Cyber Resilience Act :

entre échéances réglementaires et innovation, comment se préparer efficacement d'ici 2027 ?

Découvrez un livre blanc porté par l'équipe Cyber Softeam

SOFTEAM
UNE FILIALE DE DOCAPOSTE

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Sommaire

Introduction

Chapitre 1

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Contexte réglementaire européen

Ces dernières années, la dépendance croissante aux technologies numériques a considérablement élargi la surface d'attaque des organisations. Les cybermenaces (ransomwares), la compromission de chaînes d'approvisionnement ou encore l'exploitation de vulnérabilités dites "zero-day"[1] ne sont plus de simples risques techniques : ils constituent désormais des enjeux stratégiques et économiques majeurs.

En 2021, l'impact global des cyberattaques a été estimé à plus de 6 000 milliards d'euros[2].

Selon une étude de l'ENISA (2023) :

61%

Des organisations exigent désormais une certification de sécurité de leurs fournisseurs

43%

Des organisations utilisent des services d'évaluation de sécurité

37%

Des organisations réalisent des audits de risques avant engagement contractuel

Pour y répondre, l'Union européenne a progressivement construit un socle réglementaire visant à harmoniser les exigences de cybersécurité et à renforcer la résilience numérique.

Chronologie réglementaire :

Mais une faille persistait : aucune réglementation ne couvrait spécifiquement la cybersécurité des produits numériques mis sur le marché. Le Cyber Resilience Act comble ce vide en imposant des exigences de sécurité dès la conception et tout au long du cycle de vie des produits.

[1] Failles inédites

[2] #LaREFNum23 | Cyberattaques : tous ciblés, tous armés pour résister

Pourquoi le CRA ?

Le CRA fixe pour la première fois des **exigences communes de cybersécurité** applicables à l'ensemble des produits comportant des éléments numériques, qu'il s'agisse de logiciels ou de matériels connectés.
Ses objectifs sont multiples :

1. **Protéger les utilisateurs** en imposant un minimum de sécurité "by design" et "by default".
2. **Harmoniser les règles** au sein du marché unique pour faciliter la mise sur le marché de produits sûrs.
3. **Renforcer la compétitivité** des entreprises européennes en valorisant les solutions sécurisées.

Concrètement, le CRA impose aux fabricants, importateurs et distributeurs de **concevoir** des produits sécurisés dès leur origine, de **corriger rapidement** les vulnérabilités découvertes, de **maintenir** la sécurité tout au long de la durée d'assistance prévue, et de **notifier** sans délai tout incident grave ou toute vulnérabilité activement exploitée.

Lien avec NIS2, DORA, RGPD

Le CRA n'agit pas isolément : il complète un **écosystème réglementaire** déjà dense.

NIS2 fixe des exigences organisationnelles de cybersécurité pour les opérateurs de services essentiels et les entités importantes ; DORA encadre la résilience numérique dans le secteur financier ; le RGPD, quant à lui, protège les données personnelles mais ne traite pas spécifiquement de la sécurité des produits.

Le CRA agit donc en amont de ces textes, en s'assurant que les produits numériques eux-mêmes intègrent la robustesse nécessaire pour résister aux cybermenaces.

Public visé par ce livre blanc

Ce document s'adresse principalement aux **éditeurs de logiciels** (SaaS, applications embarquées, solutions on-premise).

Notre livre blanc ne traite pas des enjeux spécifiques aux autres acteurs concernés par le CRA, comme les fabricants d'équipements connectés, bien qu'ils puissent y retrouver les grandes lignes du règlement qui les concernent également.

Objectif de ce livre blanc

L'ambition de ce document est d'**expliquer** les obligations introduites par le CRA de manière claire et opérationnelle, d'**illustrer** chaque exigence et de **fournir** des outils pratiques (check-lists, modèles, tableaux) afin d'anticiper efficacement la mise en conformité avant l'entrée en vigueur complète du règlement.

À RETENIR

- Le CRA complète le RGPD, NIS2 et DORA en ciblant la **sécurité des produits numériques.**
- Il s'applique à la quasi-totalité des produits connectés mis sur le marché européen, sauf exceptions précises.
- Les obligations portent autant sur la conception que sur la maintenance et la gestion d'incidents.
- Anticiper sa mise en conformité dès aujourd'hui évite une course de dernière minute en 2027.

LE CONSEIL SOFTEAM

Identifiez les normes et réglementations auxquelles est soumise votre organisation pour assurer l'intégration et l'articulation des mesures portées par le CRA avec les autres textes.

Comprendre le Cyber Resilience Act

Chapitre 2

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Objectif du CRA

Le Cyber Resilience Act est le premier règlement européen[3] qui établit des **exigences communes de cybersécurité** pour **l'ensemble des produits comportant des éléments numériques**, qu'ils soient matériels ou logiciels.

L'ambition est multiple : **renforcer la sécurité** des produits tout au long de leur cycle de vie, **protéger les utilisateurs** contre les vulnérabilités et les cyberattaques, **harmoniser** les règles à l'échelle du marché unique afin d'éviter les divergences nationales, et **accroître la confiance** dans les produits numériques européens.
À noter que, contrairement à une directive, le CRA est **directement applicable** dans tous les États membres, sans nécessiter de transposition nationale.

Portée du CRA

Le champ d'application du CRA est volontairement large. Il concerne **tous les produits avec éléments numériques** mis sur le marché ou mis en service dans l'Union européenne. Cela inclut aussi bien les :

Sont donc couverts tous les **produits matériels ou logiciels connectés** directement ou indirectement à un réseau ou à un appareil, ainsi que les **services intégrés** qui influencent la cybersécurité du produit.

Exemple : Une caméra IP connectée, un ERP en SaaS ou un routeur Wi-Fi entrent ainsi dans le champ du règlement.

Certains produits restent toutefois exclus, notamment lorsqu'ils relèvent déjà d'une réglementation sectorielle spécifique imposant des exigences de cybersécurité au moins équivalentes :

- **Dispositifs médicaux** (règlement UE spécifique)
- **Aéronautique civile** (règlement sur la sécurité et cybersécurité aéronautiques)
- Produits pour la **défense** ou la **sécurité nationale**
- Logiciels **open source** développés ou mis à disposition **en dehors d'une activité commerciale**
- **Secteur automobile** (règlement cybersécurité véhicules)
- Produits destinés uniquement à la **recherche** ou aux **tests internes** non mis sur le marché

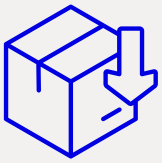
Dispositifs médicaux : Règlement (UE) 2017/746
Secteur automobile : Règlement (UE) 2019/2144
Aéronautique civile : Règlement (UE) 2018/1139

Acteurs concernés

Le règlement identifie trois catégories principales d'acteurs :

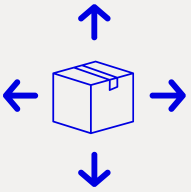
Fabricants

- Conçoivent ou font fabriquer le produit et le mettent sur le marché sous leur nom ou marque
- Responsables en premier lieu de la conformité CRA



Importateurs

- Mettent sur le marché de l'UE un produit provenant de pays tiers
- Doivent vérifier que les produits importés respectent les exigences CRA



Distributeurs

- Rendent disponible un produit sur le marché sans en être le fabricant ni l'importateur
- Ne doivent pas mettre sur le marché des produits présentant des non-conformités visibles

Cas d'un éditeur / prestataire pour un tiers

Pour traiter du cas spécifique des éditeurs de logiciel dans ce livre blanc, il est important de bien définir qui est directement concerné par le CRA dans le cadre d'un éditeur / prestataire pour un tiers.

Le fabricant est celui qui met sur le marché le produit numérique, et est le seul directement soumis à ce règlement. Lui incombe donc la conformité aux exigences prévues dans ce texte.

Concernant la chaîne d'approvisionnement, les prestataires, éditeurs sous-traitants ne sont pas directement soumis au CRA dans le cadre d'une prestation où ils ne sont pas « fabricants » ou « metteurs sur le marché ». Cependant, ils sont indirectement concernés à travers leurs obligations contractuelles passées avec le fabricant (leur client), car ce dernier est chargé de s'assurer du bon respect des exigences du CRA par sa chaîne d'approvisionnement.

En cas de manquements aux exigences du CRA, les sanctions prévues par les autorités compétentes sont destinées aux fabricants. Ces derniers peuvent tout de même se retourner contre leurs éditeurs ou prestataires en cas de manquements contractuels de leur part.

Focus sur les logiciels

Le CRA s'applique pleinement aux produits logiciels connectés, qu'ils soient indépendants (applications, systèmes d'exploitation, solution SaaS) ou intégrés dans un matériel.

Ici encore, certaines exceptions existent :

- Logiciels **open source** développés ou mis à disposition **en dehors d'une activité commerciale.**
- Produits déjà couverts par une réglementation sectorielle imposant des exigences de cybersécurité au moins équivalentes.
- Certains produits destinés uniquement à la recherche ou aux tests et non mis sur le marché.

Définitions clés

- **Produit comportant des éléments numériques :** tout logiciel ou matériel dépendant, directement ou indirectement, de données ou de connexions réseau pour fonctionner.
- **Mise sur le marché :** première mise à disposition d'un produit dans l'UE, à titre onéreux ou gratuit, dans le cadre d'une activité commerciale.
- **Vulnérabilité activement exploitée :** faille de sécurité utilisée dans le cadre d'une cyberattaque connue.
- **Incident grave :** incident ayant un impact significatif sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou services.

À RETENIR

- Le CRA est **large :** il couvre la quasi-totalité des produits connectés.
- Le **fabricant** est l'acteur clé, mais importateurs et distributeurs sont aussi responsables.
- Certaines exclusions existent, notamment pour **l'open source non commercial.**
- Les définitions officielles sont essentielles pour savoir si un produit tombe dans le champ du CRA.

LE CONSEIL SOFTEAM

Bien identifier le périmètre d'applicabilité du CRA à votre organisation en se référant à l'article 3 du texte européen (P29).

Exigences clés et obligations

Chapitre 3

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Exigences en matière de cybersécurité
cf (Annexe I – Partie II)

Le CRA établit, dans son **Annexe I – Partie II**, un socle commun d'exigences applicables à tous les produits comportant des éléments numériques.

Ces exigences visent à garantir que la sécurité est intégrée dès la conception (**Security by Design**) et maintenue tout au long du cycle de vie du produit.

Principes clés :

- **Sécurité dès la conception et par défaut :**
  - Intégrer des mesures de cybersécurité dès la phase de conception et configuration initiale.
  - Fournir un produit sécurisé « prêt à l'emploi », sans configuration complexe requise.
- **Protection des données et communications :** chiffrement, authentification forte, contrôle d'accès, défense en profondeur.
- **Journalisation :**
  - Collecte et conservation des journaux pertinents pour la cybersécurité (accès, modifications critiques, événements systèmes).
  - Protection de l'intégrité et de la confidentialité de ces journaux.
  - Disponibilité pour analyse pendant toute la période d'assistance.
- **Résilience et continuité :** détecter et limiter l'impact des incidents, restaurer les fonctions critiques rapidement.
- **Minimisation des vulnérabilités :** éviter l'utilisation de composants connus comme vulnérables, limiter la surface d'attaque.

Exemples de mesures de cybersécurité dès la phase de conception :

- Un éditeur de logiciels de gestion réduit les fonctionnalités par défaut installés sur les serveurs (désactivation des modules non utilisés, ports fermés).
- Dès la conception, prévoir un processus de validation et de suivi des bibliothèques open source utilisées (liste blanche, surveillance des CVE).

Gestion des vulnérabilités et période d'assistance

Le CRA impose aux fabricants de mettre en œuvre un **processus structuré** de gestion des vulnérabilités, incluant :

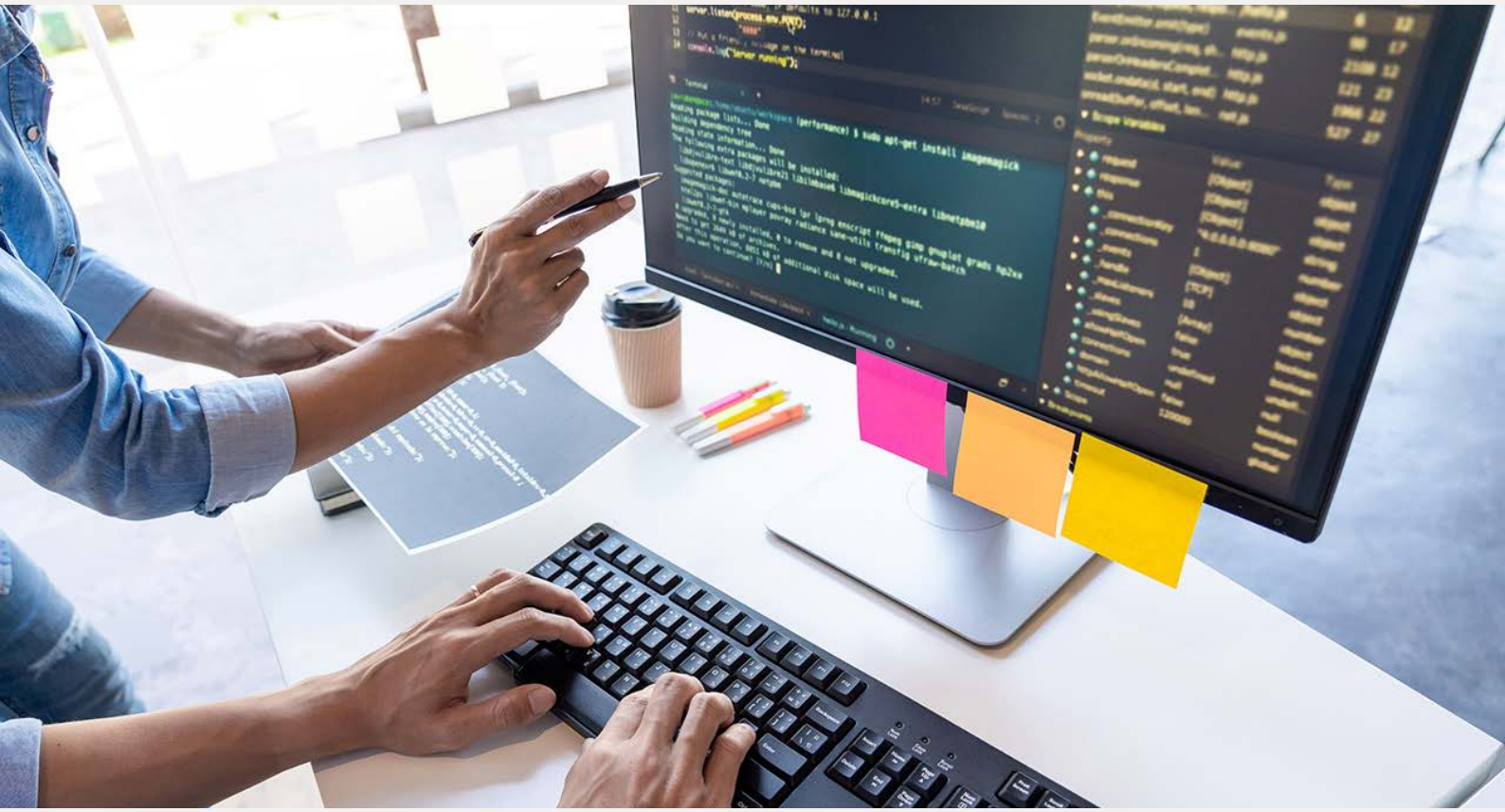
- **Surveillance active** (veille, tests, analyse des dépendances).
- **Analyse d'impact** et priorisation des correctifs.
- **Communication proactive** avec les utilisateurs sur les risques identifiés.

Période d'assistance minimale :

- **≥ 5 ans** à partir de la mise sur le marché, ou pour toute la durée de vie prévue du produit si elle est supérieure.
- Pour les produits destinés à des usages critiques ou longue durée (ex. : systèmes industriels, OS, routeurs), une assistance prolongée est attendue.
- Les mises à jour de sécurité doivent rester disponibles jusqu'à 10 ans lorsque nécessaire pour préserver la sécurité des environnements dépendants.

Obligation de mise à jour, patch management et signature

- Les mises à jour de sécurité constituent un élément central du CRA :
- **Disponibilité** gratuite pour l'utilisateur pendant toute la période d'assistance.
- **Déploiement sans retard** injustifié après identification d'une vulnérabilité.
- **Séparation** : lorsque possible, séparer les mises à jour de sécurité des mises à jour de fonctionnalités.
- **Authenticité :** signature numérique obligatoire, vérification avant installation.
- **Automatisation :** pour les produits grand public, téléchargement et installation automatiques activés par défaut, avec option de désactivation.
- **Notification :** informer l'utilisateur via l'interface produit ou un autre canal de la disponibilité et du caractère critique d'une mise à jour.

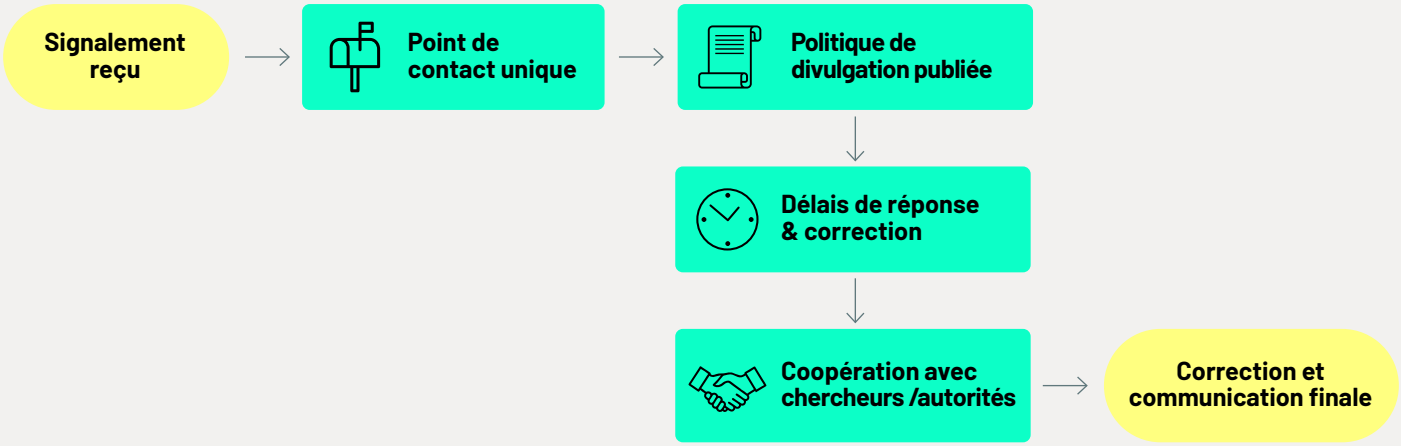


Procédure de signalement des vulnérabilités (Coordinated Vulnerability Disclosure – CVD)

Le CRA rend obligatoire la mise en place d'une **procédure formalisée de divulgation coordonnée :**

- **Point de contact unique :** adresse e-mail, formulaire web ou numéro de téléphone, facilement accessible et à jour.
- **Politique de divulgation publiée** précisant :
  - Le processus de soumission d'un rapport de vulnérabilité.
  - Les délais de réponse et de correction.
  - Les modalités de reconnaissance ou de récompense (bug bounty possible).
- **Signalement anonyme** possible via un **CSIRT** coordinateur.
- **Coopération avec les chercheurs et autorités** pour corriger la faille avant toute divulgation publique.

Objectif : assurer une correction rapide et sécurisée, tout en limitant le risque d'exploitation malveillante.



À RETENIR

- **Security by Design et by Default :** la cybersécurité doit être intégrée dès la conception et activée par défaut.
- **Journalisation :** les produits doivent enregistrer et protéger les événements de sécurité pendant toute la période d'assistance.
- **Gestion continue des vulnérabilités :** processus formalisé, veille active et correctifs prioritaires pour les failles critiques.
- **Période d'assistance minimale :** au moins 5 ans, ou la durée de vie prévue si supérieure ; jusqu'à 10 ans de mises à jour pour certains produits.
- **Mises à jour :** gratuites, authentifiées, diffusées rapidement, séparées des mises à jour de fonctionnalités lorsque possible.
- **Divulgation coordonnée :** point de contact unique, politique publique de signalement, possibilité de passer par un CSIRT coordinateur.
- **Responsabilité du fabricant :** acteur clé de la conformité, avec un rôle central dans la sécurité, la maintenance et la communication.

LE CONSEIL SOFTEAM

Demandez à vos équipes d'identifier les bonnes pratiques et mesures qu'elles mettent déjà en œuvre ainsi que celles qu'elles devront implémenter. À partir de cette dernière liste, estimez les coûts humains, techniques et financiers pour mettre votre organisation en conformité.

Notification des incidents et vulnérabilités

Chapitre 4

SOFTEAM
UNE FILIALE DE DOCAPOSTE

La gestion des incidents et la communication rapide des vulnérabilités constituent l'un des piliers du CRA.

L'objectif est simple : réduire au minimum le délai entre la découverte d'un problème et sa correction, afin de limiter les risques pour les utilisateurs et pour l'ensemble de l'écosystème numérique européen.

Le règlement définit des délais précis et impose l'utilisation d'une plateforme unique gérée par l'ENISA, en lien avec les **CSIRTs coordinateurs nationaux.**

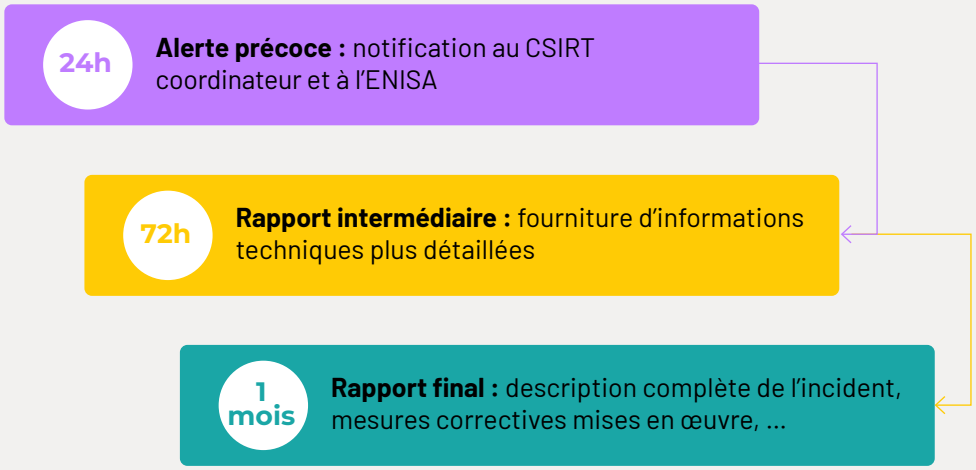
En cas d'incident de cybersécurité affectant le logiciel, l'obligation de notification incombe exclusivement au fabricant, c'est-à-dire l'entité qui met le produit sur le marché sous son nom.

Cas « incident grave »

Un **incident grave** correspond à tout événement de cybersécurité ayant un impact significatif sur la disponibilité, l'intégrité, l'authenticité ou la confidentialité d'un produit numérique ou des données qu'il traite.

Cela peut aller d'une compromission massive d'utilisateurs à l'altération d'un système de mise à jour.

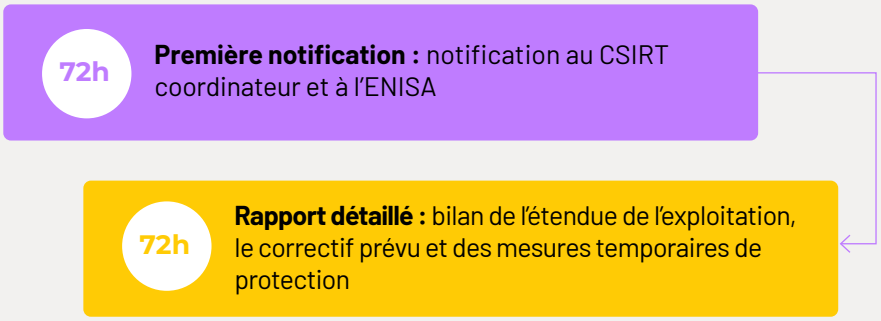
Le CRA prévoit trois niveaux de communication :



Cas « vulnérabilité activement exploitée »

Une **vulnérabilité activement exploitée** est une faille qui est déjà utilisée par un acteur malveillant.

Le fabricant doit alors :



Plateforme unique ENISA & rôle des CSIRTs

Toutes les notifications transitent par une **plateforme unique centralisée** gérée par l'ENISA. Chaque État membre désigne un **CSIRT coordinateur**, chargé de recevoir les signalements, de coordonner la réponse et, le cas échéant, d'interagir avec les chercheurs en sécurité.

Les notifications sont traitées de manière **confidentielle** tant qu'aucun correctif n'est disponible, sauf dans les cas où une divulgation anticipée est nécessaire pour protéger les utilisateurs.

Contenu attendu des notifications

Chaque notification doit contenir au minimum :

- Description du produit affecté et de sa version.
- Nature de l'incident ou de la vulnérabilité.
- Impact estimé (nombre d'utilisateurs, données affectées, fonctionnalités critiques).
- Mesures déjà prises ou prévues.
- Points de contact pour le suivi.

Cas d'un éditeur / prestataire pour un tiers

L'obligation de notification est à la décharge du fabricant du produit numérique.

Ainsi c'est à lui de notifier l'ENISA de tout incident ou vulnérabilité identifié. Cependant, l'éditeur, bien que n'ayant pas d'obligation directe de notification par le CRA, doit transmettre la vulnérabilité ou les incidents identifiés au fabricant, et peut être contractuellement tenu d'assister à la gestion de ces derniers.

À RETENIR

- **Réactivité obligatoire :** 24 h pour un incident grave (alerte précoce), 72 h pour une vulnérabilité activement exploitée.
- **Trois temps pour les incidents graves :** alerte → rapport intermédiaire → rapport final.
- **Deux temps** pour les vulnérabilités activement exploitées : notification → rapport complet sous 14 jours.
- **Coordination européenne :** toutes les notifications passent par la plateforme unique de l'ENISA et le CSIRT coordinateur national.
- **Confidentialité préservée :** éviter la divulgation publique avant disponibilité du correctif, sauf nécessité de protection immédiate.

LE CONSEIL SOFTEAM

Définissez dès à présent un processus généralisé de remontée des incidents et vulnérabilités vers un responsable unique chargé d'effectuer les notifications.

Classification et évaluation de conformité

Chapitre 5

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Le Cyber Resilience Act ne s'applique pas de manière uniforme à tous les produits. Il introduit une classification en fonction du **niveau de risque** et de **l'impact potentiel**, qui conditionne directement la procédure de conformité applicable. Selon que le produit est jugé courant, important ou critique, les obligations peuvent aller d'une simple auto-évaluation à une certification européenne complète par un organisme tiers.

Produits « importants » (classes I et II)

Les produits dits « importants » sont ceux dont la compromission pourrait avoir un impact notable sur la sécurité des utilisateurs ou sur le fonctionnement des systèmes sensibles.

CLASSE I : Produits importants à risque modéré

- → Évaluation possible par contrôle interne, si le fabricant applique des normes harmonisées ou spécifications communes reconnues.
- → Exemples : logiciels de gestion, objets connectés domestiques sans fonction critique.

CLASSE II : Produits importants à risque élevé

- → Évaluation obligatoire par un tiers, même si le produit est conforme aux normes harmonisées.
- → Exemples : systèmes de contrôle industriel, pare-feux, systèmes d'authentification.

Classe	Exemples de produits	Caractéristiques typiques
Classe I (standard)	■ Applications SaaS de gestion, (CRM, ERP, RH) ■ Logiciels métiers non critiques ■ Sites e-commerce ■ Solutions collaboratives, (messageries, visioconférences)	Impact limité en cas d'incident, dépendances technologiques classiques, fonctions de sécurité importantes mais non vitales pour la société dans son ensemble.
Classe II (critique / essentielle)	■ Systèmes d'exploitation ■ Routeurs, pare-feux, équipements réseaux critiques ■ Logiciels de cybersécurité (antivirus, EDR, SIEM) ■ Sysytèmes industriels (SCADA, ICS) ■ Solutions de gestion d'identité (IAM, SSO)	Impact majeur en cas d'incident, rôle central dans l'écosystème numérique, dépendances sensibles, effets systémiques possibles, (effondrement d'infrastructures, propagation de cyberattaques).

Produits « critiques » et certification européenne

Au-delà des produits importants, certains sont classés **« critiques »** en raison de leur rôle central dans des environnements critiques ou de leur dépendance forte pour la continuité d'infrastructures stratégiques.

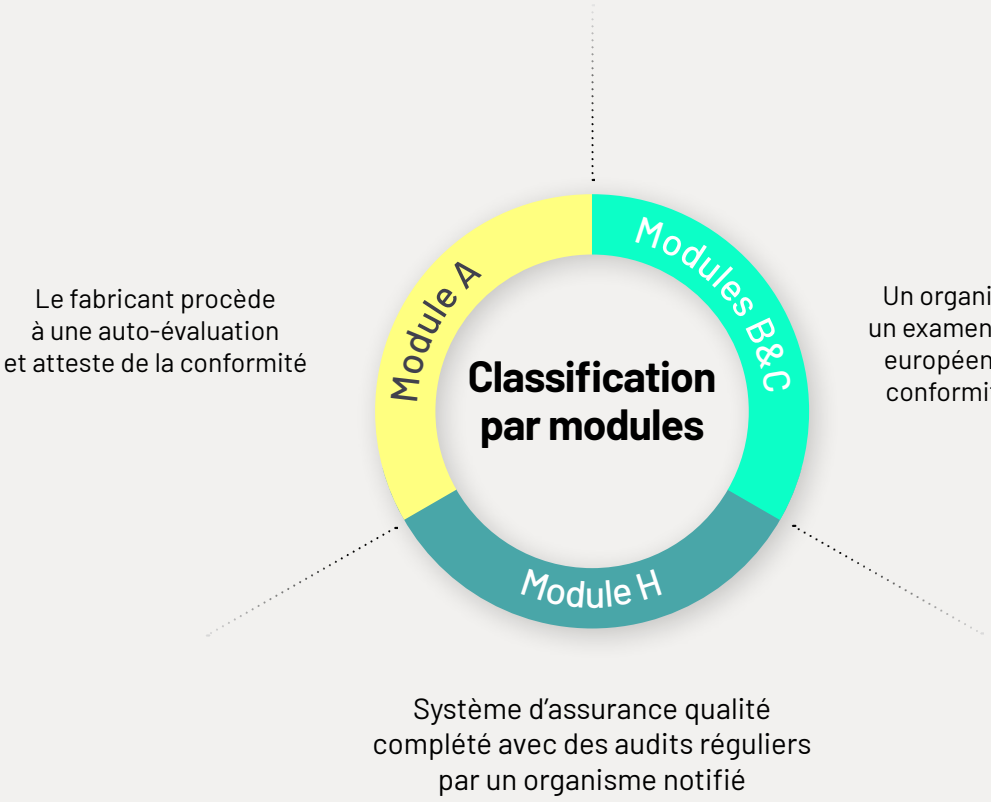
Ces produits sont soumis à une **certification européenne de cybersécurité** (EUCC)[4], avec un niveau d'assurance au moins « substantiel ».

Dès qu'un schéma pertinent est disponible, cette certification devient obligatoire.

L'objectif est clair : garantir un niveau homogène de protection au niveau européen et éviter les points faibles dans la chaîne d'approvisionnement.

Procédures de conformité

La classification conditionne les procédures de conformité, qui s'appuient sur différents modules :



Pour les produits importants de **Classe I**, le Module A reste possible si le fabricant applique des normes harmonisées.

En revanche, si ce n'est pas le cas, ou pour les produits de Classe II et les produits critiques, l'intervention obligatoire d'un tiers s'impose, via les Modules B + C ou H.

[4] European Union Cybersecurity Certification

Marquage CE, déclaration UE de conformité et documentation technique

Une fois la conformité établie, le produit doit porter le **marquage CE**, qui atteste du respect des exigences du CRA ainsi que des autres réglementations européennes applicables.

Ce marquage s'accompagne d'une **déclaration UE de conformité**, document unique qui regroupe l'attestation de conformité à toutes les législations pertinentes.

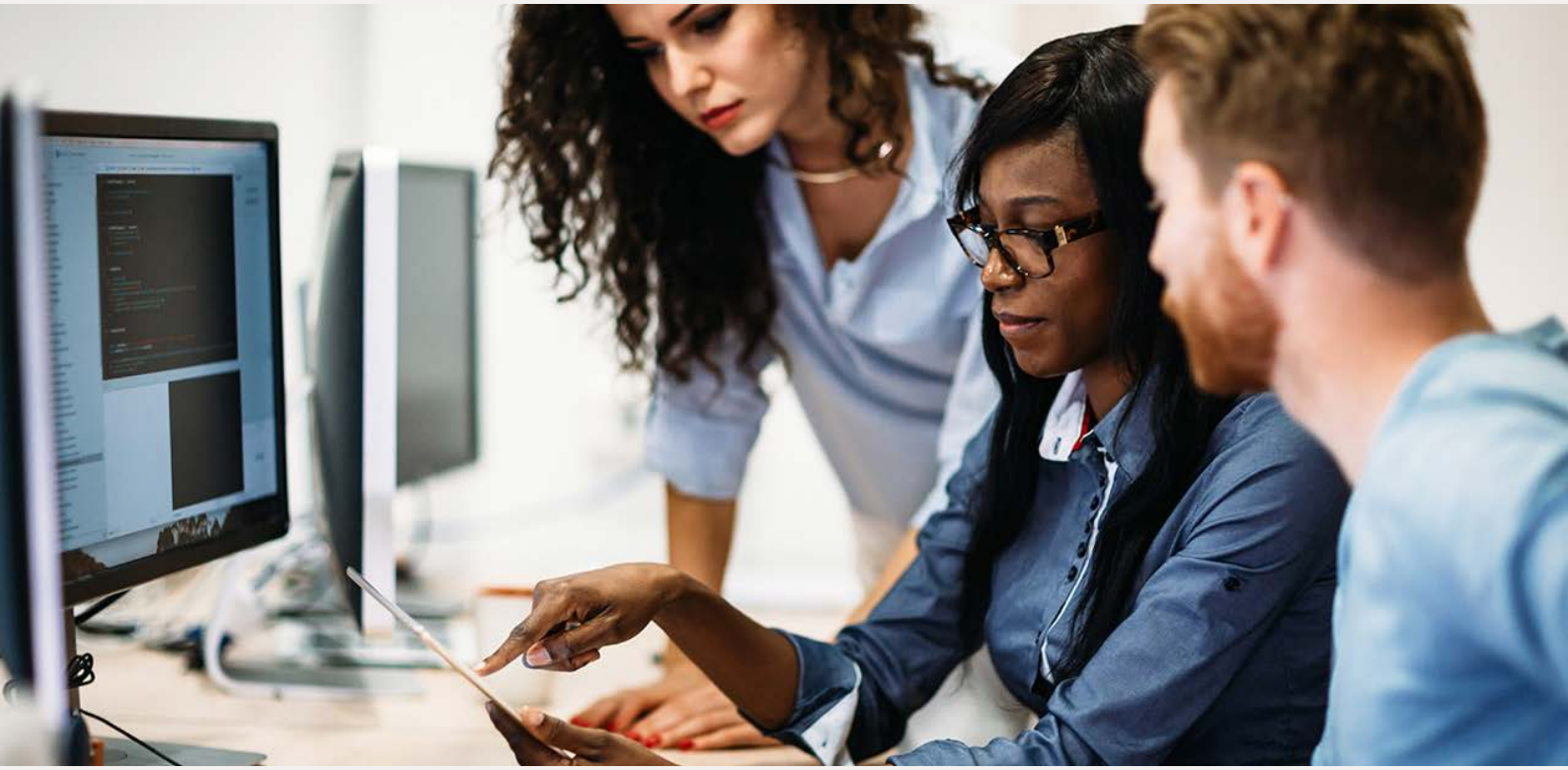
En parallèle, le fabricant doit constituer une **documentation technique** (Annexes VII/VIII), comprenant notamment l'évaluation des risques, la description des mesures de cybersécurité mises en œuvre et, sur demande des autorités, un SBOM (Software Bill of Materials) détaillant les composants logiciels utilisés.

À RETENIR

- **Trois catégories :** produits courants, produits importants (Classe I ou II), produits critiques.
- **Classe I :** auto-évaluation possible si normes reconnues utilisées.
- **Classe II :** évaluation par un tiers obligatoire.
- **Produits critiques :** certification européenne de cybersécurité requise.
- **Marquage CE et documentation technique :** indispensables pour la mise sur le marché, avec SBOM (Software Bill of Materials) sur demande.
- **Le niveau de risque détermine la lourdeur de la procédure :** plus le produit est critique, plus la conformité est encadrée.

LE CONSEIL SOFTEAM

Ne surestimez pas la classe de vos produits définie dans le CRA, au risque d'avoir une marche trop haute à franchir. Le standard supérieur n'est pas adapté à tous vos besoins et ne constitue pas un cadre pour tous vos produits.



Impacts et coûts pour les acteurs

Chapitre 6

SOFTEAM
UNE FILIALE DE DOCAPOSTE

La mise en conformité au CRA n'est pas qu'une formalité réglementaire : elle transforme en profondeur la manière dont les produits numériques sont conçus, développés, distribués et maintenus.

Pour les fabricants, éditeurs et intégrateurs, cela se traduit par des ajustements organisationnels, techniques et budgétaires.

Mais ces investissements, bien que coûteux à court terme, ouvrent aussi la voie à des gains stratégiques durables en matière de compétitivité, de réputation et de confiance.

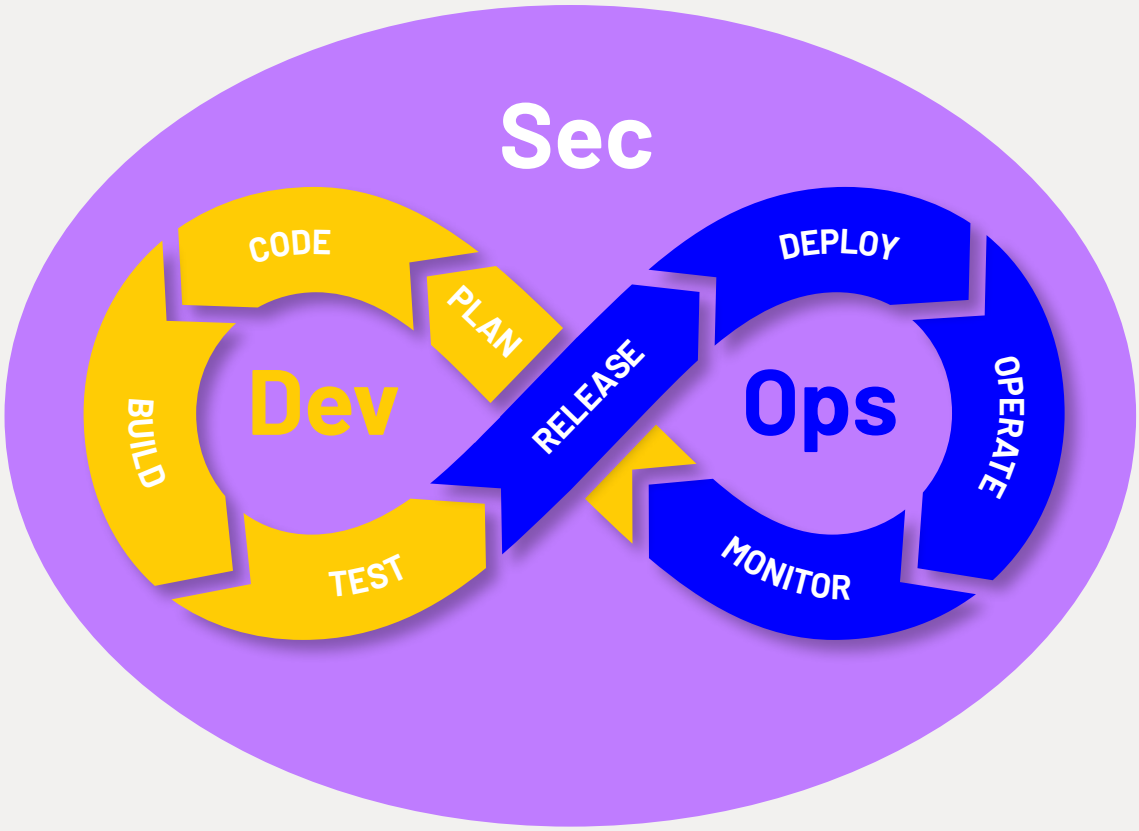
Adaptation des processus de développement (DevSecOps, tests, outillage)

L'une des évolutions majeures concerne **l'intégration de la sécurité dans tout le cycle de vie logiciel**.
Les organisations doivent adopter une approche **DevSecOps**, avec automatisation des tests de sécurité, revue de code systématique et analyse des dépendances logicielles.

Les **tests** doivent être **renforcés** grâce à des audits de code, du fuzzing ou encore des simulations d'attaques pour vérifier la résilience des produits.

L'outillage joue également un rôle clé : solutions de gestion des vulnérabilités, plateformes de patch management ou encore SIEM pour collecter et analyser les journaux deviennent indispensables.

Enfin, un **suivi continu** via une surveillance active des menaces et un dispositif d'alertes internes permet de réagir plus rapidement en cas de risque.



Gouvernance sécurité et ressources humaines

- **Rôle du RSSI ou d'une cellule cybersécurité :** supervision de la conformité, arbitrage budgétaire, gestion des incidents.
- **Création de rôles dédiés :** référents CRA, responsables gestion de vulnérabilités, coordinateurs avec les autorités (CSIRTs, ENISA).
- **Formation continue :** sensibilisation des développeurs, équipes QA et support aux nouvelles exigences du CRA.
- **Culture sécurité :** intégrer la cybersécurité dans les objectifs de performance et d'innovation.

Chaîne d'approvisionnement & gestion des tiers (open source, SaaS, API)

- **Audit des fournisseurs et prestataires :** vérifier la conformité CRA des composants et services utilisés.
- **Contrats renforcés :** inclure des clauses spécifiques sur la sécurité, la notification d'incidents et la mise à jour des composants.
- **Surveillance des dépendances open source :** mise à jour régulière, suivi des vulnérabilités signalées.
- **Évaluation des API et services SaaS tiers :** tests d'intégrité et vérification des politiques de sécurité.

À RETENIR

- **Intégration de la sécurité partout :** du développement au support post-marché.
- **Ressources dédiées :** rôles, formations et gouvernance renforcée.
- **Chaîne d'approvisionnement sous contrôle :** audit, contractualisation et suivi des composants tiers.
- **Coût initial compensé :** réduction des risques d'incidents, accès facilité aux marchés publics, meilleure image de marque.
- **Le CRA devient un moteur d'amélioration continue,** pas seulement une contrainte réglementaire.

LE CONSEIL SOFTEAM

Si vous ne l'avez pas déjà fait, définissez votre gouvernance cybersécurité claire : fixez les responsabilités de chacun, précisez les attendus qui en découlent et formalisez le tout dans une politique SSI appliquée.

Stratégies de mise en conformité

Chapitre 7

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Anticiper la mise en conformité au CRA est la meilleure manière d'éviter une course contre la montre à l'approche de l'échéance.

Plutôt que de traiter le sujet comme un projet ponctuel, il est préférable de l'intégrer dans une dynamique continue d'amélioration de la sécurité et de la qualité.

Feuille de route type

1. Diagnostic initial

- Cartographier les produits et services concernés.
- Identifier les exigences applicables en fonction du type de produit (Classe I, Classe II, critique).
- Évaluer les processus internes actuels face aux exigences CRA.

2. Gap analysis

- Comparer l'existant aux obligations du CRA.
- Classer les écarts par criticité
  (ex. : absence de point de contact CVD, mises à jour non signées, durée de support insuffisante).

3. Plan d'actions priorisées

- Démarrer par les exigences à fort impact ou à mise en œuvre longue
  (ex. : refonte du processus de mise à jour, intégration du DevSecOps).
- Fixer des échéances internes avant la date d'application réglementaire.

Intégration des exigences CRA dans le cycle de vie logiciel

- **Dès la conception :** intégrer le Security by Design dans les spécifications.
- **Pendant le développement :** tests automatisés, contrôle des dépendances, revue de code sécurité.
- **En production :** surveillance continue, journalisation centralisée, gestion active des vulnérabilités.
- **Post-marché :** support prolongé, processus de mises à jour sécurisées, notification rapide des incidents.

Modèles organisationnels

- **PMO cybersécurité :** pilotage centralisé des projets de mise en conformité.
- **Cellule vulnérabilité :** équipe chargée de la détection, du traitement et de la communication autour des vulnérabilités.
- **Réseau de correspondants :** relais CRA dans chaque équipe produit ou service.

Bonnes pratiques d'anticipation

- **Audits réguliers :** tests d'intrusion, analyses de code, revues de conformité.
- **Formations ciblées :** développeurs, chefs de produit, support technique.
- **Exercices de crise :** simulations d'incidents graves et de vulnérabilités activement exploitées.
- **Veille réglementaire et technique :** suivre les évolutions du CRA, des normes harmonisées et des menaces émergentes.

À RETENIR

- **Commencer tôt :** un diagnostic précoce réduit le risque de retard.
- **Intégrer la conformité dans le cycle de vie** plutôt que de la traiter en bout de chaîne.
- **Organisation dédiée :** PMO cybersécurité, cellule vulnérabilité, relais internes.
- **Anticiper les crises :** audits, exercices et communication interne.
- **Faire de la conformité un avantage compétitif :** un produit sûr inspire confiance et ouvre des marchés.

LE CONSEIL SOFTEAM Si vous n'êtes pas une structure habituée à implémenter des changements aussi importants au sein de votre organisation, nous vous conseillons fortement de vous faire accompagner.

Calendrier et échéances

Chapitre 8

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Le CRA suit un calendrier précis fixé par le texte européen.
Même si l'application complète n'est prévue qu'en 2027, les acteurs ont tout intérêt à avancer dès maintenant : les étapes intermédiaires seront déterminantes pour éviter les blocages de dernière minute.

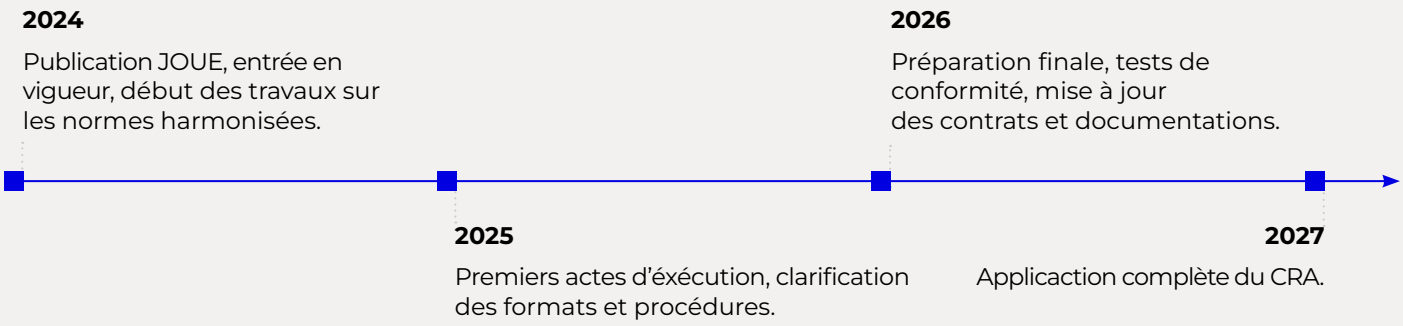
Dates clés

- **Publication au Journal officiel de l'UE :** fin 2024.
- **Entrée en vigueur :** 20 jours après la publication.
- **Application des obligations : 36 mois** après l'entrée en vigueur (prévue en 2027).
- **Obligations spécifiques de notification :** applicables dès **24 mois** après l'entrée en vigueur.
- **Actes d'exécution :** publiés progressivement entre 2024 et 2026, précisant les formats de notification, les procédures de certification et les normes harmonisées.

Dispositions transitoires

- Les produits mis sur le marché **avant la date d'application** ne sont pas soumis rétroactivement au CRA… sauf si des mises à jour majeures sont déployées après cette date, auquel cas certaines obligations peuvent s'appliquer.
- Les certifications déjà obtenues pourront être reconnues si elles sont jugées équivalentes au schéma européen.
- Les fabricants peuvent utiliser la période transitoire pour tester leurs procédures de conformité avant que les sanctions ne s'appliquent.

Frise chronologique indicative



À RETENIR

- **2027 est proche :** 3 ans passent vite en matière de refonte de process et de mise à jour de produits.
- **Notification d'incidents :** obligations applicables dès 24 mois, donc avant l'application complète.
- **Période transitoire stratégique :** tester et ajuster les procédures avant l'échéance.
- **Les normes harmonisées et actes d'exécution à venir** préciseront les modalités concrètes : rester en veille est indispensable.

LE CONSEIL SOFTEAM Anticipez 2027, et entamez dès maintenant les chantiers de mise en conformité pour lisser les coûts.

Conclusion, le regard de notre Practice

Chapitre 9

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Le **Cyber Resilience Act** marque un tournant : il redessine les contours de la confiance dans le numérique en Europe.
Il ne s'agit pas seulement de cocher des cases ou de répondre à une liste d'obligations.
Il s'agit d'entrer dans une nouvelle ère où **la sécurité n'est plus un ajout** mais une condition intrinsèque de la valeur d'un produit.

Cette transition n'est pas neutre : elle oblige les organisations à repenser leur manière de créer, livrer et maintenir leurs solutions.

Mais elle ouvre aussi de nouvelles possibilités de développement :

- Imaginer des produits plus sûrs qui inspirent la confiance dès le premier contact.
- Tisser des relations plus fortes avec les clients, fondées sur la transparence et la maîtrise des risques.
- Bâtir une réputation solide sur un marché européen qui valorise enfin la sécurité comme un atout compétitif.

En réalité, le CRA peut être vu comme **une opportunité**. En effet, les entreprises qui s'en emparent tôt peuvent :

- façonner les standards de demain,
- influencer les bonnes pratiques de leur secteur,
- et créer des alliances durables autour d'un objectif commun : un numérique plus résilient.

2027 n'est pas une ligne de départ. **C'est une invitation à se transformer maintenant**, à prendre de l'avance, à prouver que la sécurité peut être synonyme d'innovation et non de ralentissement.

Le choix est clair : subir le changement… ou le conduire.

Les autorités chargées de s'assurer de la bonne application du texte sont conscientes de l'ampleur des défis auxquels vous êtes confrontés et vont lisser leurs exigences de conformité au fil du temps (il est fort probable que l'attendu sur la gestion des correctifs de sécurité de vos produits ne souffre d'aucun délai dans l'attente de mise en conformité, là où l'intégration de la sécurité dans le développement continu fera sans doute l'objet d'une certaine tolérance dans les délais de mise en œuvre).

Il vous est ainsi possible d'**anticiper** les exigences du règlement qui sont à prioriser ou pour lesquelles une tolérance plus large sera accordée par les autorités. Pour ce faire, vous pouvez mettre en place une veille sur les différentes déclarations concernant le CRA par l'ENISA, l'ANSSI, les différentes NSA européennes (National Security Agency) tel que le BSI allemand ou **vous faire accompagner par un cabinet de conseil** aguerri aux sujets réglementaires ou de conformité cyber.

Vous pouvez ensuite construire un **plan de mise en conformité graduel** qui prend en compte non seulement le texte mais la manière dont il est appréhendé par les autorités de contrôle en ciblant leurs priorités. Vous pourrez ainsi **rationnaliser vos coûts** et **mener une conduite du changement** plus douce et adaptée au sein de votre organisation.

L’expertise cyber chez Softeam

Filiale de Docaposte, SOFTEAM et ses équipes Consulting ont développé une forte expertise Cybersécurité au fil des années.

Nous proposons une offre modulaire au service de l’accompagnement vers une **mise en conformité de votre organisation, en adéquation avec les normes actuelles et réglementations applicables (RGS/NIS/LPM…).**

Nous vous accompagnons avec une approche pragmatique – adaptée à votre niveau de maturité en cybersécurité afin d’identifier et de diriger vos efforts d’implémentation des attendus.

Nous intervenons lors des différentes phases de gouvernance de vos projets cybersécurités afin d’avoir une cohérence et une vision commune : **diagnostic – conseil – plan d’actions.**

Notre vision CRA

Nos experts sont les facilitateurs de l’appropriation et l’intégration du CRA.

Comme toute mise en conformité, le CRA nécessite une phase d’appropriation contextuelle (contexte métier, proportionnalité…) afin de l’adopter et l’adapter à votre contexte, vos enjeux.

Nos experts, anciens RSSI, s’occupent de cette phase d’accompagnement et de pédagogie pour que l’intégration du règlement CRA soit simple et fluide pour vous.

Le CRA doit s’intégrer à votre gouvernance Cybersécurité et vos pratiques existantes. Nous vous écoutons avant de vous conseiller.

Notre équipe

Nos experts RSSI sont formés par notre directeur de l’expertise Cybersécurité, Stéphane Dubreuil, un ancien de l’ANSSI.

Des cadres expérimentés :

- Ayant déjà travaillé en environnement complexe et fortement réglementé engageant leur responsabilité
- Ayant déjà travaillé en environnement en tension (projet à plusieurs M€)

Des jeunes possédant majoritairement des doubles compétences :

- Plus de la moitié des juniors ont 2 bac+5

Une politique de certification systématique :

- Tous nos consultants passent leur certification ISO 27001 et une formation à EBIOS RM.

Softeam

SOFTEAM est le cabinet de conseils et de services de Docaposte (Groupe La Poste).

Notre mission ? Mettre le numérique au service des transitions auxquelles nos sociétés font face.

Concrètement, cela se traduit dans notre attitude et dans nos engagements. Nous sommes des partenaires de confiance pour nos clients, en adoptant une posture d’écoute active et en co-construisant des solutions qui répondent à leurs besoins spécifiques.

Nous sommes conscients que les défis auxquels nous faisons face sont complexes et évolutif : la force de notre collectif de consultants experts et engagés pour le bien commun est le socle de notre mission.

Ensemble, nous voulons faire du numérique un levier pour demain.

Et cela commence justement par un **bon accompagnement Cyber.**

Annexes

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Annexe A – Glossaire CRA

- **Produit comportant des éléments numériques :** Tout logiciel ou matériel dépendant, directement ou indirectement, de données ou de connexions réseau pour fonctionner.
- **Mise sur le marché :** Première mise à disposition d'un produit dans l'UE, à titre onéreux ou gratuit, dans le cadre d'une activité commerciale.
- **Incident grave :** Incident ayant un impact significatif sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou services.
- **Vulnérabilité activement exploitée :** Faille de sécurité utilisée dans le cadre d'une cyberattaque connue.
- **Divulgation coordonnée (CVD) :** Processus formalisé permettant à un chercheur ou à un tiers de signaler une vulnérabilité de manière sécurisée et responsable.
- **SBOM (Software Bill of Materials) :** Inventaire listant les composants logiciels d'un produit, leurs versions, licences et dépendances.
- **Marquage CE :** Certification indiquant qu'un produit est conforme aux exigences européennes applicables, dont le CRA.

Annexe B – Table des articles et annexes cités

- **Article 3 :** Définitions clés (produit numérique, incident grave, vulnérabilité exploitée).
- **Article 8 :** Exigences de cybersécurité (Annexe I, Partie II).
- **Article 11 :** Obligations des fabricants.
- **Article 14 :** Notification des incidents et vulnérabilités.
- **Article 18 :** Procédures de conformité et modules.
- **Annexe I :** Exigences essentielles (Partie II : cybersécurité).
- **Annexes VII et VIII :** Contenu de la documentation technique.

Annexe C – Check-list de conformité

- Le produit intègre la sécurité dès la conception et par défaut (Security by Design & Default).
- Journalisation des événements de sécurité activée, protégée et conservée pendant la période d'assistance.
- Processus de gestion des vulnérabilités formalisé (veille, patching, communication).
- Période d'assistance minimale de 5 ans (ou durée de vie prévue si supérieure).
- Mises à jour de sécurité gratuites, signées et diffusées sans retard injustifié.
- Procédure de divulgation coordonnée (CVD) publique avec point de contact dédié.
- Capacité à notifier un incident grave en 24h et une vulnérabilité exploitée en 72h via ENISA/CSIRT.
- Documentation technique complète, incluant SBOM disponible sur demande.
- Conformité établie via la procédure appropriée (auto-évaluation ou tierce partie).
- Déclaration UE de conformité et marquage CE prêts pour la mise sur le marché.

Annexe D – Matrice « Exigences ↔ Actions »

Exigences CRA	Action opérationnelle	Acteur principal
Security by Design & by Default	Intégrer la cybersécurité dès la conception, activer les protections par défaut	Équipe R&D, architectes
Journalisation	Mettre en place une collecte, stockage et protection des journaux	DevOps / IT
Gestion des vulnérabilités	Déployer un processus formalisé de détection, suivi et correction	Cellule vulnérabilités
Période d'assistance (≥ 5 ans)	Garantir un support technique et des mises à jour de sécurité sur la durée minimale	Fabricant / éditeur
Patch management	Diffuser des correctifs signés et authentifiés, séparés des mises à jour fonctionnelles	Développement & Release management
CVD (divulgation coordonnée)	Publier une politique de signalement, désigner un point de contact	RSSI, support sécurité
Notification d'incidents	Déclarer sous 24h/72h/14j selon le cas via la plateforme ENISA	Référence CRA / CSIRT interne
Documentation technique (Annexes VII / VIII)	Constituer un dossier technique incluant SBOM et analyse de risques	Équipe conformité, qualité

Annexe E – Notification des incidents et vulnérabilités

- **Incidents graves :**
  - Alerte précoce → sous 24h à ENISA/CSIRT
  - Rapport intermédiaire → sous 72h
  - Rapport final → sous 1 mois
- **Vulnérabilités activement exploitées :**
  - Notification initiale → sous 72h
  - Rapport détaillé → sous 14 jours

→ Canal officiel : plateforme unique ENISA, en lien avec le CSIRT coordinateur national.

À ce jour, aucun modèle officiel de tableau de notification n'a été publié par la Commission européenne ou l'ENISA. Les entreprises doivent suivre les formats qui seront précisés par les actes d'exécution.

Annexe F – Références et bibliographie

- Texte officiel : Règlement (UE) .../2024 relatif aux exigences de cybersécurité pour les produits comportant des éléments numériques (Cyber Resilience Act).
- ENISA :
  - Guides sur la gestion des vulnérabilités et la CVD.
  - Travaux préparatoires sur la plateforme de notification.
- ANSSI (France) :
  - Guide de l'hygiène informatique.
  - Recommandations sur la gestion des vulnérabilités et la supply chain.
- ISO/IEC :
  - 27001 (management de la sécurité).
  - 29147 (vulnerability disclosure).
  - 30111 (vulnerability handling).
- OWASP :
  - OWASP Top 10.
  - Software Component Verification Standard (SCVS).

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Vous souhaitez échanger avec nos experts sur vos besoins d'accompagnement cyber ?

Nos experts prennent (vraiment) le temps de vous écouter et comprendre vos enjeux, votre environnement et vos objectifs.

Contactez directement nos experts via practice.cyber@softeam.fr

Crédit photo : AdobeStock