Auto-évaluation de conformité CRA

Règlement (UE) 2024/2847 · article 32, annexe I, annexe VII · RE (UE) 2025/2392

MODÈLE GRATUIT — XLSX · PDF · MD | Version 1.0 · Mise à jour 2026-07-27

Ce que contient le classeur

Champ & classification	Les données du produit, le test du champ d'application de l'article 2 et les checklists des catégories des annexes III / IV — 19 catégories importantes de classe I, 4 de classe II, 3 critiques — confrontées aux descriptions techniques du règlement d'exécution (UE) 2025/2392, avec la règle de la fonctionnalité principale qui tranche les cas limites.
Voie de conformité	La logique de décision de l'article 32 : quelles procédures (module A contrôle interne, module B+C examen UE de type, module H assurance qualité complète, ou un schéma européen de certification de cybersécurité) sont licites pour votre classe, la condition des normes harmonisées pour l'auto-évaluation de classe I, l'exception FOSS, et la nécessité éventuelle d'un organisme notifié.
Annexe I partie I	Les 14 exigences relatives aux propriétés du produit — le point (1) plus le point (2)(a)–(m) — chacune avec une liste déroulante de statut (Conforme / Partiel / Écart / N-A justifié), une référence de preuve et un responsable.
Annexe I partie II	Les 8 exigences de gestion des vulnérabilités : SBOM, remédiation sans retard, tests réguliers, divulgation publique des vulnérabilités corrigées, politique CVD, contact de signalement, distribution sécurisée des mises à jour, diffusion gratuite et rapide.
Docs & notification	Les éléments de documentation technique de l'annexe VII, la période de support de l'article 13(8) (au moins 5 ans sauf durée d'utilisation prévue plus courte), la préparation à la notification de l'article 14 et la vérification de l'exposition aux sanctions de l'article 64.

L'horloge du CRA

10 déc. 2024	Règlement (UE) 2024/2847 en vigueur.
11 juin 2026	Le chapitre IV s'applique — les organismes notifiés peuvent être désignés. La capacité s'annonce limitée ; réservez tôt si votre classe en exige un.
11 sept. 2026	Les obligations de notification de l'article 14 s'appliquent — vulnérabilités activement exploitées et incidents graves via la plateforme unique de notification de l'ENISA : alerte précoce sous 24 h, notification sous 72 h, rapport final sous 14 jours (vulnérabilités) ou 1 mois (incidents). S'applique aux produits déjà mis sur le marché.
11 déc. 2027	Application intégrale : exigences essentielles de l'annexe I, documentation technique, déclaration UE de conformité, marquage CE. Les produits mis sur le marché à partir de cette date doivent avoir achevé l'évaluation de la conformité.

Qui peut s'auto-évaluer

Les produits par défaut — la grande majorité — peuvent utiliser le contrôle interne du module A. Les produits importants de classe I ne peuvent s'auto-évaluer QUE s'ils appliquent intégralement des normes harmonisées, des spécifications communes ou des certificats EUCC couvrant les exigences pertinentes ; avec des normes harmonisées CRA encore en développement à la mi-2026 (demande de normalisation M/606, 41 normes, acceptée par le CEN, le CENELEC et l'ETSI le 3 avril 2025), la plupart des fabricants de classe I devraient planifier une voie avec organisme notifié. La classe II exige toujours le module B+C, le module H ou l'EUCC au niveau d'assurance « substantiel ». Les produits critiques (annexe IV) utilisent un schéma européen de certification lorsqu'il est rendu obligatoire, sinon les procédures de la classe II.

La classification suit la fonctionnalité PRINCIPALE (RE (UE) 2025/2392, adopté le 28 novembre 2025) : un routeur contenant un pare-feu est un routeur ; un pare-feu autonome relève de la classe II. Consignez le raisonnement — les autorités de surveillance du marché peuvent le demander, et une classification erronée invalide la voie choisie.

Sanctions

Non-respect des exigences essentielles de l'annexe I ou des articles 13/14 : amendes jusqu'à 15 millions EUR ou 2,5 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu (article 64). Les autres obligations exposent à 10 millions EUR / 2 % ; la fourniture d'informations trompeuses aux autorités à 5 millions EUR / 1 %.

Surveillance du marché en France

L'ANFR est l'autorité française de surveillance du marché pour le CRA, en coopération étroite avec l'ANSSI ; le CERT-FR, rattaché à l'ANSSI, reçoit les notifications de vulnérabilités et d'incidents de l'article 14 à partir du 11 septembre 2026. La législation française d'application est encore à l'état de projet en juillet 2026 — le règlement s'applique néanmoins directement. Le message de l'ANSSI aux fabricants : n'attendez pas les normes harmonisées — les exigences essentielles de l'annexe I s'appliquent dans tous les cas, les normes restant volontaires avec une présomption de conformité.

Royaume-Uni & Norvège

Le Royaume-Uni n'a pas encore d'équivalent du CRA : le régime PSTI (en vigueur depuis le 29 avril 2024) couvre les produits connectables grand public avec un socle de sécurité plus étroit. Le CRA est pertinent pour l'EEE et devrait être incorporé dans l'accord sur l'EEE ; les fabricants norvégiens vendant sur le marché unique de l'UE sont en pratique concernés dans tous les cas, puisque le CRA s'attache aux produits mis sur le marché de l'UE.

De la checklist à la preuve

L'auto-évaluation vous dit où vous en êtes ; les acheteurs et les autorités de surveillance du marché vous demanderont de le montrer. Orbiq publie vos preuves CRA — avis de sécurité, politique SBOM, déclarations de période de support — dans un Trust Center gouverné : orbiqhq.com/platform/trust-updates. Associez ce classeur à notre modèle d'avis de vulnérabilité CRA pour l'obligation de divulgation de l'annexe I partie II. Variante lisible par machine : /downloads/templates/fr/cra-conformity-self-assessment.md.