
# Être prêt pour intégrer le Cyber Resilience Act dans sa pratique Open Source

## Guide de conformité au Cyber Resilience Act à destination des acteurs de la filière Open Source

Version 2.1, publiée le 11/09/26

*Une étude commandée par le CNLL et réalisée par inno³, diffusée sous licence libre pour être largement partagée et améliorée.*

# Sommaire



| Version | Date | Auteur | Commentaires |
|---|---|---|---|
| 1.0 | 05/12/2024 | inno³ | Première version. |
| 1.1 | 18/12/24 | inno³ | Intégration scénario développeur indépendant |
| 2.0 | 09/12/25 | inno³ | Mise à jour globale du guide |
| 2.1 | 11/09/26 | inno³ | Mise à jour avec intégration des orientations de juillet 2026, parcours de notification, SBOM et méthode de conformité |

# Remerciements et crédits

Le CNLL, l'Union des entreprises du logiciel libre et du numérique ouvert, est, depuis 2010, l'organisation représentative en France des entreprises de la filière Open Source. Sa mission est de rassembler les entreprises du numérique libre (ENL) dans un esprit de communauté et autour de valeurs communes, dans le but de représenter et de défendre la filière professionnelle du logiciel libre et du numérique ouvert en France. Dans le cadre de ses missions, il a confié au cabinet inno³ le soin de rédiger un guide de sensibilisation au CRA pour les acteurs de l'Open Source.

⇒ Voir https://cnll.fr

inno³ est un cabinet de conseil indépendant spécialiste des modèles ouverts agissant à la croisée des acteurs privés (industriels comme économie sociale et solidaire), publics (administrations et collectivités) et communautaires. Le cabinet s'appuie sur une équipe pluridisciplinaire (droit, socio, design et génie logiciel) qui s'implique activement et mobilise ses compétences pointues en faveur d'une plus grande prise en compte des modèles ouverts et collaboratifs. Inno³ est membre fondateur de l'initiative OpenSource-Experts destinée à permettre aux grands comptes d'accéder à l'expertise Open Source disséminée chez de nombreux acteurs spécialisés.

⇒ Voir https://inno3.fr.

## Coordination et rédaction

Les rédacteurs principaux sont Benjamin Jean (CEO, inno³) et Arthur Hamonic (doctorant et consultant, inno³). Les illustrations et visualisations ont été produites par Clémence Lascombes (chargée de missions, inno³).

L'équipe éditoriale et de coordination est composée de Stéfane Fermigier (coprésident CNLL) et de Catherine Nuel (chargée de mission, CNLL).

## Comité de suivi et contributions

Un comité de suivi a participé aux différents échanges, permettant d'alimenter le travail sur le fond et la forme du guide dans sa première version. Il était composé d'experts techniques, de juristes, et d'acteurs de l'Open Source : Camille Moulin (inno³), Cedric Temple (Bluemind), Clément Oudot (Worteks), Florent Zara (Fondation Eclipse), Gaël Blondelle (Fondation Eclipse),

Pierre-Yves Gibello (OW2), Simon Urli (xwiki), Victor ROLAND (Obéo), Vincent Picavet (Oslandia), Vincent Pouzol (Systerel) et Yannick Moy (AdaCore).

Cette étude a été présentée pour la première fois lors de la conférence European Opensource & free sofware Law Event le 29 novembre 2024 à Turin. Elle a ensuite été diffusée largement pour collecter et intégrer un grand nombre de remarques et commentaires de juristes et experts européens (tels que Frédéric Duflot, cofondateur de la société Examin, Frédéric Babin, manager à l'ANSSI, Maarteen Aersten de Nlnet Labs, Brian Fox de Sonatype, etc.).

## Mentions légales



Les éditions publiées du guide sont disponibles sur le site du CNLL (https://cnll.fr/publications). Les ressources sont également réunies dans le dépôt public hébergé par inno³.

Adresse et contact des organismes porteurs : hello@inno3.fr et contact@cnll.fr.

Les polices de caractères sont Roboto (par Christian Robertson, diffusée sous Apache-2.0) et Mina (©2015 Mina Project Authors, diffusée sous SIL Open Font License 1.1). L'illustration utilisée en première page (Illustration of cyber security concept) est issue de la plateforme free digital license.

# Préface

Dans un contexte marqué par une vulnérabilité croissante de la société européenne face aux risques informatiques, la Commission européenne a présenté en septembre 2022 le *Cyber Resilience Act* (CRA), un règlement ambitieux visant à améliorer la cybersécurité et la cyberrésilience des produits numériques commercialisés au sein de l'Union européenne. Adopté formellement en 2024, ce texte introduit des obligations strictes pour les acteurs économiques concernés et consacre le principe de la sécurité numérique « *by design* » à chaque étape du cycle de vie des produits.

Le CRA appelle des adaptations techniques, organisationnelles et documentaires pour les acteurs de la filière (y compris Open Source) qui fournissent des produits dans son champ. Le régime dépend de leur rôle : fabricant, importateur, distributeur ou intendant, tandis que certaines fournitures non commerciales et contributions sont exclues. Il faut préserver cette distinction pour construire une conformité proportionnée et éviter de reporter indistinctement les obligations des fabricants sur les communautés, prestataires ou partenaires.

Conscients de ces enjeux, le CNLL (Union des entreprises du logiciel libre et du numérique ouvert) et le cabinet inno³ ont collaboré pour élaborer ce guide pratique. Destiné à accompagner les acteurs de l'Open Source dans leur mise en conformité avec le CRA, ce guide repose sur une démarche collaborative, enrichie par des échanges approfondis avec des experts techniques, juridiques et économiques au sein de la filière. Il vise à offrir des outils concrets et adaptés pour relever ces défis tout en valorisant les forces intrinsèques du logiciel libre dans la construction d'un numérique plus sûr et résilient.

Ce guide a pour objectif de :

- Clarifier les principales exigences du CRA et leur application spécifique aux pratiques Open Source.
- Fournir des recommandations concrètes et atteignables pour intégrer ces nouvelles obligations dans les processus existants.
- Favoriser une compréhension partagée des enjeux du CRA au sein de l'écosystème Open Source, en articulant théorie et retours d'expérience.
- Proposer des pistes pour influencer positivement l'interprétation et la mise en œuvre des exigences du Règlement au niveau européen.

Ce travail repose sur une étude menée par inno³, enrichie par deux réunions de cadrage et de restitution, ainsi qu'un atelier réunissant les acteurs clés du CNLL, membres de l'association et partenaires extérieurs.

Au-delà de son ambition initiale, ce document constitue une invitation à poursuivre le dialogue entre législateurs, industriels et communautés Open Source, afin d'assurer une mise en œuvre équilibrée et pérenne des objectifs du CRA. Il pourra également évoluer dans le temps pour intégrer de nouvelles spécificités et retours d'expérience issus de nos membres mais également des grands utilisateurs, administrations publiques et autres contributeurs.

Le CRA marque un tournant pour les acteurs du logiciel libre en Europe, avec la fin du principe d'absence de responsabilité en dehors d'une relation commerciale, qui constituait jusqu'à présent le fondement de nombreux *business models* d'éditeurs de logiciel libre. Par ce guide, le CNLL entend néanmoins offrir aux acteurs de l'Open Source les premières clés pour transformer cette contrainte réglementaire en opportunité, en identifiant et en adoptant des pratiques renforçant la confiance et la résilience de leurs produits et services.

**Stéfane Fermigier**

Co-président du CNLL

# 1 | Introduction

## 1.1 | Contexte de régulation croissante du numérique

Dans une démarche de régulation[1] du marché intérieur de l'Union européenne (UE) en matière numérique, le législateur européen a produit ces dix dernières années plusieurs réglementations[2] visant à encadrer et à accompagner les usages et les pratiques des « opérateurs économiques ». Parmi elles, le *Cyber Resilience Act* (CRA) – en français règlement sur la cyberrésilience[3] – vise à renforcer la cybersécurité au bénéfice des consommateurs et des entreprises. Mêlant considérations techniques, économiques et humaines, l'UE soutient par cette politique le développement d'une société reposant sur un **numérique fort et de confiance qui laisse la priorité à l'humain**[4].

Publié au Journal Officiel de l'UE le 20 novembre 2024, le CRA vise à renforcer la cybersécurité et la cyberrésilience des produits logiciels (et matériels qui comportent des éléments numériques) connectés. L'Europe réaffirme ainsi la **cybersécurité comme un enjeu croissant pour l'économie européenne**, la numérisation massive des entreprises et des services publics ayant accru la vulnérabilité aux cyberattaques.

D'une portée très large[5], le Règlement s'articule autour de trois axes principaux :

| | |
|---|---|
| **#1** | Garantir une **sécurité « par principe »** des produits lors de leur mise sur le marché et tout au long de leur cycle de vie ; |
| **#2** | Assurer la livraison de produits en **limitant les failles de sécurité** potentielles ; |
| **#3** | **Renforcer le niveau d'information** à destination des utilisateurs et des entreprises. |

1 Le concept de régulation, tel que formalisé en droit économique, englobe un processus visant à orienter et superviser les comportements des acteurs économiques (dont les entreprises) afin d'atteindre des objectifs d'intérêt général, tout en s'adaptant aux évolutions du marché. Ainsi, la régulation ne se limite pas à l'imposition de normes, mais inclut également des mécanismes de surveillance, d'incitation et de sanction pour assurer le bon fonctionnement des marchés et la protection des consommateurs.

2 Voir notamment « A Europe fit for the digital age », https://commission.europa.eu/

3 Règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

4 Déclaration sur les droits et principes numériques : les valeurs et les citoyens de l'UE au cœur de la transition numérique, Conseil de l'Union européenne, Communiqué de presse, 15 décembre 2022 09:30, https://www.consilium.europa.eu/ que l'on retrouve aussi dans l'article premier de IA Act du 13 juin 2024.

5 Sur des textes plus spécifiques, voir le Règlement (UE) 2022/2554 dit DORA (*Digital Operational Resilience Act*) dédié à la résilience opérationnelle numérique des entités du secteur financier.

Le texte matérialise ainsi une approche de régulation du marché intérieur de l'Union européenne, dans la lignée du règlement 2019/1020 sur la surveillance du marché et la conformité des produits (qui complète le *New Legislative framework* de 2008). Le CRA complète aussi les directives *Network and Information Security* (NIS) de 2016[6] et 2022 (NIS2)[7] qui imposent aux entités essentielles et aux entités importantes d'adopter des mesures de sécurité importantes, et s'appuie sur le Cybersecurity Act de 2019[8] qui marque une étape clé dans la construction d'une cybersécurité européenne unifiée (renforcement du rôle de l'Agence de l'Union européenne pour la cybersécurité (ENISA) comme agence permanente destinée à accompagner tous les États membres et introduction d'un cadre de certification en cybersécurité). Le CRA s'insère aussi dans la continuité de réglementations spéciales applicables aux services financiers (tel le *Digital Operational Resilience Act* dit DORA[9] applicable dès 2025) ou du paiement et aux équipements médicaux ou radio, etc. À cela s'ajoutent des textes transversaux, mais aux effets sectoriels prononcés, tels que l'*Artificial Intelligence Act* (AI Act)[10] de 2024, imposant des exigences pour les systèmes à haut risque, ou la directive CER sur la résilience des entités critiques (2022)[11] renforçant la résilience des entités critiques dans des secteurs sensibles. Le tout impose un certain nombre de bonnes pratiques dont le non-respect pourra être autant de bases d'indemnisation sur le fondement de la directive 2024/2853 relative aux produits défectueux (NPLD pour *New Product Liability Directive*)[12] du 23 octobre 2024.

Cette complexité apparente, qui reflète celle de notre société numérique, n'est néanmoins pas nécessairement synonyme d'une lourdeur inutile – certains cadres venant simplifier les usages par l'harmonisation des pratiques hétérogènes. Enfin, le numérique est aussi un allié pour venir appréhender et réduire cette complexité, permettant de créer des outils qui partagent le traitement et l'automatisent.

Conçu pour renforcer la sécurité des produits numériques dans leur ensemble, le *Cyber Resilience Act* couvre **tous les produits comportant des éléments numériques dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte à un dispositif ou à un réseau, lorsqu'ils sont mis à disposition sur le marché de l'Union** (et sous réserve des exclusions prévues). S'il ne prenait pas en considération dans ses premières versions les particularités inhérentes aux projets Open Source – qui sont par essence perméables aux enjeux de commercialisation – le texte a évolué après l'intervention de nombreux acteurs du secteur mettant en lumière les défis d'application du CRA dans le contexte décentralisé de l'Open Source. Ainsi, certaines adaptations ont été intégrées en prévoyant

6 Directive (UE) 2016/1148
7 Directive (UE) 2022/2555
8 Règlement (UE) 2019/881
9 Règlement (UE) 2022/2554
10 Règlement (UE) 2024/1689
11 Directive (UE) 2022/2557
12 Directive (UE) 2024/2853

notamment plusieurs formes d'exceptions ou de limitations au bénéfice des projets non commerciaux et à but non lucratif qui seraient publiquement disponibles sous une licence libre ou Open Source[13]. La publication du Règlement au Journal Officiel a ouvert la phase d'accompagnement (production de guides de bonnes pratiques) et de normalisation qui permettra à terme d'avoir une application uniforme et souple de la loi[14].

Cette répartition de la responsabilité entre les différents opérateurs économiques vise à préserver l'écosystème Open Source, en évitant de décourager les développeurs de logiciels Open Source à but non commercial de contribuer à des projets ouverts par crainte de responsabilisation. Ainsi, ce texte **devrait conduire les fabricants de produits finaux intégrant de tels logiciels à mettre en place des procédures de vérification de l'ensemble des composants logiciels** (au travers des SBOM, rendues centrales dans la mise en œuvre du CRA). Cela peut être vu comme une opportunité pour l'écosystème de l'Open Source afin d'avoir, demain, plus d'utilisateurs conscients et de contributeurs responsables.

## 1.2 | Enjeux des acteurs du numérique et de l'Open Source

Daté du 23 octobre 2024, le Règlement a été publié au Journal Officiel le 20 novembre 2024 et est entré en vigueur le 10 décembre 2024. Les acteurs économiques (entreprises, mais potentiellement aussi des acteurs publics ou non lucratifs qui auraient une activité économique) concernés disposent ensuite d'une période de transition de 21 mois (jusqu'au 11 septembre 2026) pour se mettre en conformité avec certaines obligations critiques (notification des vulnérabilités activement exploitées et des incidents graves) et de 36 mois (jusqu'au 11 décembre 2027) pour s'adapter à l'ensemble des autres exigences du texte telles que la sécurité par principe[15] ou la transparence vis-à-vis des consommateurs. Il s'agit donc d'un **moment charnière pour l'ensemble de l'écosystème numérique français et européen, qui doit anticiper la mise en place de nouvelles pratiques pour se mettre en conformité rapidement**. Au-delà des acteurs directement contrôlés par le régulateur, les contrats pourront organiser des engagements adaptés au rôle des partenaires commerciaux[16], fournisseurs, sous-

13 Le Règlement définit en son article 2 les logiciels libres et ouverts comme ceux 1) dont le code source est partagé de manière ouverte ; 2) via une mise à disposition sous licence libre et ouverte qui prévoit tous les droits pour qu'il soit librement accessible, utilisable, modifiable et redistribuable (tout logiciel public diffusé sous une licence libre (au sens de la *Free Software Definition*) ou Open Source (au sens de l'*Open Source Definition*) rentre dans cette seconde condition).

14 Ce chantier de coconstruction a été anticipé par les acteurs de l'Open Source qui ont coordonné leurs efforts dans le cadre de l'*Open Regulatory Compliance Working Group* (https://orcwg.org/) sous l'égide de la fondation Eclipse et lors de laquelle ils s'impliqueront directement en tant que membres du *CRA Expert Group on Cybersecurity of Products with Digital Elements* de la Commission européenne.

15 Ou « by design », au sens où la conception intègre naturellement ces concepts. Cf 2.3.1 Mise en œuvre d'un haut niveau de cybersécurité pour les produits.

16 Ainsi, in fine tous les acteurs économiques qui participent à la fourniture des produits logiciels devront les accompagner d'une documentation précise détaillant leur niveau de sécurité, le support technique proposé par

traitants, clients finaux jusqu'aux consommateurs. **Les produits comportant des éléments numériques mis sur le marché avant le 11 décembre 2027 ne relèvent du CRA qu'en cas de modification substantielle après cette date, à l'exception des obligations de notification de l'article 14 (vulnérabilités activement exploitées et incidents graves), qui s'appliquent à tous ces produits dès le 11 septembre 2026.**

Acteurs d'une chaîne de production et d'approvisionnement plus étendue, l'ensemble des acteurs impliqués dans l'usage, le développement ou encore l'intégration de logiciels Open Source sont ainsi **directement potentiellement concernés par le Règlement et indirectement certainement concernés**. Plus encore, nous verrons que l'ensemble des acteurs Open Source, économiques ou non, ont un intérêt certain à se préparer proactivement à l'entrée en application d'un règlement susceptible de leur ouvrir des opportunités réelles. C'est en effet l'opportunité d'être **accompagnés activement par un régulateur qui fait de la cybersécurité l'une des priorités des prochaines années** et qui prévoit une série de mesures favorables aux logiciels libres et ouverts ainsi qu'aux micro, petites et moyennes entreprises. C'est aussi l'opportunité de **bénéficier de contributions plus régulières et plus soutenues** en provenance de l'ensemble des acteurs régulés qui seront soucieux de se montrer diligents, créant ainsi de nouvelles relations et pratiques collaboratives.

Néanmoins, il reste un enjeu de **clarification de l'articulation entre cette réglementation et les spécificités des pratiques de la filière des entreprises de l'Open Source**. Si certaines situations sont parfois pleinement assimilables aux pratiques des fabricants de solutions commerciales, le modèle Open Source ouvre en effet une **diversité de modalités d'implications** qui peuvent avoir des incidences fortes en matière de droit de la concurrence, de pratiques de marchés publics, etc. Cela s'explique notamment par le **caractère décentralisé et la gratuité associée à l'usage des droits de propriété intellectuelle**. Ainsi, d'une part, le produit n'est pas nécessairement, directement ou indirectement, vendu à des tiers[17] (ou peut l'être par un autre acteur que son éditeur) et, d'autre part, il n'y a pas de recouvrement automatique entre celui qui produit le code et celui (ou ceux) qui contrôle son exploitation. Enfin, les pratiques Open Source incitent à l'adaptation et la modification des produits publiés, ce qui rendra parfois très floues les frontières entre les fabricants-éditeurs et les distributeurs-intégrateurs.

le fournisseur ou encore l'installation des mises à jour de sécurité.
Si le fabricant reste responsable de ses obligations, les contrats pourront organiser les contributions et les preuves attendues des partenaires : partager et corriger les vulnérabilités des projets Open Source utilisés, maintenir à jour un inventaire des composants Open Source utilisés, etc.

17 Toute activité n'étant pas nécessairement « commerciale » au titre du CRA, fût-elle pourvue par un acteur économique (voir notamment les considérants 15,16, 18, 20).

## 1.3 | Objectifs d'une plus grande sensibilisation au CRA

Ce guide de mise en application du CRA est destiné à accompagner les membres du CNLL, et plus généralement les acteurs français du numérique qui produisent ou intègrent des logiciels libres et Open Source dans leurs produits et/ou services. Il synthétise l'impact du CRA et opérationnalise les principales attentes du législateur européen. L'objectif est de **préparer les acteurs de la filière**, pour leur permettre d'identifier les modalités raisonnables susceptibles d'être mises en œuvre au sein de leur organisation, et de modifier autant que nécessaire leurs processus de gestion de l'Open Source afin d'intégrer les attentes spécifiques et complémentaires en matière de cybersécurité (notamment en matière de constitution de *Software Bill of Materials* et de gestion des vulnérabilités).

En présentant les principales règles du CRA en quelques dizaines de pages, ce guide n'a pas pour objectif d'être exhaustif. Il est destiné à être partagé largement au sein de l'écosystème professionnel Open Source, pour favoriser notamment les échanges avec le législateur européen. Il est destiné à évoluer dans le temps pour suivre les évolutions de la réglementation d'une part, et d'autre part, pour répondre aux enjeux complémentaires (grands utilisateurs, administrations[18], etc.).

## 1.4 | Méthodologie

L'édition 2.0 du guide a été publiée à l'occasion de l'événement Open Source Experience 2025 qui s'est tenu à Paris les 10 et 11 décembre 2025. Elle s'appuie sur un travail de veille incluant la doctrine théorique et pratique autour du règlement ainsi que des éléments partagés par la Commission européenne. Elle est également nourrie des échanges du comité de suivi. Le projet prévoyait ensuite qu'elle serait complétée courant 2026 par des cas d'usages supplémentaires permettant d'illustrer l'application du CRA au sein de projets Open Source très utilisés.

Cette révision 2.1 prolonge l'édition 2.0 du 9 décembre 2025. Elle intègre la relecture reçue en août, une vérification du règlement et de ses rectificatifs, les orientations rendues publiques par la Commission le 27 juillet 2026, et une méthode de préparation à la conformité. Les sources et leur statut sont précisés dans les ajouts.

18 Pour les achats publics de produits relevant du CRA, l'article 5 § 2 impose aux États membres de prendre en compte le respect des exigences essentielles, y compris la capacité du fabricant à traiter les vulnérabilités.

# 2 | Explicitation des obligations et attendus du règlement

Afin de faciliter la compréhension du CRA et les effets attendus, les développements qui suivent décomposent ses principales exigences dans un premier temps avant d'apprécier, dans un second temps, les conditions et modalités de son application aux pratiques et acteurs de l'Open Source.

## 2.1 | Champ d'application du CRA

### 2.1.1 La régulation des produits comportant des éléments numériques

#### Une application généralisée

L'article 2, paragraphe 1, du CRA stipule que le règlement s'applique « *aux produits comportant des éléments numériques mis à disposition sur le marché dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau* ».

Trois conditions cumulatives doivent être réunies pour l'application du CRA :

1. **« Un produit comportant des éléments numériques »** : c'est-à-dire une solution logicielle ou un matériel qui embarque des logiciels. L'article 3 (définition) permet de comprendre qu'une solution de traitement de données à distance entre dans le périmètre lorsque son logiciel est « *conçu et développé par le fabricant ou sous la responsabilité de ce dernier, et dont l'absence empêcherait le produit [...] d'exécuter une de ses fonctions* »[19] ainsi qu'à tous les composants logiciels ou matériels mis sur le marché séparément (et interagissant avec ce premier) ;
2. **« qui est mis à disposition sur le marché »** : c'est-à-dire destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale[20], à titre onéreux ou gratuit ;

19 L'article 3 Définition appréhende le traitement de données à distance comme : « Tout traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant ou sous la responsabilité de ce dernier, et dont l'absence empêcherait le produit comportant des éléments numériques d'exécuter une de ses fonctions ». Il est à noter que l'article 26 du Règlement indique que la Commission donnera des orientations relatives à cette notion de traitement de données à distance et les logiciels libres et ouverts.

20 L'activité commerciale étant entendue comme la mise à disposition (c'est-à-dire fourniture de biens pour distribution ou utilisation dans le cadre d'une activité économique), voir article 2.2. « Mise à disposition sur le marché » du Blue Guide https://eur-lex.europa.eu/legal-content/. La mise sur le marché est la première de ces mises à disposition.

3. « **dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau** » : sont ainsi concernés à la fois les produits explicitement conçus ou commercialisés pour un tel usage (par exemple un routeur Wi-Fi), et ceux pour lesquels la connexion à un réseau est une conséquence logique du fonctionnement du produit (par exemple un smartphone peut être utilisé pour accéder à des services IoT). Sont concernées les connexions soit à d'autres dispositifs (logiciels ou matériels), soit à un réseau (par définition connecté à d'autres dispositifs) et peut se faire par câbles ou au travers de logiciels.

**Cette formulation est volontairement très large afin de pouvoir s'étendre à la majorité des produits susceptibles d'introduire des risques pour la cybersécurité sans néanmoins couvrir les situations non évidentes pour lesquelles un produit aurait été fortement détourné de ses usages prévisibles.**

### Une application différenciée

Au sein des produits concernés le règlement distingue :

- Les produits numériques standards ;
- Les produits importants :
  - de classe 1 (ex : systèmes de gestion des identités, navigateurs autonomes et intégrés, gestionnaires de mots de passe, etc.) ;
  - de classe 2 (ex : hyperviseurs, pare-feu, microprocesseurs et microcontrôleurs résistants aux manipulations, etc.) ;
- Les produits critiques de l'annexe IV : dispositifs matériels avec boîtier de sécurité, passerelles pour compteur intelligent et autres dispositifs à des fins de sécurité avancées, cartes à puce ou dispositifs similaires, y compris éléments sécurisés.

Afin de déterminer la typologie du produit, le fabricant devra évaluer la fonctionnalité essentielle de celui-ci qui conduira le classement éventuel comme produit important ou critique et l'assujettissement aux procédures de conformité applicables[21]. Les fabricants devront ensuite appliquer les exigences essentielles de cybersécurité de manière proportionnée aux risques propres à chaque produit numérique, sur la base d'une évaluation complète tenant compte de l'usage prévu, des conditions d'utilisation et de la durée de vie du produit. Ils devront ainsi adapter le niveau de mesures et de garanties, même pour des produits similaires, afin d'assurer une mitigation adéquate des risques identifiés.

21 Les spécifications techniques relatives à ces catégories sont définies par le règlement d'exécution (UE) 2025/2392 du 28 novembre 2025 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202502392

Les produits numériques standards peuvent relever du contrôle interne (module A), mais restent soumis à toutes les exigences essentielles applicables selon les risques. Pour les classes I et II et les produits critiques, la procédure dépend des articles 8 et 32. Le recours à un tiers n'est pas systématique pour tous les logiciels Open Source importants : l'article 32 § 5 ouvre notamment le module A si la documentation technique est rendue publique lors de la mise sur le marché. Cette faculté ne couvre pas les produits critiques de l'annexe IV (voir plus en détail 2.3.1 Mise en œuvre d'un haut niveau de cybersécurité pour les produits).

Par ailleurs, le règlement exclut spécifiquement les catégories de produits auxquels s'appliquent déjà des réglementations assurant un niveau de protection identique ou supérieur à celui prévu par le CRA. Cela concerne notamment :

- Les dispositifs médicaux soumis aux règlements (UE) 2017/745 et (UE) 2017/746 ;
- Les dispositifs en lien avec les véhicules à moteur soumis au règlement (EU) 2019/2144 ;
- Les produits aéronautiques couverts par une certification au titre du règlement (UE) 2018/1139, dans les limites de l'exclusion prévue à l'article 2 du CRA ;
- Les équipements marins qui relèvent du champ d'application de la directive 2014/90/UE.

Sont également exclus les produits développés ou modifiés exclusivement à des fins de sécurité nationale ou de défense, ou les produits spécifiquement conçus pour traiter des informations classifiées. Les pièces de rechange fabriquées conformément aux mêmes spécifications que les composants qu'elles sont destinées à remplacer sont également exclues (article 2 § 6).

Par ailleurs, la Commission a précisé dans sa FAQ, le lien entre le CRA et d'autres réglementations européennes pouvant être résumés dans le tableau disponible en annexe (cf. 4.2 Lien entre le CRA et les autres réglementations ).

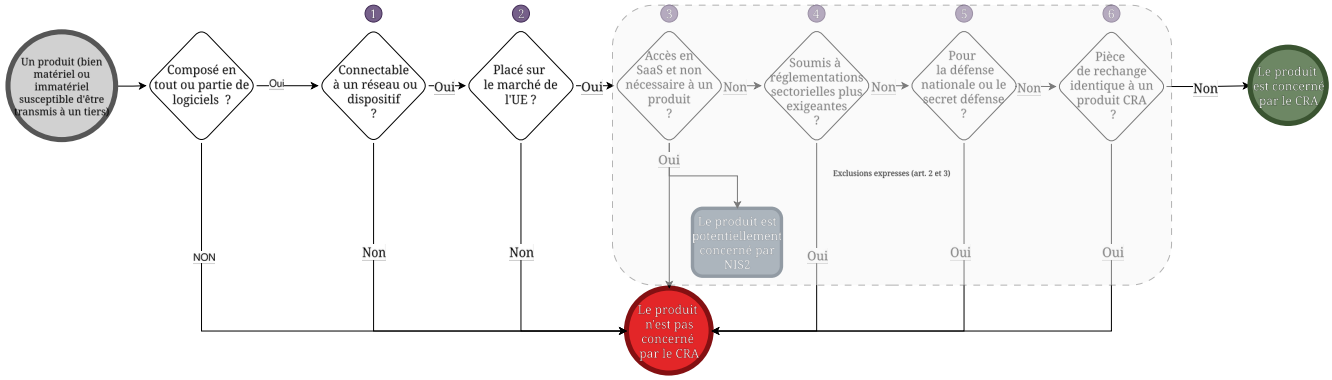



*Figure 1: Logigramme relatif à la qualification des produits concernés*

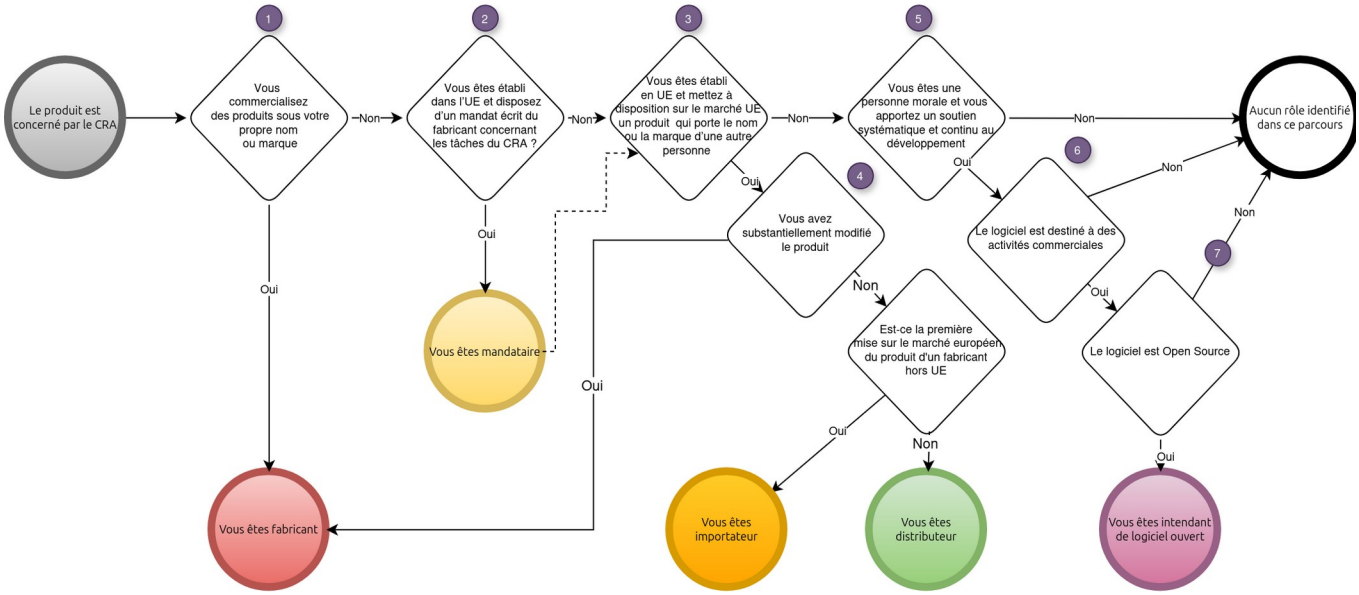
### 2.1.2 Les opérateurs économiques concernés au titre du CRA

Le Règlement s'applique aux **acteurs économiques indépendamment du statut juridique** (sociétés, associations, administrations, etc.) **ou du mode de financement** (notamment public ou privé) **de l'acteur**.

S'appuyant sur un raisonnement classique en matière de régulation du marché intérieur, il distingue plusieurs opérateurs économiques aux responsabilités distinctes : **le fabricant, le mandataire, l'importateur, le distributeur**. À noter que certains rôles non définis par le CRA (notamment celui des fournisseurs et sous-traitants du fabricant) ne seront pas **régulés directement,** mais seront indirectement impactés – sous réserve d'une éventuelle requalification pour tout ou partie de leur activité – **par le truchement du vecteur contractuel qui les liera au fabricant ou à l'importateur**. Les **administrations** (au sens européen du terme, c'est-à-dire tous les acteurs publics) participeront aussi activement à renforcer ce cadre puisque l'article 5§2 du CRA prévoit que « *lors des achats publics de produits comportant des éléments numériques relevant du champ d'application du présent règlement, les États membres veillent à la prise en compte, au cours du processus d'achat public, du respect des exigences essentielles énoncées à l'annexe I du présent règlement, y compris la capacité du fabricant à traiter efficacement les vulnérabilités.* »

Dans un second temps, le rôle particulier d'« **intendant de logiciels ouverts** » (*open source software steward*) a été ajouté afin de proposer un cadre préférentiel aux communautés Open Source industrielles qui sont considérées comme essentielles au développement durable de produits libres et ouverts destinés à des usages commerciaux. Afin de pallier une application stricte du CRA ayant des conséquences contraires aux objectifs de l'UE et sur la structuration actuelle de l'écosystème, ils bénéficient d'obligations réglementaires « allégées » permettant à la fois de les associer à la régulation du CRA tout en tenant compte de leur nature spécifique. Ainsi, les intendants de logiciels ouverts peuvent continuer à soutenir le développement des logiciels Open Source destinés à l'activité commerciale de leurs membres **dès lors qu'ils fournissent à ces derniers l'information et la sécurité dont ils ont besoin pour respecter à leur tour pleinement le CRA**. Agissant en amont de la mise sur le marché, l'**intendant n'appose pas lui-même le marquage CE aux produits ainsi soutenus**.

*Figure 2: Logigramme relatif à la qualification des opérateurs économiques au titre du CRA*




L'ensemble de ces opérateurs ont différentes obligations complémentaires. Ainsi, les acteurs devront vérifier s'ils répondent à l'une ou l'autre des catégories suivantes et s'ils respectent le cas échéant les obligations sous-jacentes. Compte tenu des définitions de chacun des opérateurs économiques, il n'est **pas possible pour un acteur de cumuler plusieurs rôles pour une même version d'un produit**, mais il est possible pour un acteur d'avoir **des rôles différents pour des versions différentes d'un même produit sujettes à des opérations de fourniture différentes (cf 2.2.2 L'application distributive du CRA selon les mises à disposition).**

| Rôle | | Définition |
|---|---|---|
| | **Fabricant** | **Personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux, monétisé ou gratuit.** |
| | **Intendant de logiciels ouverts (*open source steward*)** | Personne morale, autre que le fabricant, qui a pour objectif ou finalité de **fournir un soutien systématique et continu au développement** de produits spécifiques comportant des éléments numériques qui répondent aux **critères de logiciels libres et ouverts** et sont **destinés à des activités commerciales**, et qui assure la viabilité de ces produits. |
| | **Mandataire** | Personne physique ou morale établie dans l'Union **ayant reçu mandat écrit du fabricant** pour agir en son nom aux fins de l'accomplissement de tâches déterminées[22]. |
| | **Importateur** | Personne physique ou morale **établie dans l'Union** qui **met sur le marché un produit comportant des éléments numériques**, lequel porte le nom ou la marque |

22 L'article 3.2 du Blue Guide précise « *les tâches pouvant être déléguées au mandataire conformément à la législation d'harmonisation de l'Union sont de nature administrative. Dès lors, le fabricant ne peut déléguer ni les mesures nécessaires pour faire en sorte que le procédé de fabrication garantisse la conformité des produits, ni l'établissement d'une documentation technique, sauf disposition contraire. En outre, un mandataire ne peut modifier le produit de sa propre initiative en vue de le rendre conforme à la législation d'harmonisation de l'Union applicable* ». https://eur-lex.europa.eu/

| | | |
|---|---|---|
| | | d'une personne physique ou morale établie en dehors de l'Union. |
| | **Distributeur** | Personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui **met un produit comportant des éléments numériques** à disposition sur le marché de l'Union sans altérer ses propriétés. |

## 2.2 | Application du CRA aux logiciels et activités Open Source

Toute qualification au titre du CRA nécessite d'identifier d'abord le produit et ses modalités de fourniture (la publication d'un code source sous licence Open Source ne constitue pas, à elle seule, une mise à disposition dans le cadre d'une activité commerciale). Il faut examiner la monétisation, y compris indirecte, et la responsabilité de la personne qui fournit le produit : le seul usage commercial en aval, le financement ou une contribution au code ne suffisent pas à rendre commerciale la fourniture du composant par son auteur. Par ailleurs, une personne morale qui n'est pas le fabricant, mais qui a pour objet ou objectif de soutenir systématiquement et durablement le développement de produits spécifiques répondant aux critères de logiciels libres et ouverts et destinés à des activités commerciales, peut relever de l'article 3(14) relatif aux intendants de logiciel libre.

Contrairement aux définitions de l'Open Source (https://opensource.org/osd) et du logiciel libre (https://www.gnu.org/) qui n'excluent ni ne discriminent l'exploitation commerciale, le CRA différencie expressément les logiciels Open Source fournis dans le cadre d'une activité commerciale (directe ou indirecte[23]), d'une part et les logiciels Open Source publiés sans être rattachables à une activité commerciale[24]. Le principe développé par le CRA est que **seuls les**

23 Le considérant 15 du CRA précise ainsi que « *La fourniture dans le cadre d'une activité commerciale peut être caractérisée non seulement par le prix facturé pour un produit comportant des éléments numériques, mais également par le prix des services d'assistance technique lorsqu'il ne sert pas uniquement à récupérer les coûts réels, par une intention de monétisation, par exemple par la fourniture d'une plate-forme logicielle par l'intermédiaire de laquelle le fabricant monétise d'autres services, par l'exigence, comme condition à l'utilisation, du traitement des données à caractère personnel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel, ou par l'acceptation de dons supérieurs aux coûts associés à la conception, au développement et à la fourniture d'un produit comportant des éléments numériques. Le fait d'accepter des dons sans intention lucrative ne devrait pas être considéré comme constitutif d'une activité commerciale* ».

24 À noter que ces éléments sont rappelés dans le Considérant 18 du CRA: « *En ce qui concerne les opérateurs économiques auxquels s'applique le présent règlement, seuls les logiciels libres et ouverts mis à disposition sur le marché, donc fournis pour être distribués ou utilisés dans le cadre d'une activité commerciale, devraient relever du champ d'application du présent règlement. [...] En outre, la fourniture de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts, destinés à être intégrés par d'autres fabricants à leurs propres produits comportant des éléments numériques, ne devrait être considérée comme une mise à disposition sur le marché que si le composant est monétisé par son fabricant d'origine. Par exemple, le simple fait qu'un fabricant verse un soutien financier à un logiciel libre comportant des éléments numériques ou qu'il contribue au développement d'un tel produit ne devrait pas en soi suffire à déterminer que cette activité est de nature commerciale* ». « *Le présent règlement ne s'applique pas aux personnes physiques ou morales qui contribuent, sous forme de code source, à des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne relevant pas de leur responsabilité.* »

**produits distribués dans un cadre commercial sont soumis aux exigences de cybersécurité du Règlement**, avec des obligations plus ou moins fortes selon que l'éditeur est un fabricant ou un intendant de logiciel libre.

### 2.2.1 *La notion d'activité commerciale*

En droit européen, la qualification d'une activité comme commerciale repose sur la notion d'**activité économique**. La Cour de justice de l'Union européenne (CJUE) précise que « […] *la notion d'entreprise comprend toute entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement, et […] constitue une activité économique toute activité consistant à offrir des biens ou des services sur un marché donné* »[25]. Le statut lucratif ou non lucratif, l'existence de salariés et le financement sont des éléments de contexte, aucun ne permettant en eux-seuls d'apprécier les modalités concrètes de fourniture et des indices de monétisation mentionnés aux considérants 15 et 18 du CRA.

À ce titre, il apparaît que certaines activités d'acteurs économiques (indépendamment de leur statut juridique et de leur mode de financement) peuvent permettre de prouver le caractère non commercial de l'activité. Les situations suivantes constituent des indices à apprécier ensemble et dans leur contexte pour qualifier la fourniture :

1. **La distribution est gratuite et sans objectif lucratif**[26] (c'est-à-dire sans contrepartie financière directe – sans paiement conditionnant son accès ou celui de ses fonctionnalités – et sans intention de profit) ;
2. **Le financement est assuré par des dons ou des subventions** (pour les projets Open Source soutenus par des contributions volontaires ou des subventions publiques sans revenus tirés de la vente de produits ou services – dès lors que ce financement ne constitue pas en pratique le prix d'accès au logiciel, à une édition, à une mise à jour ou à une fonctionnalité) ;
3. **L'absence de services payants associés** (services associés tels que le support technique, la formation, l'hébergement ou la personnalisation[27]).

25 CJCE, 23 avril 1991, Höfner et Elser, C-41/90, point 21, ECLI:EU:C:1991:161. Rapprochement doctrinal avec la notion d'entreprise en droit de la concurrence ; la qualification au titre du CRA demeure fondée sur ses dispositions propres.

26 Voir notamment le considérant 18 : « *Enfin, aux fins du présent règlement, le développement par des organisations à but non lucratif de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne devrait pas être considéré comme une activité commerciale, pour autant que l'organisation concernée soit constituée de telle façon que tous les bénéfices sont utilisés pour atteindre des objectifs non lucratifs.* »

27 À noter que la guidance suggère qu'un service payant indépendant du fournisseur du logiciel, ou limité à la récupération des coûts réels dans les conditions pertinentes, ne rend pas automatiquement commerciale la fourniture du logiciel.

**En conclusion et sous réserve de qualification cas par cas, certaines pratiques d'acteurs de l'Open Source semblent sortir du champ d'application du CRA compte tenu de l'absence d'activité commerciale.** Cela va concerner notamment les logiciels Open Source diffusés à des fins de test[28], à des fins exclusives de recherche, etc. dès lors qu'il n'y a pas de monétisation susceptible d'être rattachée à cette mise à disposition. Dans cette situation, la première publication du logiciel sur le territoire européen ne sera pas qualifiée de mise sur le marché au titre du CRA.

**Cette exclusion des logiciels libres et ouverts qui ne sont ni développés ni fournis dans le cadre d'une activité commerciale permet de sécuriser l'écosystème de contributeurs et mainteneurs actuels,** tout en faisant reporter cette charge sur les opérateurs économiques (qu'ils soient ou non fortement impliqués dans l'écosystème des projets Open Source). Ces mêmes idées se retrouvent dans l'AI Act ainsi que dans la directive NPLD relative aux produits défectueux, avec néanmoins leurs propres conditions[29].

Cette distinction sera certainement centrale dans son application aux instituts de recherche (et leurs valorisations), pour lesquels il conviendra certainement de différencier les logiciels faisant l'objet d'une **valorisation économique** (en interne ou par maturation par les Sociétés d'accélération du transfert de technologie (SATT) par exemple) qui seront a priori **pleinement soumis aux contraintes du CRA** et ceux essentiellement **diffusés en Open Source dans le cadre des missions de l'organisme** qui seront a priori exclus de ce cadre.

### 2.2.2 *L'application distributive du CRA selon les mises à disposition*

L'application du CRA devrait s'apprécier « produit par produit » et « activité par activité », il sera alors possible de considérer que certains produits sont « mis à disposition sur le marché » alors que d'autres ne le seront pas. La temporalité peut varier, ainsi que les rôles.

Ainsi, dans le cadre d'une mise à disposition d'une version payante et d'une version « communautaire » d'un même logiciel, la version communautaire et non monétisée n'est pas considérée comme mise sur le marché au sens du CRA contrairement à la version monétisée. L'**entité qui publie ces deux versions devra respecter les obligations applicables à chaque situation, la qualification comme intendants de logiciels ouverts pour la version communautaire n'étant à envisager que si les conditions de l'article 3 sont réunies. Les obligations applicables aux fabricants vis-à-vis de la version payante** (les deux copies

28 La diffusion à des fins de test est soumise à la condition que ce logiciel soit mis à disposition uniquement pendant le temps nécessaire pour le tester et recueillir des commentaires et qu'il soit accompagné d'un signe visible indiquant sa non-conformité. (FAQs on the Cyber Resilience Act §1.6)

29 À ce sujet, voir la série de billets rédigée sur Open Source et IA, et notamment Open Source et IA : trois règlements européens, trois logiques, un même écosystème, inno³, CC BY-SA 4.0.

numériques identiques d'un même logiciel étant considérées comme différentes lorsque leurs modalités d'exploitation sont différentes) étant a priori retenues.

La notion de **mise à disposition** est en cours de clarification par la Commission. À ce jour, il semblerait que chaque copie d'un logiciel constitue un produit distinct, mis sur le marché séparément, même lorsqu'il est identique. Toutefois, toutes les copies disponibles sur une même plateforme partageraient la date de leur première mise en vente sur celle-ci, tandis que la mise en ligne du même logiciel sur une autre plateforme à une date ultérieure entraînerait une nouvelle date de mise sur le marché propre à cette seconde plateforme uniquement si elle est assortie de modifications substantielles[30].

Néanmoins, autant il est envisageable de calquer le régime des produits physiques sur des produits numériques lorsqu'il est fait usage de la propriété intellectuelle pour rendre rival un bien qui ne l'est pas par nature, autant il semble difficilement envisageable (et pratiquement impossible) de vouloir étendre ce régime à des biens numériques soumis à des licences Open Source qui assurent le maintien de cette non-rivalité[31]. Ainsi, dans le domaine des logiciels Open Source, il semble préférable de considérer que la date de mise sur le marché d'une copie numérique « maître » soit « héritée » pour toute mise en circulation d'une copie subséquente « enfant » (la guidance parlerait ici de variante) du même logiciel. Mais cette interprétation devra être vérifiée au fur et à mesure que les juges appliqueront le texte. La bonne pratique sera a minima de conserver un registre des versions et variantes avec toutes les informations utiles : leur date de première fourniture commerciale, les canaux de diffusion, l'analyse des modifications substantielles et la période d'assistance retenue.

### 2.2.3 L'influence du CRA sur les modèles économiques associés à l'Open Source

En application de l'adage « Libre ne veut pas dire gratuit », de nombreuses activités relatives à des logiciels Open Source rentrent dans le cadre des activités commerciales pleinement soumises à l'application du CRA. Il existe une grande variété de modèles économiques associés au développement sous licence Open Source d'un logiciel et chaque situation devra ainsi être évaluée à l'aune des critères du CRA (le seul fait de vendre un service autour du logiciel ne suffit pas à rendre son prestataire fabricant).

Quelques premières mises en application semblent ressortir naturellement :

30 Pour le logiciel autonome, les orientations de juillet 2026 (§ 13 à 16) retiennent une mise sur le marché simultanée des copies d'un même logiciel lors de sa première fourniture commerciale. Les variantes différant par leurs composants, configurations ou fonctionnalités sont des produits distincts. Une itération ne renouvelle pas cette date si elle ne constitue pas une modification substantielle.

31 Pour étayer précisément la distinction entre non-rivalité et droits exclusifs, voir Lawrence Lessig, The Architecture of Innovation, version diffusée par Duke, p. 189 (page 13 du PDF)

- **Activité commerciale directe** :
  - Dans le cadre du **modèle économique dit de *dual licence*** (le code est soumis à deux licences, l'une étant Open Source – généralement relativement contraignante : GPL-3.0 ou AGPL-3.0 étant aujourd'hui les plus utilisées – et l'autre étant commerciale) ;
  - En **présence d'abonnement ou de garanties additionnelles** ayant pour finalité de faciliter l'utilisation des solutions Open Source ;
  - Lorsqu'une **centralisation est opérée parallèlement par l'éditeur** au travers d'un service de SaaS et/ou de place de marché (vente de plugin, etc.) ;
  - Et enfin des **services complémentaires opérés indépendamment de la diffusion du logiciel** peuvent être proposés, sous réserve de qui développe ou fait développer le produit et le commercialise sous son nom ou sa marque.
- **Activité commerciale indirecte, c'est-à-dire réalisée par les réutilisateurs de la solution communautairement développée** : c'est le cas des logiciels Open Source qui sont développés de façon communautaire afin de répondre aux besoins d'acteurs (privés ou publics) qui peuvent soit en faire une distribution dans le cadre de leur activité commerciale (ils seront soumis à ce titre au CRA) soit en faire un simple usage à l'appui de leur activité. Ainsi, l'usage d'un logiciel par une entreprise pour ses besoins internes ne rend pas commerciale sa fourniture par le projet amont. Inversement, la redistribution commerciale par un tiers se qualifie séparément, selon les actes accomplis par ce tiers.

### 2.2.4 L'influence du CRA sur les acteurs de l'écosystème Open Source

#### | *Le cas des éditeurs Open Source*

En mettant en avant le nom ou la marque du fabricant, le Règlement souhaite imposer ses obligations les plus importantes aux acteurs économiques qui assurent la maîtrise du produit : (contrôle de la conception, fabrication et commercialisation). Ainsi ne seront considérés comme fabricants que **les acteurs économiques qui maîtrisent (même partiellement, par exemple par l'usage de la marque[32]) le développement et l'exploitation du produit**. Les orientations

32 À noter que le CRA n'encadre pas spécifiquement les situations de contrôle technique ou matériel, alors qu'il est possible de ménager une exclusivité et un contrôle de l'évolution du logiciel par la seule maîtrise de la plateforme qui héberge le code (qu'il s'agisse de limiter l'accès, les contributions ou encore les évolutions du projet). Cette absence de référence explicite au contrôle dans le texte final du CRA est d'autant plus notable que, dans la pratique, un acteur peut exercer une influence déterminante sur l'évolution d'un logiciel libre par la seule maîtrise de l'infrastructure de développement — un point que la définition provisoire de « *collaborative development* » tentait précisément d'encadrer avant d'être abandonnée au cours du trilogue.

(§ 49) mobilisent elles-mêmes le contrôle principal de ces décisions pour distinguer la responsabilité d'un logiciel Open Source d'une simple contribution au travers d'une lecture des responsabilités effectives : le contrôle ne constitue pas une condition autonome de la définition légale, ni l'exigence de maîtriser toute l'infrastructure ou tous les droits sur le code.

À l'inverse, les personnes qui **contribuent au développement de logiciels libres et ouverts ne relevant pas de leur responsabilité**[33] ne sont pas soumises au CRA au seul titre de cette contribution (que ce soit en qualité de fabricant ou distributeur)**.**

Si plusieurs versions d'un même logiciel Open Source sont mises à disposition dans des conditions différentes (certaines pouvant être associées à une activité commerciale d'autres ne l'étant pas), il est nécessaire de qualifier chaque produit et sa fourniture : monétisation directe ou indirecte, personne responsable, fonctionnalités, composants et modification substantielle éventuelle. À noter que la simple fourniture gratuite n'induit pas à elle-seuile le caractère d'activité non commerciale. Ainsi, les utilisateurs d'une version particulière du logiciel bénéficieront des garanties du CRA dès lors que cette version particulière fera l'objet d'une activité commerciale.

Dans certains cas (par exemple dans la situation d'une monétisation par la publicité), l'absence de flux financiers directs entre le fabriant et les utilisateurs du logiciel soumis au CRA rendra certainement complexe le respect de certaines obligations d'information. Une telle situation sera certainement appréciée conformément au contexte Open Source particulier et il semble raisonnable de considérer, dans une telle hypothèse, qu'une information via les canaux traditionnels d'information et de communication serait considérée comme suffisante (site web du projet, liste de diffusion à destination des développeurs et/ou de la communauté d'utilisateurs, etc.).

### | *Les nombreux distributeurs*

Au sein de l'écosystème Open Source, la pluralité d'acteurs susceptibles de redistribuer un même logiciel est inhérente au modèle, ce qui inclut la majorité des entreprises de services numériques (ESN) lorsqu'elles mettent sur le marché un produit numérique dans un cadre commercial. Plus encore, dès lors que l'un d'eux modifie substantiellement le logiciel ou le redistribue sous sa propre marque, il est requalifié en fabricant au sens du CRA et assume à ce titre des obligations renforcées. Ainsi, la responsabilité étant attribuée en fonction du rôle effectivement joué dans la chaîne d'approvisionnement, il y aura potentiellement un plus grand nombre d'acteurs juridiquement engagés compte tenu de leurs contributions respectives.

33 Cf notamment le considérant 18 : « *Le présent règlement ne s'applique pas aux personnes physiques ou morales qui contribuent, sous forme de code source, à des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne relevant pas de leur responsabilité.* »

De même, il semble probable que des places de marchés participant à la distribution de logiciels entrent pleinement dans la qualification de **distributeur**[34]. Inversement et en dépit du rôle matériel qu'elles jouent dans la dissémination des logiciels Open Source, y compris commerciaux, les acteurs qui ont un rôle limité à celui de forges logicielles (*Github*, *Gitlab*, etc.) semblent a priori exclues du champ d'application du CRA en ce qu'elles ne visent pas à mettre à disposition le produit sur le marché de l'Union (au sens économique).

### | *Le rôle particulier des intendants de logiciels ouverts*

Les intendants de logiciels ouverts (ou « *open source software steward* ») sont :

- Des **personnes morales ;**
- **Autres que des fabricants** ;
- Qui ont pour mission un **soutien systématique et continu au développement de logiciels Open Source** ;
- Dès lors que ces logiciels ont pour finalité d'être utilisés **dans le cadre d'activités commerciales par d'autres organisations** (ces dernières pouvant être soumises au CRA au titre de leurs propres activités).

À la différence du fabricant qui commercialise le produit sous son nom ou sa marque, l'intendant de logiciels ouverts revêt uniquement le rôle de support au développement et à la viabilité des produits Open Source.

À la lecture du règlement et de ses considérants, la notion semble être envisagée de manière suffisamment large pour couvrir les hypothèses des principales fondations (notamment Fondation Eclipse, Fondation Linux, Fondation Apache, OSGeo ou OW2), mais aussi des entreprises qui pourraient souhaiter jouer ce rôle pour la version Open Source dite « communautaire » du logiciel qu'elles éditent. Inversement, des fondations telle la fondation Mozilla (dédié au développement du logiciel Firefox) qui possède leur propre entreprise qui salarie leurs développeurs pourraient semble-t-il être considérées comme fabricants au titre du CRA. Il faudra ainsi vérifier, produit par produit, le soutien durable, la viabilité du produit et sa destination commerciale pour l'intendant présumé, ainsi que d'autres indices tels que le développement et la commercialisation sous son nom ou sa marque pour le fabricant.

34 En ce sens, voir notamment le considérant 20 : « *Le seul fait d'héberger des produits comportant des éléments numériques sur des dépôts ouverts, y compris par l'intermédiaire de progiciels ou de plates-formes collaboratives, ne constitue pas en soi la mise à disposition sur le marché d'un produit comportant des éléments numériques. Les fournisseurs de ces services ne devraient être considérés comme des distributeurs que s'ils mettent ces logiciels à disposition sur le marché, donc s'ils les fournissent pour qu'ils soient distribués ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale.* »

Des analyses au cas par cas seront certainement nécessaires afin de comprendre leur rôle particulier et l'influence (économique et politique) des sociétés impliquées. En effet, certains opérateurs économiques chercheront certainement à se démettre de leurs responsabilités alors qu'ils commercialisent potentiellement parallèlement sous leur nom ou leur marque le produit.

Enfin, cette qualification ne permet pas de couvrir les gouvernances informelles de communautés Open Source – une communauté sans personnalité morale ne peut pas être elle-même un intendant au sens de l'article 3 –, agissant souvent grâce à un portage par ses membres plus ou moins décentralisé. De même, le rôle des « hôtes fiscaux » (tel que le projet Open Collective) devra certainement être reconsidéré face à l'application des responsabilités individuelles que le CRA risque d'entraîner.

## | *Synthèse des qualifications dans un contexte Open Source au regard des activités commerciales*

Le tableau qui suit reprend les activités économiques présentées plus haut afin de montrer la diversité d'application du CRA vis-à-vis des parties prenantes mobilisées (Fabricant, Distributeur, Intendant de logiciels ouverts, etc.) susceptibles d'être retenues au titre du CRA.

*Tableau 1: Proposition de qualification des opérateurs économiques au titre du CRA.*

| Produits ou services utilisant le logiciel | Services autour du logiciel | Offres en Saas (Software as a service) | Abonnement | Licences propriétaires |
|---|---|---|---|---|
| Leur activité économique requiert que le logiciel existe et soit adéquatement maintenu :<br><br>*OpenStack, Noyau Linux, etc.* | Les contributeurs au logiciel vendent des services autour de celui-ci, en utilisant leur expertise (support ou formation) :<br>*PostGreSQL, QGIS, etc.* | La société qui développe le logiciel propose alternativement une offre en SaaS à partir de son logiciel :<br><br>*Wordpress, Dolibarr, etc.* | Un abonnement offre accès à des mises à jour faciles et du support :<br><br>*RHEL, Jboss, etc.* | Les éditeurs vendent alternativement des licences propriétaires (dual licensing ou offre freemium) :<br><br>*Alfresco, MySQL, etc.* |
| Intendant de logiciels ouverts | Fabricant (si commercialisation sous leur nom ou modification substantielle) | Fabricant si activités directement liées | Fabricant si monétisation du produit sous son nom ou sa marque. | Fabricant |
| Fabricant (si commercialisation sous leur nom) | Importateur (si première commercialisation en UE) | | | Importateur (si première commercialisation en UE) |
| Importateur (si première commercialisation en UE) | Distributeur (si acteur tiers) | | | Distributeur (si acteur tiers) |
| Distributeur (si acteur tiers) | | | | |

## 2.3 | Les obligations prévues par le CRA

Le CRA répartit des obligations entre les opérateurs selon leur rôle. Les contrats peuvent organiser les contributions, les informations et les preuves attendues des sous-traitants et partenaires, ainsi que des engagements complémentaires adaptés au produit et à la relation. Ils ne transfèrent pas la responsabilité réglementaire du fabricant et ne rendent pas automatiquement un mainteneur amont débiteur des mêmes obligations. Dans les achats publics, l'article 5 impose également la prise en compte des exigences essentielles et de la capacité du fabricant à traiter efficacement les vulnérabilités.

### 2.3.1 Mise en œuvre d'un haut niveau de cybersécurité pour les produits

Le CRA implique de **concevoir, développer et produire le produit de manière à garantir un niveau de cybersécurité suffisant.**

Dans un premier temps, cette obligation passe par le fait de faire preuve de **diligence raisonnable** (« *due diligence* » en anglais) lors de l'intégration des composants obtenus auprès de tiers. Si le Règlement ne définit pas cette obligation de *due diligence*, la FAQ de la Commission européenne l'explicite plus en détail[35]. Le niveau de diligence requis dépend ainsi du risque de cybersécurité du composant intégré et de l'impact possible sur le produit final. Selon la FAQ, les fabricants peuvent, par exemple, vérifier si le composant porte le marquage CE, s'assurer qu'il reçoit régulièrement des mises à jour de sécurité, consulter les bases de données de vulnérabilités européennes, réaliser des tests de sécurité comme le *fuzz testing*, les tests d'intrusion, l'analyse de *firmware* ou des exercices de *red-team*. D'autres actions incluent l'analyse de la composition logicielle, l'isolation de composants critiques, la consultation du SBOM, la vérification de la durée de support et l'évaluation de la sécurité du fabricant du composant, ainsi que la cohérence de l'usage prévu du composant avec celui du produit final[36]. Autant que possible, il s'appuiera sur le travail de *due diligence* réalisé par les fabricants de ces composants. Dans ce cadre, le fabricant peut néanmoins valablement mettre un produit sur le marché sans que tous les composants tiers du produit aient une attestation de conformité dès lors qu'il vérifie les exigences de chaque composant intégré propre à cette diligence raisonnable. Le programme volontaire d'attestation prévu par l'article 25 du CRA a donc pour but de faciliter la mise sur le marché[37].

35 FAQs on the Cyber Resilience Act §4.4.2.

36 Cette liste n'est pas exhaustive et l'on peut également penser à la prise en compte du nombre de mainteneurs du composant utilisé, de la réalisation de tests, de l'observation de l'existence de mise à jour régulière, etc.

37 Voir 2.4.2Les accompagnements associés au CRA

Dans un deuxième temps, le fabricant devra réaliser ou faire réaliser (selon la classification du produit)[38] une **évaluation de conformité** du produit. Cette procédure juridique vise à attester qu'un produit comportant des éléments numériques respecte les exigences essentielles du CRA. Les modules présentés ci-dessous sont trois voies possibles : le module A (contrôle interne), les modules B+C (examen UE de type) et le module H (assurance qualité complète) qui dépendent de la classe des produits concernés (par défaut, critiques, importants) présentée précédemment dans le chapitre 2.1.1 La régulation des produits comportant des éléments numériques).

Une quatrième voie peut être ouverte par un schéma européen de certification de cybersécurité disponible et applicable dans les conditions des articles 8, 27 et 32. La simple possession d'une certification de sécurité ne remplace pas la procédure CRA.

Dans le droit de l'Union européenne, le terme « module » renvoie à une définition juridique précise (fixée par la décision n° 768/2008/CE) qui permet de distinguer plusieurs "modules d'évaluation de la conformité" (allant du Module A au Module H) pour décrire les différentes phases par lesquelles un produit doit passer (conception, fabrication, contrôle) avant d'être mis sur le marché.

*Tableau 2: Présentation des modules relatifs aux évaluations de conformité*

| Module | Produits concernés | Obligations | Rôle de l'organisme notifié |
|---|---|---|---|
| **Module A**<br>Contrôle interne de la fabrication<br>(annexe VIII, partie I)<br><br>Auto-évaluation : le **fabricant vérifie seul**, sous sa responsabilité, la conformité du produit et de ses processus aux exigences essentielles de l'annexe I. | - Produits par défaut (ni importants ni critiques) : voie ouverte par l'article 32 § 1, point a).<br>- Produits importants de classe I (annexe III) : uniquement si les normes harmonisées, spécifications communes ou schémas européens de certification de cybersécurité (règlement (UE) 2019/881, niveau d'assurance au moins « substantiel ») couvrant les exigences concernées sont pleinement appliqués (article 32 § 2, a contrario).<br>- Produits FOSS relevant des catégories de l'annexe III (classes I et II) : faculté de recourir aux procédures de l'article 32 § 1, dont le module A, à condition que la documentation technique de l'article 31 soit mise à la disposition du public au moment de la mise sur le marché (article 32 § 5). | - Mise en œuvre des mesures de cybersécurité selon l'analyse de risques.<br>- Tests et vérification de conformité.<br>- Rédaction de la documentation technique (article 31).<br>- Apposition du marquage CE et déclaration UE de conformité.<br>- Maintien de la conformité en production. | Aucun organisme notifié. |
| **Modules B + C**<br>Examen UE de type + conformité au type sur la base du contrôle interne de la production<br>(annexe VIII, parties II et III)<br><br>Le fabricant vérifie la conformité **et un organisme notifié évalue la conception** (documentation, puis spécimen selon la procédure) avant de délivrer un certificat | - Produits par défaut : voie possible (article 32 § 1, point b).<br>- Produits importants de classe I : obligatoire, en alternative au module H, pour les exigences que les normes harmonisées, spécifications communes ou schémas européens ne couvrent pas ou ne sont pas pleinement appliqués (article 32 § 2).<br>- Produits importants de classe II : voie ouverte, en alternative au module H ou à un schéma européen de certification au niveau au moins « substantiel » (article 32 § 3). | - Mise en œuvre des mesures de cybersécurité.<br>- Tests du produit.<br>- Documentation technique.<br>- Déclaration UE de conformité et apposition du marquage CE.<br>- Maintien de la conformité au type par le contrôle interne de la | - Examen de la documentation et, selon la procédure, d'un spécimen.<br>- Réalisation ou supervision des essais appropriés.<br>- Délivrance du certificat d'examen UE de type.<br>- Examen des modifications du type approuvé |

38 Comme évoqué dans le paragraphe 2.1.1La régulation des produits comportant des éléments numériques

| | | | |
|---|---|---|---|
| d'examen UE de type. | - Produits critiques (annexe IV) : voie ouverte, en alternative au module H, tant que les conditions de l'article 8 § 1 (acte délégué imposant la certification européenne) ne sont pas remplies (article 32 § 4, point b). | production. | selon les conditions de l'annexe VIII. |
| **Module H**<br>Conformité sur la base de l'assurance complète de la qualité<br>(annexe VIII, partie IV)<br><br>Le fabricant **met en place un système de qualité approuvé** couvrant conception, développement, production et contrôle final ; un **organisme notifié évalue ce système et le surveille**. | - Voie ouverte pour toutes les catégories : produits par défaut (article 32 § 1, point c), produits importants de classe I ne remplissant pas les conditions du module A (article 32 § 2), produits importants de classe II (article 32 § 3) et produits critiques hors certification européenne obligatoire (article 32 § 4, point b).<br>- Particulièrement adaptée lorsque le fabricant organise ses activités autour d'un système de qualité couvrant la conception, le développement, la production et le traitement des vulnérabilités. | - Système de qualité couvrant les activités requises par l'annexe VIII, partie IV.<br>- Mise en œuvre des mesures de cybersécurité, tests et documentation.<br>- Approbation du système et surveillance par un organisme notifié.<br>- Déclaration UE de conformité et marquage CE accompagné du numéro de cet organisme.<br>- Maintien de la conformité du système approuvé. | - Évaluation et approbation du système qualité.<br>- Vérification de sa conformité aux exigences de l'annexe VIII.<br>- Surveillance par des audits périodiques, avec transmission des rapports au fabricant. |

L'évaluation des risques de cybersécurité doit prendre en compte l'usage prévu et raisonnablement prévisible du produit, ses conditions réelles d'utilisation et ses intégrations possibles, afin de minimiser les risques tout au long de son cycle de vie. Les fabricants doivent traiter les risques pertinents, fournir des instructions claires pour une utilisation sécurisée et considérer les comportements réels des utilisateurs, y compris lorsque ceux-ci diffèrent de l'usage initialement prévu[39]. Le fabricant devra tenir cette évaluation à jour tout au long du cycle de vie du produit, c'est-à-dire lors des phases de planification, de conception, de développement, de production, de livraison et de maintenance du produit.

Pour réaliser cette évaluation, le Règlement prévoit dans son Annexe 1, un ensemble d'exigences essentielles de cybersécurité relatives aux propriétés du produit : absence de vulnérabilités exploitables connues, configuration de sécurité par défaut, mécanismes de contrôle appropriés, protection de la confidentialité et de l'intégrité des données, ainsi que la possibilité pour les utilisateurs de supprimer facilement toutes les données et tous les paramètres[40]. Toute non-applicabilité doit être justifiée dans l'évaluation et la documentation technique.

**Responsables principaux :**

- Fabricant ;

39 Voir notamment à ce sujet : FAQs on the Cyber Resilience Act §4.1.4

40 4.3.1Exigences de cybersécurité relatives aux propriétés des produits comportant des éléments numériques

- Intendants de logiciels ouverts dans le cas de logiciels Open Source destinés à des activités commerciales (il n'assume pas les obligations générales du fabricant au seul titre de ce statut, mais doit notamment disposer d'une politique de cybersécurité et respecter une coopération au titre de l'article 24 du CRA).

**Responsables subséquents :**

- Distributeur ;
- Importateur.

### 2.3.2 Déclaration de conformité et marquage CE

Condition préalable à l'apposition d'un marquage CE, la déclaration de conformité est l'engagement que le produit respecte les exigences de cybersécurité établies par le CRA[41]. Elle est établie selon le modèle reproduit en Annexe 4.5 Modèles de déclaration de conformité. Disponible dans les langues requises par l'État membre concerné, la déclaration contient les éléments précisés dans les procédures d'évaluation et doit être mise à jour tout au long du cycle de vie du produit. Cette attestation engage légalement le fabricant en cas de non-conformité et doit être conservée au moins dix ans après la mise sur le marché ou pendant la période d'assistance, la durée la plus longue étant retenue.

Par la suite, le fabricant devra apposer le marquage CE de manière visible, lisible et indélébile sur le produit. Pour les produits de type logiciel, le CRA précise que le marquage CE est apposé soit avec la déclaration UE de conformité, soit sur le site internet qui l'accompagne[42].

Les distributeurs et importateurs sont responsables dans un second temps de s'assurer que les produits respectent les exigences du CRA avant de les mettre sur le marché (importateur) et que les autres opérateurs ont bien respecté leurs obligations (distributeurs).

**Responsable principal :**

- Fabricant ;

**Responsables subséquents :**

- Mandataire
- Distributeur ;
- Importateur (si fabricant hors UE).

41 Article 28§4
42 Voir en annexe 4.4 | Marquage CE le détail des modalités prévues par le législateur.

### 2.3.3 Documentation technique

Le CRA prévoit ainsi une obligation forte en matière de documentation technique associée au produit et à la charge du fabricant. Décrite à l'annexe VII du Règlement, la documentation technique doit comprendre un certain nombre d'éléments :

1. **La description générale du produit** : usage prévu du produit, versions logicielles importantes pour la cybersécurité, photos ou schémas montrant les caractéristiques externes et internes, instructions pour les utilisateurs ;
2. **La description de la conception et de la fabrication** : détails sur la conception et le développement, incluant des schémas ou une description de l'architecture, informations sur le processus de gestion des vulnérabilités (liste des logiciels utilisés, politique de divulgation des vulnérabilités, contact pour le signalement des vulnérabilités, méthodes de distribution sécurisée des mises à jour) détails sur les processus de fabrication et de suivi ;
3. **L'évaluation des risques de cybersécurité** : document attestant de la bonne mise en œuvre d'un haut niveau de cybersécurité pour les produits publiés (analyse des risques de cybersécurité intégrée dans la conception et le développement du produit, application des exigences essentielles de cybersécurité) ;
4. **Les informations sur la période d'assistance** : critères considérés pour déterminer la durée d'assistance du produit ;
5. **La liste des normes et certifications appliquées** : normes harmonisées, spécifications communes, et certifications européennes de cybersécurité utilisées, solutions adoptées si certaines normes ou certifications ne sont pas appliquées en totalité ;
6. **Les rapports d'essais de conformité** : résultats des tests de conformité avec les exigences de cybersécurité ;
7. **La déclaration de conformité UE** ;
8. **La nomenclature des logiciels** (volontairement ou à la demande du régulateur[43]) : liste détaillée des composants logiciels.

**Responsable principal :**

- Fabricant ;

43 « *La documentation contient* [...] : *le cas échéant, la nomenclature des logiciels, à la suite d'une demande motivée d'une autorité de surveillance du marché, pour autant que celle-ci soit nécessaire pour permettre à cette autorité de vérifier le bon respect des exigences essentielles de cybersécurité énoncées à l'annexe I* ». Annexe VII, Contenu de la documentation technique.

**Responsables subséquents :**

- Mandataire : conserve la documentation technique et la déclaration UE de conformité à disposition des autorités dans les conditions de l'article 18 et de son mandat ;
- Distributeur : réalise les vérifications et la coopération prévues à l'article 20 ; il n'établit pas le dossier technique du fabricant ;
- Importateur (si fabricant hors UE) : conserve une copie de la déclaration UE de conformité et s'assure que la documentation technique peut être fournie aux autorités sur demande (article 19 § 6).

### 2.3.4 Nomenclature des logiciels (SBOM)

L'obligation de produire et maintenir à jour une nomenclature des logiciels[44] (ou *Software Bill of Materials* – SBOM)[45] apparaît comme une nouveauté majeure de la régulation européenne pour améliorer la transparence, la sécurité et la résilience des produits numériques. Les fabricants de produits numériques devront donc au titre du CRA :

- **Recenser et documenter les vulnérabilités et les composants des produits**, notamment par l'établissement d'une nomenclature des logiciels dans un format couramment utilisé et lisible par une machine (*document dual*) couvrant au moins les dépendances de niveau supérieur des produits[46] ;
- **Fournir cette SBOM en cas de demande des autorités de surveillance**[47] : principalement destiné à la gestion interne de la sécurité par les fabricants et les autorités compétentes, la communication du SBOM aux utilisateurs résultera soit d'un engagement contractuel soit d'une volonté de transparence du fabricant ;
- **Partager les informations sur l'endroit où celle-ci peut être consultée** lorsque le fabricant décide de la mettre à la disposition de l'utilisateur.

Le CRA entérine ainsi une pratique encore trop minoritaire qui permettra à terme une plus grande transparence des logiciels, une meilleure gestion des composants Open Source et des dépendances, une aide au respect des obligations légales et réglementaires, l'identification des

44 Article 3 : Définitions : « *document officiel contenant les détails et les relations avec la chaîne d'approvisionnement des différents composants utilisés dans la fabrication d'un produit comportant des éléments numériques*. »

45 Une SBOM est un inventaire détaillé des composants logiciels, bibliothèques et dépendances qui composent un produit numérique ou un système embarqué. Le terme de SBOM est utilisé dans la version originale du CRA et celui de nomenclature des logiciels est utilisé dans la version française. Par souci de concision et de clarté, on utilisera par la suite l'acronyme anglais.

46 Annexe 1 Partie II. L'article 13 §24 du CRA prévoit que la Commission pourra être amenée à préciser le format et les éléments qui constituent les SBOM.

47 Article 13 § 22 et annexe VII, point 8 ; article 13 § 25 pour le cas distinct d'une évaluation des dépendances décidée par l'ADCO. L'article 13 § 24 concerne le format et les éléments de la SBOM.

failles de sécurité et des éventuels composants de substitution, la maintenance dans la durée, etc.

Par chance, les écosystèmes de l'Open Source et de la cybersécurité collaborent depuis plusieurs années pour simplifier la génération de SBOM. En effet, cet outil est à la convergence des enjeux de cybersécurité (permettant de vérifier les composants Open Source et leurs dépendances), de soutenabilité (connaître les acteurs impliqués dans le développement des logiciels que l'on utilise) ou encore de conformité (pour vérifier la conformité de l'exploitation du produit au regard des licences concernées).[48] En imposant la mise en place d'une documentation détaillée et en rendant obligatoire la fourniture d'une SBOM en cas de demande des autorités de surveillance, le CRA **vise à rendre l'écosystème numérique plus résilient et à généraliser des bonnes pratiques de l'écosystème de l'Open Source**. Si cette obligation de fourniture est orientée sur la dimension cybersécurité, il est recommandé de la dépasser en incluant les aspects soutenabilité et conformité précédemment évoqués.

Les entreprises auront une meilleure visibilité sur leurs chaînes d'approvisionnement logicielles, ce qui leur permettra de détecter rapidement des composants obsolètes ou vulnérables, et de les mettre à jour ou remplacer avant qu'ils ne deviennent une menace active. Les clients finaux, qu'il s'agisse d'entreprises ou de particuliers, auront une bien meilleure compréhension des composants qui constituent les produits qu'ils achètent. Ils pourront ainsi évaluer les risques et mettre en place des stratégies de sécurité appropriées pour leurs propres infrastructures. Pour ce faire les SBOM doivent :

- S'insérer dans le cadre d'une chaîne de production (*supply chain*) potentiellement complexe grâce à une standardisation des formats de SBOM ;
- Être les plus précises et exhaustives possibles afin de couvrir l'étendue la plus large des risques. À l'inverse des pratiques existantes qui visent une granularité relativement fine, l'obligation de fourniture des SBOM établie par le CRA n'impose à ce jour que l**es dépendances de premier niveau**[49]. Ce minimum ne dispense néanmoins pas de recenser et traiter les risques provenant de dépendances transitives.

48 Ainsi, le considérant 77 du CRA rappelle que « [a]*fin de faciliter l'analyse de la vulnérabilité, les fabricants devraient répertorier et documenter les composants contenus dans les produits comportant des éléments numériques, notamment en établissant une nomenclature des logiciels. Une telle nomenclature peut fournir à ceux qui fabriquent, achètent et exploitent des logiciels des informations de nature à améliorer leur compréhension de la chaîne d'approvisionnement, ce qui présente de multiples avantages. Elle peut en particulier aider les fabricants et les utilisateurs à suivre les vulnérabilités et les risques émergents nouvellement apparus en matière de cybersécurité. Il est particulièrement important pour les fabricants de s'assurer que leurs produits comportant des éléments numériques ne contiennent pas de composants vulnérables développés par des tiers. Les fabricants ne devraient pas être tenus de rendre publique la nomenclature des logiciels* »

49 Annexe 1 Partie II :« *Les fabricants des produits comportant des éléments numériques : 1) recensent et documentent les vulnérabilités et les composants des produits, notamment par l'établissement d'une nomenclature des logiciels dans un format couramment utilisé et lisible par machine couvrant au moins les dépendances de niveau supérieur des produits* »

Il existe actuellement **deux standards principaux** pour la constitution de SBOM : SPDX et CycloneDX. SPDX et CycloneDX sont deux formats utilisables pour documenter les composants et leurs relations. Le choix doit être accompagné d'un profil de données, d'une version explicite et d'une validation de la qualité. Le purl[50] (Package URL) peut aider à identifier un paquet, sans constituer une preuve autonome d'identité ni d'exploitabilité.

| SPDX® https://spdx.dev | CycloneDX https://cyclonedx.org/ |
|---|---|
| Développée par les acteurs de la conformité juridique sous l'égide de la Linux Foundation, la première version de SPDX (pour System Package Data Exchange) date de 2011. Sa création a notamment donné lieu à l'élaboration d'une liste d'identifiants pour les licences Open Source qui est largement réutilisée, notamment dans le standard CycloneDX.<br><br>Sa version 2.2.1 a été publiée comme norme ISO/IEC 5962:2021. La version 3.0 a introduit la notion de profil, pour adresser des domaines spécifiques, dont celui de la sécurité. | Spécification plus récente, développée par les acteurs de la sécurité sous l'égide de la fondation OWASP (Open Worldwide Application Security Project).<br><br>CycloneDX a évolué pour mieux prendre en compte les informations de licences. Sa version 1.7, publiée en octobre 2025, est normalisée par ECMA-424, deuxième édition de décembre 2025. Le choix de la version doit tenir compte des informations nécessaires et de son support effectif dans les outils utilisés. |

A priori, ces deux standards peuvent permettre de répondre aux attendus du CRA dès lors qu'ils permettent de représenter le produit effectivement fourni, ses composants et leurs relations, avec une couverture explicite et des données exploitables pour la gestion des vulnérabilités. Ainsi, une acculturation sera nécessaire afin que les SBOM générés soient effectivement exploitables : au regard de la qualité des informations manipulées (la génération ou la curation de SBOM étant encore insuffisamment automatisables) et de la pertinence des informations ainsi partagées (il est nécessaire de limiter la SBOM aux seuls composants effectivement concernés dans un contexte précis).

Pour les organisations, il s'agira ensuite de s'assurer de pouvoir relier chaque SBOM au produit, à la version, à la variante distribuée et à l'empreinte de l'artefact. Pour ce faire, il faudrait distinguer ce qui est livré, les services distants compris dans le produit et les outils de construction. Le fabricant devra être en mesure de justifier les limites, composants inconnus et exclusions, et ne devra surtout pas effacer une dépendance au seul motif qu'elle complique la conformité[51]. Ce travail induit un travail de conformité encore relativement nouveau qui impose notamment de :

50 La syntaxe Package-URL est normalisée par ECMA-427, première édition de décembre 2025. Les définitions des types de paquets sont maintenues dans le dépôt communautaire PURL : https://github.com/package-url/purl-spec. Voir https://ecma-international.org/publications-and-standards/standards/ecma-427/ .

51 Voir l'article SBOM et CRA : ce que le règlement demande et pourquoi cela ne suffit pas, inno³, CC BY-SA 4.0.

- vérifier le nom, la version, la provenance ou le fournisseur, ainsi que les identifiants pertinents, les relations de dépendance, les licences et l'horodatage ;
- distinguer licence déclarée par la source et conclusion d'analyse (lorsque le format choisi le permet).
- croiser la SBOM avec les avis de sécurité et les bases de vulnérabilités, puis analyser la présence du code affecté, sa configuration et son exploitabilité dans le produit.

**Responsable principal :**

- Fabricant.

### 2.3.5 Gestion des vulnérabilités et obligations de notification

Les fabricants et les autres opérateurs économiques sont autant de pièces d'un système complet organisé pour surveiller, identifier et gérer les vulnérabilités. En combinant leurs obligations respectives, le législateur européen s'assure :

- D'un signalement aux autorités pour les événements et dans les conditions prévues par le CRA, et d'une information des utilisateurs adaptée à la situation ;
- D'un retrait des produits ou de correctifs rapides (notamment de correctifs de sécurité en cas de vulnérabilité critique) ;
- D'une surveillance en amont de la mise sur le marché (par les fabricants et importateurs) ou en aval (par les distributeurs) ;
- D'un contrôle possible par les régulateurs, permettant notamment d'accéder à la documentation technique complète pendant une période donnée.

À ce titre, lors de la mise sur le marché du produit, le fabricant aura l'obligation de fixer une période d'assistance d'au moins cinq années, sauf si la durée d'utilisation prévue du produit est inférieure, pour la version ou variante concernée, en appliquant les règles de mise sur le marché pertinentes[52]. Ce minimum de cinq ans n'est pas un plafond ; la période d'assistance doit refléter la durée d'utilisation attendue (les éléments retenus et la date de fin d'assistance doivent être documentés et communiqués dans les conditions du règlement).

Durant cette période, il aura l'obligation de systématiquement documenter et mettre à jour l'évaluation des risques de cybersécurité du produit, mais aussi de veiller à ce que les vulnérabilités du produit, y compris de ses composants, soient gérées efficacement et conformément aux exigences du CRA. Celles-ci sont précisées au sein de la partie 2 de l'Annexe

52 La FAQ de la Commission européenne nous informe que cette durée peut être différente, voire inférieure pour les produits avec une durée de vie plus courte.(FAQs on the Cyber Resilience Act §4.5.2)

1 du Règlement : documentation via une SBOM, tests et examens de sécurité, mise à jour de sécurité[53], partage rapide des correctifs, etc.[54]. À partir du 11 septembre 2026, les fabricants concernés doivent pouvoir qualifier les déclencheurs de l'article 14 et notifier dans les délais qui suivent :

| Événement | Alerte précoce | Notification | Rapport final |
|---|---|---|---|
| Vulnérabilité activement exploitée | Sous 24 heures après prise de connaissance | Sous 72 heures après prise de connaissance | Au plus tard 14 jours après disponibilité d'une mesure corrective ou d'atténuation |
| Incident grave affectant la sécurité du produit | Sous 24 heures après prise de connaissance | Sous 72 heures après prise de connaissance | Dans le mois suivant la notification à 72 heures, avec les règles particulières applicables si l'incident est encore en cours |

Ainsi, chaque événement devra être qualifié (pour savoir s'il s'agit effectivement d'une vulnérabilité activement exploitée ou encore d'un incident grave) et daté (le t0 part de cette prise de connaissance de l'événement, et ensuite éventuellement être notifié sur la plateforme unique de signalement de l'ENISA (Single Reporting Platform, SRP) en selectionnant le CSIRT compétent (en principe celui de l'état membre).

Afin de diminuer le nombre de versions supportées du logiciel et de réduire la couverture des risques, le fabricant pourra inciter ses utilisateurs à mettre à jour régulièrement les versions de la solution commercialisée et mentionner clairement quels sont les produits dépréciés qui ne font plus l'objet d'une mise sur le marché. Sauf accords spécifiques entre un fabricant et un utilisateur professionnel[55], l'obligation de gratuité des correctifs de sécurité contraint les fabricants à abandonner la monétisation des correctifs de sécurité (partie importante de la maintenance corrective) et à réinventer leur modèle économique, en intégrant ce coût dans le prix de vente initial ou en ne facturant désormais que des services à réelle valeur ajoutée (fonctionnalités, assistance)[56]. Ainsi, les mises à jour de sécurité pourront être clairement séparées des évolutions fonctionnelles lorsque cela est techniquement possible.

À noter que la notification aux autorités ne remplacera pas l'information des utilisateurs touchés et, s'il y a lieu, de tous les utilisateurs. Après prise de connaissance, le fabricant les informe (en « temps utile » et sans attendre le rapport final) de l'événement et, si nécessaire,

53 Le CRA impose par ailleurs de fournir les mises à jour de sécurité séparément des mises à jour fonctionnelles lorsque c'est techniquement possible, tout en permettant de les combiner lorsqu'une correction de sécurité nécessite aussi une modification fonctionnelle ou lorsque la modification fonctionnelle constitue elle-même la mise à jour de sécurité. . FAQs on the Cyber Resilience Act §4.3.5

54 4.3.2Exigences relatives à la gestion des vulnérabilités

55 Voir la FAQs on the Cyber Resilience Act, https://ec.europa.eu/newsroom/dae/redirection/document/122331

56 Dans le cas des logiciels libres et Open Source qui resteraient utilisés même après la fin des services de support payants, le fabricant doit garantir une période de support correspondant à la durée de l'abonnement actif aux services payants, afin d'assurer la maintenance et la sécurité pendant cette période FAQs on the Cyber Resilience Act §4.5.2

des mesures qu'ils peuvent applique. En pratique, il est recommandé de préparer un avis identifiant les produits et versions concernés, les mesures immédiates, le correctif disponible et les modalités de suivi.

**Responsable principal :**

- Fabricant ;

**Responsables subséquents :**

- Distributeur ;
- Importateur (si fabricant hors UE) ;
- Intendants de logiciels ouverts dans le cas de logiciels Open Source destinés à des activités commerciales : obligations de l'article 24 à distinguer des obligations générales d'assistance et de gestion du fabricant.

### 2.3.6 Synthèse

Le tableau qui suit synthétise les principales obligations pour chacun des rôles prévus par le CRA.

| Rôle | Obligations |
|---|---|
| **Fabricant**<br><br>Personne physique ou morale qui **développe ou fabrique** des produits comportant des éléments numériques ou **fait concevoir, développer ou fabriquer** des produits comportant des éléments numériques, et les **commercialise sous son propre nom ou sa propre marque**, à titre onéreux, monétisé ou gratuit. | **1.** Le fabricant sera tenu d'**appliquer, ou de faire appliquer, les procédures de conformité établies par le CRA pour les produits qu'il commercialise**. Cela inclut notamment l'établissement de la **déclaration UE de conformité** et l'**apposition du marquage CE**.<br>**2.** Le fabricant devra également **établir et maintenir une documentation précise, incluant une SBOM**.<br>**3.** En cas d'**incident grave ou de vulnérabilité activement exploitées** sur l'un de ses produits, il sera dans l'obligation de le **signaler aux autorités compétentes, aux responsables de la maintenance et aux utilisateurs concernés** (si possible via l'interface utilisateur[57]**).** Il devra également **prendre toutes les mesures nécessaires pour corriger la vulnérabilité et diffuser les correctifs correspondants à la personne ou à l'entité qui en assure la maintenance.** |
| **Intendant de logiciels ouverts (*open source steward*)**<br><br>Personne morale, autre que le fabricant, qui a pour objectif ou finalité de **fournir un soutien systématique et continu au développement** de produits spécifiques comportant des éléments numériques qui répondent aux **critères de logiciels libres et ouverts** et sont **destinés à des** | **1.** À compter du 11 décembre 2027, l'article 24, paragraphe 3, prévoit l'application aux intendants des obligations de l'article 14, paragraphe 1, dans la mesure où ils participent au développement des produits concernés (**mise en place et documenter d'une politique de cybersécurité claire et vérifiable**). Il prévoit également l'application des obligations de l'article 14, paragraphes 3 et 8, dans la mesure où des incidents graves affectant la sécurité de ces produits ont une incidence sur les réseaux et systèmes d'information qu'ils fournissent pour leur développement.<br>**2.** L'intendant de logiciels ouverts doit **coopérer avec les autorités de surveillance pour réduire les risques de cybersécurité** liés aux produits numériques utilisant des logiciels libres. À la demande des autorités, il doit fournir la documentation relative à leur politique de cybersécurité, sous |

57 Voir notamment l'article 14 § 8 pour l'information des utilisateurs en cas de vulnérabilité activement exploitée ou d'incident grave ; l'annexe I, partie II, point 4 pour la publication d'informations sur les vulnérabilités corrigées ; le considérant 56 et l'article 13 § 19 concernent quant à l'information sur la fin de la période d'assistance.

| | | |
|---|---|---|
| | **activités commerciales**, et qui assure la viabilité de ces produits. | format papier ou électronique, dans une langue claire.<br>**3.** À partir du 11 décembre 2027, les obligations de l'article 14 § 1 s'appliquent à l'intendant lorsqu'il participe au développement des produits concernés lorsque des incidents graves affectant la sécurité de ces produits touchent les réseaux et systèmes d'information qu'il fournit pour leur développement[58]. |
| | **Mandataire**<br><br>Personne physique ou morale établie dans l'Union **ayant reçu mandat écrit du fabricant** pour agir en son nom aux fins de l'accomplissement de tâches déterminées[59]. | Le mandataire réalise les tâches qui lui sont confiées par le fabricant. À la demande des autorités de surveillance, il leur fournit une copie de son mandat. Ce mandat lui donne a minima les responsabilités suivantes :<br>**1.** **Conserver et mettre à disposition des autorités la déclaration de conformité et la documentation technique** pendant au moins dix ans après la mise sur le marché du produit, ou pendant la durée de l'assistance, selon la période la plus longue.<br>**2.** Fournir, à la demande des autorités, toutes les informations et tous les **documents nécessaires pour prouver que le produit est conforme.**<br>**3.** **Collaborer avec les autorités** pour toute action visant à éliminer les risques liés au produit. |
| | **Importateur**<br><br>Personne physique ou morale **établie dans l'Union** qui **met sur le marché un produit comportant des éléments numériques**, lequel porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union. | **1.** L'importateur doit vérifier que le fabricant a respecté toutes ses obligations légales et il ne peut mettre sur le marché que des **produits comportant des éléments numériques conformes aux exigences de cybersécurité**. Avant de les commercialiser, il **doit s'assurer que le fabricant a bien suivi les procédures de conformité, que la documentation technique est en place, que le produit porte le marquage CE, et qu'il est accompagné de la déclaration de conformité et des instructions, rédigées dans une langue claire**.<br>**2.** Si l'importateur a des raisons de croire qu'un produit ou les processus du fabricant ne respectent pas ces exigences, il ne doit pas le mettre sur le marché tant que les problèmes ne sont pas corrigés. En cas de **risque de cybersécurité important, il doit immédiatement en informer le fabricant et les autorités compétentes**. De plus, il est tenu de rendre ses coordonnées (nom, adresse, e-mail) facilement accessibles sur le produit ou l'emballage ou dans un document l'accompagnant, afin que les utilisateurs et les autorités puissent le contacter si nécessaire.<br>**3.** Si un produit déjà mis en circulation s'avère non conforme, l'importateur doit rapidement **prendre des mesures correctives, telles que le retrait ou le rappel du produit**. Lorsqu'il identifie une vulnérabilité, il en informe sans délai le fabricant et, si le risque est important, il doit aussi **alerter les autorités compétentes**.<br>**4.** Il est responsable de **conserver, pendant au moins dix ans** (ou pour la durée de l'assistance si elle est plus longue), une copie de la déclaration UE de conformité et des documents techniques, afin de les fournir aux autorités sur demande.<br>**5.** Enfin, si l'importateur découvre que le fabricant a cessé ses activités et ne peut plus respecter ses obligations, il doit immédiatement en **informer les autorités de surveillance** et, si possible, les utilisateurs concernés par les produits déjà mis sur le marché. |
| | **Distributeur**<br><br>Personne physique ou morale | **1.** Lorsque le distributeur met à disposition sur le marché un produit contenant des éléments numériques, il doit réaliser plusieurs vérifications **relatives aux exigences de cybersécurité** (marquage CE, fourniture des |

58 La portée exacte de cette obligation, notamment quant à l'infrastructure directement fournie par l'intendant et aux composants tiers dont elle dépend, reste discutée au sein de la communauté. À la date de rédaction, elle n'a pas fait l'objet d'une clarification de la Commission européenne.

59 L'article 3.2 du Blue Guide précise « *les tâches pouvant être déléguées au mandataire conformément à la législation d'harmonisation de l'Union sont de nature administrative. Dès lors, le fabricant ne peut déléguer ni les mesures nécessaires pour faire en sorte que le procédé de fabrication garantisse la conformité des produits, ni l'établissement d'une documentation technique, sauf disposition contraire. En outre, un mandataire ne peut modifier le produit de sa propre initiative en vue de le rendre conforme à la législation d'harmonisation de l'Union applicable* ». https://eur-lex.europa.eu/

| | | |
|---|---|---|
| | faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui **met un produit comportant des éléments numériques** à disposition sur le marché de l'Union sans altérer ses propriétés. | documents requis, exécution des obligations du fabricant ainsi que de l'importateur)[60]. Si le distributeur a des raisons de croire qu'un produit ou ses processus de fabrication ne sont pas conformes aux exigences, il **ne doit pas le mettre à disposition (vendre, louer, etc.) tant que la conformité n'est pas assurée.** En cas de risque de cybersécurité important, il doit en informer immédiatement le fabricant et les autorités de surveillance du marché.<br>**2.** Si un produit déjà mis en circulation s'avère non conforme, le distributeur doit **s'assurer que des mesures correctives sont prises,** telles que le retrait ou le rappel du produit. S'il découvre une vulnérabilité, il doit prévenir rapidement le fabricant, et si le risque est jugé important, il doit aussi alerter les autorités de surveillance. De plus, à la demande des autorités, le distributeur doit être en mesure de fournir les documents prouvant la conformité du produit et coopérer pour résoudre les risques de cybersécurité.<br>**3.** Enfin, si le distributeur apprend que le fabricant a cessé ses activités et ne peut plus respecter ses obligations, il doit en **informer sans délai les autorités concernées** et, si possible, les utilisateurs affectés. |

*Tableau 3: Synthèse des principales obligations pour chacun des rôles prévus par le CRA.*

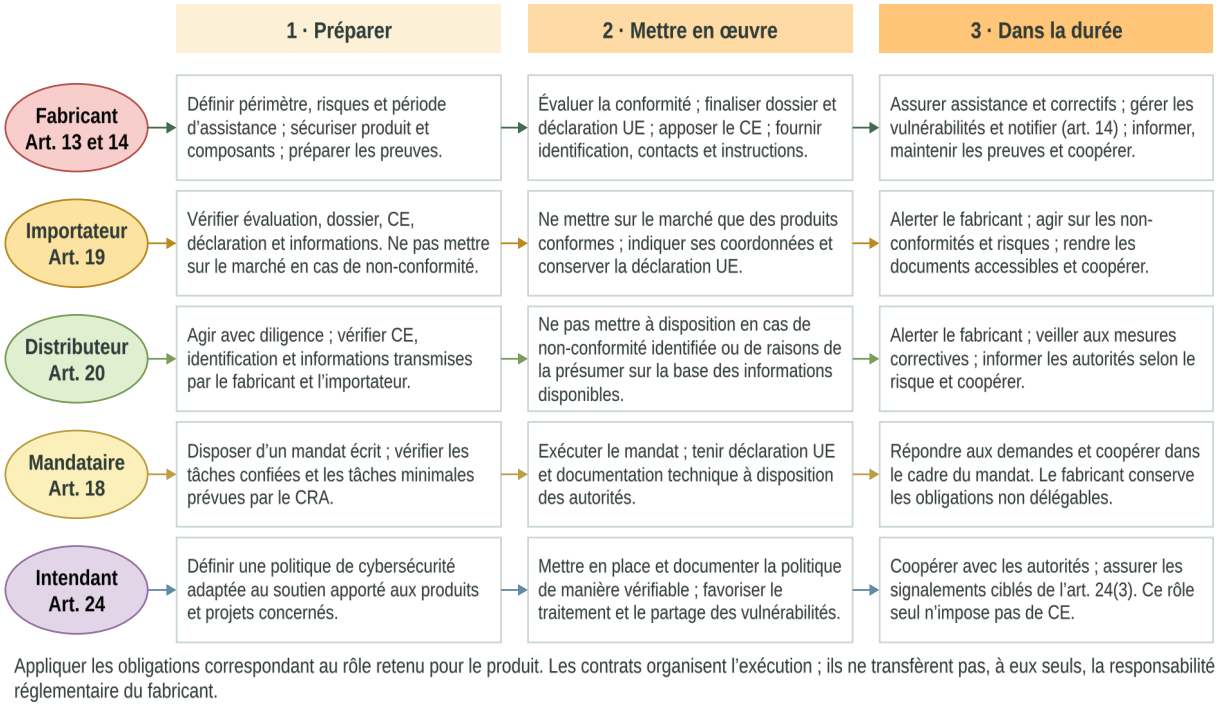



*Figure 3: Représentation des différents rôles et responsabilités des opérateurs, en amont et en aval de la mise sur le marché d'une solution numérique.*

60 Le Règlement ne donne pas de précisions concernant le format de ces documents hormis qu'ils peuvent être « *sur support papier ou par voie électronique* ».

## 2.4 | Régulation, sanctions et accompagnements

### 2.4.1 Les autorités de régulation

Le CRA établit une approche coordonnée en désignant plusieurs autorités de régulations qui auront pour mission de mettre en œuvre et de faire respecter le Règlement.

En France, les pages officielles consultées présentent l'ANSSI comme autorité notifiante des organismes d'évaluation, le CERT-FR pour le traitement des signalements et l'ANFR comme autorité de surveillance du marché.

Chaque État membre est par ailleurs encouragé à établir un point d'entrée unique national pour toutes les notifications de sécurité.

*Table 4: Définition des différentes autorités de régulation et de leurs missions respectives*

| Autorités | Organisation concernée (France ou UE) | Missions |
|---|---|---|
| **Autorités de surveillance du marché** | ANFR (Agence nationale des fréquences, avec l'appui technique de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). | 1. Assurent la conformité des produits numériques avec les standards de cybersécurité établis. Elles veillent ainsi à ce que les produits mis sur le marché respectent les exigences de sécurité pour protéger les consommateurs et les infrastructures.<br>2. Informent les consommateurs pour faciliter les signalements.<br>3. Coopèrent entre elles, avec les CSIRT (Computer Security Incident Response Team) et d'autres agences nationales et européennes pour garantir une approche cohérente.<br>4. Partagent des statistiques et des données sur leurs activités de surveillance et d'application du règlement |
| **Agence européenne chargée de la plateforme de signalement et de l'appui technique** | ENISA (Agence de l'Union européenne pour la cybersécurité) | 1. Développer, exploiter et maintenir la plateforme unique de signalement : Single Reporting Platform (SRP)<br>2. Adopte des normes strictes de sécurité et de confidentialité. La plateforme sera intégrée avec la base de données européenne des vulnérabilités.<br>3. Prépare un rapport tous les deux ans destiné à identifier les tendances émergentes en cybersécurité des produits numériques. |
| **Groupe de coopération administrative des autorités de surveillance du marché** | CRA ADCO, groupe européen réunissant les représentants des autorités nationales de surveillance du marché. L'autorité française concernée par cette fonction est l'ANFR. | 1. Traite des questions spécifiques liées aux activités de surveillance du marché en ce qui concerne les obligations imposées aux intendants de logiciels ouverts.<br>2. Centralise les informations sur les composants logiciels utilisés dans les produits numériques pour surveiller les dépendances critiques en matière de cybersécurité (les autorités peuvent demander les SBOM pertinentes aux fabricants et transmettre à l'ADCO des informations anonymisées et agrégées).<br>3. Publie des statistiques sur les périodes d'assistance moyennes et propose des durées indicatives de support pour chaque catégorie de produit, en identifiant ceux qui nécessitent une surveillance accrue. |
| **CSIRT désigné comme coordonnateur national** | CERT-FR, le centre gouvernemental et national de réponse aux incidents de sécurité informatique, rattaché à l'ANSSI. | 1. Traite les notifications de vulnérabilité.<br>2. Assure la coordination et la notification entre les autorités de surveillance et l'ENISA.<br>3. Peut retarder la diffusion d'une notification dans des situations exceptionnelles où la sécurité de certains États membres est en jeu. |
| **Autorité notifiante** | ANSSI (Agence nationale de la sécurité des systèmes d'information) | 1. Évaluer,<br>2. notifier à la Commission européenne<br>3. et contrôler les organismes d'évaluation de la conformité autorisés à intervenir dans le cadre du CRA. |
| **Organisme national d'accréditation** | Cofrac (Comité français d'accréditation) | 1. Évaluer la compétence et l'impartialité des organismes d'évaluation de la conformité ;<br>2. délivrer et suivre les accréditations servant de base à leur notification par l'ANSSI, selon les modalités du dispositif français. |

## 2.4.2 Les accompagnements associés au CRA

Le CRA prévoit un rôle d'accompagnement de ces autorités au bénéfice :

- **Des microentreprises[61] ou des petites[62] ou moyennes[63] entreprises** : service d'assistance en ce qui concerne les obligations de signalement énoncées à l'article 14 (Article 17) ; publication d'orientations destinées à aider à l'application du règlement (Article 26) ;
- **Des projets et acteurs de l'Open Source** : programmes volontaires d'attestation de sécurité des logiciels libres et ouverts (Article 25), prise en compte des logiciels libres et ouverts dans les orientations futures de la Commission (Article 26) et relations privilégiées avec les intendants de logiciels libres et ouverts.

Au-delà des obligations ciblées de signalement des vulnérabilités aux mainteneurs des composants Open Source intégrés (*upstream*) et, le cas échéant, de partage des correctifs développés (article 13, paragraphe 6), ces programmes viseraient à répondre aux spécificités des logiciels libres et ouverts et seraient accessibles à toute personne ou entité développant ou utilisant ce type de logiciel, y compris les fabricants tiers qui intègrent les produits, les utilisateurs finaux et les administrations publiques de l'Union européenne.

Afin de permettre une convergence vertueuse entre la dynamique de cybersécurité et celle de l'Open Source, il reste ainsi un travail d'anticipation important à mener par les projets Open Source – avec l'aide des régulateurs – pour **s'assurer que les contributions susceptibles d'être reversées aux projets ne créent pas des situations non soutenables dans la durée** : soit que les projets Open Source ne soient pas en capacité de répondre aux sollicitations (et demandes de contributions), soit que les projets se retrouvent trop fortement influencés par les besoins des fabricants (et dans l'incapacité de mener à bien leurs propres missions).

À noter que le dispositif est encore en pleine construction et pour le moment partiellement contraignant :

- les normes harmonisées restent volontaires (leurs publications au Journal officiel ouvrira une présomption de conformité, limitée aux exigences qu'elles couvrent et aux conditions de leur citation).
- des programmes volontaires d'attestation de sécurité pour les logiciels libres et ouverts sont prévus par le règlement ;

61 Moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros. Cf Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (Texte présentant de l'intérêt pour l'EEE) [notifiée sous le numéro C(2003) 1422].

62 Moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros.

63 Moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total du bilan annuel n'excède pas 43 millions d'euros.

- la Commission européenne a publié, le 7 juillet 2026, son Plan d'action sur la cybersécurité et l'intelligence artificielle[64]. Parmi les actions prévues au quatrième trimestre 2026 figure une Critical Open Source Resilience Campaign, visant à cartographier les composants open source critiques et à accélérer le déploiement de correctifs, notamment grâce à l'IA. Encore au stade pilote, cette initiative pourrait interagir avec les obligations de diligence du CRA.
- enfin, des bonnes pratiques sont déjà largement diffusées, tel que ce guide ou les analyses de l'intendance et des ressources de préparation de ORC WG, les repères de gouvernance et de sécurité d'OpenSSF, ou encore les programmes tels qu'OCCTET qui propose une autoévaluation et une chaîne d'outillage.

### 2.4.3 Les sanctions associées au non-respect du CRA

Chaque État membre détermine le régime des sanctions applicables aux violations du CRA et est chargé de les mettre en œuvre. Ces sanctions **doivent être effectives, proportionnées et dissuasives**. Elles sont **prises au cas par cas**. Dans ce but, le CRA explicite certains critères devant être pris en considération pour décider du montant des amendes administratives :

- **La nature, la gravité et la durée** de l'infraction et de ses conséquences ;
- D'éventuelles **amendes administratives précédemment imposées au même opérateur** économique pour une infraction similaire ;
- **La taille et la part de marché** de l'opérateur économique qui commet l'infraction.

Afin d'accompagner les États membres, le CRA détaille différents plafonds en fonction des typologies de violations des obligations et des acteurs concernés.

*Tableau 5: Typologie de sanctions prévues dans le cadre du CRA pour les opérateurs économiques non conformes.*

| Opérateurs économiques concernées | Obligations concernées | Montant de la sanction |
|---|---|---|
| ➔ Les fabricants | Exigences essentielles de l'annexe I et obligations des articles 13 et 14. | Jusqu'à 15 000 000 euros ; ou 2,5 % du CA annuel mondial de l'exercice précédent si ce montant est supérieur pour une entreprise. |
| ➔ Les fabricants ;<br>➔ Les mandataires ;<br>➔ Les importateurs ;<br>➔ Les distributeurs. | Déclarations de conformité, marquage CE, documentation technique, procédures d'évaluation de conformité, actions suites à une notification. | Jusqu'à 10 000 000 euros ou 2 % du CA annuel mondial de l'exercice précédent si ce montant est supérieur. |
| ➔ Les fabricants ;<br>➔ Les mandataires ;<br>➔ Les importateurs ;<br>➔ Les distributeurs. | La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés et aux autorités de surveillance du marché en réponse à une demande. | Jusqu'à 5 000 000 euros ; pour une entreprise, 1 % du CA annuel mondial de l'exercice précédent si ce montant est supérieur. |

64 https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence

Le CRA prévoit néanmoins quelques dérogations[65] quant à l'application de ces sanctions (sans supprimer néanmoins les obligations) :

- Aux fabricants considérés comme des **microentreprises** ou des **petites entreprises**[66] en cas de :
  - Non-respect du délai en matière d'alerte précoce de vulnérabilité activement exploitée au plus tard 24 heures après en avoir eu connaissance (article 14, paragraphe 2, point a)) ;
  - Ou d'alerte précoce d'incident grave ayant des répercussions sur la sécurité du produit au plus tard 24 heures après en avoir eu connaissance (article 14, paragraphe 4, point a).
- À toute violation du règlement par les **intendants de logiciels ouverts**.

Pour finir, les sanctions prévues par le CRA sont importantes, mais le texte laisse une certaine marge de manœuvre aux États membres à l'instar du Règlement Général sur la Protection des Données (RGPD)[67]. De même, chaque État membre établit les règles déterminant si, et dans quelles mesures, des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

65 Article 64, paragraphe 10. Voir le considérant 120 : « Étant donné qu'une amende administrative ne peut être infligée à une microentreprise ou une petite entreprise pour non-respect du délai de vingt-quatre heures fixé pour notifier une alerte précoce de vulnérabilités activement exploitées ou d'incidents graves ayant des répercussions sur la sécurité du produit comportant des éléments numériques, ni à un intendant de logiciels ouverts pour quelque infraction au présent règlement que ce soit, et compte tenu du principe qui prévoit que les sanctions soient efficaces, proportionnées et dissuasives, il convient que les États membres n'imposent auxdites entités aucun autre type de sanction de nature pécuniaire. »

66 Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (Texte présentant de l'intérêt pour l'EEE) [notifiée sous le numéro C(2003) 1422].

67 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

# 3 Méthodologie de travail pour une mise en conformité

Le guide promeut une mise en conformité pensée en prolongation des démarches de gestion de l'Open Source et de cybersécurité déjà engagées par les organisations (production de SBOM, mise en place d'un Open Source Program Office, etc.). En effet, le CRA n'impose pas de méthode unique pour organiser ce travail et une démarche efficace cherchera à s'appuyer sur les outils existants du projet pour relier les exigences applicables aux décisions, aux actions et aux preuves qui permettent d'en vérifier le résultat (étant entendu que le niveau de détail dépendra des produits, des risques et du rôle exercé par chaque organisation).

La méthodologie qui suit propose six étapes adaptables à chaque organisation et fait référence à des documents types proposés comme aides méthodologiques qui seront partagés sur le dépôt public du guide. Elle s'appuie sur des ateliers consacrés au produit et à ses rôles, aux vulnérabilités, puis à l'assistance et aux preuves, pour partir des pratiques réelles :

1. Cadrer et qualifier
2. Construire le registre des exigences et des preuves
3. Évaluer les risques de cybersécurité
4. Mettre en place les processus attendus
5. Constituer le dossier adapté au rôle
6. Vérifier puis suivre

Le diagnostic initial alimentera un premier plan d'actions (avec des responsables et des priorités) qui devra ensuite être mis à jour d'année en année. Certaines étapes pointeront des corrections et notifications urgentes, pouvant être rapidement mises en œuvre, alors que d'autres demanderont une transformation globale de l'organisation. Les urgences seront traitées sans attendre la fin du diagnostic.

## 3.1 | Cadrage et qualification

Les différents régimes applicables sont dépendants de la typologie de produits concernés et des activités de l'organisation concernée ; une étude au cas par cas est ainsi nécessaire pour définir ensuite les processus communs au sein de l'organisation.

Pour commencer, il est généralement recommandé l'instauration d'une **fiche par produit** et variante ou de s'appuyer sur des référentiels ou catalogues internes. Elle devra préciser l'entité

responsable, les fonctionnalités apportées, les composants concernés, les services distants associés, les utilisateurs actuels ou pressentis, le mode de fourniture actuel ou pressenti, la date de mise sur le marché ainsi que certaines considérations relatives à l'usage de la marque ainsi que le modèle économique associé (contrats, règles de gouvernance en cas de portage collectif, considérations d'architecture en cas de modèle de type Open Core, etc.).

Ce type de fiche permet de justifier (et tracer) les rôles et les exclusions, et de catégoriser lorsque nécessaire le produit selon les régimes des annexes III et IV et du règlement d'exécution (UE) 2025/2392. Cette procédure doit être pilotée en interne de manière neutre afin de ne pas « choisir » librement un statut qui contredirait les faits. En cas de doute, il est possible d'anticiper les mesures les plus protectrices, tout en documentant les interprétations en présence et les faits à établir pour trancher la qualification.

En fonction des rôles, les obligations ne seront pas de même nature, même si les acteurs pourront s'appuyer sur une démarche commune pour inventorier les produits et les flux, et désigner les processus et personnes responsables. Les produits déjà mis sur le marché doivent aussi être examinés car deux règles doivent être distinguées :

- Les obligations de signalement s'appliquent dès le 11 septembre 2026 à tous les produits même si le produit n'a pas été modifié.
- Les autres exigences du CRA ne deviennent applicables à ces produits que s'ils font l'objet d'une modification substantielle à compter du 11 décembre 2027 qui affecterait leur conformité aux exigences essentielles de cybersécurité ou change l'utilisation prévue pour laquelle ils avaient été évalués (une simple opération de maintenance n'est donc pas concernées).

Cette « **Fiche de périmètre et de qualification** » listera, au-delà du périmètre examiné (rôles et catégories retenus), les justifications ainsi que les questions restant à résoudre, avec une personne chargée de chacune.

## 3.2 | Diagnostic et création des registres des exigences et des preuves

Les ateliers s'appuieront sur une « **Trame d'ateliers et diagnostic** » et permettront d'alimenter le « **Diagnostic initial** » qui distinguera une exigence encore à clarifier, une pratique mise en œuvre mais non documentée, et une mesure dont la preuve a été vérifiée. Les écarts alimenteront le « **Plan d'actions** », en précisant pour chaque action le résultat attendu, son responsable, son échéance et la preuve qui permettra de la clôturer.

Les processus définis devront notamment s'appuyer sur un registre interne qui est le pendant des fiches préalablement constituées. Il comporte une ligne par exigence applicable et par produit, et distingue ce qui est réalisé de ce qui a été vérifié : la référence précise de l'exigence, la justification d'applicabilité (en cas de non-application, il est nécessaire de conserver les éléments techniques et juridiques qui justifient cette décision), la mesure prévue (dans les limites de ce que permet le CRA), son état de mise en œuvre, son responsable, son échéance, la ou les preuves et la décision de validation, etc.

Il n'est pas imposé de registre unique interne ; la bonne pratique sera certainement de s'appuyer sur les registres préexistants autant que possible en intégrant la dimension des « exigences » identifiant ce qui est demandé et la dimension « des preuves » qui indiquera, pour chaque pièce, le produit et la version concernés, sa date, son emplacement et le contrôle effectué. Ces deux vues peuvent être réunies dans un même outil.

## 3.3 | L'évaluation des risques de cybersécurité

Le CRA impose au fabricant une « **évaluation des risques de cybersécurité** », documentée et mise à jour selon les besoins pendant la période d'assistance (art. 13 § 2 et 3). Pour la conduire, l'organisation décrira l'architecture, les actifs à protéger, les menaces, les interfaces et les usages prévus ou raisonnablement prévisibles. Elle examinera les scénarios d'atteinte, les mesures déjà en place et celles à ajouter, puis les essais permettant d'en vérifier l'efficacité. Cette évaluation reliera les risques aux exigences de l'annexe I et précisera les risques résiduels.

La méthode retenue dans ce cadre doit produire des preuves de mise en œuvre et de vérification. Pour les composants tiers, l'origine, la version, les correctifs et la capacité de traitement des vulnérabilités sont documentés. Ainsi, le contrôle de la SBOM portera sur la validité du format, l'exactitude des données, sa correspondance avec le produit et la possibilité de retrouver un composant concerné par une alerte de manière automatisée et transversale. Les limites de couverture et les mesures compensatoires sont explicitées, sans écarter une obligation applicable[68].

Cette étape produira un document interne de référence qui pourra être accompagné des schémas utiles et des rapports d'essais. Pour les composants, le « **Référentiel des composants** » indiquera les données vérifiées (le contrôle de chaque SBOM donnera lieu à un rapport conservé avec la version du fichier examiné -- les insuffisances identifiées rejoindront le plan d'actions). Ces éléments doivent être pensés comme une matérialisation de la maturité de l'organisation en matière de cybersecurité.

68 Règlement (UE) 2024/2847 (CRA), art. 13 § 2, 3, 5 et 6 ; annexe I.

## 3.4 | Mise en place des processus attendus

Le CRA imposant la mise en place de processus effectifs, l'organisation devra préciser pour chaque mesure retenue qui la réalise, à quel moment et avec quelle condition de contrôle. Les contrôles de conception, les essais de sécurité, la production de la SBOM et la distribution sécurisée des mises à jour pourront être intégrés aux processus de développement et de livraison existants afin d'être utilement alimentés par les équipes de développement. Chaque contrôle devra laisser une preuve identifiable, reliée à la version concernée dans le registre.

Pour les vulnérabilités, la « **Politique de traitement et de divulgation des vulnérabilités** » décrira le canal de réception, la qualification des signalements, la correction, l'information des utilisateurs, les notifications et la coordination avec les mainteneurs de composants. Elle désignera les responsables et leurs suppléants. Elle s'appuiera sur la tenue d'un « **registre des vulnérabilités** » qui permettra de conserver, pour chaque cas, les versions affectées, les heures de connaissance, les mesures prises, les échanges et les preuves.

Enfin, le « **Dossier de notification et exercice de préparation** » regroupera les critères de déclenchement, les destinataires, les informations à recueillir et les règles de calcul des délais. Un tel dossier permet aussi de matérialiser les processus attendus, d'identifier les manquements ou difficultés à anticiper.

La préparation comprend les comptes personnels EU Login, l'authentification multifacteur, la suppléance, les informations produit et la détermination du CSIRT compétent. Les consignes de l'ENISA récemment publiées recommandent l'inscription à la SRP lorsqu'une notification devient nécessaire ; la validation du déclarant par le CSIRT se déroule en parallèle du dépôt initial. Pour les intendants, le circuit de l'article 24 § 3 dépend du soutien réellement fourni et s'applique à partir du 11 décembre 2027.

## 3.5 | Constitution de dossier adapté au rôle

Le fabricant rassemblera les pièces de l'annexe VII dans un « Dossier technique du fabricant » :

- description du produit et de son architecture,
- évaluation des risques,
- processus de gestion des vulnérabilités,
- essais,
- informations utilisateur
- et autres pièces requises.

La procédure d'évaluation de conformité de l'article 32 sera déterminée suffisamment tôt pour prévoir les contrôles et, lorsqu'il est requis, le recours à un organisme notifié. Le registre des preuves permettra de vérifier que les pièces correspondent au produit effectivement fourni. Le fabricant établira ensuite la « Déclaration UE de conformité » et apposera le marquage CE lorsque les conditions seront satisfaites.

L'intendant constituera aussi un dossier réunissant sa **politique de cybersécurité vérifiable**, le périmètre des activités soutenues et les éléments démontrant la mise en œuvre de cette politique et la coopération prévue à l'article 24. L'adoption de bonnes pratiques de sécurité ne lui impose pas, du seul fait de ce rôle, un dossier de fabricant ou un marquage CE.

Pour les autres rôles, le dossier identifiera les contrôles à effectuer et les pièces à conserver ou à pouvoir fournir :

- mandat écrit du mandataire,
- copie de la déclaration UE et accès organisé à la documentation technique pour l'importateur,
- preuves des vérifications du distributeur.

La trame « Adapter les outils à l'intendant, à l'importateur, au distributeur et au mandataire » aidera à sélectionner les rubriques pertinentes, en les reliant au registre des exigences.

## 3.6 | Vérification et suivi

Le registre sera revu avant chaque livraison importante et après une vulnérabilité significative, une modification substantielle ou une évolution du modèle économique. Cette revue vérifiera, selon le rôle et les obligations applicables, que la qualification, l'évaluation des risques, la SBOM, les essais et les informations utilisateur correspondent toujours à la version distribuée. Le registre consignera les contrôles réalisés, les écarts, les décisions et les conditions éventuelles à satisfaire avant la fourniture du produit. Un audit de maturité favorable ne vaut pas, à lui seul, conformité juridique.

Le « **Plan d'actions** » sera ensuite mis à jour au fil des travaux ; une action ne sera clôturée qu'après vérification du résultat et de sa preuve. Le registre permettra de suivre les évolutions du produit, de l'organisation et des textes, avec leurs conséquences sur les documents existants. Les versions antérieures et les décisions remplacées seront conservées selon les règles applicables. L'objectif est de pouvoir retrouver et expliquer, pour une livraison déterminée, les exigences retenues, les mesures réalisées et les preuves correspondantes.

# 4 | Annexes

## 4.1 | Mise en application du règlement dans le cadre des activités Open Source

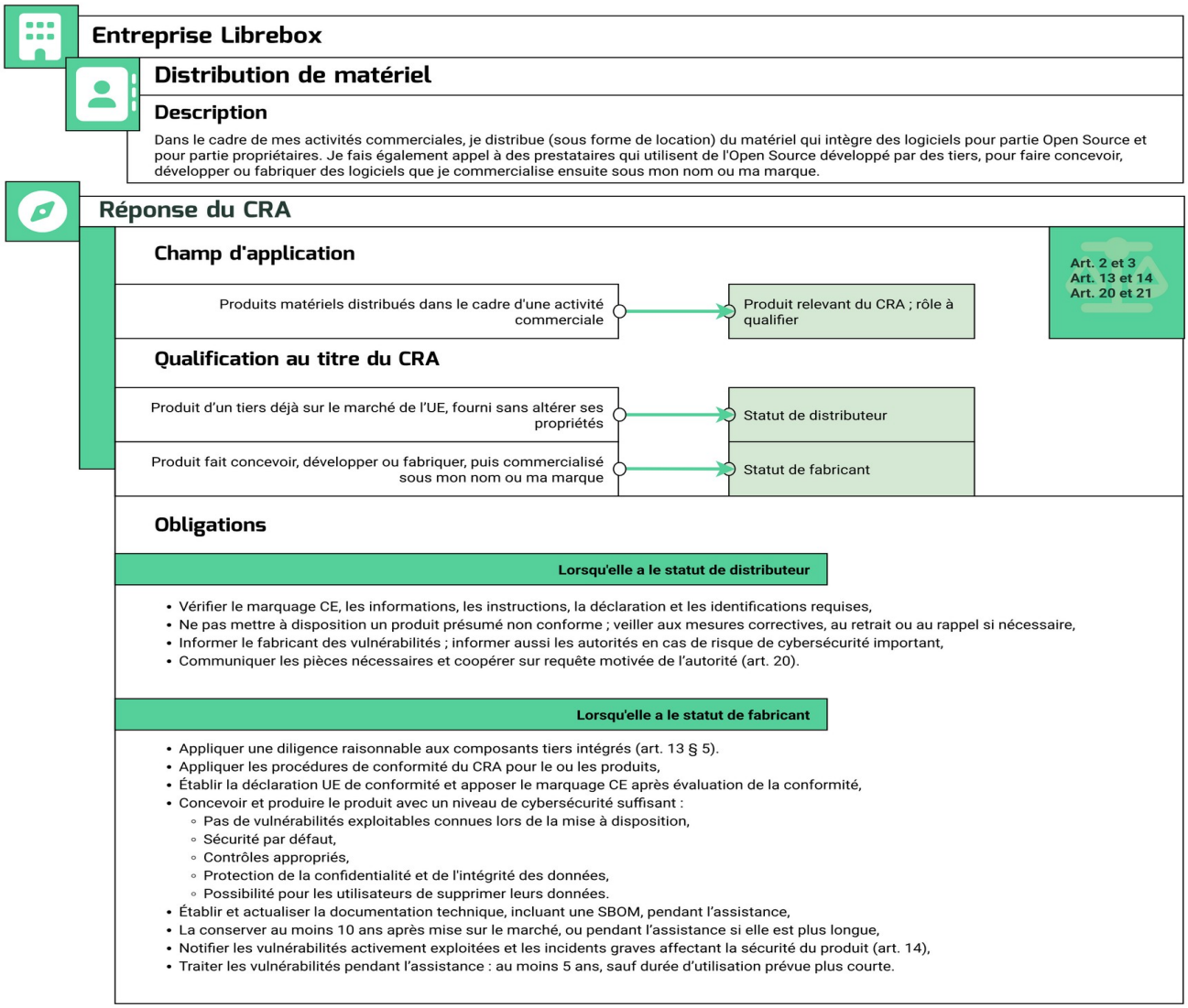
Les pages qui suivent visent à se projeter dans la mise en application du CRA dans le cadre d'un certain nombre d'activités économiques repérées au sein des membres du CNLL. Les cas sont fictifs et volontairement simplifiés.

### 4.1.1 Synthèse des différentes mises en situation

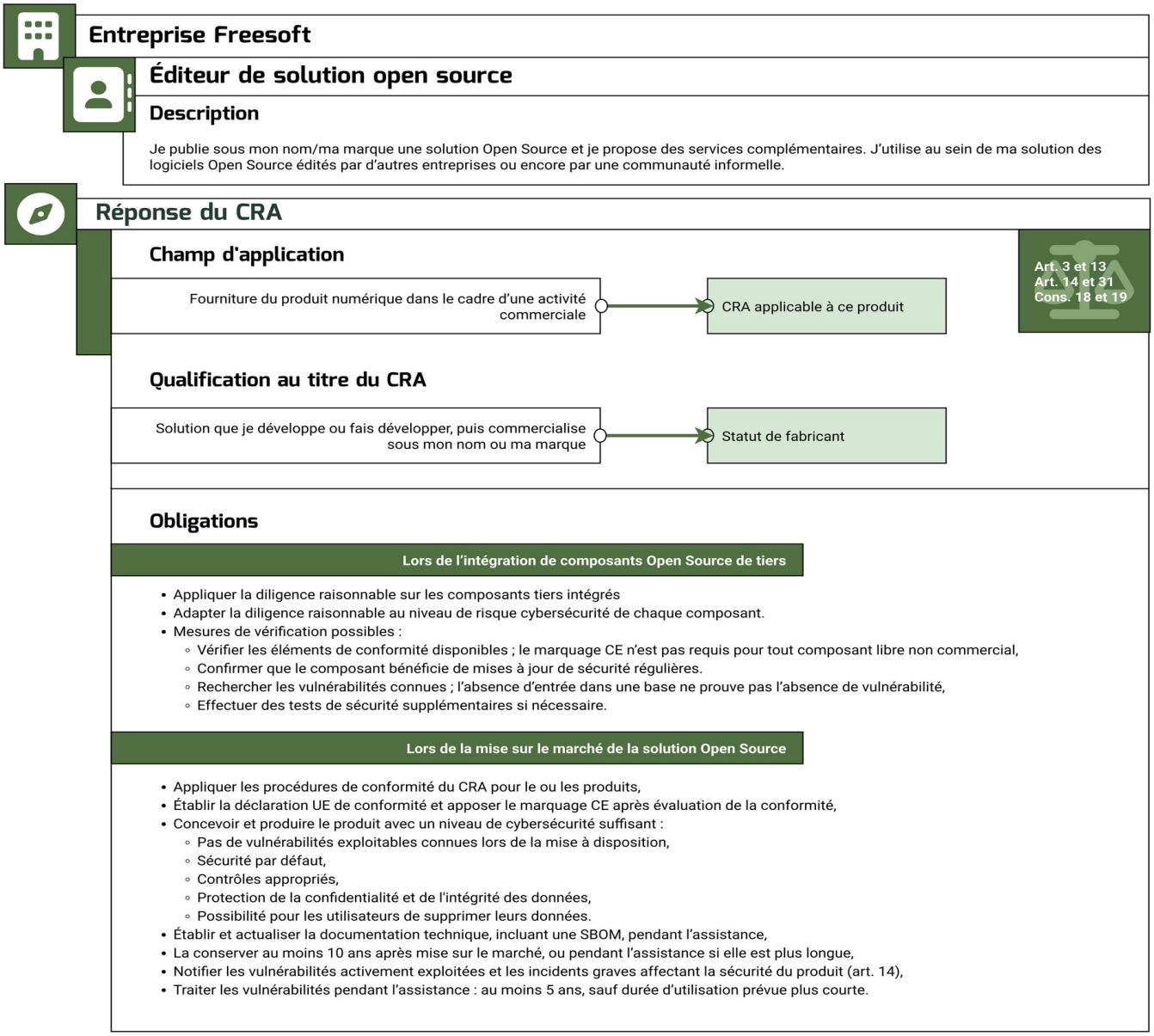
| | ***Opérateurs nommés dans le CRA*** | | | | |
|---|---|---|---|---|---|
| | Fabricant | ***Intendant de logiciels ouverts (open source software steward)*** | ***Mandataire*** | ***Importateur*** | ***Distributeur*** |
| **Distributeur** de matériel intégrant des composants Open Source | (X) | | | | X |
| **Éditeur** d'une solution Open Source | X | | | | |
| **Contributeur** au projet d'une Fondation Open Source commercialisé sur le territoire européen | | | | (X) | |
| Entreprise **intégratrice** de solutions Open Source (avec modification substantielle) | X | | | | |
| Entreprise **opérant des services en SaaS** s'appuyant sur une solution numérique interne. | (X) | | | | |
| Entreprise **utilisatrice** d'un logiciel Open Source modifié | (X) | | | | |
| Développeur indépendant et consultant IT | | | | | |

*Tableau 6: Synthèse des différentes qualifications d'opérateur économique au titre du CRA.*

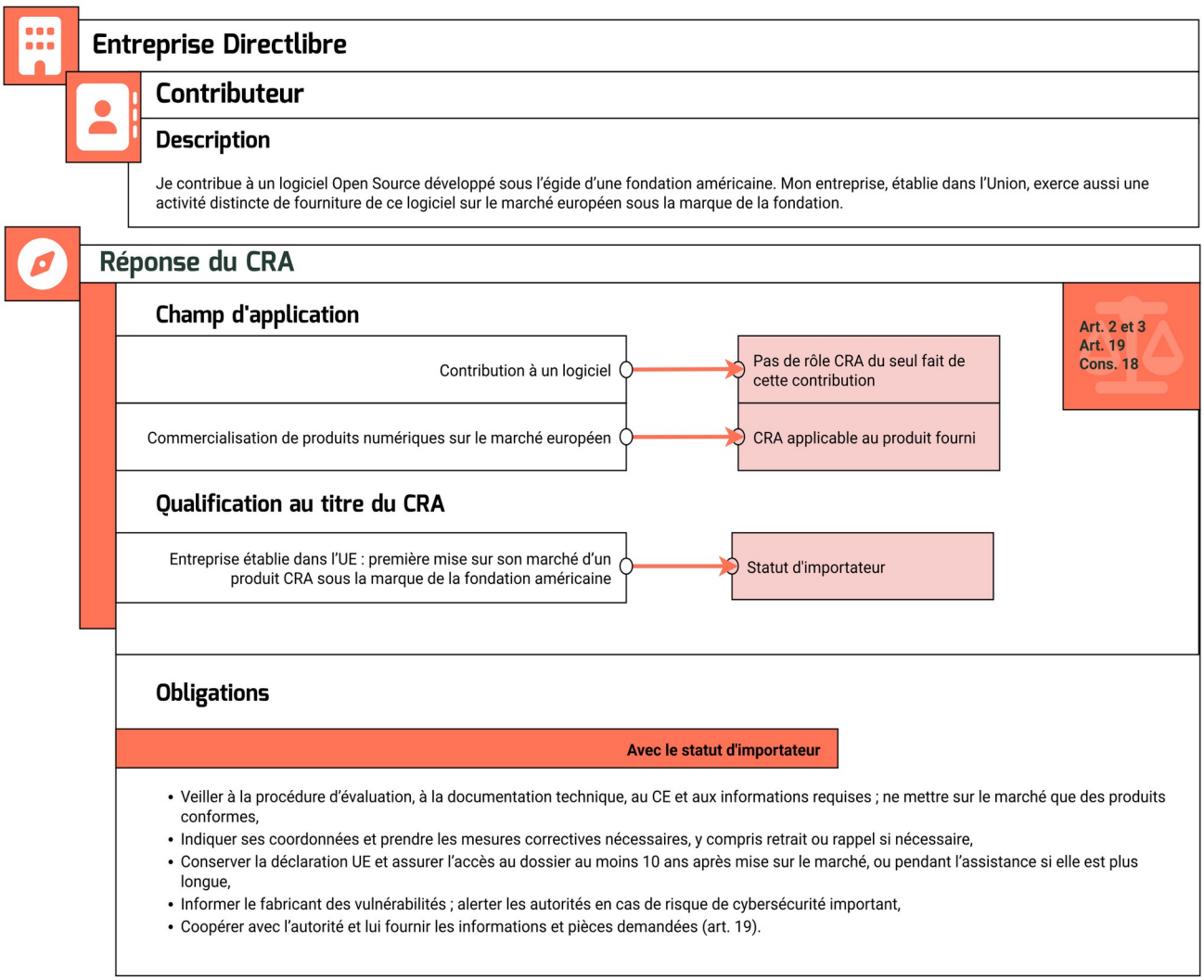
## 4.1.2 Entreprise distributrice de solution numérique



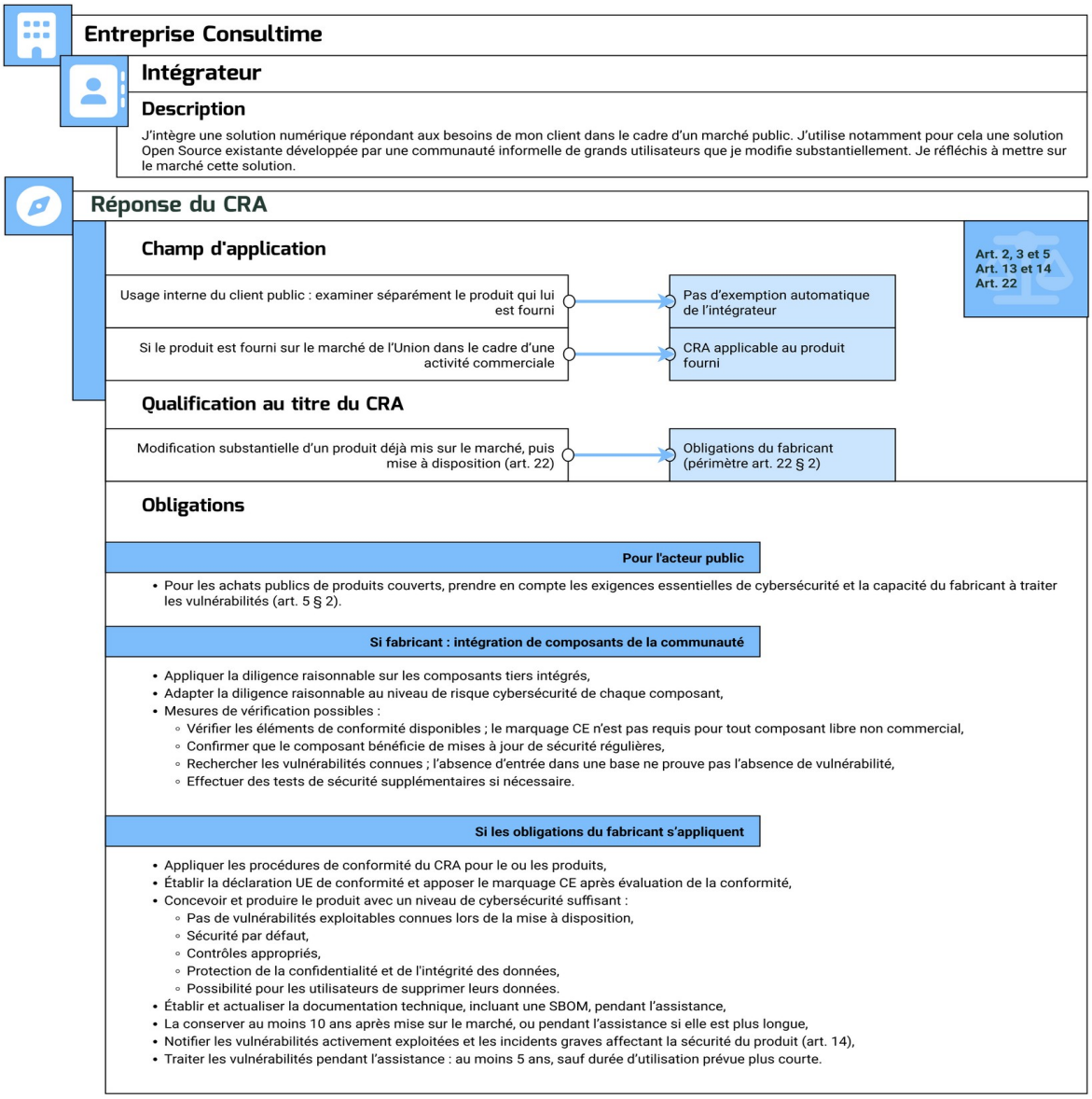
## 4.1.3 Entreprise Éditrice Open Source



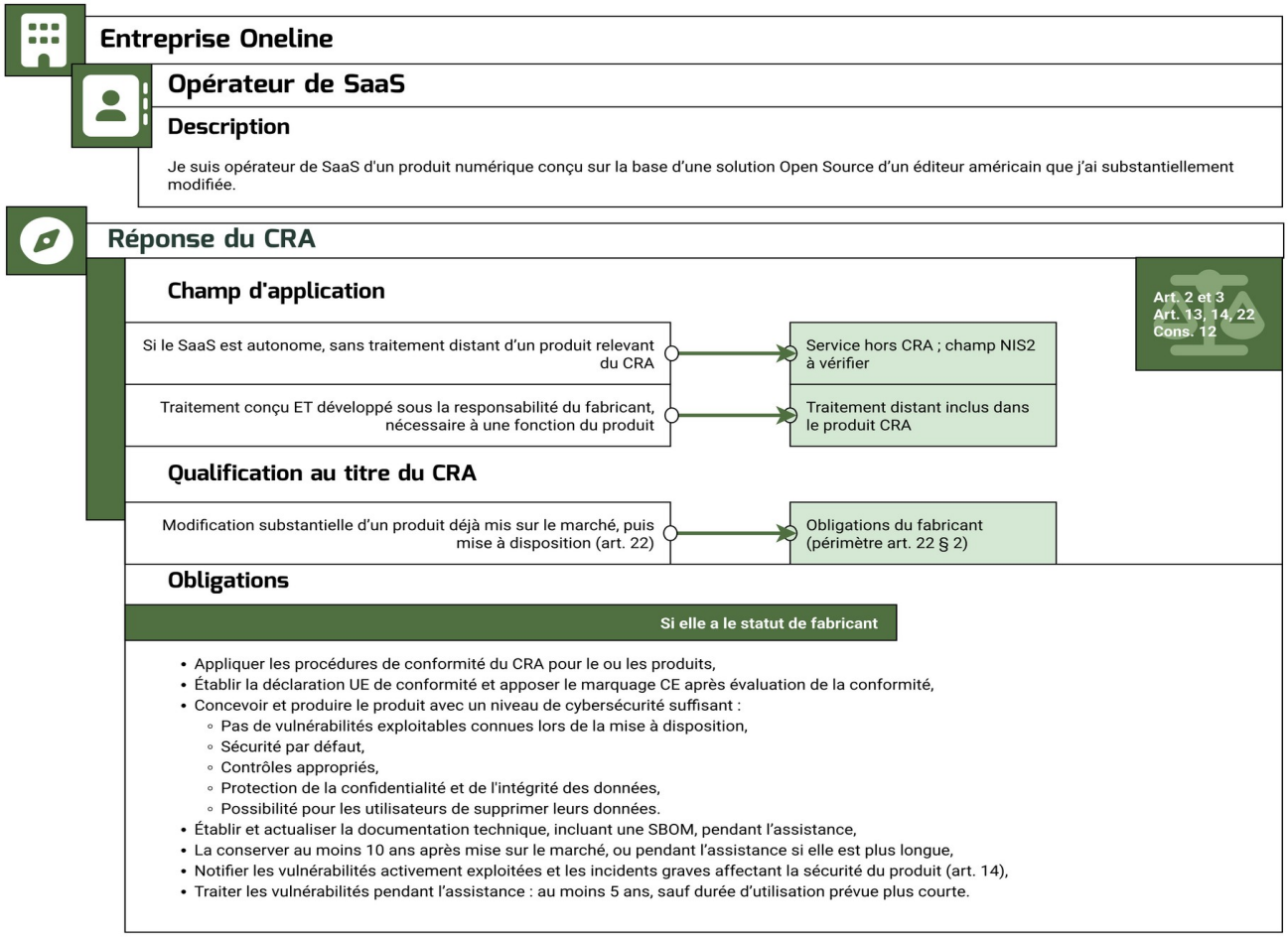
## 4.1.4 Entreprise contributrice à un projet Open Source



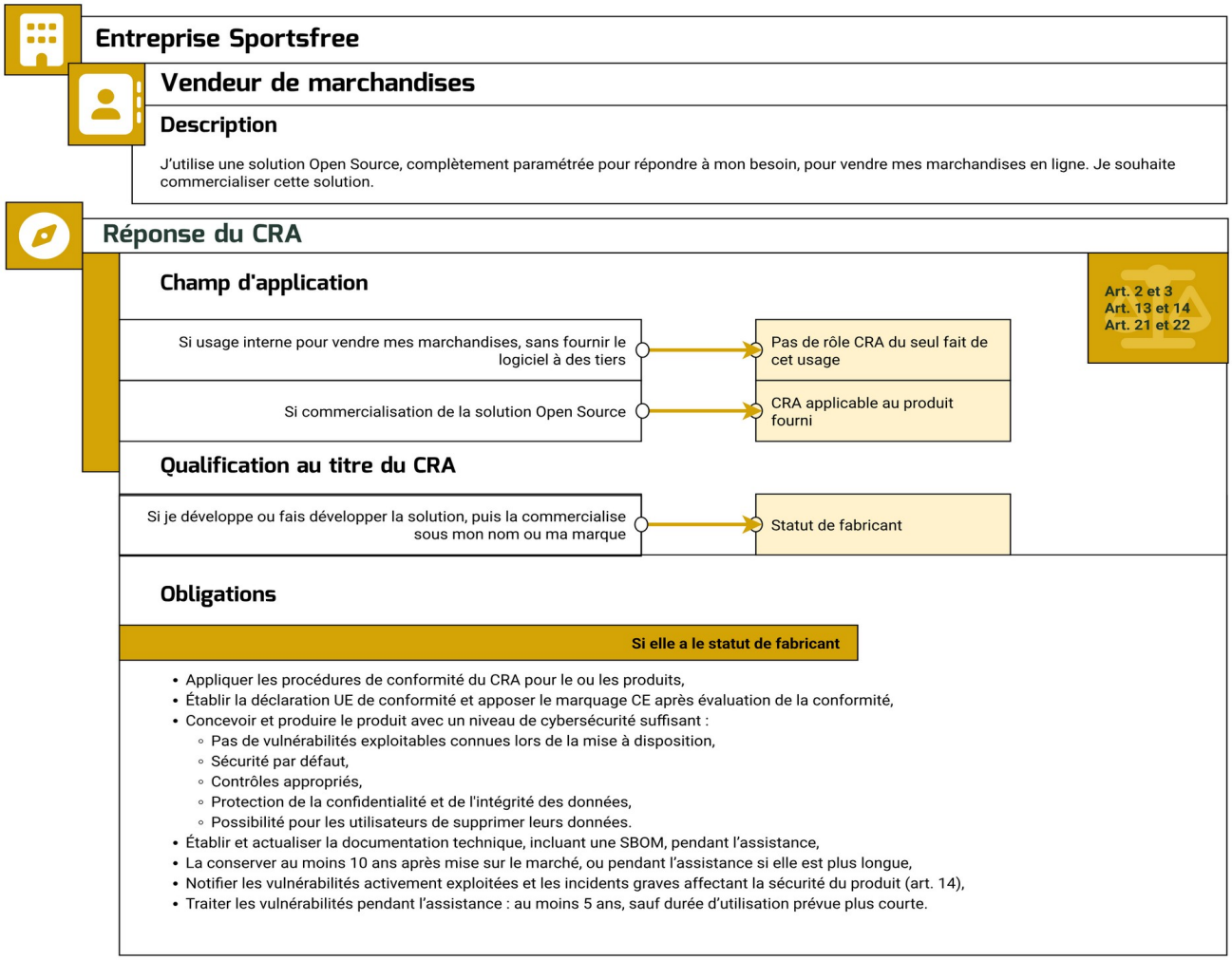
## 4.1.5 Entreprise intégratrice de solutions Open Source



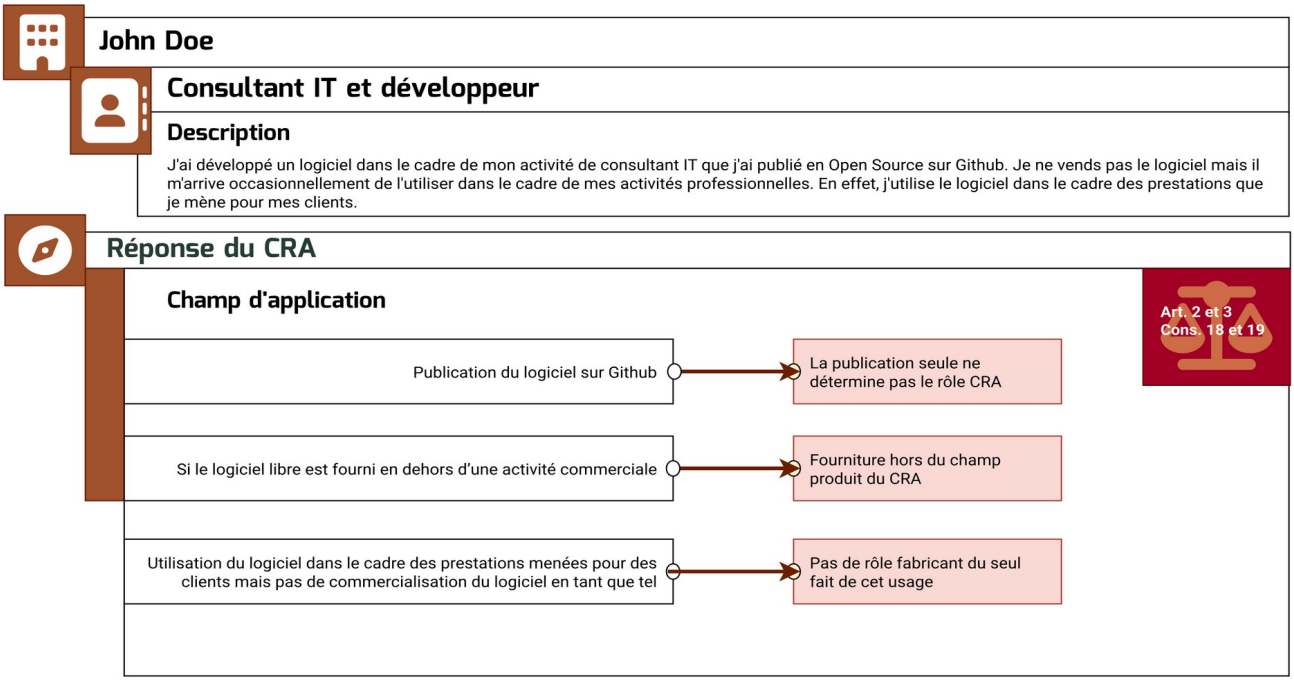
## 4.1.6 Entreprise Opérant un service en SaaS



## 4.1.7 Entreprise utilisatrice de solutions Open Source



### 4.1.8 Développeur indépendant




## 4.2 | Lien entre le CRA et les autres réglementations

*Tableau 7: Lien entre le CRA et les autres réglementations*

| Réglementation | Champs d'application | Interaction avec le CRA |
|---|---|---|
| **Product Liability Directive (PLD) 2024/2853** | Responsabilité stricte pour produits défectueux. | Complémentaire au CRA; pas de chevauchement légal. |
| **Machinery Regulation (MR) 2023/1230** | Exigences essentielles santé et sécurité pour machines | CRA et MR peuvent s'appliquer simultanément aux machines avec éléments numériques. |
| **General Product Safety Regulation (GPSR) 2023/988** | Sécurité générale des produits pour consommateurs. | CRA et GPSR se complètent selon risques : le CRA est centré sur la cybersécurité et le GPSR = sécurité générale. |
| **Radio Equipment Directive 2014/53/EU - RED & Delegated Regulation 2022/30** | Équipements radio. | Le CRA applique exigences essentielles RED cybersécurité via RED Delegated Regulation du 1er août 2025 au 10 décembre 2027 |
| **European Health Data Space Regulation (EU) 2025/327 - EHDS** | Systèmes de dossiers de santé électroniques (EHR). | Un produit peut être simultanément soumis au CRA et à l'EHR. |
| **General Data Protection Regulation (EU) 2016/679 - GDPR** | Protection des données personnelles. | Complémentaire au CRA; pas de chevauchement légal. |
| **Data Act (EU) 2023/2854 – DA** | Accès aux données des produits connectés et services associés. | Des produits soumis au CRA peuvent être aussi soumis au DA. |

## 4.3 | Exigences essentielles de cybersécurité

### 4.3.1 Exigences de cybersécurité relatives aux propriétés des produits comportant des éléments numériques

Les produits comportant des éléments numériques doivent, le cas échéant :

a) être mis à disposition sur le marché sans vulnérabilité exploitable connue;

b) être mis à disposition sur le marché avec une configuration de sécurité par défaut, sauf accord contraire entre le fabricant et l'entreprise utilisatrice en ce qui concerne un produit sur mesure comportant des éléments numériques, y compris la possibilité de réinitialiser le produit à son état d'origine;

c) être conçus de façon à ce que leurs vulnérabilités puissent être corrigées par des mises à jour de sécurité, y compris, le cas échéant, par des mises à jour automatiques de sécurité régulières activées par défaut, mais faciles à désactiver, par la communication aux utilisateurs des mises à jour disponibles et par la possibilité de les différer temporairement;

d) assurer la protection contre les accès non autorisés par des mécanismes de contrôle appropriés, y compris, mais sans s'y limiter, par des systèmes d'authentification, d'identité ou de gestion des accès et signaler tout accès non autorisé;

e) protéger la confidentialité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, par exemple en chiffrant les données pertinentes au repos ou en transit au moyen de mécanismes de pointe et par d'autres moyens techniques;

f) protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, des commandes, des programmes et de la configuration contre toute manipulation ou modification non autorisée par l'utilisateur et signaler les corruptions;

g) ne traiter que les données, à caractère personnel ou autres, qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité prévue du produit comportant des éléments numériques (minimisation des données);

h) protéger la disponibilité des fonctions essentielles et de base, notamment après un incident, y compris par des mesures de résilience et d'atténuation face aux attaques par déni de service;

i) réduire au maximum les répercussions négatives générées par les produits eux-mêmes ou par les appareils connectés sur la disponibilité des services fournis par d'autres dispositifs ou réseaux;

j) être conçus, développés et fabriqués de manière à limiter les surfaces d'attaque, y compris les interfaces externes;

k) être conçus, développés et fabriqués de manière à réduire les répercussions d'un incident, en utilisant des mécanismes et des techniques appropriés de limitation de l'exploitation de failles;

l) fournir des informations relatives à la sécurité en enregistrant et en surveillant les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions, tout en laissant à l'utilisateur la possibilité de désactiver le mécanisme;

m) donner aux utilisateurs la possibilité de supprimer facilement, en toute sécurité et de manière permanente toutes les données et tous les paramètres et, lorsque ces données peuvent être transférées vers d'autres produits ou systèmes, veiller à ce que cela puisse se faire de manière sécurisée.

Annexe I – Exigences essentielles de cybersécurité, Partie I – Exigences de cybersécurité relatives aux propriétés des produits comportant des éléments numériques

### 4.3.2 Exigences relatives à la gestion des vulnérabilités

Les fabricants des produits comportant des éléments numériques :

1) recensent et documentent les vulnérabilités et les composants des produits, notamment par l'établissement d'une nomenclature des logiciels dans un format couramment utilisé et lisible par machine couvrant au moins les dépendances de niveau supérieur des produits;

2) gèrent et corrigent sans retard les vulnérabilités qui touchent les produits comportant des éléments numériques, y compris par des mises à jour de sécurité; lorsque cela est techniquement possible, de nouvelles mises à jour de sécurité sont fournies séparément des mises à jour de fonctionnalité;

3) soumettent régulièrement les produits comportant des éléments numériques à des tests et examens de sécurité efficaces;

4) dès la publication d'une mise à jour de sécurité, communiquent sur les vulnérabilités corrigées, en publiant notamment une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit comportant des éléments numériques concerné, les conséquences de ces vulnérabilités, leur gravité et des informations claires et accessibles aidant les utilisateurs à y remédier; dans des cas dûment justifiés, lorsque les fabricants considèrent que les risques pour la sécurité liés à la publication l'emportent sur les avantages en matière de sécurité, ils peuvent retarder la publication des informations relatives à une vulnérabilité corrigée jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif adapté;

5) mettent en place et appliquent une politique de divulgation coordonnée des vulnérabilités;

6) prennent des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits comportant des éléments numériques ainsi que des composants tiers contenus dans ces produits, y compris en fournissant une adresse de contact pour le signalement des vulnérabilités découvertes dans les produits concernés;

7) prévoient des mécanismes de distribution sécurisée des mises à jour pour les produits comportant des éléments numériques afin de garantir que les vulnérabilités soient corrigées ou atténuées rapidement et, le cas échéant, automatisent les mises à jour de sécurité;

8) veillent à ce que, lorsque des correctifs ou des mises à jour de sécurité sont disponibles pour remédier à des problèmes de sécurité constatés, ils soient diffusés sans retard et, sauf accord contraire entre un fabricant et un utilisateur professionnel en ce qui concerne un produit sur mesure comportant des éléments numériques, gratuitement et accompagnées de messages consultatifs fournissant aux utilisateurs les informations pertinentes, y compris sur les éventuelles mesures à prendre.

Annexe I – Exigences essentielles de cybersécurité, Partie II – Exigences relatives à la gestion des vulnérabilités

## 4.4 | Marquage CE

### 4.4.1 Définition

Marquage CE : « un marquage par lequel un fabricant indique qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant sont conformes aux exigences essentielles de cybersécurité énoncées à l'annexe I et toute autre législation d'harmonisation de l'Union applicable prévoyant son apposition ».

*Article 3 – Définitions*

### 4.4.2 Mise en place

*« 1. Le marquage CE est apposé de manière visible, lisible et indélébile sur le produit comportant des éléments numériques. Lorsque la nature du produit comportant des*

*éléments numériques ne le permet pas ou ne le justifie pas, il est apposé sur son emballage et sur la déclaration UE de conformité mentionnée à l'article 28 qui accompagne le produit comportant des éléments numériques. Pour les produits comportant des éléments numériques qui se présentent sous la forme d'un logiciel, le marquage CE est apposé soit sur la déclaration UE de conformité mentionnée à l'article 28, soit sur le site internet qui accompagne le logiciel. Dans ce dernier cas, la section correspondante du site internet est aisément et directement accessible aux consommateurs.*

*2. En raison de la nature du produit comportant des éléments numériques, la hauteur du marquage CE apposé sur le produit comportant des éléments numériques peut être inférieure à 5 mm, à condition qu'il reste visible et lisible.*

*3. Le marquage CE est apposé avant que le produit comportant des éléments numériques ne soit mis sur le marché. Il peut être suivi d'un pictogramme ou de tout autre marquage indiquant un risque en matière de cybersécurité ou un usage particulier énoncés dans les actes d'exécution visés au paragraphe 6.*

*4. Le marquage CE est suivi du numéro d'identification de l'organisme notifié, lorsque cet organisme participe à la procédure d'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) visée à l'article 32. Le numéro d'identification de l'organisme notifié est apposé par l'organisme lui-même ou, sur instruction de celui-ci, par le fabricant ou le mandataire du fabricant.*

*5. Les États membres s'appuient sur les mécanismes existants pour assurer la bonne application du régime régissant le marquage CE et prennent les mesures nécessaires en cas d'usage abusif de ce marquage. Lorsque le produit comportant des éléments numériques relève d'une législation d'harmonisation de l'Union autre que le présent règlement qui prévoit aussi l'apposition du marquage CE, le marquage CE indique que le produit satisfait également aux exigences énoncées dans cette autre législation d'harmonisation de l'Union.*

*6. La Commission peut, par voie d'actes d'exécution, définir des spécifications techniques pour les étiquettes, les pictogrammes ou tout autre marquage en lien avec la sécurité des produits comportant des éléments numériques, leurs périodes d'assistance ainsi que des mécanismes visant à promouvoir leur utilisation et à sensibiliser le public à la sécurité des produits comportant des éléments numériques. Lors de l'élaboration des projets d'actes d'exécution, la Commission consulte les parties prenantes concernées et, s'il a déjà été établi en vertu de l'article 52, paragraphe 15, l'ADCO. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2. »*

*Article 30 – Règles et conditions d'apposition du marquage CE*

## 4.5 | Modèles de déclaration de conformité

### 4.5.1 Déclaration de conformité (ANNEXE V)

La déclaration UE de conformité prévue à l'article 28 contient l'ensemble des informations suivantes :

1) nom et type, ainsi que toute information supplémentaire permettant l'identification unique du produit comportant des éléments numériques ;

2) nom et adresse du fabricant ou de son mandataire ;

3) attestation certifiant que la déclaration UE de conformité est établie sous la seule responsabilité du fournisseur ;

4) objet de la déclaration (identification du produit comportant des éléments numériques permettant sa traçabilité et pouvant inclure une photographie) ;

5) une mention indiquant que l'objet de la déclaration décrit ci-dessus est conforme à la législation d'harmonisation de l'Union applicable ;

6) les références de toute norme harmonisée pertinente appliquée ou de toute autre spécification commune ou certification de cybersécurité par rapport auxquelles la conformité est déclarée ;

7) le cas échéant, le nom et le numéro de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré ;

8) informations supplémentaires :

Signé par et au nom de : .....

(date et lieu d'établissement) :

(nom, fonction) (signature) :

### 4.5.2 Déclaration de conformité simplifiée (ANNEXE VI)

La déclaration UE de conformité simplifiée visée à l'article 13, paragraphe 20, est établie comme suit :

[Nom du fabricant] déclare que le produit comportant des éléments numériques de type [désignation du type de produit comportant un élément numérique] est conforme au règlement (UE) 2024/2847 du Parlement européen et du Conseil.

Le texte complet de la déclaration UE de conformité est disponible à l'adresse internet suivante : .....

## 4.6 | Liens utiles

- Lien du Cyber Resilience Act : https://eur-lex.europa.eu/eli/reg/2024/2847/oj
- Lien du Blue Guide : https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en
- Pour suivre le statut du CRA : https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act
- Lien Contact : https://www.europarl.europa.eu/portal/en/contact