EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

REPÈRES POUR LA CONCEPTION ET L'EXPLOITATION

Cyber Resilience Act

Des produits sûrs.
Une exploitation fiable.



Illustration IA · scène fictive

Règlement (UE) 2024/2847 · Mise à jour du 19 novembre 2026

La sécurité fait partie du produit dès sa conception.

Le podcast commence par une question : accepterions-nous une voiture sans freins ?

01 **Conception**
Connaître les risques

→

02 **Livraison**
Sécuriser les réglages par défaut

→

03 **Utilisation**
Traiter les vulnérabilités

→

04 **Support**
Fournir les mises à jour

Le CRA intègre la cybersécurité tout au long du cycle de vie du produit.

Podcast 00:00–01:45 · CRA art. 1, 13

L’EXEMPLE DU PODCAST

Smart Baby 3000

Une petite caméra.
Un espace très privé.

- Caméra dans la chambre d’enfant
- Application sur le smartphone
- Service cloud du fabricant



Illustration IA · scène fictive

Podcast 01:49–03:54 · produit fictif

La connexion de données est le premier point à vérifier.

Directe ou indirecte. Avec un appareil ou un réseau.

Produit numérique

Matériel ou logiciel

→

Connexion de données ?

Prévue ou prévisible

→

Vérifier le CRA

Champ d’application et exceptions

Même hors ligne : des données numériques échangées avec un badge ou un programmateur peuvent suffire.

Une serrure purement mécanique ne relève pas de cette notion de produit numérique.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Le cloud peut faire partie du produit.

Trois critères rattachent le traitement distant au produit.

EXEMPLE : SMART BABY 3000 ET SON CLOUD ASSOCIÉ



1. **Traitement de données à distance**
2. **Sans lui, au moins une fonction du produit ne fonctionne plus.**
3. **Logiciel développé par le fabricant ou sous sa responsabilité.**

CRA art. 3, points 1–2 · Lignes directrices, points 184, 189, 202

La sécurité dès la première utilisation.

L’évaluation des risques détermine la mise en œuvre concrète.

01	**Protéger l’accès**	Empêcher les accès non autorisés.
02	**Limiter les données**	Traiter uniquement les données nécessaires à la finalité.
03	**Traiter les failles**	Fournir le produit sans vulnérabilité exploitable connue.
04	**Terminer en sécurité**	Effacer simplement et sûrement les données et paramètres.

CRA annexe I, partie I · Podcast 03:55–05:11

La chaîne d’approvisionnement participe à la sécurité.

Même lorsque le fabricant est établi hors de l’UE.

Fabricant
Évaluer et démontrer

→

Importateur
Vérifier les preuves en amont

→

Distributeur
Vérifier le marquage et agir

Sa propre marque ou une modification substantielle peuvent conférer le rôle de fabricant.

CRA art. 13, 19–22 · Podcast 05:54–06:55

Le code libre reste dans le périmètre de responsabilité.

Le babyphone utilise une bibliothèque de caméra open source.

Développement libre

Hors activité commerciale

→

Produit commercial

Le fabricant vérifie les composants intégrés

Pas d'obligations générales de fabricant pour le développement libre.

La responsabilité du produit final incombe au fabricant.

Intendant de logiciels libres

Des obligations propres et adaptées au soutien systématique.

CRA art. 13, par. 5–6, art. 24 · Considérants 18–19

Le support suit l’utilisation prévisible.

Le fabricant justifie la durée pour le produit concerné.

Règle et exception

Au moins cinq ans.
Si l’utilisation est plus courte,
la durée prévue s’applique.

Utilisation prolongée

Un cycle de vie plus long
exige un support
prolongé en conséquence.

Fin précise du support

Au moins le mois et l’année.
Clairement indiqués
à l’acheteur lors de l’achat.

L’engagement doit correspondre au cycle de vie prévu du produit.

CRA art. 13, § 8–9, 19 · Lignes directrices C/2026/6013, points 125–135

Une mise à jour de sécurité doit parvenir en sécurité.

En principe, sans délai et gratuitement.

01

Fournir

Corriger la vulnérabilité

→

02

Distribuer

Canal de mise à jour sûr

→

03

Installer

Automatiquement, si applicable

→

04

Continuer l’usage

Maintenir la fonction

Séparer les mises à jour de sécurité et de fonctions lorsque c’est techniquement possible.

CRA annexe I, partie I, point 2 c), partie II, points 2, 7–8

La SBOM permet de localiser le composant vulnérable.

Nomenclature logicielle : lisible par machine, comprenant au moins les dépendances principales.

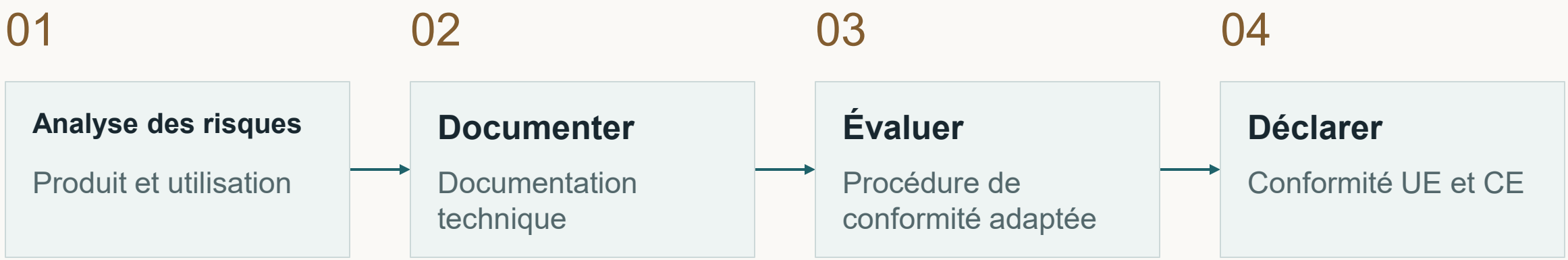


Exploiter les informations sur les composants.

CRA annexe I, partie II, point 1 · Annexe II, point 9

Le marquage CE exige une base traçable.

Il couvrira aussi les exigences CRA applicables.



Le marquage CE ne promet pas une sécurité absolue.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

La catégorie du produit détermine l’évaluation.

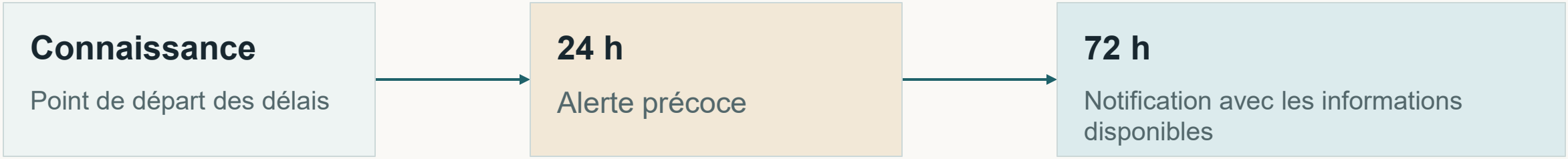
Catégorie	Exemples	Procédure de conformité
Cas général	Absent des annexes III / IV	Le contrôle interne est possible.
Important : classe I	Babyphones, serrures domotiques, lecteurs d’authentification*	Évaluation par un tiers si les références appropriées ne sont pas entièrement appliquées.
Important : classe II	Pare-feu, environnements d’exécution de conteneurs	Évaluation par un tiers ou certification autorisée.
Critique	Passerelles de compteurs intelligents, certains dispositifs de sécurité	Art. 8 ou procédure selon l’art. 32.

***La fonction principale et la description technique précise sont déterminantes.**

CRA art. 7–8, 32 · Annexes III–IV · Règl. (UE) 2025/2392

Notifier sans délai, au plus tard sous 24 heures.

Dès connaissance d’une exploitation active ou d’un incident grave affectant la sécurité du produit.



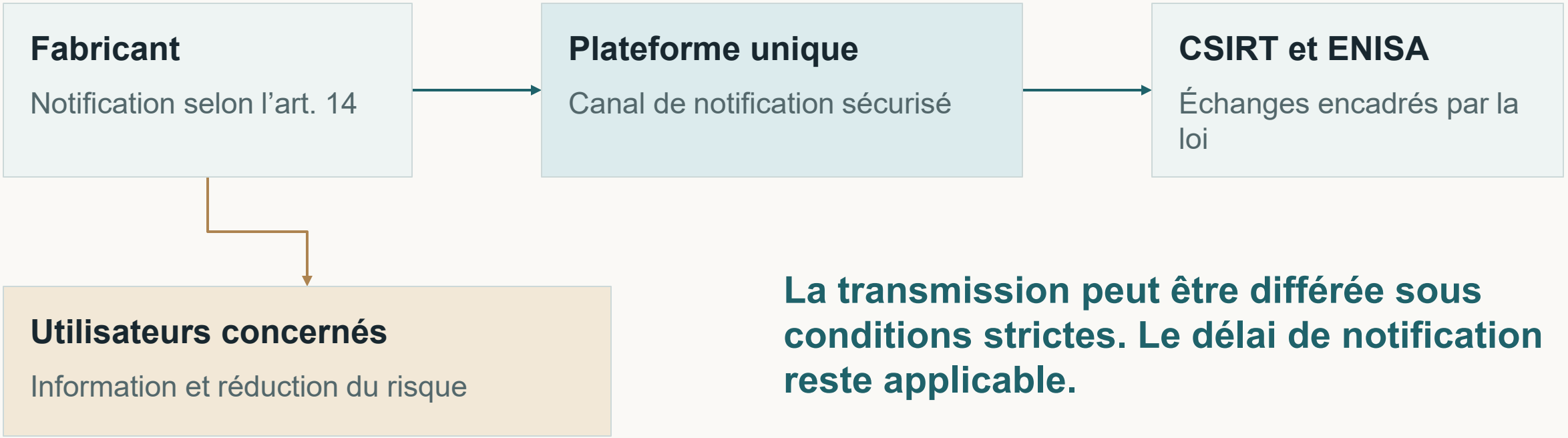
RAPPORT FINAL

Vulnérabilité
Au plus tard 14 jours après la disponibilité d’une correction.

Incident
Dans le mois suivant la notification à 72 h.

CRA art. 14, 16, 71 · Lignes directrices, points 209–218 · Notifications des fabricants depuis le 11.09.2026

Notifier en sécurité. Informer les utilisateurs concernés.



La transmission peut être différée sous conditions strictes. Le délai de notification reste applicable.

CRA art. 14, par. 8, art. 16, 63

Les règles ont des conséquences économiques.

Certains manquements sont assortis de plafonds d’amende élevés.

15 millions €

ou 2,5 % du chiffre d’affaires annuel mondial

Le montant le plus élevé s’applique.

L’accès au marché est aussi concerné.

Corrections
Restriction de la commercialisation
Rappels

CRA art. 54, 58, 64 · Podcast 20:06–21:47

Les notifications s’appliquent déjà. Le reste suivra.

Trois dates illustrent la transition.

10.12.2024

Entrée en vigueur

Intégration au droit de l’UE

11.09.2026

Obligations de notification

L’art. 14 s’applique déjà

11.12.2027

Obligations principales

Exigences produit et conformité

Depuis le 11.06.2026 : dispositions sur la notification des organismes d’évaluation.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

La Commission précise l’application.

Un guide officiel d’interprétation du Cyber Resilience Act existant.

17.11.2026

C/2026/6013

67 exemples pratiques
24 langues officielles de l’UE

Sans force juridique obligatoire

Les lignes directrices expliquent le périmètre, le support, les modifications et les notifications.

Les dates d’application sont maintenues

11.09.2026 Notifications des fabricants
11.12.2027 Application générale

Communication de la Commission, points 6–8 · Actualité mise à jour le 18.11.2026

Produits existants : modification et notification.

La mise sur le marché est déterminante, pas seulement la date d’achat.

Avant le 11.12.2027
Déjà mis sur le marché

→

Dès le 11.12.2027
Modification substantielle ?

→

Obligations principales
Examiner le cas concret

L’art. 14 couvre aussi les anciens produits et la période après le support.
Respecter les obligations de notification dès connaissance d’un événement concerné.

CRA art. 69, § 2–3 · Lignes directrices, points 210, 217

Quand une modification devient-elle substantielle ?

La destination et les effets sur la conformité sont déterminants.

Dans le cadre évalué

La réparation, la configuration et la correction prévues ne sont pas automatiquement substantielles.

Nouvelle fonction ou nouveau risque

Ouverture à distance, connexion cloud ou gestion externe des clés : évaluer les effets au cas par cas.

Un possible rôle de fabricant

Modifier substantiellement, puis mettre sur le marché : examiner les obligations du fabricant selon l’art. 22.

CRA art. 3, point 30, art. 21–22 · Lignes directrices, section 4 · Obligations principales dès le 11.12.2027

Sécurité du produit et responsabilité se complètent.

CRA Exigences produit, conformité et traitement des vulnérabilités

Droit à réparation

Défaut du produit + **Dommage réparable** + **Lien de causalité**

L’absence de mise à jour n’entraîne pas automatiquement l’indemnisation de tout dommage informatique.

CRA considérant 31 · Directive (UE) 2024/2853

La sécurité numérique contribue à déterminer qui peut entrer.

Qui obtient l’accès ?

Les lecteurs vérifient les identités.
Les contrôleurs libèrent les portes.
Le logiciel gère les droits.



Illustration IA · scène fictive

Exemple EIWTC · Annexe III, classe I, point 1 · Règl. (UE) 2025/2392

Une mise à jour doit fonctionner dans le bâtiment.

Exemple illustratif : une vulnérabilité touche le logiciel de contrôle d’accès.

01 **Vérifier le parc installé**

Identifier les versions concernées

02 **Coordonner la correction**

Préciser le risque et la fenêtre de maintenance

03 **Mettre à jour et contrôler**

Tester les portes et le redémarrage



Illustration IA · scène fictive

Exemple illustratif d’exploitation EIWTC

Informations du fabricant pour une exploitation sûre

Information du fabricant	Utilité pour la conception et l’exploitation
Produit, version et périmètre du système	Identifier composants et dépendances cloud
Fin et étendue du support	Planifier le support restant et la migration
Mises à jour de sécurité et leur distribution	Définir responsabilités et créneaux de maintenance
Conformité et procédure d’évaluation	Identifier les justificatifs applicables au produit
Contact de sécurité et alertes	Évaluer l’exposition et coordonner les mesures

Des informations produit claires favorisent une exploitation fiable.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

D’abord la fonction. Ensuite la technique.



L’usage et les objectifs de protection déterminent les exigences relatives aux produits, aux interfaces et à l’exploitation.

Les preuves et les mises à jour font partie de la conception.

Illustration IA · scène fictive

L’étape suivante : une procédure de travail claire.

Une personne responsable centralise les points en suspens et les échéances.

Recenser le parc

Versions, cloud, fin du support

→

Clarifier les responsabilités

Contact fabricant et processus de mise à jour

→

Tester les procédures

Alerte, décision, mise à jour

Les informations produit deviennent ainsi des décisions étayées.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting



La sécurité devient un élément de la qualité du produit.

De la conception au support.
Traçable pour les fabricants et les exploitants.

La sécurité dans le produit. La clarté dans la conception.

Illustration IA · scène fictive

eiwtc.lu/fr/security/

Sources et mise en contexte

Base juridique	Règlement (UE) 2024/2847 : exigences et dates d’application.
Catégories de produits	Règl. (UE) 2025/2392 : descriptions techniques contraignantes.
Aide à l’interprétation	C/2026/6013 du 17.11.2026 : lignes directrices non contraignantes.
Actualité de la Commission	67 exemples pratiques, 24 langues officielles. Mise à jour le 18.11.2026.
Responsabilité du fait des produits	Directive (UE) 2024/2853 : régime distinct de responsabilité.

Podcast comme trame narrative et autres sources dans les notes. État au 19.11.2026.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting