GRCForce

Guide pratique d’intégration réglementaire européenne

24 juin 2026

grcforce.com/fr/#contact

Practical governance, risk and compliance guidance for European organisations.

Un modèle opérationnel unique pour NIS2, DORA, ISO 27001 et TISAX

Un canevas pratique destiné aux organisations européennes qui ont besoin d'une seule colonne vertébrale de gouvernance plutôt que de quatre programmes de conformité distincts.

Objectif : Intégrer NIS2, DORA, ISO 27001 et TISAX dans un modèle opérationnel unique afin de réduire les preuves en double, le reporting fragmenté et les programmes locaux parallèles.

Public visé : CISOs, responsables GRC, directeurs des risques et responsables de la conformité d'organisations européennes moyennes ou grandes opérant dans plusieurs pays.

Positionnement : Définir une philosophie de contrôle commune, puis documenter des adaptations locales uniquement lorsque la législation ou les orientations du régulateur diffèrent réellement.

Canevas d'intégration réglementaire

Cartographiez chaque domaine de contrôle une seule fois, puis définissez la base commune et les adaptations justifiées.

Domaine	NIS2	DORA	ISO 27001	TISAX
Gouvernance	Responsabilité du conseil, supervision de la direction et clarté des rôles	Responsabilité de l'organe de direction sur le risque TIC et la résilience	Engagement de la direction, périmètre du SMSI et responsabilité des contrôles	Gouvernance de la sécurité de l'information au service de la confiance dans le secteur automobile
Évaluation des risques	Mesures de gestion des risques pour les entités essentielles et importantes	Cadre de gestion du risque TIC et connaissance des scénarios	Méthodologie d'évaluation et de traitement des risques	Classification des risques alignée sur les attentes des partenaires
Notification des incidents	Classification des incidents significatifs et délais de notification	Classification, escalade et notification des incidents TIC majeurs	Processus de gestion des incidents, preuves et amélioration	Traitement des incidents de sécurité et logique de notification des clients
Risque lié aux tiers	Supervision du risque de sécurité des fournisseurs et prestataires	Cycle de vie du risque lié aux tiers TIC et discipline du registre	Contrôles des relations fournisseurs et preuves d'assurance	Contrôles fournisseurs inclus dans le périmètre TISAX
Tests	Tests de sécurité proportionnés au risque et à la criticité	Tests de résilience opérationnelle numérique et remédiation	Audit interne, surveillance et tests de contrôle	Preuves d'évaluation et remédiation guidée par la maturité
Documentation et preuves	Politiques, mesures et preuves démontrant la diligence raisonnable	Registres, rapports, résultats de tests et preuves destinées au conseil	Enregistrements du SMSI, preuves de contrôle et pistes d'audit	Artefacts prêts pour l'évaluation et dossiers de preuves
Adaptations locales	Transposition nationale et attentes de l'autorité compétente	Attentes sectorielles et prudentielles lorsqu'elles s'appliquent	Périmètre local de certification ou exigences juridiques complémentaires	Exigences automobiles propres au client ou au marché

Comment utiliser le guide

1. Sélectionnez un domaine de contrôle, par exemple le contrôle des accès, la notification des incidents ou la gouvernance des fournisseurs.
2. Recensez les obligations actuelles de chaque réglementation ou référentiel.
3. Définissez une politique de base unique et un ensemble de contrôles satisfaisant l'exigence la plus stricte.
4. Documentez les adaptations locales uniquement lorsque la loi, les orientations du régulateur ou les attentes du client diffèrent réellement.
5. Convenez d'une preuve une seule fois, rattachez-la à tous les référentiels et réutilisez-la.

Anti-modèles courants à éviter

- Quatre modèles d’évaluation des risques distincts
- Des définitions d’incident différentes selon la réglementation
- Des équipes locales créant des politiques parallèles plutôt que des adaptations
- Des programmes statiques qui ne réexaminent jamais les correspondances lorsque les orientations changent

Étape suivante

Utilisez ce canevas lors d’un court atelier d’intégration réglementaire. Pour évaluer votre modèle actuel, contactez GRCForce pour une Revue ciblée de l’Intégration Réglementaire via https://grcforce.com/fr/#contact.

GRCForce | Gouvernance, risque et conformité pratiques pour les organisations européennes | grcforce.com