LIVRE BLANC CRA EVIDENCE

Le règlement sur la cyberrésilience de l’UE: guide pratique de conformité

Livre blanc destiné aux fabricants, importateurs et distributeurs de produits comportant des éléments numériques.

Version	1.0
Statut	Document vivant
Base	Règlement (UE) 2024/2847

Historique des modifications

Liste des modifications apportées à ce livre blanc depuis sa première publication.

Version	Date	Description
1.0	17 mai 2026	Première publication. Parité structurelle complète avec la version EN: ajout du §5 sur la modification substantielle, des sous-sections classification (fonctionnalité principale, cloud, chaîne d'approvisionnement), des blocs détermination du support, diligence raisonnable composants, délais article 14 et mesures correctives, fusion des exigences vulnérabilités 4-5-6 en §4 réception/ CVD/avis.

Sommaire

Synthèse

EN 60 SECONDES

Champ couvert: produits matériels et logiciels connectés mis sur le marché de l'UE, avec une sécurité traitée comme une exigence de conformité produit plutôt que comme une bonne pratique.

Date d'effet: signalements au titre de l'article 14 à partir du 11 septembre 2026; obligations techniques, documentaires et de marquage CE complètes à partir du 11 décembre 2027.

Éléments à produire: évaluation des risques de cybersécurité, SBOM, documentation technique, instructions destinées aux utilisateurs, déclaration UE de conformité, marquage CE, et signalements d'incidents et de vulnérabilités au titre de l'article 14.

Qui doit agir

Les fabricants portent l'essentiel de la charge. Importateurs et distributeurs doivent effectuer des vérifications de diligence avant de mettre les produits à disposition.

Ce qui change

La cybersécurité devient une composante de la conformité produit: conception sécurisée, traitement des vulnérabilités, documentation, marquage CE et actions après mise sur le marché.

Premier délai

Le signalement au titre de l'article 14 commence le **11 septembre 2026** pour les vulnérabilités activement exploitées et les incidents graves.

Application complète

La conformité technique complète s'applique à partir du **11 décembre 2027**. Les produits antérieurs sont couverts après modification substantielle, mais le signalement reste applicable.

Socle de preuves

La documentation technique doit contenir l'évaluation des risques, la SBOM, la justification de la période de support, les preuves de tests, les instructions aux utilisateurs, la déclaration et les preuves de conformité aux exigences essentielles de cybersécurité.

Voie de conformité

La plupart des produits peuvent utiliser l'autoévaluation du module A. Les produits importants et critiques peuvent nécessiter un organisme notifié ou une certification européenne de cybersécurité.

Qu’est-ce que le règlement sur la cyberrésilience?

Le Cyber Resilience Act (CRA), formellement le Règlement (UE) 2024/2847, est le premier cadre applicable dans toute l’UE qui rend la cybersécurité obligatoire pour les produits comportant des éléments numériques mis sur le marché de l’UE. Le texte de référence est disponible sur EUR-Lex.

Le CRA s’applique aux fabricants, importateurs et distributeurs de matériels et logiciels connectés. Il couvre des produits allant des objets connectés grand public aux systèmes de contrôle industriels. Le changement pratique est simple: la cybersécurité doit désormais être conçue, démontrée, maintenue et surveillée comme une composante de la conformité produit.

Le non-respect des exigences essentielles de cybersécurité ou des obligations des articles 13 et 14 peut entraîner des amendes allant jusqu’à 15 millions d’euros ou 2,5 % du chiffre d’affaires annuel mondial, selon le montant le plus élevé. Des tranches inférieures s’appliquent: jusqu’à 10 millions d’euros ou 2 % pour la violation d’autres obligations spécifiées, et jusqu’à 5 millions d’euros ou 1 % pour la fourniture d’informations incorrectes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités de surveillance du marché. Les autorités de surveillance du marché peuvent aussi exiger des mesures correctives, limiter la mise à disposition, retirer des produits ou imposer des rappels.

Dates clés pour planifier la conformité

Le CRA est entré en vigueur le **10 décembre 2024**. Le travail pratique de conformité s'organise autour de trois jalons: organismes notifiés en **juin 2026**, signalement en **septembre 2026** et conformité technique complète en **décembre 2027**.

NOTE

État des lignes directrices de la Commission: La Commission européenne a publié le projet de lignes directrices CRA le 3 mars 2026. La consultation s'est close le 13 avril 2026. Ces lignes directrices ne sont pas finales, mais elles servent de matériau de planification pour la mise sur le marché, les logiciels libres et ouverts, les périodes de support, les modifications substantielles, la classification des produits, la diligence raisonnable sur les composants, le traitement de données à distance, la gestion des vulnérabilités et les recoupements avec d'autres textes de l'UE. Certaines questions de frontière, notamment avec l'AI Act et DORA, pourraient encore nécessiter des précisions.

10 décembre 2024

Entrée en vigueur

Début de la période transitoire

11 juin 2026

Organismes notifiés

Le chapitre IV s'applique

11 septembre 2026

Signalement

Début des signalements au titre de l'article 14

11 décembre 2027

Application complète

Exigences techniques, marquage CE, documentation et évaluation de la conformité

À FAIRE D'ABORD

Commencez par la préparation au signalement. L'échéance de l'article 14 arrive avant la conformité technique complète et s'applique aux produits déjà présents sur le marché de l'UE.

Comme le signalement commence le **11 septembre 2026**, la préparation au signalement doit être le premier chantier de mise en œuvre: **détection, triage, information des utilisateurs et signalement aux autorités** doivent fonctionner avant l'échéance de conformité technique complète.

Les produits comportant des éléments numériques mis sur le marché avant le **11 décembre 2027** ne sont soumis aux exigences techniques du CRA que s'ils font l'objet d'une **modification substantielle** à partir de cette date. Le signalement suit une règle différente: l'article 14 s'applique à **tous les produits concernés**, y compris ceux déjà présents sur le marché de l'UE.

Le CRA sur le cycle de vie du produit

ÉTAPE 01

Définir le périmètre

Champ, classification, période de support et évaluation des risques

ÉTAPE 02

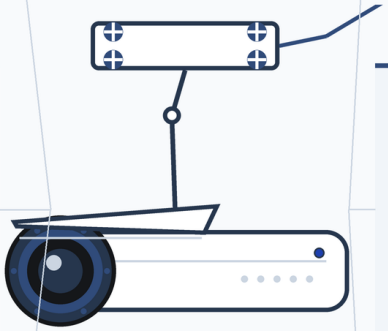
Développer de façon sécurisée

Réglages sûrs par défaut, analyse de code, SBOM et maîtrise des dépendances

ÉTAPE 03

Valider et documenter

Tests, triage des vulnérabilités, dossier technique et notices utilisateur



ÉTAPE 04

Mettre sur le marché

Déclaration UE de conformité, marquage CE et décision de release

ÉTAPE 05

Surveiller et mettre à jour

CVE, avis, activité d’exploitation, mises à jour de sécurité et divulgation

ÉTAPE 06

Support et coopération

Signalement article 14, avis utilisateurs, demandes des autorités et fin de support

Caméra IP connectée, de la planification produit au support après mise sur le marché au titre du CRA

Produits concernés

Champ d’application et exclusions

Le CRA s’applique aux produits matériels et logiciels dont l’usage prévu ou raisonnablement prévisible comprend une connexion de données directe ou indirecte à un dispositif ou à un réseau. Cela inclut les ordinateurs, smartphones, équipements réseau, objets connectés, systèmes de contrôle industriels et applications de traitement de données.

Les catégories suivantes sont explicitement exclues:

- Dispositifs médicaux et dispositifs médicaux de diagnostic in vitro couverts par les règlements (UE) 2017/745 et 2017/746
- Systèmes automobiles couverts par le Règlement (UE) 2019/2144
- Équipements aéronautiques couverts par le Règlement (UE) 2018/1139
- Équipements marins couverts par la Directive 2014/90/UE
- Produits développés exclusivement à des fins de sécurité nationale ou de défense
- Produits purement mécaniques sans éléments numériques ni connectivité réseau

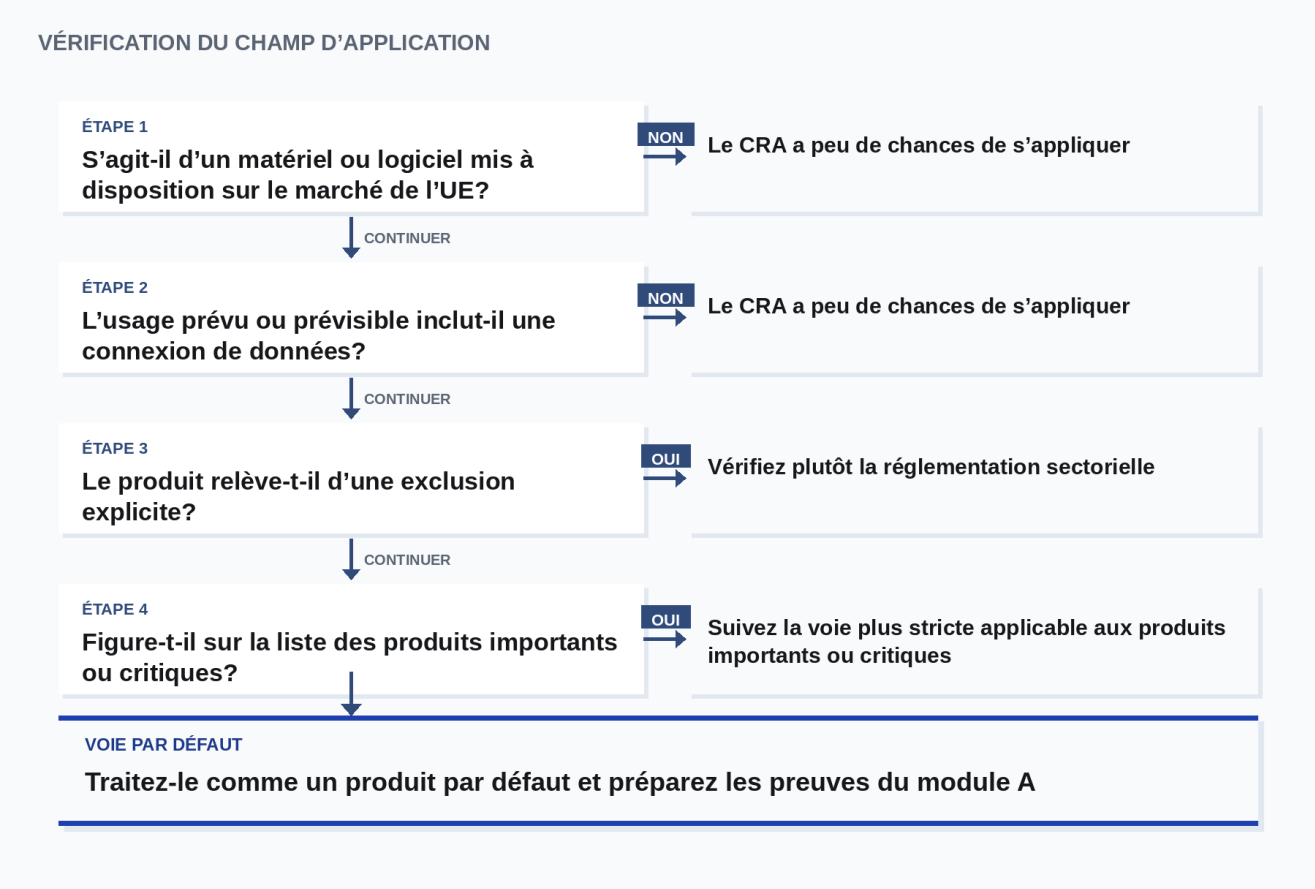
Sauf exclusion claire, partez du principe que votre produit connecté entre dans le champ du CRA.

NOTE

Produits sur mesure: une dérogation étroite. Si vous construisez un produit ajusté à un utilisateur professionnel précis, dans le cadre d’un accord écrit entre vous et cet utilisateur, vous pouvez déroger à deux exigences seulement: la configuration sécurisée par défaut (vous devez tout de même offrir un chemin de retour vers un état initial sécurisé) et la gratuité des mises à jour de sécurité (l’accord peut fixer une base commerciale différente). Tout le reste s’applique pleinement: traitement des vulnérabilités, autres exigences de sécurité produit, signalement au titre de l’article 14, documentation technique, marquage CE, évaluation de la conformité et période de support. Ce n’est pas une dérogation B2B générale; elle ne couvre pas les produits sur catalogue vendus à des entreprises.

RESPONSABILITÉS DES OPÉRATEURS ÉCONOMIQUES

Fabricant	Concevoir des produits sûrs, évaluer les risques, préparer la documentation technique, mener l’évaluation de la conformité, traiter les vulnérabilités, signaler les événements relevant de l’article 14.
Importateur	Vérifier la conformité du fabricant, contrôler le marquage CE et la documentation, tenir la déclaration disponible, agir sur les vulnérabilités connues.
Distributeur	Contrôler les indices de diligence avant la fourniture, vérifier les informations et instructions requises, éviter de mettre à disposition des produits non conformes.



La classification du produit détermine la voie d'évaluation

Votre catégorie de produit détermine la manière dont vous démontrez la conformité.

Catégorie	Exemples	Évaluation de la conformité
Par défaut « non classé »	Logiciels généraux et produits connectés grand public qui ne figurent pas dans les catégories importantes ou critiques	Module A: autoévaluation
Important « classe I »	Identité, navigateur, gestionnaire de mots de passe, antivirus, VPN, gestion de réseau, routeur, serrure connectée, caméra de sécurité et produits similaires	Module A uniquement lorsque les normes harmonisées, spécifications communes ou schémas de certification applicables sont appliqués comme requis; sinon module B+C ou module H
Important « classe II »	Hyperviseurs, environnements d'exécution de conteneurs, pare-feu, IDS/IPS et microprocesseurs résistants aux manipulations	Module B+C, module H ou schéma européen de certification de cybersécurité applicable avec un niveau d'assurance au moins « substantiel »
Produits critiques	Éléments sécurisés, cartes à puce, passerelles de compteurs intelligents et boîtiers matériels de sécurité	Certification européenne de cybersécurité lorsqu'elle est requise et disponible; sinon les voies de classe II s'appliquent

Les quatre catégories de produits

Le tableau ci-dessus présente des exemples. La référence complète, à laquelle vous comparez la fonctionnalité principale de votre produit, est exposée ci-dessous.

Produits par défaut

La plupart des produits se rangent ici. Tout produit comportant des éléments numériques dont la fonctionnalité principale ne correspond à aucune entrée des listes importantes ou critiques ci-dessous est traité comme un produit par défaut. La voie de conformité est l'autoévaluation du module A.

Exemples courants:

- Téléviseurs intelligents et boîtiers de diffusion en continu.
- Imprimantes réseau et appareils de bureau multifonctions.
- Enceintes Bluetooth et produits audio grand public.
- Applications logicielles de lecture multimédia.
- Consoles de jeu, liseuses et autres équipements électroniques grand public.
- Appareils de cuisine intelligents tels que fours, réfrigérateurs et lave-vaisselle sans fonctions de sécurité.
- Ampoules intelligentes et éclairage connecté sans fonctions de sécurité.
- Trackers de fitness sans visée de suivi médical.
- Applications mobiles polyvalentes qui ne sont ni des navigateurs, ni des gestionnaires de mots de passe, ni des applications VPN.
- Logiciels bureautiques tels que traitements de texte et tableurs.

La liste ci-dessus est illustrative. Les listes importantes et critiques ci-dessous sont exhaustives.

Produits importants (classe I)

Évaluation par un tiers obligatoire, sauf application des normes harmonisées, spécifications communes ou schémas de certification applicables comme requis.

1. Logiciels et matériels de gestion des identités et de gestion des accès privilégiés, y compris les lecteurs d'authentification et de contrôle d'accès (lecteurs biométriques compris).
2. Navigateurs autonomes et embarqués.
3. Gestionnaires de mots de passe.
4. Logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants.
5. Produits VPN.
6. Systèmes de gestion de réseau.
7. Systèmes de gestion des informations et des événements de sécurité (SIEM).
8. Gestionnaires de démarrage.
9. Logiciels d'infrastructure à clé publique et de délivrance de certificats numériques.
10. Interfaces réseau physiques et virtuelles.
11. Systèmes d'exploitation.
12. Routeurs, modems destinés à la connexion à internet et commutateurs.

13. Microprocesseurs dotés de fonctionnalités liées à la sécurité.
14. Microcontrôleurs dotés de fonctionnalités liées à la sécurité.
15. ASIC et FPGA dotés de fonctionnalités liées à la sécurité.
16. Assistants virtuels polyvalents pour la maison connectée.
17. Produits de maison connectée dotés de fonctionnalités de sécurité (serrures connectées, caméras de sécurité, écoute-bébés, systèmes d'alarme).
18. Jouets connectés à internet à fonctions interactives (parole, captation d'images, suivi de localisation).
19. Wearables personnels à visée de suivi médical (lorsque les règlements (UE) 2017/745 ou 2017/746 ne s'appliquent pas), ou wearables destinés à un usage par des enfants.

Produits importants (classe II)

Évaluation par un tiers obligatoire, voie plus stricte. L'autoévaluation n'est pas disponible même lorsque des normes harmonisées existent.

1. Hyperviseurs et environnements d'exécution de conteneurs prenant en charge l'exécution virtualisée de systèmes d'exploitation et d'environnements similaires.
2. Pare-feu, systèmes de détection et de prévention des intrusions.
3. Microprocesseurs résistants aux manipulations.
4. Microcontrôleurs résistants aux manipulations.

Produits critiques

Certification européenne de cybersécurité requise lorsque le schéma est disponible. Sinon, la voie de classe II s'applique.

1. Dispositifs matériels avec boîtiers de sécurité.
2. Passerelles pour compteur intelligent au sein des systèmes intelligents de mesure tels que définis à l'article 2, point 23, de la directive (UE) 2019/944, et autres dispositifs à des fins de sécurité avancées, y compris pour un traitement cryptographique sécurisé.
3. Cartes à puce et dispositifs similaires, y compris les éléments sécurisés.

Si la fonctionnalité principale de votre produit correspond à une entrée des listes importantes ou critiques, vous êtes dans cette classe. Si votre produit intègre une de ces entrées en tant que composant mais que sa propre fonctionnalité principale est autre chose, l'intégration ne modifie pas votre classe.

Comment classer: fonctionnalité principale, pas intégration

Les listes ci-dessus vous disent ce que sont les catégories. Elles ne vous disent pas comment les appliquer à votre produit. La réponse du CRA tient en un terme: **fonctionnalité principale**.

Votre classe est déterminée par la fonctionnalité principale de votre produit, pas par les composants qu'il intègre. Si elle correspond à une entrée des listes importantes, le produit est important (classe I ou classe II). Si elle correspond à la liste critique, le produit est critique. Sinon, le produit est par défaut. C'est tout le test.

Le garde-fou pratique se trouve dans la deuxième phrase de l'article 7, paragraphe 1. Intégrer un composant important ne pousse pas le produit intégrateur dans la classe importante. Embarquer une bibliothèque de pare-feu dans un hub domotique ne fait pas du hub un pare-feu. Le considérant 45 le dit en termes simples: les pare-feu et systèmes de détection d'intrusion sont importants de classe II, mais les autres produits qui les intègrent ne le sont pas.

Utilisez cette séquence pour vous classer vous-même.

1. **Nommez la fonctionnalité principale de votre produit en une phrase.** Si vous ne le pouvez pas, le reste de l'analyse échoue. Concentrez-vous sur ce sans quoi le produit ne fonctionnerait pas.
2. **Vérifiez les listes importantes ci-dessus.** Une correspondance en classe I ou II rend le produit important.
3. **Vérifiez la liste critique ci-dessus.** Une correspondance rend le produit critique. Une voie de certification européenne de cybersécurité s'applique lorsque le schéma est disponible; sinon, la voie de classe II s'applique.
4. **Aucune correspondance dans aucune liste.** Le produit est par défaut. L'autoévaluation du module A est la voie.
5. **Documentez le raisonnement.** Une note d'une page avec l'énoncé de la fonctionnalité principale, la vérification des listes et la voie retenue trouve sa place dans la documentation technique.

Deux exemples concrets.

Hub de maison connectée avec gestionnaire de mots de passe embarqué. Fonctionnalité principale: orchestrer des routines entre objets connectés grand public dans un logement. Le composant gestionnaire de mots de passe, vendu séparément par son propre fabricant, est un produit important de classe I à part entière. La fonctionnalité principale du hub est la domotique, pas la gestion d'identifiants. Le hub reste par défaut.

Système d'exploitation par ensemble de fonctions. Un produit est commercialisé comme appareil de maison connectée, mais ses fonctions principales sont l'initialisation du matériel et des périphériques, l'ordonnancement des processus, la gestion de la mémoire et une interface d'appels système. C'est la fonctionnalité principale d'un système d'exploitation. Les systèmes d'exploitation sont un produit important de classe I. Le produit est important de classe I, quel que soit le discours marketing.

Si votre classification atterrit sur une classe qui surprend le reste de l'équipe, l'énoncé de la fonctionnalité principale mérite une passe supplémentaire avant la mise sur le marché.

Quand le cloud fait partie de votre produit

La plupart des produits comportant des éléments numériques s'appuient sur quelque chose en dehors du dispositif: un backend cloud, une application mobile compagnon, un serveur de mises à jour à distance, un portail d'authentification, un système de gestion de flotte. Le CRA ne traite pas tous ces éléments comme votre produit. Il les traite comme partie du produit uniquement lorsque **deux** conditions sont réunies:

- Le logiciel a été **conçu et développé par votre équipe, ou sous votre responsabilité**.
- Le produit **n'assurerait pas l'une de ses fonctions** sans lui.

Si l'une des deux conditions n'est pas remplie, le service distant se trouve hors du périmètre du produit pour le CRA. Un SaaS tiers que vous ne possédez pas, même si votre produit dialogue avec lui, ne fait pas partie de votre produit. Un site web qui promeut le produit mais ne soutient pas ses fonctions n'en fait pas partie non plus.

Lorsqu'un composant distant entre dans le périmètre, il y entre **en tant que partie du produit**. La documentation technique, l'évaluation de la conformité, la déclaration UE de conformité, le traitement des vulnérabilités et les délais de signalement au titre de l'article 14 couvrent alors le composant cloud comme le dispositif.

Utilisez cette matrice pour trancher rapidement.

Composant	Dans le périmètre, en tant que partie du produit?
Application mobile compagnon qui s'apparie au dispositif	**Oui.** Vous l'avez conçue, et le dispositif ne peut pas être configuré ou utilisé sans elle.
Backend cloud qui stocke et traite les données du dispositif	**Oui.** Vous l'avez conçu, et le tableau de bord ou la fonction principale ne fonctionne pas sans lui.
Serveur de mises à jour à distance	**Oui.** Vous l'avez conçu, et le dispositif ne peut pas recevoir de mises à jour de sécurité sans lui.
Portail d'authentification qui contrôle l'accès au dispositif	**Oui.** Vous l'avez conçu, et les utilisateurs ne peuvent pas se connecter sans lui.
Site marketing du produit	**Non.** Il ne soutient aucune fonction du produit.
SaaS tiers avec lequel le produit s'intègre (vous ne le possédez pas)	**Non.** Non conçu par vous. Le fournisseur tiers porte ses propres obligations au titre de NIS 2.
Infrastructure cloud générique sur laquelle tourne votre service (IaaS ou PaaS)	**Non.** Non conçue par vous. Le fournisseur d'infrastructure relève de NIS 2.

Schéma courant: un dispositif de maison connectée avec une application mobile, un serveur de mises à jour et un backend cloud. Les trois sont conçus par le fabricant, et le dispositif ne peut pas assurer ses fonctions annoncées sans eux. Les trois font partie du produit. Les obligations CRA s'appliquent à l'ensemble. Si le backend cloud dialogue ensuite avec un SaaS tiers d'analytique, ce SaaS ne fait pas partie du produit. Le fournisseur tiers porte ses propres obligations au titre de NIS 2.

Le CRA n'exige pas de mesures de sécurité pour le réseau et les systèmes d'information du fabricant pris dans leur ensemble. Il exige la sécurité pour les services distants qui font partie du produit. La frontière, c'est celle du produit, pas celle de l'entreprise.

Votre chaîne d’approvisionnement: qui fait quoi sous le CRA

Le CRA fait peser les obligations principales sur vous en tant que fabricant, mais importateurs et distributeurs portent aussi des devoirs qui influent sur la façon dont votre produit atteint le marché. Trois points comptent pour vous.

Qui	Ce qu’ils vérifient avant la fourniture	Ce qu’ils font sur une vulnérabilité	Quand ils reprennent vos obligations
Importateur	Marquage CE, déclaration UE de conformité, instructions destinées aux utilisateurs dans la bonne langue, vos coordonnées sur ou avec le produit	Vous informe sans retard injustifié; informe directement les autorités de surveillance du marché si le produit présente un risque cyber significatif	Lorsqu’ils mettent votre produit sur le marché sous leur propre nom ou marque, ou le modifient substantiellement
Distributeur	Marquage CE, le fait que vous et l’importateur avez fait votre part, le fait que les documents requis accompagnent le produit	Vous informe sans retard injustifié; informe directement les autorités de surveillance du marché en cas de risque cyber significatif; peut cesser la mise à disposition	Même déclencheur que pour les importateurs

Pour un fabricant, cela se traduit par trois choses pratiques:

- Votre marquage CE, votre déclaration UE de conformité et vos instructions doivent être corrects et dans la bonne langue au moment où un distributeur les vérifie. Les partenaires de distribution sont tenus de procéder à ces vérifications et peuvent refuser de mettre le produit à disposition s’ils manquent ou sont incorrects.
- Vous avez besoin d’un canal de contact clair et accessible que les importateurs et distributeurs peuvent utiliser pour remonter des vulnérabilités dans votre processus de traitement. Ils s’en serviront.
- Tout partenaire qui rebadge, met votre produit sur le marché sous son propre nom ou marque, ou le modifie substantiellement devient le fabricant pour cette variante. L’ensemble complet des obligations de documentation technique, d’évaluation de la conformité, de signalement et de période de support bascule alors sur lui pour cette version. Voir *Quand quelqu’un d’autre devient le fabricant* dans la section suivante pour la règle de modification substantielle.

Modification substantielle: quand la re-conformité s’applique

Une fois votre produit sur le marché, le CRA répartit les changements ultérieurs en deux camps. La plupart sont de routine et ne déclenchent rien de plus. Certains sont substantiels. Une modification substantielle est traitée, au sens du CRA, comme une nouvelle mise sur le marché. Cela suppose une nouvelle évaluation de la conformité, une documentation technique rafraîchie, une nouvelle déclaration UE de conformité et un marquage CE sur la nouvelle version.

Le test est court et il se trouve dans la définition de modification substantielle. Un changement est substantiel si l’une de ces conditions est vraie:

- Il **a une incidence sur la conformité** aux exigences essentielles de cybersécurité.
- Il **modifie l’utilisation prévue** pour laquelle le produit a été évalué.

Si aucune ne s’applique, le changement n’est pas substantiel. Documentez quand même le raisonnement et conservez-le. L’analyse fait partie de la trace de preuves.

Ce qui ne compte pas comme substantiel

Deux dérogations font l’essentiel du travail en pratique.

Les mises à jour de sécurité et corrections de bogues qui réduisent le risque cyber sans changer l’utilisation prévue ne sont pas substantielles. Corriger une vulnérabilité connue, ajuster la validation des entrées pour fermer une faille ou reconstruire un composant pour traiter un CVE relèvent tous de ce côté de la ligne.

La remise à neuf, la maintenance et les réparations ne sont pas non plus automatiquement substantielles. Elles ne le deviennent que si elles modifient l’utilisation prévue ou ont une incidence sur la conformité aux exigences essentielles de cybersécurité.

Les retouches mineures d’interface utilisateur restent aussi du bon côté. Ajouter une langue, changer un jeu d’icônes ou peaufiner la mise en page d’un écran n’est pas une modification substantielle en soi. Ajouter un nouvel élément de saisie qui requiert une validation d’entrée adéquate peut l’être.

Pièces de rechange

Le CRA exempte les pièces de rechange de manière étroite et précise. Les **pièces de rechange identiques**, fabriquées aux mêmes spécifications que les composants qu’elles remplacent, sont entièrement hors du champ du règlement. Les remplacements fonctionnels ne le sont pas.

Utilisez cette matrice pour trancher rapidement.

Remplacement	Hôte mis sur le marché avant le 11 décembre 2027	Hôte mis sur le marché à partir du 11 décembre 2027
Identique au composant d'origine, mêmes spécifications	Pièce hors champ CRA. Aucune obligation déclenchée par l'échange.	Pièce hors champ CRA. Aucune obligation déclenchée par l'échange.
Fonctionnellement équivalent, conception ou spécification différente	Le remplacement est un produit CRA à part entière. L'hôte n'a pas d'obligations CRA, car il est antérieur à la date d'application.	Le remplacement est un produit CRA. Évaluez si l'intégration dans l'hôte constitue une modification substantielle de l'hôte selon le test à deux branches ci-dessus.

Deux conséquences pratiques. D'abord, l'exemption dépend de la spécification identique. Un module sans fil reconstruit sur un autre chipset n'est pas une pièce identique, même si le client ne perçoit pas la différence. Ensuite, le fabricant qui fournit un remplacement fonctionnel porte les obligations CRA pour cette pièce, indépendamment de qui a fabriqué l'hôte.

Mises à jour logicielles et feature flags

Les releases logicielles sont la source la plus courante de questions sur la modification substantielle. Le test à deux branches les tranche toutes.

Un correctif qui ferme une vulnérabilité n'est pas substantiel. Un feature flag qui active une capacité pour laquelle le produit n'a jamais été évalué l'est. Une montée de version de modèle qui permet au produit de décider sur de nouvelles catégories d'entrées l'est aussi. Si une release embarque à la fois un correctif et une nouvelle fonctionnalité, évaluez la fonctionnalité.

Le regroupement compte moins que le fond. Qu'une nouvelle fonctionnalité arrive seule ou dans la même release qu'un correctif de sécurité n'a pas d'incidence sur l'évaluation.

Si vous opérez des feature flags ou des déploiements échelonnés, le moment qui compte est l'activation pour les utilisateurs finaux en production, pas la livraison du binaire qui contient le drapeau.

La décision en pratique

Utilisez cette séquence sur chaque changement avant la mise à disposition.

1. **Le changement modifie-t-il l'utilisation prévue du produit?** Si oui: substantiel. Relancez l'évaluation de la conformité pour la nouvelle version.
2. **Le changement a-t-il une incidence sur la conformité aux exigences essentielles de cybersécurité?** Si oui: substantiel. Relancez l'évaluation de la conformité pour la nouvelle version.
3. **Sinon:** non substantiel. Documentez l'analyse et continuez sous la documentation technique existante.

Si le produit est dans la classe importante ou critique et que la voie a exigé une évaluation par un tiers la première fois, une modification substantielle vous remet sur la même voie. Notifiez le tiers à l'avance de tout changement susceptible d'être substantiel. L'autoévaluation n'est pas une porte dérobée pour reclasser après coup un produit important.

Conséquences quand une modification est substantielle

Une modification substantielle est traitée comme une nouvelle mise sur le marché. Pour le fabricant, cela signifie:

- Rafraîchir la documentation technique pour la version modifiée.
- Relancer l'évaluation de la conformité selon la voie exigée par la classe du produit.
- Émettre une nouvelle déclaration UE de conformité pour la version modifiée.
- Apposer à nouveau le marquage CE, avec la nouvelle déclaration au dossier.
- Conserver la documentation de la version précédente pendant toute la durée de conservation. La nouvelle version ne l'efface pas.

Pour les produits logiciels en particulier, vous pouvez limiter les mises à jour de sécurité pendant la période de support à la dernière version que vous avez mise sur le marché, à condition que les utilisateurs des versions antérieures puissent passer gratuitement à la dernière version et sans nouveau matériel.

Les unités de terrain déjà vendues sous la conformité précédente ne sont pas affectées. L'obligation porte sur la version modifiée mise à disposition, pas sur des unités identiques antérieures.

Quand quelqu'un d'autre devient le fabricant

Si vous n'êtes pas le fabricant d'origine et que vous procédez à une modification substantielle, le CRA vous traite comme le fabricant pour cette version. L'ensemble complet des obligations des articles 13 et 14 vous incombe. La même règle s'applique si vous mettez le produit sur le marché sous votre propre nom ou marque.

Cela attrape plus de situations que les équipes ne le supposent généralement:

- Un intégrateur de systèmes qui livre un build firmware spécifique à un client, avec de nouvelles fonctionnalités.
- Un revendeur qui propose un produit en marque blanche et change l'utilisation prévue annoncée.
- Un prestataire de services qui regroupe un dispositif tiers avec son propre firmware.

Dans chaque cas, l'acteur qui a fait le changement hérite des obligations de fabricant pour cette version: documentation technique, évaluation de la conformité, signalement, traitement des vulnérabilités et le reste. L'étiquette « importateur » ou « distributeur » cesse de les protéger dès qu'ils franchissent l'une des deux lignes.

Ce que vous devez mettre en place

Utilisez cette section comme une liste de contrôle opérationnelle. Le détail exigence par exigence suit ensuite.

Évaluation des risques de cybersécurité

Avant de mettre un produit sur le marché, vous devez disposer d'une évaluation des risques de cybersécurité. C'est le document qui explique, dans vos propres termes, pourquoi le produit est sûr à mettre sur le marché et à y maintenir.

L'évaluation doit couvrir:

- L'utilisation prévue du produit, et les usages que vous pouvez raisonnablement anticiper
- Les conditions et l'environnement d'exploitation du produit
- Les données et fonctions à protéger
- Les menaces applicables, et les contrôles sur lesquels vous vous appuyez pour les gérer
- La durée pendant laquelle le produit est censé être utilisé

Comment la plupart des équipes structurent l'exercice. Les méthodologies crédibles convergent vers les mêmes étapes: identifier les actifs (données traitées par le produit, éléments de sécurité comme les clés et identifiants, fonctions dont la perte nuirait aux utilisateurs), cartographier l'endroit où chaque actif réside ou se déplace, modéliser les menaces par actif et par environnement en prenant la confidentialité, l'intégrité et la disponibilité comme axes, scorer impact et vraisemblance, décider quels risques résiduels accepter et lesquels atténuer, puis ré-évaluer après chaque tour de contrôles (chaque nouvelle clé, certificat ou fonction d'authentification devient lui-même un nouvel actif à analyser).

Modélisation des menaces. L'étape trois ci-dessus est la plus technique et dispose de techniques établies. STRIDE catégorise les menaces selon spoofing, tampering, repudiation, information disclosure, denial of service et elevation of privilege; largement utilisée, elle convient à la plupart des produits connectés. LINDDUN étend la grille pour les produits qui traitent des données à caractère personnel, en ajoutant linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness et non-compliance; utile quand le régime de protection des données recouvre les devoirs CRA. PASTA déroule un processus en sept étapes des objectifs métier jusqu'à l'acceptation du risque résiduel; utile pour les systèmes complexes où la cartographie d'attaque oriente la conception. Aucune n'est spécifique au CRA, et le CRA n'en exige aucune. Choisissez celle qui colle au profil d'exposition de votre produit.

Où trouver une méthodologie aboutie. Le CRA ne prescrit pas de méthode. L'Office fédéral allemand de la sécurité informatique (BSI) publie la Directive technique TR-03183, la méthodologie d'évaluation des risques alignée sur le CRA la plus détaillée en circulation publique. L'ENISA publie une orientation plus large sur la mise en œuvre du CRA.

Maintenez l'évaluation à jour pendant toute la période de support. Quand la cartographie des menaces, les composants ou le cas d'usage changent, l'évaluation doit changer avec eux.

Détermination de la période de support

Chaque produit a besoin d'une période de support définie, et vous devez en publier la date de fin au point d'achat. La période de support est la fenêtre pendant laquelle vous traitez les vulnérabilités, livrez les mises à jour de sécurité et tenez à jour la documentation technique.

Quelle durée minimale

Au moins cinq ans. Si le produit est censé être utilisé moins de cinq ans, la période de support doit correspondre à la durée d'utilisation attendue. S'il est censé être utilisé plus longtemps, la période doit refléter cette durée plus longue; des produits comme les routeurs, les systèmes d'exploitation et les contrôleurs industriels justifient régulièrement plus de cinq ans.

Facteurs à peser

Lorsque vous fixez la période, prenez en compte, de manière proportionnée:

- Les attentes raisonnables des utilisateurs pour le produit
- La nature du produit, y compris son utilisation prévue
- Toute législation de l'UE qui fixe déjà une durée de vie pour cette catégorie de produit
- Les périodes de support de produits comparables sur le marché
- La disponibilité de l'environnement opérationnel dont le produit dépend
- Les périodes de support des composants intégrés qui assurent des fonctions principales
- Toute orientation de l'ADCO ou de la Commission pour la catégorie de produit

Le raisonnement derrière la période retenue doit figurer dans la documentation technique. Les autorités de surveillance du marché peuvent le demander.

Ce que vous devez publier

Indiquez la fin de la période de support au moment de l'achat, avec au moins le mois et l'année, dans un endroit facilement accessible. Lorsque le produit dispose d'une interface utilisateur, affichez une notification au moment où il atteint la fin de sa période de support.

Conservation des mises à jour

Chaque mise à jour de sécurité mise à disposition des utilisateurs pendant la période de support doit rester disponible pendant au moins 10 ans après son émission, ou pendant le reste de la période de support si cette durée est plus longue.

Diligence raisonnable sur les composants

Un produit est fait de composants. Certains, vous les avez écrits; d'autres, vous les avez achetés; d'autres encore viennent d'un dépôt open source. Le CRA traite le produit comme un tout pour la conformité, donc les composants comptent. Si une vulnérabilité réside dans un composant, elle réside dans votre produit. Si un composant ne reçoit pas de mises à jour de sécurité, votre produit n'en reçoit pas non plus.

Les fabricants doivent exercer une diligence raisonnable sur les composants tiers, y compris les composants libres et ouverts. Les composants ne doivent pas compromettre la cybersécurité du produit.

L’ampleur de la diligence dépend du risque cyber que porte le composant. Une bibliothèque qui gère l’authentification ne se traite pas comme une bibliothèque de rendu de polices. Utilisez une ou plusieurs de ces vérifications, proportionnellement au risque:

1. **Vérifiez le marquage CE sur le composant.** Si le composant est lui-même un produit CRA et que le fournisseur a démontré la conformité, le marquage CE est sur le composant. Cela atteste du travail CRA propre au fournisseur.
2. **Vérifiez l’historique des mises à jour de sécurité.** Un composant qui livre régulièrement des mises à jour de sécurité est un meilleur risque qu’un composant resté silencieux pendant des années. Cherchez une cadence de release et un historique récent d’avis de sécurité.
3. **Vérifiez le composant contre les bases de vulnérabilités.** La base de vulnérabilités européenne et les bases CVE publiques vous disent ce qui est connu sur le composant. Un CVE connu sans correctif est un signal d’alerte.
4. **Effectuez des tests de sécurité supplémentaires.** Lorsque ce qui précède ne suffit pas, testez le composant dans votre contexte d’intégration: analyse statique, analyse dynamique, fuzzing ou revue de sécurité ciblée.

Pour les composants intégrés avant que leur propre fournisseur ne soit pleinement soumis au CRA (donc sans marquage CE encore disponible), utilisez les trois autres vérifications à la place. L’obligation de diligence raisonnable ne se met pas en pause sous prétexte que la chaîne d’approvisionnement rattrape encore son retard.

Preuves à conserver

La documentation technique doit montrer votre diligence, pas seulement l’affirmer. Conservez:

- Une liste des composants tiers présents dans le produit, traçable par version, incluant les composants open source. La SBOM est l’endroit naturel.
- La documentation de sécurité fournisseur que vous avez examinée: politiques de sécurité, programmes de divulgation des vulnérabilités, engagements de période de support.
- Les rapports de tests d’intégration qui montrent que le composant se comporte de façon sûre dans votre produit.
- Les clauses de sécurité dans les contrats ou SLA avec les fournisseurs commerciaux: délais de notification de vulnérabilités, engagements de période de support, règles d’escalade.
- Un enregistrement des mesures d’atténuation au niveau produit que vous avez ajoutées lorsque la diligence sur le composant a révélé des limites: sandboxing, permissions restreintes, validation des entrées, segmentation réseau.

Quand vous trouvez une vulnérabilité dans un composant

Si votre diligence ou votre surveillance après mise sur le marché identifie une vulnérabilité dans un composant, vous devez faire deux choses. D’abord, notifier la personne ou l’entité qui maintient le composant. Si le composant est open source, c’est le projet amont. Ensuite, traiter et remédier à la vulnérabilité dans votre produit dans les mêmes délais que pour toute autre vulnérabilité que vous découvrez. Si vous avez développé un correctif, partagez le code ou la documentation avec le mainteneur, dans un format lisible par machine lorsque cela s’applique.

Le CRA ne vous autorise pas à attendre que le mainteneur du composant agisse pour protéger vos propres utilisateurs. Le calendrier de traitement des vulnérabilités de votre produit court indépendamment de celui du projet amont.

Les 13 exigences de sécurité produit

Chaque produit comportant des éléments numériques doit respecter treize exigences de sécurité de référence lors de sa mise sur le marché et continuer à les respecter pendant toute la période de support. Elles constituent le plancher de ce que signifie la cybersécurité en termes de produit sous le CRA.

Les treize exigences sont:

- Aucune vulnérabilité exploitable connue au moment de la mise sur le marché
- Configuration sécurisée par défaut à la sortie
- Mises à jour de sécurité, y compris mises à jour automatiques avec possibilité de refus
- Protection contre les accès non autorisés
- Confidentialité des données stockées, transmises et traitées
- Intégrité des données, du micrologiciel et de la configuration
- Minimisation des données
- Disponibilité et résilience, y compris contre les attaques par déni de service
- Absence d'incidence négative sur d'autres dispositifs ou réseaux connectés
- Surface d'attaque limitée, y compris pour les interfaces externes
- Réduction de l'impact des incidents par des mesures d'atténuation de l'exploitation
- Journalisation de l'activité pertinente pour la sécurité, avec possibilité de refus par l'utilisateur
- Suppression sécurisée et permanente des données et portabilité

Chaque exigence est détaillée plus loin dans le guide, avec ce qu'elle signifie en pratique et les preuves à conserver.

Les 8 exigences de traitement des vulnérabilités

Les fabricants doivent aussi disposer de processus de traitement des vulnérabilités pendant toute la période de support du produit:

1. Identifier et documenter les vulnérabilités (inclut la nomenclature logicielle, SBOM)
2. Gérer les risques et fournir les mises à jour de sécurité dans les délais
3. Effectuer des tests de sécurité réguliers
4. Informer sur les mises à jour de sécurité et la divulgation des vulnérabilités
5. Mettre en place une politique de divulgation coordonnée des vulnérabilités (CVD)
6. Prévoir un contact pour le partage et le signalement des vulnérabilités
7. Distribuer les mises à jour par des mécanismes sécurisés
8. Fournir gratuitement les mises à jour de sécurité, accompagnées de messages d'avis

Délais de signalement au titre de l'article 14

Ces obligations s'appliquent à partir du **11 septembre 2026**. Elles concernent les fabricants de produits comportant des éléments numériques entrant dans le champ du CRA, y compris les produits mis sur le marché avant le **11 décembre 2027**. Les microentreprises et petites entreprises ne sont pas généralement exemptées du signalement. L'allègement des amendes pour les petites entreprises est limité: il ne concerne que le premier délai d'**alerte précoce de 24 heures**.

Le CRA distingue trois niveaux de statut pour les vulnérabilités:

- **Vulnérabilité:** toute faiblesse susceptible d'être exploitée
- **Vulnérabilité exploitable:** faiblesse exploitable dans des conditions réelles
- **Vulnérabilité activement exploitée:** vulnérabilité dont l'utilisation dans une attaque a été confirmée

Quand le compteur démarre

Vous n'êtes pas sur le compteur à l'instant où un signal arrive. Le compteur démarre une fois que vous avez effectué une évaluation initiale et obtenu un degré raisonnable de certitude qu'une vulnérabilité de votre produit est activement exploitée, ou qu'un incident grave a compromis la sécurité de votre produit. L'accent est mis sur la promptitude de l'évaluation initiale, pas sur l'attente de la clôture de l'enquête complète. Si un client, un chercheur, une autorité ou un autre tiers porte un problème potentiel à votre attention, évaluez-le sans délai et démarrez le compteur dès que cette évaluation vous donne la certitude raisonnable.

Lorsque vous détectez une **vulnérabilité activement exploitée**, le calendrier de signalement suivant s'applique:

Délai	Ce qui est requis	Où signaler
Dans les 24 heures	Alerte précoce d'exploitation active	ENISA via le CSIRT national
Dans les 72 heures	Notification de vulnérabilité: produit concerné, nature générale de l'exploitation et de la vulnérabilité, mesures d'atténuation, mesures correctives que les utilisateurs peuvent prendre et marquage de sensibilité le cas échéant	ENISA via le CSIRT national
Au plus tard 14 jours après la mise à disposition d'une mesure corrective ou d'atténuation	Rapport final: description de la vulnérabilité, gravité, impact, informations disponibles sur les acteurs malveillants et détails de la mise à jour de sécurité ou des autres mesures correctives	ENISA via le CSIRT national

Lorsque vous détectez un **incident grave** ayant une incidence sur la sécurité du produit, le calendrier de signalement suivant s'applique:

Délai	Ce qui est requis	Où signaler
Dans les 24 heures	Alerte précoce indiquant notamment si l'incident est soupçonné d'être causé par des actes illicites ou malveillants	ENISA via le CSIRT national
Dans les 72 heures	Notification d'incident: nature de l'incident, première évaluation, mesures d'atténuation, mesures correctives que les utilisateurs peuvent prendre et marquage de sensibilité le cas échéant	ENISA via le CSIRT national
Dans le mois suivant la notification d'incident à 72 heures	Rapport final: description détaillée de l'incident, gravité, impact, menace probable ou cause profonde, et mesures d'atténuation appliquées ou en cours	ENISA via le CSIRT national

Les notifications s'enrichissent au fil de l'enquête

Les remontées à 24 heures, 72 heures et 14 jours (ou un mois) sont des étapes d'une même notification, pas des dépôts séparés. Chaque étape ajoute l'information qui n'était pas encore disponible à la précédente. Le CSIRT désigné comme coordinateur peut aussi demander une mise à jour intermédiaire à tout moment. Vous n'avez pas à répéter l'information déjà fournie.

Les signalements sont déposés via la **plateforme de signalement unique du CRA**, puis acheminés par l'équipe nationale de réponse aux incidents de sécurité informatique (CSIRT) de l'État membre principal du fabricant, avec un accès simultané pour l'ENISA.

Informer vos utilisateurs

Après en avoir eu connaissance, vous devez informer les utilisateurs touchés par la vulnérabilité ou l'incident, et le cas échéant tous les utilisateurs, de toute mesure de réduction du risque et de toute mesure corrective qu'ils peuvent déployer. Ce n'est pas la même chose qu'une divulgation publique. Le devoir consiste à faire parvenir l'information aux utilisateurs qui en ont besoin pour se protéger, proportionnellement au risque. Pour les produits utilisés dans des environnements sensibles ou essentiels, limitez les détails techniques aux clients concernés tant que la vulnérabilité n'est pas atténuée; un détail public prématuré peut faciliter l'exploitation.

Une fois la vulnérabilité corrigée ou atténuée, une divulgation plus large peut devenir appropriée pour aider les utilisateurs à vérifier que leurs produits ne sont plus touchés et pour sensibiliser plus largement. Gardez le niveau de détail et le calendrier proportionnés au risque résiduel. Si vous n'informez pas les utilisateurs en temps utile, le CSIRT peut intervenir et fournir lui-même l'information lorsqu'il l'estime proportionné et nécessaire.

Vulnérabilité activement exploitée	
24 heures	alerte précoce
72 heures	notification de vulnérabilité
14 jours après la mesure corrective	rapport final

Incident grave	
24 heures	alerte précoce
72 heures	notification d’incident
un mois après la notification à 72 heures	rapport final

Mesures correctives quand un produit n’est pas conforme

Si vous savez, ou avez des raisons de croire, qu’un produit que vous avez mis sur le marché, ou l’un de vos processus, n’est pas conforme aux exigences essentielles de cybersécurité du CRA, vous devez agir immédiatement. Le devoir court depuis la mise sur le marché et pour toute la période de support.

Les trois options

1. **Mettre en conformité.** Corriger le produit ou le processus. Pour les produits logiciels, il s’agit habituellement d’une mise à jour de sécurité ou d’un changement de processus. Appliquez le correctif aux versions prises en charge.
2. **Retirer.** Cesser la mise à disposition du produit sur le marché. Le rappeler de votre chaîne d’approvisionnement et de tout revendeur, intégrateur ou détaillant qui en détient des stocks.
3. **Rappeler.** Récupérer le produit auprès des utilisateurs qui l’ont déjà. À utiliser lorsque le risque cyber pour les utilisateurs est significatif et qu’une correction ou un retrait ne suffit pas.

Le choix est proportionné au risque, pas une séquence figée. Une vulnérabilité corrigeable avec un correctif disponible appelle habituellement *mettre en conformité*. Un produit qui ne peut pas être corrigé en toute sécurité sur le terrain appelle habituellement *retirer* et, lorsqu’il est en usage actif avec un risque significatif, *rappeler*.

Ce que vous devez aussi faire

- **Notifier au titre de l’article 14** lorsque la non-conformité est une vulnérabilité activement exploitée ou un incident grave. Le calendrier de signalement est exposé ci-dessus.
- **Informer les utilisateurs** de la non-conformité et de toute mesure corrective qu’ils peuvent appliquer eux-mêmes. Voir *Informer vos utilisateurs* ci-dessus pour les règles de proportionnalité.
- **Coopérer** avec toute demande motivée d’une autorité de surveillance du marché, y compris fournir la documentation technique dans une langue qu’elle peut lire.
- **Préserver les preuves.** Conserver les enregistrements qui montrent ce que vous avez trouvé, quand vous l’avez trouvé, ce que vous avez fait et comment vous avez communiqué avec les utilisateurs et les autorités. La documentation technique et la déclaration UE de conformité doivent rester disponibles pendant au moins 10 ans après la mise sur le marché, ou pendant toute la période de support si cette durée est plus longue.

Exigences de documentation produit

La documentation doit être conservée pendant au moins 10 ans après la mise sur le marché du produit, ou pendant la période de support si celle-ci est plus longue. Au niveau de synthèse, la documentation technique requiert huit familles de preuves:

1. Description générale du produit
2. Détails de conception, de développement et de production (y compris la SBOM)
3. Évaluation des risques de cybersécurité
4. Détermination de la période de support
5. Normes harmonisées et spécifications appliquées
6. Rapports d’essai
7. Déclaration UE de conformité
8. SBOM complète (sur demande des autorités de surveillance du marché)

Checklist de la voie d’évaluation de la conformité

Utilisez le tableau de classification ci-dessus pour identifier la voie. Conservez ensuite la décision de route dans la documentation technique avec les normes, spécifications, schéma de certification ou preuves d’organisme notifié utilisés pour la justifier.

Un exemple concret. La même structure par niveaux s'applique à tout produit comportant des éléments numériques, pas seulement aux caméras de sécurité.

Les exigences de sécurité produit

a. Aucune vulnérabilité exploitable connue au moment de la mise sur le marché

Ne mettez pas sur le marché un produit qui contient des vulnérabilités exploitables connues du public et encore non traitées. Une vulnérabilité connue peut venir d'une base publique, d'un avis fournisseur, d'un signalement client ou de votre propre suivi interne.

Pour satisfaire à cette exigence:

- Vérifiez les bases de vulnérabilités, y compris Common Vulnerabilities and Exposures, CVE, avant chaque version
- Utilisez des tests statiques et dynamiques de sécurité applicative (SAST/DAST) dans votre pipeline de build
- Analysez les dépendances pour tous les composants tiers et open source
- Documentez votre décision d'acceptation du risque ou d'atténuation pour chaque problème identifié

b. Configuration sécurisée par défaut

Le produit doit être sûr dans son état par défaut. Désactivez les services inutiles, évitez les identifiants par défaut faibles et limitez tout mode de mise en service non sécurisé dans le temps et dans son périmètre. L'obligation de configuration sécurisée par défaut peut être adaptée pour des produits sur mesure fournis à des utilisateurs professionnels par accord écrit, à condition de conserver la possibilité de réinitialiser le produit dans son état initial.

Pour satisfaire à cette exigence:

- Désactivez les ports d'accès à distance et les interfaces de débogage dans les builds par défaut
- Imposez des mécanismes d'authentification solides par défaut
- Réservez les fonctions d'administration aux seuls utilisateurs autorisés
- Mettez en place une réinitialisation d'usine sécurisée qui restaure tous les paramètres et le micrologiciel dans un état sécurisé connu, tout en supprimant les données utilisateur

c. Mises à jour de sécurité, y compris mises à jour automatiques avec possibilité de refus

Le produit a besoin d'un mécanisme de correction capable de traiter les problèmes de sécurité après le déploiement. Lorsque les mises à jour automatiques sont adaptées, activez-les par défaut et donnez aux utilisateurs un moyen clair de les reporter ou de les refuser.

Pour satisfaire à cette exigence:

- Mettez en place une signature cryptographique et une vérification d'intégrité pour les paquets de mise à jour
- Prévoyez une prévention du retour arrière et une journalisation des événements de mise à jour
- Créez des systèmes de notification qui alertent les utilisateurs des mises à jour en attente
- Permettez aux utilisateurs de reporter ou de désactiver les mises à jour automatiques via une interface de configuration claire

d. Protection contre les accès non autorisés

Les contrôles d'accès doivent protéger les interfaces locales comme les interfaces distantes. L'objectif est d'empêcher les utilisateurs non autorisés d'accéder aux fonctions, aux données, à la configuration ou aux surfaces d'administration.

Pour satisfaire à cette exigence:

- Imposez des politiques de complexité des mots de passe et des identifiants solides par défaut
- Mettez en place l'authentification multifacteur (MFA) lorsque le contexte le justifie
- Appliquez un contrôle d'accès fondé sur les rôles (RBAC) et une gestion de l'expiration des sessions
- Journalisez les tentatives d'accès infructueuses, utilisez la détection d'anomalies pour signaler les activités non autorisées et faites remonter ces événements pour examen et signalement

e. Confidentialité des données stockées, transmises et traitées

Les données sensibles doivent être protégées au repos, en transit et pendant leur traitement.

Pour satisfaire à cette exigence:

- Utilisez des algorithmes de chiffrement normalisés, par exemple AES-256 pour les données au repos et TLS pour les données en transit
- Appliquez des pratiques sécurisées de gestion des clés
- Séparez les données confidentielles des composants système non critiques
- Conservez des journaux d'audit pour tous les événements d'accès aux données

f. Intégrité des données, du micrologiciel et de la configuration

Cette exigence couvre le système lui-même, c'est-à-dire le micrologiciel, le logiciel et les fichiers de configuration, ainsi que les données qu'il traite, comme les mesures, les commandes de contrôle et les saisies utilisateur.

Pour satisfaire à cette exigence:

- Mettez en place un démarrage sécurisé et un micrologiciel signé afin que seul du code de confiance soit exécuté
- Utilisez une vérification à l'exécution pour détecter et signaler les tentatives d'altération
- Appliquez le hachage cryptographique et les signatures numériques pour protéger l'intégrité des données
- Créez une infrastructure capable de générer, distribuer et vérifier des clés cryptographiques entre systèmes ou entre organisations

g. Minimisation des données

Collectez et traitez uniquement les données nécessaires à la finalité prévue du produit. Cela vaut pour les données à caractère personnel comme pour les données techniques.

Pour satisfaire à cette exigence:

- Réalisez des analyses d'impact relatives à la protection des données ou des exercices de protection des données dès la conception afin d'identifier les flux de données inutiles
- Supprimez ou rendez facultatives la télémétrie, les diagnostics ou les collectes de données en arrière-plan qui ne sont pas utilisés
- Mettez en place des paramètres configurables de collecte des données afin que la collecte étendue puisse être activée ou désactivée selon le contexte

h. Disponibilité et résilience, y compris contre les attaques par déni de service

Pendant un incident ou une attaque, les fonctions clés du produit doivent rester disponibles ou se dégrader de manière contrôlée.

Pour satisfaire à cette exigence:

- Mettez en place des disjoncteurs logiciels, des logiques de nouvelle tentative, des mécanismes de repli et des minuteries de surveillance
- Appliquez des limites de ressources pour éviter leur épuisement
- Utilisez la limitation de débit et la validation des entrées pour vous protéger contre les scénarios de déni de service
- Appliquez un filtrage au niveau réseau pour bloquer les tentatives de surcharge

i. Absence d’incidence négative sur d’autres dispositifs ou réseaux connectés

Le produit ne doit pas perturber les autres systèmes du même environnement. Il doit avoir un comportement prévisible et éviter une consommation excessive des ressources partagées.

Pour satisfaire à cette exigence:

- Mettez en place une gestion du trafic et limitez l’usage des diffusions broadcast ou multicast
- Assurez la conformité aux spécifications des protocoles de communication
- Utilisez l’autosurveillance pour détecter et prévenir les comportements perturbateurs, comme l’inondation réseau ou l’épuisement des ressources

j. Surface d’attaque limitée, y compris pour les interfaces externes

Réduisez au minimum les points d’entrée et les fonctionnalités exposées. Cela couvre les ports physiques, les interfaces sans fil, les API, les services de débogage et les composants logiciels inutiles.

Pour satisfaire à cette exigence:

- Désactivez les services, ports et interfaces inutilisés dans les builds de production
- Durcissez les paramètres par défaut du système et limitez les privilèges des utilisateurs
- Modularisez les architectures logicielles afin d’isoler les composants les uns des autres
- Appliquez les principes de conception logicielle sécurisée et menez une modélisation des menaces pour identifier et supprimer les expositions inutiles

k. Réduction de l’impact des incidents par des mesures d’atténuation de l’exploitation

Partez du principe que certaines attaques réussiront. La conception du produit doit limiter l’étendue des dommages.

Pour satisfaire à cette exigence:

- Séparez les composants système et exécutez-les dans des environnements isolés au moyen du sandboxing ou de la conteneurisation
- Imposez la séparation des privilèges afin que les fonctions critiques s’exécutent avec les droits minimaux nécessaires
- Concevez le produit de sorte que la compromission d’un composant ne permette pas à un attaquant de prendre le contrôle de l’ensemble du système

l. Journalisation de l’activité pertinente pour la sécurité, avec possibilité de refus par l’utilisateur

Enregistrez l’activité pertinente pour la sécurité, comme les tentatives d’accès et les modifications de données, afin qu’elle puisse être surveillée et auditée. Les utilisateurs doivent disposer d’un mécanisme de refus lorsque le CRA l’exige.

Pour satisfaire à cette exigence:

- Mettez en place une journalisation structurée, par exemple des journaux JSON avec horodatage
- Prévoyez un stockage local des journaux avec rotation et des options de transmission distante des journaux
- Surveillez les événements comme les tentatives de connexion, les changements de configuration et les mises à jour logicielles afin de détecter les anomalies
- Fournissez un mécanisme clair côté utilisateur pour désactiver la journalisation lorsque cela est autorisé

m. Suppression sécurisée et permanente des données et portabilité

Les utilisateurs ont besoin d’un moyen pratique de supprimer définitivement leurs données et leurs paramètres. Lorsque les données peuvent être transférées vers un autre produit ou système, le transfert doit être sécurisé.

Pour satisfaire à cette exigence:

- Mettez en place une fonction d’effacement sécurisé qui écrase les zones de stockage ou supprime les clés par des moyens cryptographiques
- Utilisez des canaux authentifiés et chiffrés pour les transferts liés à la portabilité des données afin d’éviter toute exposition pendant le transfert

Les exigences de traitement des vulnérabilités

1. Identifier et documenter les vulnérabilités

Vous devez savoir quels composants logiciels se trouvent dans le produit et quelles vulnérabilités connues les affectent. Une nomenclature logicielle (SBOM) vous donne cet inventaire lisible par machine.

Pour satisfaire à cette exigence:

- Intégrez la génération de SBOM directement dans votre pipeline CI/CD afin que chaque build produise un inventaire de composants à jour
- Utilisez des formats établis comme CycloneDX, SPDX ou SWID pour l’interopérabilité
- Exécutez des analyses automatisées des vulnérabilités à partir des listes CVE et de bases comme CISA KEV et ENISA EUVD
- Conservez la SBOM dans votre documentation technique pendant toute la période de support et fournissez-la aux autorités de surveillance du marché sur demande

2. Gestion des risques et mises à jour de sécurité dans les délais

Lorsque des vulnérabilités sont découvertes, corrigez-les rapidement et fournissez des mises à jour de sécurité. Lorsque c'est possible, séparez les correctifs de sécurité des mises à jour fonctionnelles afin que les corrections critiques puissent être installées sans attendre.

Pour satisfaire à cette exigence:

- Concevez votre mécanisme de mise à jour afin que les correctifs de sécurité puissent être déployés sans exiger une mise à jour complète du système
- Structurez les logiciels et les micrologiciels afin que les composants critiques puissent être corrigés indépendamment
- Diffusez les mises à jour par des canaux sécurisés avec contrôles d'intégrité
- Conservez les enregistrements des activités de mise à jour pour assurer la traçabilité et démontrer la conformité

3. Tests de sécurité réguliers

Les tests de sécurité ne sont pas un exercice ponctuel. Testez les produits tout au long du cycle de vie, à mesure que les menaces, les dépendances et le comportement du produit évoluent. L'évaluation des risques doit déterminer le type et la fréquence des tests.

Pour satisfaire à cette exigence:

- Réalisez des tests d'intrusion pour simuler des attaques réelles
- Appliquez l'analyse statique et dynamique du code pour identifier les faiblesses de sécurité
- Utilisez le fuzzing pour révéler les défauts de traitement des entrées
- Planifiez et documentez formellement les revues de code de sécurité et les revues d'architecture, en particulier après des changements importants de conception ou de fonctionnalités

4. Réception des signalements, politique CVD et avis

Couvre les devoirs de réception, de divulgation coordonnée et d'avis (points 4, 5 et 6 du résumé ci-dessus), qui en pratique forment un seul flux de travail.

Le CRA nomme trois exigences distinctes pour la communication autour des vulnérabilités: un canal de signalement pour les tiers, une politique de divulgation coordonnée et un avis lors de la livraison d'un correctif. Voici ce que chaque devoir demande.

Réception

Donnez aux personnes qui signalent un canal d'entrée clair et accessible. Publiez un moyen de contact visible pour le signalement des vulnérabilités (adresse e-mail dédiée ou formulaire web). Prenez en charge la communication sécurisée, par exemple en publiant une clé PGP. Le devoir couvre les signalements concernant votre propre produit et les composants tiers qu'il contient.

Triage

Accusez réception de chaque signalement, enregistrez-le dans un système de suivi, attribuez-le pour examen et résolvez-le dans des délais définis. Envoyez des confirmations et des mises à jour de statut à la personne qui signale. Lorsque le problème se situe dans un composant tiers, transmettez-le au mainteneur amont en parallèle de votre propre remédiation.

Politique de divulgation coordonnée des vulnérabilités

Publiez une politique CVD qui pose les attentes pour les personnes qui signalent et pour les partenaires: moyen de contact, délais de réponse attendus, ce sur quoi vous vous engagez, ce que vous leur demandez. Coordonnez la divulgation pour protéger les utilisateurs tout en reconnaissant le rôle de la personne qui signale.

Avis lors d'un correctif

Une fois un correctif disponible, publiez un avis pour le problème résolu. Incluez l'identifiant CVE, les versions du produit concernées, un score de gravité normalisé (par exemple CVSS) et des informations claires et accessibles sur l'action à mener. Rédigez dans une langue accessible aux administrateurs techniques comme aux utilisateurs non techniques.

Divulgation publique différée

Vous ne pouvez différer la divulgation publique que lorsque vous avez une raison dûment justifiée que les risques cyber d'une divulgation immédiate l'emportent sur les bénéfices, et seulement jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif. Documentez le raisonnement.

5. Mécanismes sécurisés de distribution des mises à jour

Le mécanisme de mise à jour doit être fiable et résistant aux altérations. Lorsque les mises à jour automatiques sont techniquement possibles, elles réduisent la durée pendant laquelle les utilisateurs restent exposés.

Pour satisfaire à cette exigence:

- Transmettez les mises à jour par des canaux sécurisés et vérifiez-les au moyen de signatures numériques
- Appliquez les mises à jour d'une manière qui évite les installations incomplètes ou corrompues
- Utilisez des mises à jour différentielles ou modulaires pour réduire les perturbations et livrer plus rapidement les corrections aux systèmes
- Conservez des journaux de mise à jour afin que les utilisateurs ou les administrateurs puissent vérifier l'état des mises à jour

6. Mises à jour de sécurité gratuites avec messages d'avis

Diffusez les mises à jour de sécurité rapidement et sans coût supplémentaire, sauf lorsqu'un accord distinct existe pour des produits professionnels sur mesure. Chaque mise à jour a besoin d'un message d'avis clair qui dit aux utilisateurs ce qui a changé et ce qu'il faut faire.

Pour satisfaire à cette exigence:

- Maintenez un système de distribution capable de notifier les utilisateurs directement ou d'appliquer les mises à jour automatiquement, selon le contexte du produit
- Rédigez les messages d'avis dans une langue compréhensible par les utilisateurs techniques et non techniques
- Incluez les informations de gravité dans les messages d'avis lorsque c'est pertinent
- Dites aux utilisateurs quelle action mener: appliquer la mise à jour, modifier une configuration ou surveiller les symptômes d'une compromission
- Diffusez les mises à jour de sécurité sans retard une fois qu'elles sont disponibles, afin que les utilisateurs ne restent pas exposés alors que le correctif existe déjà
- Publiez les avis via un canal contrôlé par le fabricant et liez-les depuis la page de support du produit

Les devoirs de gratuité et de diffusion sans retard courent pour toute la durée de la période de support déclarée. La dérogation sur mesure ne change que la base commerciale; les messages d'avis s'appliquent quand même.

Contenu de la documentation technique

Documentation technique

La documentation technique est la preuve centrale de conformité au CRA. Elle doit couvrir les mesures de conception, les mesures techniques et les processus utilisés pour répondre aux exigences essentielles de cybersécurité. Elle doit exister **avant la mise sur le marché** et rester à jour pendant toute la **période de support**.

Preuves de documentation technique dans le flux d'ingénierie

Étape 1	**Cadrer et classer**	Finalité du produit, usage prévu, décision de mise sur le marché, classe du produit, voie normative.
Étape 2	**Architecture et risque**	Architecture, connexions de données, conditions d'utilisation, évaluation des risques, mesures de réduction.
Étape 3	**Composants et SBOM**	SBOM lisible par machine, composants tiers, apports fournisseurs, suivi des vulnérabilités.
Étape 4	**Construire, tester, mettre à jour**	Configuration sûre par défaut, durcissement, rapports de test, mécanisme de mise à jour sécurisé, avis aux utilisateurs.
Étape 5	**Release et support**	Instructions destinées aux utilisateurs, déclaration UE, preuves CE, justification du support, enregistrements de mise à jour.

La documentation technique comporte huit éléments requis. Ensemble, ils expliquent **ce qu'est le produit**, **comment il a été construit et testé**, **quels risques ont été pris en compte**, **quelles normes ont été appliquées** et **comment il sera pris en charge** une fois sur le marché. Vous n'avez pas à recopier les intitulés juridiques, mais chaque sujet doit être couvert.

N°	Composant	Contenu attendu
1	Description générale du produit	Finalité prévue et fonctions, versions logicielles pertinentes, photos ou illustrations pour le matériel, informations et instructions destinées aux utilisateurs
2	Détails de conception, de développement et de production	Description de l'architecture (composants et interactions), nomenclature logicielle (SBOM), processus de traitement des vulnérabilités (politique CVD, point de contact, mécanismes de mise à jour sécurisés), processus de production et de surveillance, validation comprise
3	Évaluation des risques de cybersécurité	Analyse documentée des risques produit, explication de l'application de chaque exigence essentielle de cybersécurité au produit, réduction des risques identifiés
4	Détermination de la période de support	Documentation des facteurs utilisés pour fixer la période de support, par exemple les attentes des utilisateurs, les produits comparables et les orientations juridiques
5	Normes harmonisées et spécifications appliquées	Liste des normes harmonisées, spécifications communes ou schémas de certification de l'UE appliqués; indication d'application totale ou partielle; solutions alternatives lorsque les normes ne sont pas appliquées
6	Rapports d'essai	Preuves de conformité pour le produit et pour les processus de traitement des vulnérabilités
7	Déclaration UE de conformité	Copie de la déclaration reliant la documentation technique aux obligations de marquage CE
8	SBOM complète (sur demande)	Les autorités de surveillance du marché peuvent exiger la SBOM complète pour vérifier la conformité

Une documentation technique consolidée peut couvrir le CRA et d'autres législations de l'UE applicables, par exemple la directive sur les équipements radio ou l'ESPR, à condition d'inclure toutes les obligations applicables.

Déclaration UE de conformité

La déclaration UE de conformité est la déclaration formelle du fabricant selon laquelle le produit satisfait aux exigences de cybersécurité applicables du CRA. Chaque déclaration doit comprendre:

- Nom, type et identifiants uniques du produit
- Nom et adresse du fabricant, ou de son mandataire
- Déclaration de responsabilité exclusive du fabricant
- Description du produit assurant sa traçabilité, avec image si utile
- Déclaration explicite de conformité avec la législation de l'Union pertinente
- Références aux normes harmonisées, spécifications ou certifications utilisées
- Détails de tout organisme notifié intervenu, avec son nom, son numéro, la procédure suivie et le numéro de certificat
- Bloc de signature: lieu, date, nom, fonction et signature du signataire

Une fois signée, la déclaration engage juridiquement le fabricant et confirme son entière responsabilité pour la conformité en matière de cybersécurité.

Une déclaration simplifiée peut être utilisée sur l'emballage ou dans les manuels, sous la forme: « Par la présente, [fabricant] déclare que le produit [type/désignation] est conforme au Règlement (UE) 2024/2847. Le texte complet de la déclaration UE de conformité est disponible à l'adresse internet suivante: [adresse internet]. » Cette forme simplifiée maintient la transparence tout en réduisant la charge documentaire. Elle est particulièrement utile pour les petits fabricants ou les portefeuilles comprenant plusieurs produits.

Informations et instructions destinées aux utilisateurs

Les informations et instructions destinées aux utilisateurs sont une condition de mise sur le marché licite. Les fabricants doivent garder les instructions disponibles pendant **au moins 10 ans** ou pendant toute la **période de support**. Les importateurs et les distributeurs doivent vérifier que les instructions existent, sont à jour et sont fournies dans la bonne langue de l'UE avant de mettre le produit sur le marché ou de le fournir.

Les instructions doivent contenir:

- Identité et coordonnées du fabricant
- Point de contact unique pour le signalement des vulnérabilités
- Identification du produit, finalité prévue et contexte d'utilisation sécurisée
- Cyberrisques connus ou raisonnablement prévisibles
- Lien vers la déclaration UE de conformité
- Conditions de support et date claire de fin de support
- Instructions de sécurité étape par étape pour la configuration, les mises à jour, l'utilisation sécurisée, la mise hors service et, le cas échéant, l'intégration et l'accès à la SBOM

Choisir la bonne voie d'évaluation de la conformité

Module A: autoévaluation

Le module A, contrôle interne, permet de certifier vous-même que votre produit respecte les exigences essentielles de cybersécurité. Vous assumez alors l'entière responsabilité de sa conception et de sa production. Cette voie est ouverte aux fabricants de produits par défaut, c'est-à-dire non classés. Elle est aussi ouverte aux produits importants de classe I uniquement lorsque les normes harmonisées, spécifications communes ou schémas européens de certification de cybersécurité pertinents sont disponibles et appliqués comme l'exigent les règles de route du CRA.

Avec le module A, vous devez:

- Préparer une documentation technique complète
- Détailler la conception du produit, les processus de production, les mécanismes de cybersécurité et les procédures de traitement des vulnérabilités
- Maintenir une responsabilité continue pour la conformité pendant tout le cycle de vie du produit
- Mettre en place un plan de mises à jour de sécurité et de gestion des vulnérabilités pendant la durée d'exploitation du produit
- Conserver les enregistrements disponibles pendant au moins 10 ans

Modules B et C: évaluation centrée sur le produit

Les modules B et C s'appliquent lorsqu'une vérification par un tiers est exigée pour un type de produit précis. Ils s'appliquent aux produits importants de classe I lorsque le fabricant n'a pas appliqué, n'a appliqué qu'en partie ou ne peut pas appliquer les normes harmonisées, spécifications communes ou schémas de certification pertinents. Pour les produits importants de classe II, le fabricant doit utiliser le module B+C, le module H ou un schéma européen de certification de cybersécurité applicable avec un niveau d'assurance au moins « substantiel ».

Module B, examen UE de type: un organisme notifié examine un échantillon représentatif du produit et la documentation technique associée. Il vérifie la conformité à toutes les exigences essentielles de cybersécurité et délivre un certificat d'examen UE de type lorsque la conception du produit répond aux critères du CRA.

Module C, conformité au type et contrôle de la production: le fabricant veille à ce que toutes les unités produites soient conformes au type approuvé au titre du module B. Le fabricant appose le marquage CE, établit la déclaration UE de conformité et conserve les enregistrements pendant au moins 10 ans. Ensemble, les modules B et C démontrent qu'un modèle de produit précis est techniquement conforme et que chaque lot de production reste cohérent avec la conception approuvée.

Module H: évaluation centrée sur le processus, assurance complète de la qualité

Le module H, assurance complète de la qualité, porte sur l'ensemble du système qualité interne du fabricant plutôt que sur les essais d'un produit isolé. Il est disponible pour les produits importants de classe I et de classe II. Les produits critiques empruntent la voie de certification lorsque les conditions pertinentes sont réunies; lorsque ces conditions ne sont pas réunies, ils empruntent les mêmes voies que celles disponibles pour les produits importants de classe II.

Avec le module H, vous devez:

- Établir et maintenir un système qualité couvrant la conception, le développement, la production, les essais et le traitement des vulnérabilités pour toute la catégorie de produits
- Soumettre le système qualité à un organisme notifié pour évaluation et approbation
- Accepter une surveillance continue par l'organisme notifié, avec audits, inspections et revues de processus, afin de vérifier la conformité dans le temps

Une fois le système approuvé, vous pouvez établir des déclarations de conformité pour tous les produits fabriqués sous ce système qualité, sans répéter l'examen de l'organisme notifié pour chaque type de produit.

La distinction clé entre les voies est simple:

- Modules B+C: l'accent porte sur le produit. Un type de produit représentatif est testé et certifié.
- Module H: l'accent porte sur le processus. L'ensemble du système de conception et de production du fabricant est certifié et surveillé.

VOIES D'ÉVALUATION DE LA CONFORMITÉ

A

module

Autoévaluation

Produits par défaut et produits importants de classe I lorsque les normes harmonisées, spécifications communes ou schémas de certification sont pleinement appliqués. Le fabricant assume l'entière responsabilité de la conception et de la production.

B+C

module

Type et production

Requis pour les produits importants de classe I sans normes applicables, et comme partie de la voie des produits importants de classe II. Un organisme notifié examine un type représentatif; le fabricant veille à ce que chaque unité produite soit conforme.

H

module

Assurance complète de la qualité

Disponible pour les produits importants de classe I et II. L'organisme notifié approuve et audite de bout en bout le système de conception, de développement, de production, d'essai et de traitement des vulnérabilités du fabricant.

Flux de mise sur le marché

Le CRA dans le paysage réglementaire européen

Le CRA ne fonctionne pas seul. La question pour un fabricant est pratique: où mon travail CRA me fait-il gagner du temps sous un autre régime de l'UE, et où ai-je encore des obligations séparées à mener en parallèle?

Où votre travail CRA peut être réutilisé

- **Systèmes d'IA à haut risque (AI Act, Règlement 2024/1689).** Si votre produit est un système d'IA à haut risque entrant dans le champ du CRA, satisfaire aux exigences essentielles de cybersécurité du CRA est réputé satisfaire aux exigences de cybersécurité de l'AI Act, dans la mesure couverte par votre déclaration UE de conformité. La procédure d'évaluation de la conformité passe en règle générale par le régime de l'AI Act, avec une exception pour les produits CRA importants et critiques. L'évaluation des risques de cybersécurité CRA doit prendre en compte les risques propres à l'IA, comme l'empoisonnement de données et les attaques adverses.
- **Évaluation des risques consolidée avec d'autres textes de l'Union.** Le CRA permet expressément que l'évaluation des risques de cybersécurité s'intègre dans une évaluation des risques plus large exigée par un autre acte de l'Union, lorsque le produit relève des deux régimes. Un seul artefact d'évaluation, deux usages réglementaires.
- **Une seule documentation technique pour plusieurs régimes.** Comme déjà noté dans la section sur la documentation technique, une documentation consolidée peut couvrir le CRA avec d'autres législations de l'Union applicables, à condition que les obligations de chaque régime soient traitées. Utile lorsque le même produit a déjà besoin de documentation au titre de la directive sur les équipements radio, du règlement ESPR ou d'une autre législation produit.
- **Définitions partagées de remise à neuf, maintenance et réparation.** Le CRA reprend ces définitions du règlement ESPR. Lorsque vous analysez si une opération de service compte comme une modification substantielle, les définitions ESPR sont la référence, et non un terme propre au CRA.

Où des obligations séparées subsistent

- **AI Act, tout le reste.** La cybersécurité n'est qu'une tranche de l'AI Act. La classification des risques, la transparence, la gouvernance des jeux de données, la supervision humaine, la surveillance après mise sur le marché du comportement de l'IA et le reste sont des devoirs de l'AI Act que le CRA ne traite pas. Une cybersécurité conforme au CRA ne vaut pas présomption de conformité globale à l'AI Act.
- **ESPR et contenu du passeport numérique de produit.** Les exigences ESPR sur l'efficacité énergétique, la durabilité, le scoring de réparabilité et le contenu durabilité du passeport numérique de produit ne sont pas du périmètre CRA. La trace de preuves CRA peut accompagner le travail ESPR, mais elle ne le remplace pas.
- **Droits d'accès aux données IoT du Data Act.** Le Data Act donne aux utilisateurs des droits contractuels d'accès, de partage et de transfert des données générées par leurs produits connectés. Le CRA couvre la sécurité de ces données; il ne fixe pas le régime des droits d'accès. Obligation différente, preuves différentes.
- **Responsabilité des produits défectueux.** La directive 2024/2853 maintient une responsabilité stricte du fabricant. L'absence de mises à jour de sécurité après mise sur le marché peut la déclencher. Contrats, assurance et playbooks d'incident doivent couvrir ce risque au-delà de la conformité CRA.

Comment CRA Evidence vous aide

CRA Evidence transforme les obligations du Cyber Resilience Act de l'UE en preuves produit vérifiables, en combinant une plateforme de conformité et du conseil technique.

Plateforme

Un seul endroit pour gérer les preuves qui soutiennent la préparation CRA:

- **Inventaire SBOM et composants:** enregistrements CycloneDX, SPDX et HBOM par version et release produit
- **Automatisation des preuves CI/CD:** workflows CLI et API pour scans, dépôts SBOM, portes de release et traces d'audit
- **SBOM signée et provenance:** preuves versionnées, attestations fournisseurs et dossiers de diligence
- **Opérations de vulnérabilités:** CISA KEV, EPSS, VEX, surveillance, triage et workflows de signalement
- **Documentation technique et preuves CE:** déclarations UE, historique de conservation et passeports de conformité produit liés par QR code

Conseil technique

Un accompagnement ciblé pour traduire les obligations CRA en décisions d'ingénierie sur le produit, l'architecture, la release et les fournisseurs.

- **Sprint de préparation technique:** revue des écarts sur les exigences essentielles, recommandations d'architecture et plan d'action priorisé
- **Pilotage du programme CRA:** modèle de responsabilité, suivi des obligations, jalons de preuves et maintenance de la documentation technique
- **Plan de réponse aux autorités et aux incidents:** workflows de signalement, playbooks de demandes, communications utilisateurs et préparation de dossiers de preuves
- **Alignement réglementaire:** relier les preuves CRA au Data Act, à l'ESPR, à l'AI Act, à RED et aux exigences sectorielles
- **Ateliers techniques:** sessions à distance ou sur site avec produit, ingénierie, sécurité, conformité et fournisseurs

Indépendant des outils: CRA Evidence s'intègre avec CycloneDX, SPDX, Grype, Trivy, les pipelines CI/CD et les gestionnaires de tickets.

Un premier pas pratique

Choisissez une famille de produits. Cartographiez le responsable, la décision de périmètre, la SBOM, le workflow de vulnérabilités, les écarts de documentation technique et les preuves de release. L'équipe obtient ainsi une base CRA concrète sans transformer la conformité en projet séparé.

Découvrez ce que CRA Evidence couvre pour votre produit sur craevidence.com/fr. Les tarifs et options de plan sont disponibles sur craevidence.com/fr/tarifs.