GRCForce

Liste de contrôle pour l’audit des contrats fournisseurs au regard de NIS2 et DORA

15 juin 2026

grcforce.com/fr/#contact

Practical governance, risk and compliance guidance for European organisations.

Publié le 15 juin 2026 | GRCForce

Utilisez cette liste pour vérifier si les contrats conclus avec vos fournisseurs critiques soutiennent une résilience opérationnelle réelle, et pas seulement la finalisation du processus d'achat.

Elle est destinée aux organisations qui examinent des relations importantes avec des tiers dans les domaines des TIC, du cloud, du SaaS, des services managés et d'autres prestations entrant dans le champ de NIS2 et/ou DORA.

Comment utiliser cette liste

Pour chaque clause ou question ci-dessous, sélectionnez l'une des options suivantes :

- En place et adéquate
- Partiellement couverte
- Absente
- Nécessite une revue juridique

Un contrat n'a pas besoin d'une rédaction parfaite dès le premier jour. En revanche, les lacunes doivent avoir un responsable clairement identifié et faire l'objet d'une décision quant à l'acceptabilité du risque.

12 clauses et questions contractuelles à examiner

1. Droit d'audit

Le contrat confère-t-il à votre organisation un droit concret d'obtenir des éléments probants d'audit, d'examiner des rapports de contrôle et de demander des actions de suivi lorsque des lacunes significatives sont identifiées ?

Pourquoi c'est important : si vous ne pouvez pas tester ou examiner les contrôles du fournisseur de manière crédible, vous reposez sur la confiance plutôt que sur une assurance vérifiable.

2. Obligations de sécurité

Les obligations minimales de sécurité du fournisseur sont-elles clairement énoncées, notamment en matière de protection des systèmes, de contrôle des accès, de gestion des vulnérabilités, de journalisation, de sauvegarde, de reprise et de gestion sécurisée des changements ?

Pourquoi c'est important : les références vagues à une « sécurité conforme aux normes du secteur » sont généralement trop faibles lorsqu'un incident survient.

3. Délai de notification des incidents

Le contrat définit-il dans quel délai le fournisseur doit vous notifier un incident de sécurité, une interruption de service, une violation de données ou une défaillance matérielle d'un contrôle ?

Pourquoi c'est important : des expressions telles que « sans retard injustifié » sont souvent trop imprécises pour les services critiques. Vous avez besoin de délais opérationnellement exploitables.

4. Contrôle des accès et des identités

Le contrat définit-il la gestion des accès privilégiés, la révision des comptes et la révocation des accès lorsqu'un membre du personnel quitte l'organisation ou lorsque le service prend fin ?

Pourquoi c’est important : de nombreux incidents chez les fournisseurs commencent par des accès administratifs insuffisamment protégés et une mauvaise hygiène des identités.

5. Transparence sur la localisation et le traitement des données

Pouvez-vous déterminer où vos données sont traitées, stockées, sauvegardées et consultées, y compris en cas de recours à des sous-traitants ou à des équipes d’assistance situées à l’étranger ?

Pourquoi c’est important : la résilience et l’exposition réglementaire sont plus difficiles à maîtriser lorsque le traitement des données manque de transparence.

6. Contrôle des sous-traitants

Le fournisseur doit-il obtenir votre approbation, ou au minimum vous informer au préalable, avant de désigner des sous-traitants importants susceptibles d’affecter la prestation, la sécurité ou la conformité ?

Pourquoi c’est important : le risque de quatrième partie apparaît souvent au travers de dépendances cachées que vous n’avez jamais évaluées.

7. Continuité d’activité et reprise après sinistre

Le contrat exige-t-il que le fournisseur maintienne et teste des dispositifs de continuité d’activité et de reprise après sinistre proportionnés à la criticité du service ?

Pourquoi c’est important : la résilience n’est pas une déclaration. Elle nécessite des objectifs de reprise, des procédures testées et des éléments probants.

8. Niveaux de service liés à la criticité

Les niveaux de service, les délais de reprise, les engagements d’assistance et les circuits d’escalade sont-ils alignés sur l’importance réelle du service pour l’activité ?

Pourquoi c’est important : de nombreux contrats sont rédigés comme si le service était courant alors qu’il soutient un processus critique.

9. Restitution, extraction et suppression des données

Le contrat précise-t-il comment vos données seront restituées, dans quel format, dans quel délai, à quel coût et comment les données résiduelles seront supprimées à la sortie ?

Pourquoi c’est important : si les conditions de sortie ne sont pas claires, vous risquez de vous retrouver dans une situation de dépendance opérationnelle.

10. Clauses de changement de contrôle et de modification substantielle

Le contrat vous protège-t-il si le fournisseur est acquis, modifie substantiellement son modèle de service, déplace ses opérations ou change de sous-traitants clés ?

Pourquoi c’est important : le risque fournisseur peut changer du jour au lendemain sans aucune modification de votre côté.

11. Obligations en matière de preuves et de reporting

Le fournisseur doit-il fournir régulièrement des éléments tels que des rapports d’audit, des résultats de tests, des certifications, des mises à jour des risques ou des attestations de contrôle ?

Pourquoi c’est important : une diligence raisonnable ponctuelle ne suffit pas pour les relations critiques.

12. Assistance à la sortie et à la transition

Le contrat oblige-t-il le fournisseur à soutenir une transition vers un autre prestataire ou vers un service interne, notamment par la coopération, la documentation et l'assistance technique ?

Pourquoi c'est important : la résilience inclut la capacité de quitter un fournisseur sans perturbation grave.

Signaux d'alerte nécessitant une attention immédiate

- Aucun droit d'audit, ou une rédaction laissant l'audit entièrement à la discrétion du fournisseur
- Aucun délai clair de notification des incidents
- Aucune clause couvrant les changements de sous-traitants
- Aucun engagement de reprise testé pour les services critiques
- Aucune condition pratique d'extraction ou de suppression des données
- Aucune obligation d'assistance à la sortie
- Aucune obligation de fournir des preuves d'assurance actualisées
- Aucune protection en cas de changement de contrôle

Guide de notation rapide

- 10 à 12 éléments en place et adéquats : base contractuelle solide
- 7 à 9 éléments en place : base exploitable, mais lacunes prioritaires à examiner
- 4 à 6 éléments en place : risque contractuel élevé
- 0 à 3 éléments en place : contrat à considérer comme hautement prioritaire pour remédiation

Cas d'usage recommandés

Cette liste est particulièrement utile pour :

- Les revues d'intégration de fournisseurs
- Les revues de renouvellement contractuel
- Les évaluations des tiers TIC au titre de DORA
- Les revues du risque fournisseur au titre de NIS2
- Les ateliers d'alignement entre achats et juridique
- Le reporting au conseil ou à la direction sur la résilience des tiers

Sources officielles de référence

Sources de l'Union européenne

- Texte officiel de la directive NIS2 sur EUR-Lex : https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Texte officiel du règlement DORA sur EUR-Lex : https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- Page de la Commission européenne consacrée aux actes d'exécution et actes délégués de DORA : https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en
- Page de présentation de DORA par l'ESMA : https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- Page de la Commission européenne consacrée à la mise en œuvre de NIS2 en Belgique : https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Sources belges

- Portail d’information NIS2 du Centre for Cybersecurity Belgium : https://belgium-nis2.be/en/
- Site principal du Centre for Cybersecurity Belgium : https://ccb.belgium.be/en
- Point de contact CERT.be via la page de la Commission européenne sur la mise en œuvre en Belgique : https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Bloc court pour publications ou encadrés d’articles

Sources officielles utiles pour travailler sur NIS2 ou DORA :

- Texte officiel de NIS2 : directive (UE) 2022/2555 sur EUR-Lex
- Texte officiel de DORA : règlement (UE) 2022/2554 sur EUR-Lex
- Présentation et mises à jour de DORA : ESMA
- Mise en œuvre de NIS2 et points de contact en Belgique : page Stratégie numérique de la Commission européenne
- Informations pratiques sur NIS2 en Belgique : Centre for Cybersecurity Belgium

Appui pour une revue pratique

Contactez GRCForce afin d’identifier les décalages entre la rédaction des contrats fournisseurs, la gouvernance et la résilience opérationnelle : https://grcforce.com/fr/#contact

Cette liste fournit des orientations pratiques et ne remplace pas un avis juridique. La rédaction des contrats et l’interprétation réglementaire doivent faire l’objet de la revue juridique appropriée.