# GRCForce

# Liste de contrôle de la structure de préparation aux audits

1 juillet 2026

grcforce.com/fr/#contact

Practical governance, risk and compliance guidance for European organisations.

Utilisez ce canevas pour vérifier si le périmètre, les preuves, les responsabilités, la cadence et la culture sont suffisamment solides avant l'arrivée de la pression d'un audit.

## Page 1 — Canevas de la structure de préparation aux audits

| Couche | Signification | Contrôle ISO 27001 | Contrôle TISAX | Responsable des preuves | Statut |
|---|---|---|---|---|---|
| Périmètre | Les limites sont claires et correspondent à la réalité | La déclaration de périmètre est à jour et reflète les services, sites et systèmes | Le périmètre d'évaluation correspond aux besoins de protection des données des clients | Responsable SMSI / GRC | Vert / Orange / Rouge |
| Preuves | Les éléments probants sont produits par les opérations normales et non dans l'urgence | Les revues d'accès, décisions de risque et approbations sont horodatées et conservées | Les preuves de chaque objectif de contrôle sont à jour et vérifiables | Responsables de contrôles | Vert / Orange / Rouge |
| Responsabilité | Chaque contrôle a une personne responsable identifiée | Une liste à jour des responsables de contrôles existe | Chaque contrôle TISAX a une personne responsable | Responsable GRC / Risques | Vert / Orange / Rouge |
| Cadence | Les revues ont lieu de manière prévisible et non aléatoire | Les revues de risques, revues de direction et audits internes sont planifiés et réalisés | La préparation TISAX est revue à des intervalles définis | Responsable de programme | Vert / Orange / Rouge |
| Culture | L'organisation remonte les problèmes au lieu de les cacher | Les constats sont communiqués et corrigés de manière transparente | Les surprises sont réduites grâce à un reporting ouvert | Équipe de direction | Vert / Orange / Rouge |

## Page 2 — 10 contrôles de santé critiques

### 1. L'évaluation des risques est à jour

L'évaluation des risques a été réalisée au cours des 12 derniers mois ou après un changement significatif. Les décisions de traitement ont des responsables et des dates.

Statut : Prêt / Travail nécessaire / Non prêt

### 2. La Déclaration d'Applicabilité reflète la réalité

La SoA est revue, justifiée, approuvée et étayée par des preuves de mise en œuvre.

Statut : Prêt / Travail nécessaire / Non prêt

### 3. Le programme d'audit interne fonctionne

Un calendrier annuel d'audit interne existe, il est respecté et les constats antérieurs sont clôturés avec des preuves.

Statut : Prêt / Travail nécessaire / Non prêt

### 4. La revue de direction a eu lieu

Les procès-verbaux, décisions et actions formels de la revue de direction sont documentés et conservés.

Statut : Prêt / Travail nécessaire / Non prêt

### 5. Les politiques sont reliées aux pratiques
Les politiques principales sont revues selon le cycle prévu et correspondent à la manière dont le travail est réellement effectué aujourd'hui.

Statut : Prêt / Travail nécessaire / Non prêt

### 6. Les revues d'accès sont étayées par des preuves
Des revues formelles des accès sont réalisées pour les systèmes critiques et les preuves sont conservées à la source.

Statut : Prêt / Travail nécessaire / Non prêt

### 7. Les contrôles fournisseurs sont maintenus
Les fournisseurs critiques sont évalués selon le cycle défini et l'exposition aux sous-traitants ultérieurs est documentée.

Statut : Prêt / Travail nécessaire / Non prêt

### 8. Les registres d'incidents sont exacts et complets
Le registre des incidents est à jour et revu, et les circuits d'escalade ont été testés.

Statut : Prêt / Travail nécessaire / Non prêt

### 9. Les objectifs sont suivis et pertinents
Les objectifs de sécurité comportent des cibles mesurables et sont revus par la direction.

Statut : Prêt / Travail nécessaire / Non prêt

### 10. Les actions correctives sont clôturées
Les éléments ouverts ont des responsables identifiés, une cause racine, des dates cibles et des critères de preuve pour la clôture.

Statut : Prêt / Travail nécessaire / Non prêt

## Page 3 — Comment utiliser cette liste

### Évaluez votre situation actuelle
Parcourez honnêtement le canevas et la liste en 10 points avec l'équipe responsable du périmètre SMSI ou TISAX.

### Priorisez les points faibles
Concentrez-vous d'abord sur les lacunes susceptibles de provoquer une non-conformité majeure, une inquiétude client ou une piste de preuve insuffisante.

### Attribuez des responsables et des échéances
Chaque élément ouvert doit avoir un responsable, une date de clôture réaliste et une attente précise en matière de preuve.

### Réalisez une revue 30 jours avant l’audit

Réévaluez la situation 30 jours avant l’audit. Les éléments toujours non prêts nécessitent une décision d’escalade.

### Maintenez la liste active chaque trimestre

Utilisez-la entre les audits afin que la préparation reste intégrée au modèle opérationnel.

## Points de défaillance courants

| Défaillance | Manifestation | Action corrective |
|---|---|---|
| Dérive des politiques | Les politiques ne correspondent plus aux pratiques | Attribuer des responsables et revoir chaque trimestre |
| Preuves produites uniquement pour l’audit | Des captures et dossiers sont créés pendant la préparation | Intégrer les preuves aux flux de travail normaux |
| Actions correctives ouvertes | Les constats sont reconnus mais non clôturés | Attribuer des responsables, dates et critères de preuve |
| Décalage du périmètre | Le périmètre du certificat ne correspond plus aux opérations | Revoir chaque année et après un changement majeur |

## Étape suivante avec GRCForce

Pour évaluer votre programme à l’aide de cette liste, demandez une Revue de Préparation aux Audits de 30 minutes sur https://grcforce.com/fr/#contact.