HodeiShield · Évaluation des plateformes de risque tiers

Checklist d'évaluation des plateformes TPRM par secteur

Cochez chaque point pendant la démo avec vos propres fournisseurs et notez ce que l'outil ne fait pas.

Critères valables pour tout secteur

- [ ] Un inventaire des tiers avec responsable interne, criticité, données du contrat et sous-traitants.
- [ ] Des preuves avec responsable, date de validité et statut, et une preuve périmée qui cesse de compter.
- [ ] Comment l'information du fournisseur est obtenue : questionnaire, documents, scan externe, SBOM. Chaque voie mesure autre chose.
- [ ] Comment le score ou le risque est calculé : entrées visibles, méthode documentée et estimations signalées comme telles.
- [ ] Un journal des modifications, l'export de vos données et une API, pour pouvoir quitter l'outil.
- [ ] Où les données sont hébergées, quels sous-traitants ultérieurs interviennent et ce que la plateforme ne fait pas. Aucune ne vous rend conforme à elle seule.

DORA : entités financières de l'UE

- [ ] Un registre avec LEI, juridiction, fonction soutenue et criticité par prestataire et par contrat.
- [ ] Un export au format des modèles officiels (les guides des superviseurs citent des paquets xBRL-CSV), le dépôt par le canal officiel restant entre vos mains.
- [ ] Le suivi par contrat du plan de sortie, du droit d'audit et de la chaîne de sous-traitance.
- [ ] Une vue de concentration : combien de fonctions dépendent du même prestataire.

Source : Règlement (UE) 2022/2554 (DORA), articles 28 à 31, sur EUR-Lex https://eur-lex.europa.eu/eli/reg/2022/2554/oj
Règlement d'exécution (UE) 2024/2956, modèles du registre d'informations, sur EUR-Lex https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

NIS2 : entités essentielles et importantes de l'UE

- [ ] Une évaluation par fournisseur couvrant vulnérabilités et pratiques de sécurité, pas seulement un questionnaire générique.
- [ ] Des clauses de notification d'incident du fournisseur vers vous, avec suivi du délai.
- [ ] Des rapports que l'organe de direction peut approuver et réexaminer.
- [ ] Une gestion des incidents avec les délais de l'article 23 : 24 heures, 72 heures et un mois.

Source : Directive (UE) 2022/2555 (NIS2), articles 20, 21 et 23, sur EUR-Lex https://eur-lex.europa.eu/eli/dir/2022/2555/oj
Règlement d'exécution (UE) 2024/2690, exigences techniques et méthodologiques, sur EUR-Lex https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

---

ENS : secteur public espagnol et ses fournisseurs

- [ ] Qu'elle distingue la catégorie du système (basique, moyenne, haute) et montre quelles mesures op.ext s'appliquent.
- [ ] Des accords de niveau de service par fournisseur et une mesure périodique de leur respect.
- [ ] Une analyse d'impact et de risque pour un incident né dans la chaîne d'approvisionnement, avec des mesures de confinement.
- [ ] L'état de conformité ENS du fournisseur lui-même lorsqu'il sert un organisme public.

Source : Real Decreto 311/2022 (ENS), article 2 et annexe II, mesures op.ext, au BOE (en espagnol) https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

HIPAA : santé aux États-Unis et business associates

- [ ] Un marquage des tiers qui touchent des informations de santé et l'état du contrat de business associate de chacun, avec dates.
- [ ] Un registre des sous-traitants du business associate et de leurs garanties.
- [ ] Le suivi des clauses de notification de violation et du délai de 60 jours.
- [ ] Si la plateforme stockera elle-même des informations de santé, elle est business associate : demandez le contrat avant de charger des données.

Source : 45 CFR 164.308(b), contrats avec les business associates, sur eCFR https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.314(a), contrats avec les business associates (Security Rule), sur eCFR https://www.ecfr.gov/current/title-45/section-164.314
45 CFR 164.502(e), divulgations aux business associates, sur eCFR https://www.ecfr.gov/current/title-45/section-164.502
45 CFR 164.504(e), contenu des contrats avec les business associates, sur eCFR https://www.ecfr.gov/current/title-45/section-164.504
45 CFR 164.410, notification par un business associate, sur eCFR https://www.ecfr.gov/current/title-45/section-164.410

CMMC 2.0 : chaîne d'approvisionnement de défense américaine

- [ ] Un champ par fournisseur pour le type d'information traitée (FCI ou CUI) et le niveau CMMC exigé.
- [ ] La preuve que vous avez répercuté les exigences dans le contrat (flow-down).
- [ ] L'état de chaque sous-traitant face au niveau exigé, avec la date de la dernière preuve.
- [ ] Si vous chargez des CUI dans l'outil, que son hébergement respecte l'exigence cloud de 170.16(c).

Source : 32 CFR 170.23, application aux sous-traitants, sur eCFR https://www.ecfr.gov/current/title-32/section-170.23
32 CFR Part 170 (programme CMMC), sur eCFR https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

SAMA et ECC de la NCA : secteurs financier et national saoudiens

- [ ] Que la bibliothèque de référentiels inclue SAMA et ECC et indique l'édition (celle que nous avons consultée est ECC-2:2024).
- [ ] Un inventaire des tiers ayant accès aux systèmes ou aux données et des clauses contractuelles par fournisseur.
- [ ] Un marquage des prestataires d'externalisation et de cloud, qui ont leur propre sous-domaine dans SAMA.
- [ ] Des preuves par contrôle, avec responsable et date, pour répondre à l'organisme de supervision.

Source : SAMA Cyber Security Framework, domaine 3.4 «Third Party Cyber Security», dans le SAMA Rulebook https://rulebook.sama.gov.sa/en/34-third-party-cyber-security-0
NCA Essential Cybersecurity Controls (ECC-2:2024), domaine 4 https://cdn.nca.gov.sa/api/files/public/upload/da829b21-c4ef-4a6e-9f6e-82690d612ee9_ECC-2-2024-.pdf

---

Notes