la laïcité, de la citoyenneté et des valeurs de la République pour adopter une posture professionnelle respectueuse, favoriser le vivre-ensemble et réagir de manière adaptée aux situations rencontrées.	**4 heures**
Passage certification (ISO 27001 Lead Implementer)	Préparation et passage de la certification PECB - ISO 27001 Lead Implementer	**35 heures**
Techniques de recherche d'emploi	Maîtriser les techniques de recherche d'emploi, les techniques de création d'un profil professionnel numérique ainsi que les stratégies nécessaires pour s'engager dans un processus actif de recherche d'emploi.	**21 heures**
Examens	Passage d'examen pour validation des compétences et remise d'une attestation de compétences	**33 heures**
Bilans	Bilan intermédiaire : point d'étape sur les apprentissages et l'évolution des apprenants, identification des difficultés éventuelles et ajustement des méthodes pédagogiques. Bilan final : évaluation de l'ensemble du parcours des apprenants et mesure de l'atteinte des objectifs pédagogiques de la formation. Bilan des taux d'insertion dans l'emploi des stagiaires (départs en stage et perspectives d'emploi au terme de la formation). Recueil des impressions des participants sur le contenu, les méthodes et l'animation de la formation, dans une dynamique d'amélioration continue.	**7 heures**