

GRC (Gouvernance, Risques et Conformité) dans le Cloud

3 jours (21 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

2 925 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Produire un audit formel des infrastructures, applications et services Cloud selon les bonnes pratiques et référentiels (ISO 27017, ISO 27018, CSA STAR...)
- Identifier et évaluer les risques liés aux environnements Cloud (IaaS, PaaS, SaaS)
- Concevoir un cadre de gouvernance et de conformité adapté au Cloud (politiques, rôles, processus)
- Etablir un plan de remédiation et de suivi des écarts détectés lors de l'audit.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Responsables GRC et RSSI, auditeurs internes / externes de la sécurité Cloud, architectes et ingénieurs Cloud, consultants en conformité et transformation digitale.

Prérequis

Avoir des connaissances de base des modèles de services Cloud (IaaS, PaaS, SaaS) et des notions de gestion des risques et de référentiels de sécurité (ISO 27001...). Etre familier avec les concepts de sécurité IT (IAM, chiffrement, réseau).

Programme

1 Pendant votre formation

GRC (Gouvernance, Risques et Conformité) dans le Cloud

Jour 1 – Matin

Fondations et préparation de l'audit

- Etat des lieux : enjeux et spécificités de la GRC dans le Cloud
- Panorama des référentiels clés : ISO 27017, ISO 27018, CSA Cloud Controls Matrix

Exemple de travaux pratiques (à titre indicatif)

- Cartographie de votre Footprint Cloud et des responsabilités partagées (Shared Responsibility Model)

Jour 1 – Après-midi

Fondations et préparation de l'audit – Suite

- Elaboration du périmètre d'audit : périmètre IaaS, PaaS et SaaS
- Définition des rôles et responsabilités (Cloud governance)

Exemple de travaux pratiques (à titre indicatif)

- Rédaction d'une charte de gouvernance Cloud et des procédures associées

Jour 2 – Matin

Audit des contrôles techniques et organisationnels

- Audit des contrôles d'identité et d'accès (IAM) : MFA, rôles, politiques de moindre privilège
- Vérification des configurations réseau (CSP native firewalls, VPC / Subnet)

Exemple de travaux pratiques (à titre indicatif)

- Revue de set de politiques IAM et simulation d'attaque en lecture seule

Jour 2 – Après-midi

Audit des contrôles techniques et organisationnels – Suite

- Contrôles de protection des données : chiffrement au repos et en transit, gestion des clés KMS
- Audit des journaux et de la surveillance (CloudTrail, Azure Monitor, Stackdriver)

Exemple de travaux pratiques (à titre indicatif)

- Extraction et analyse de logs pour vérifier la traçabilité des actions

Jour 3 – Matin

Reporting, remédiation et suivi

- Rédaction du rapport d'audit : structure, scoring des écarts, mise en perspective des risques
- Méthodologie de priorisation des remédiations (impact vs effort)

Exemple de travaux pratiques (à titre indicatif)

- Construction d'un tableau de bord GRC Cloud (dashboards, KPIs)

Jour 3 – Après-midi

Reporting, remédiation et suivi – Suite

- Mise en place d'un plan de suivi : calendarisation des revues, indicateurs de conformité continue
- Processus de ré-audit automatisé (scripts, API des CSP)

Exemple de travaux pratiques (à titre indicatif)

- Présentation synthétique devant un comité – constats, plan d'action, KPI de suivi

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 14 décembre 2027 au 16 décembre 2027 (3 jours / 21 heures)

Paris La Défense

Du 14 décembre 2027 au 16 décembre 2027

Paris La Défense

- 14 décembre 2027 9h00 – 16h00
- 15 décembre 2027 9h00 – 16h00
- 16 décembre 2027 9h00 – 16h00