CONFIRMATE

**CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act**

# Guide de conformité à la législation sur la cyberrésilience (CRA) pour les PME

**Date de publication: 30/10/2025**
**Statut: final**
**Version: 1.0**

Le projet financé dans le cadre de la convention de subvention **n° 101190193** bénéficie du soutien du Centre européen de compétences en matière de cybersécurité. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement ceux de l'Union européenne ou du Centre européen de compétences en matière de cybersécurité. Ni l'Union européenne ni l'autorité octroyant la subvention ne peuvent en être tenus responsables.

## Liste des modifications

| Version | Date | Description | Auteur(s) |
|---|---|---|---|
| 0.1 | 07.04.2025 | Première ébauche | CYEN |
| 0.2 | 27.06.2025 | Texte supplémentaire ajouté | CYEN |
| 0,3 | 06.08.2025 | Première version finalisée, texte supplémentaire / conseils ajoutés | CYEN |
| 0.4 | 03.09.2025 | Version révisée par les partenaires du projet, à distribuer pour examen externe par des pairs | CYEN |
| 0.5 | 24.10.2025 | Version révisée tenant compte de l'évaluation par les pairs | CYEN |
| 1.0 | 30.10.2025 | Version finale publiée | CYEN |

## Contributeurs

| Rôle | Nom du contributeur | Nom de l'entité - Bénéficiaire |
|---|---|---|
| Responsable des livrables | Iva Tasheva, Steve Purser, Krasimir Simonski, Azeez Kamal | CYEN |
| Contributeur | Christine Demeter, Gabriel Niculescu | DNSC |
| Contributeur | Andreas Binder | AISEC Fraunhofer |
| Évaluation par les pairs | Harald Fischer | Balena |
| Évaluation par les pairs | Argyro Chatzopoulou et al. | Projet CURIUM |
| Évaluation par les pairs | Romain Muguet et al. | Red Alert Labs |
| Révision de la traduction française | Kayle Giroud | Women4Cyber Belgium |

**Avertissement:** les outils CONFIRMATE, y compris le guide de conformité CRA, sont destinés uniquement à des fins d'information générale et éducative. Ils fournissent une introduction de haut niveau au processus de conformité CRA et ne sont pas adaptés aux circonstances d'une organisation, d'un produit ou d'une situation spécifique. Le contenu reflète l'expérience et les opinions individuelles des experts, auteurs et pairs évaluateurs qui y ont contribué, et peut ne pas être exhaustif, mis à jour en permanence ou applicable à tous les cas.

Aucun élément de ces outils ne constitue un conseil juridique, réglementaire ou professionnel. CONFIRMATE décline toute responsabilité quant aux mesures prises sur la base des informations fournies. Les utilisateurs restent seuls responsables du respect des lois, réglementations et normes applicables.

Les exigences réglementaires évoluant, nous vous recommandons vivement de consulter un professionnel du droit ou un expert en réglementation qualifié pour obtenir des conseils spécifiques à votre situation.

# Sommaire

# 1. Glossaire: acronymes, termes et abréviations

Les termes suivants apparaissent dans le texte des présentes lignes directrices:

| | |
|---|---|
| **Représentant autorisé** | Personne physique ou morale établie dans l'Union qui a reçu un mandat écrit d'un fabricant pour agir en son nom dans le cadre de tâches spécifiques. |
| **Marquage CE** | Marquage par lequel un fabricant indique qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant sont conformes aux exigences essentielles en matière de cybersécurité énoncées à l'annexe I du CRA et dans d'autres actes législatifs d'harmonisation de l'Union applicables prévoyant son apposition. |
| **Déclaration de conformité (DoC)** | Document juridique, rédigé par le fabricant, attestant qu'un produit satisfait aux exigences essentielles applicables du CRA. Il doit être mis à la disposition des autorités compétentes ainsi que des utilisateurs dans le cadre de la documentation technique. |
| **Évaluation de la conformité** | Processus visant à vérifier si les exigences essentielles en matière de cybersécurité énoncées à l'annexe I du CRA ont été respectées. |
| **Norme harmonisée** | Spécification technique élaborée par un organisme européen de normalisation (OEN) à la demande de la Commission européenne afin de faciliter la mise en œuvre de la législation européenne. Il s'agit de normes européennes officiellement reconnues qui confèrent une présomption de conformité avec des exigences légales spécifiques de la législation de l'UE. |
| **Incident** | Événement qui affecte négativement ou est susceptible d'affecter négativement la capacité d'un produit comportant des éléments numériques à protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou des fonctions. |
| **Distributeur** | Une personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit comportant des éléments numériques à disposition sur le marché de l'Union sans altérer ses propriétés. |
| **Importateur** | Une personne physique ou morale établie dans l'Union qui met sur le marché un produit comportant des éléments numériques, lequel porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union |
| **Fabricant** | Une personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux, monétisé ou gratuit. |
| **Nouveau cadre législatif (NLF)** | Réglementations qui fixent des exigences structurées et harmonisées concernant la manière dont la conformité des produits est évaluée avant leur mise sur le marché de l'UE. |
| **Produit comportant des éléments numériques (PDE)** | Un produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels mis sur le marché séparément. |
| **PME:** | La catégorie des petites et moyennes entreprises (PME) comprend les entreprises qui emploient moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros et/ou dont le total du bilan annuel n'excède pas 43 millions |

| | |
|---|---|
| | d'euros. Dans la catégorie des PME, une petite entreprise est définie comme une entreprise qui emploie moins de 50 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel n'excède pas 10 millions d'euros, tandis que pour une microentreprise, ces seuils sont inférieurs à 10 employés et à 2 millions d'euros. |
| **Nomenclature logicielle** | Document officiel contenant les détails et les relations de la chaîne d'approvisionnement des composants inclus dans les éléments logiciels d'un produit comportant des éléments numériques. |
| **période d'assistance** | Période pendant laquelle un fabricant est tenu de veiller à ce que les vulnérabilités d'un produit comportant des éléments numériques soient traitées efficacement et conformément aux exigences essentielles en matière de cybersécurité énoncées dans la partie II de l'annexe I du CRA. |
| **Vulnérabilité** | Faiblesse, vulnérabilité ou défaut d'un produit comportant des éléments numériques pouvant être exploités par une cybermenace.<br>- Une vulnérabilité exploitable est une vulnérabilité qui peut être utilisée efficacement par un adversaire en conditions de fonctionnement effectives.<br>- Une vulnérabilité activement exploitée est une vulnérabilité pour laquelle il existe des preuves fiables qu'elle a été exploitée par un acteur malveillant dans un système sans l'autorisation du propriétaire du système. |

# 2. Introduction

## À propos du projet Confirmate

CONFIRMATE est un projet innovant cofinancé par l'Union européenne (UE) et le Centre européen de compétences et de réseau en matière de cybersécurité (ECCC), conçu pour aider les PME manufacturières à rester en avance sur l'évolution des réglementations en matière de cybersécurité. En rationalisant la conformité avec la loi européenne sur la cyber-résilience (CRA), CONFIRMATE fournit des logiciels ouverts (open source), des formations pratiques et des méthodes standardisées qui rendent la conformité au CRA plus accessible, plus efficace et plus rentable.

Le nom du projet signifie « Conformity Assessment, Metrics, and Automation for the Cyber Resilience Act » (Évaluation de la conformité, mesures et automatisation pour la législation sur la cyberrésilience). Basé sur le logiciel ouvert Clouditor, CONFIRMATE fournit une décomposition automatisée des services et des vues de conformité, des résultats d'évaluation clairs, une méthodologie robuste de tests de pénétration, des modules de formation multilingues sur la cybersécurité[1] et un guide complet de conformité au CRA (le présent document). Voir les documents publiés à l'annexe E.

Réunissant des partenaires de premier plan, notamment CYEN, Fraunhofer AISEC, ITKAM et la Direction nationale roumaine de la cybersécurité (DNSC), CONFIRMATE fournit aux PME les connaissances et les ressources nécessaires pour répondre en toute confiance aux exigences essentielles en matière de cybersécurité et garantir la résilience de leurs produits numériques. Les autres projets européens actuellement en cours et la conformité des PME avec le CRA sont répertoriés à l'annexe F.

## 2.1 Objectif et public cible du présent guide

Le guide de conformité est une ressource gratuite dédiée conçue pour aider les PME manufacturières de l'UE à comprendre les exigences essentielles en matière de cybersécurité de la législation européenne sur la cyberrésilience (CRA)[2]. Le guide est spécialement conçu pour donner un aperçu des exigences de conformité et aider les PME à décomposer leurs attentes en étapes concrètes et faciles à comprendre. Il est adapté aux besoins et aux défis spécifiques des PME du secteur manufacturier. Rédigé à l'origine en anglais, il sera traduit en quatre langues européennes: allemand, français, italien et roumain, touchant ainsi plus de 60 % de la population de l'UE.

[1] Voir la vidéo d'introduction sur YouTube: https://youtu.be/QeIjDeVvbL0
[2] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202402847

Le guide fournit un aperçu complet de la législation européenne sur la cyberrésilience (CRA), couvrant des aspects clés tels que les rôles et responsabilités, les exigences essentielles en matière de cybersécurité, les procédures d'évaluation de la conformité et la notification des incidents avec les obligations post-commercialisation. Il propose également des mesures pratiques pour aider les PME à mettre en œuvre le CRA, ainsi que des suggestions d'outils, de modèles et de ressources pour renforcer leur posture de sécurité et soutenir l'amélioration continue.

**Objectif:** L'objectif principal du guide est de donner aux PME les moyens d'agir en leur fournissant les connaissances et les outils nécessaires pour se conformer au CRA et maintenir cette conformité. Il vise à réduire la complexité des exigences réglementaires, afin de permettre aux entreprises de remplir leurs obligations en toute confiance tout en se concentrant sur leurs activités principales. En outre, le guide sert à souligner l'importance pour les PME de gérer les risques liés à la cybersécurité, de protéger leur réputation et de garantir la sécurité et la fiabilité de leurs produits numériques. En fin de compte, il permettra aux PME d'acquérir les connaissances et les mesures pratiques nécessaires pour améliorer la cyber-résilience de leurs produits.

**Public cible:** le guide est spécialement conçu pour les PME européennes qui développent, produisent ou commercialisent des produits comportant des éléments numériques. Ces entreprises ne disposent souvent pas des ressources et de l'expertise étendues des grandes organisations, ce qui rend la conformité à des réglementations complexes telles que le CRA particulièrement difficile. En se concentrant sur les PME, le guide cherche à répondre à leurs défis spécifiques, tels que les budgets limités, les équipes réduites et le besoin de solutions pratiques et évolutives.

Bien que les obligations du CRA tiennent compte des défis auxquels sont confrontées les PME, elles sont les mêmes pour les PME que pour les grandes entreprises, à quelques exceptions près, à savoir les modèles de documentation simplifiés (documentation technique et déclaration de conformité) et les orientations prioritaires, qui sont également abordées dans le présent guide.

En ce sens, sauf mention contraire explicite, toutes les orientations présentées dans le présent document s'appliquent aux PME.

En résumé, ce guide de conformité est une ressource précieuse pour les PME manufacturières de l'UE, leur offrant clarté, confiance et outils pratiques pour naviguer dans les exigences de la législation européenne sur la cyberrésilience. Il favorise non seulement la conformité, mais aussi une culture de maturité en matière de cybersécurité, aidant les PME à protéger leurs produits, leurs clients et leur réputation dans un marché de plus en plus numérisé.

## 2.2 Questions et réponses clés sur la loi sur la cyber-résilience (CRA)

**Q1. Qu'est-ce que la législation sur la cyberrésilience (CRA) ?**
Le CRA est un règlement européen visant à garantir la cybersécurité des produits comportant des éléments numériques (PDE), tels que les appareils connectés et les logiciels. Elle introduit des exigences de sécurité obligatoires tout au long du cycle de vie du produit, de la conception au service après-vente.

Bien que largement reconnue, la définition du CRA des « produits comportant des éléments numériques » mérite d'être précisée, car elle détermine si les produits des PME doivent répondre à ses exigences.

Par définition, les PDE comprennent les produits logiciels ou matériels et leurs solutions de traitement de données à distance. En ce qui concerne les logiciels, il n'y a pas lieu d'interprétation, car ils sont facilement reconnaissables en tant que code de programmation. Mais en ce qui concerne le matériel, il est précisé qu'il doit être capable de traiter, stocker ou transmettre des données numériques et être commercialisé séparément, même s'il fait partie d'une chaîne d'approvisionnement en tant que composant d'un autre produit.

**Q2. Le CRA s'applique-t-il à nos produits ?**
Si votre entreprise fabrique ou commercialise des produits comportant des éléments numériques sur le marché de l'UE (par exemple, des appareils IoT, des logiciels intégrés, des machines industrielles avec interfaces réseau), alors oui, le CRA s'applique probablement. Des exemptions existent pour les produits déjà réglementés, tels que les dispositifs médicaux, les véhicules légers, l'aviation, les produits conçus exclusivement pour l'armée, la sécurité nationale et l'utilisation d'informations classifiées.

**Q3. Suis-je concerné par le CRA ?**
Si vous êtes fabricant, importateur, distributeur ou intendants d'un PDE mis sur le marché de l'UE, vous avez des obligations spécifiques en vertu du CRA.

**Q4. Quelles sont les principales obligations des fabricants ?**

- Réaliser et documenter **des évaluations des risques liés à la cybersécurité,** y compris les risques liés à la chaîne d'approvisionnement.
- Garantir des pratiques **de sécurité dès la conception** et **par défaut.**
- Mettre en œuvre des processus **de gestion des vulnérabilités**, y compris le signalement et la tolérance zéro pour les vulnérabilités activement exploitées et connues du public.
- Fournir **des mises à jour de sécurité** pendant le cycle de vie du produit.
- **Entreprendre des procédures d'évaluation de la conformité** adaptées à la catégorie de produits.
- Créer et tenir à jour **la documentation technique, les fichiers d'information destinés aux utilisateurs, la déclaration de conformité UE** (dans les langues du pays de commercialisation).

**Q5. Quand le CRA entrera-t-il en vigueur ?**
Le CRA sera mise en œuvre de manière progressive. Les dates clés pour les fabricants sont les suivantes:

- ➔ **11 septembre 2026,** date à laquelle les obligations de déclaration des vulnérabilités et des incidents de sécurité deviendront applicables.
- ➔ **11 décembre 2027,** date à laquelle le CRA sera pleinement applicable.

**Q6. Quelles sont les sanctions en cas de non-conformité ?**
La non-conformité peut entraîner des amendes pouvant atteindre **15 millions d'euros ou 2,5 % du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu. Le retrait du marché et l'atteinte à la réputation constituent également des risques.

**Q7. Que doivent faire les fabricants dès maintenant ?**

- **Cartographiez votre portefeuille de produits** pour déterminer l'applicabilité du CRA.
- Commencez à **évaluer les risques liés à la cybersécurité et à analyser les lacunes.**
- Mettez à jour **la conception, la documentation technique et les politiques d'assistance.**
- **Envisagez de vous aligner sur les normes de cybersécurité** (par exemple, EUCC, ISO/IEC 2700x, ETSI EN 303 645).

## 2.3 Contexte et objectif de la législation sur la cyberrésilience (CRA)

La législation sur la cyberrésilience s'inscrit dans la continuité de la première législation horizontale sur la sécurité des produits, la directive sur les équipements radioélectriques (RED)[3], qui a introduit les premières exigences en matière de cybersécurité pour une large gamme de produits vendus dans l'UE, en particulier pour les appareils connectés à Internet et ceux qui traitent des données à caractère personnel, qui deviendront obligatoires à partir du 1er août 2025. Ces exigences, énoncées à l'article 3, paragraphe 3, de la RED, visent à renforcer la sécurité et la sûreté des utilisateurs et des réseaux en traitant de la protection des réseaux, de la confidentialité des données et de la prévention de la fraude. le CRA est également lié à la directive sur la responsabilité du fait des produits défectueux (PLD)[4], qui traite de la responsabilité pour les produits défectueux, y compris ceux comportant des éléments numériques.

Les objectifs de la législation européenne sur la cyberrésilience (CRA) sont *« d'améliorer les normes de cybersécurité des produits contenant une composante numérique, en exigeant des fabricants et des détaillants qu'ils garantissent la cybersécurité tout au long du cycle de vie de leurs produits (...) La législation sur la cyberrésilience traite du niveau insuffisant de cybersécurité de nombreux produits et du manque de mises à jour de sécurité en temps utile pour les produits et les logiciels »*[5]. Elle vise à établir un niveau élevé et cohérent de cybersécurité en fixant des exigences claires pour les fabricants, les développeurs, les

[3] Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014L0053
[4] Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/fr
[5] Commission européenne (2025) Loi sur la cyber-résilience, consultée le 14 avril 2025 ici: https://digital-strategy.ec.europa.eu/fr/policies/cyber-resilience-act

importateurs et les distributeurs, tout en favorisant la transparence en matière de risques liés à la cybersécurité.

*« La législation sur la cyberrésilience garantira que:*

- *que les produits filaires et sans fil qui sont connectés à l'internet et les logiciels mis sur le marché de l'UE soient plus sûrs;*
- *que les fabricants restent responsables de la cybersécurité d'un produit tout au long de son cycle de vie*
- *et que les consommateurs disposent d'informations suffisantes sur la cybersécurité des produits qu'ils achètent et utilisent. »*[6]

*Elle « introduit des exigences obligatoires en matière de cybersécurité pour les fabricants, qui couvrent la planification, la conception, le développement et la maintenance de ces produits »*[7]. Ces obligations doivent être respectées à chaque étape de la chaîne de valeur. Elle met l'accent sur les principes de sécurité dès la conception, les évaluations de conformité et le signalement des incidents cybernétiques et des vulnérabilités activement exploitées, afin de créer un écosystème numérique plus sûr.

L'impact du CRA ne se limite pas à un secteur spécifique, ce qui lui permet d'avoir un impact plus large et d'établir un niveau minimum de sécurité acceptable pour les produits vendus dans l'ensemble de l'UE. Elle contribue ainsi à une meilleure cyber-résilience. Pour les PME en particulier, le CRA fournit un cadre permettant d'intégrer la cybersécurité dans leurs processus, les aidant ainsi à être compétitives sur un marché sûr et fiable.

Le lien et la relation entre le CRA et d'autres réglementations européennes pertinentes en matière de sûreté et de sécurité sont décrits dans l'annexe G « Relation avec d'autres législations européennes ».

## 2.4 Champ d'application et mise en œuvre de la législation sur la cyberrésilience (CRA)

Champ d'application: le CRA s'applique à tous les produits à composants numériques mis sur le marché de l'UE (c'est-à-dire vendus séparément, et non dans le cadre d'un service), « *connectées de manière directe ou indirecte à un autre appareil ou réseau, à l'exception de certaines exclusions spécifiques telles que certains logiciels ou services open source déjà couverts par les règles existantes, comme c'est le cas pour les dispositifs médicaux, l'aviation et les voitures. Les produits porteront le marquage CE pour indiquer qu'ils sont conformes aux exigences du CRA ».*[8] Les obligations couvrent l'ensemble du cycle de vie du produit, depuis sa conception, sa fabrication et sa maintenance jusqu'à son élimination.

[6] Commission européenne (2025) Loi sur la cyber-résilience - Questions et réponses, consulté le 14 avril 2025 ici: https://ec.europa.eu/commission/presscorner/detail/fr/qanda_22_5375
[7] Commission européenne (2025) Loi sur la cyber-résilience, consultée le 14 avril 2025 ici: https://digital-strategy.ec.europa.eu/fr/policies/cyber-resilience-act
[8] ibid

Il convient de préciser que si un PDE n'est pas connecté directement à un réseau ou à un autre système d'information électronique, il peut néanmoins propager indirectement une menace vers une certaine cible par le biais de fichiers infectés, de clés USB, etc. (considérant 9). Il peut s'agir d'un appareil autonome tel qu'une serrure intelligente, un jouet ou autre (considérant 10).

*« Sur la base du nouveau cadre législatif pour la législation sur les produits dans l'UE, les fabricants seraient soumis à un processus d'évaluation de la conformité afin de démontrer que les exigences spécifiées relatives à un produit ont été respectées. Cela pourrait se faire par le biais d'une auto-évaluation ou d'une évaluation de la conformité par un tiers, en fonction du niveau de risque associé au produit en question. »*[9]

Le CRA classe les produits comportant des éléments numériques en quatre catégories (par défaut, classe I importante, classe II importante, critique). Toutes les catégories de produits doivent mettre en œuvre les mêmes exigences essentielles en matière de cybersécurité (définies par la loi, qui sont examinées dans la section 3 du présent document), mais supposent un niveau de protection adéquat en fonction du risque et doivent suivre différentes procédures d'application (évaluation de la conformité):

- **Les produits par défaut comportant des éléments numériques** représentent environ 90 % de tous les PDE. Ils doivent satisfaire aux exigences essentielles en matière de cybersécurité, ce qu'ils affirment par une auto-évaluation et une déclaration de conformité.
- **Les produits importants comportant des éléments numériques** sont énumérés à l'annexe III et divisés en deux catégories: classe I et classe II**.** Ces produits sont considérés comme remplissant des fonctions essentielles pour la cybersécurité d'autres produits, réseaux ou services et, en ce sens, présentent un risque important. Outre le respect des exigences essentielles en matière de cybersécurité, ils sont soumis à des exigences de vérification plus strictes en matière de cybersécurité avant leur mise sur le marché.
- **Les produits critiques comportant des éléments numériques** sont énumérés à l'annexe IV. Il s'agit d'une liste très limitée de produits considérés comme les plus risqués, qui devront obtenir un certificat européen de cybersécurité d'un niveau d'assurance au moins « substantiel » dans le cadre d'un système européen de certification de la cybersécurité adopté conformément au règlement (UE) 2019/881.

[9] Commission européenne (2025) Loi sur la cyber-résilience, consultée le 14 avril 2025 ici: https://digital-strategy.ec.europa.eu/fr/policies/cyber-resilience-act

# 3. Rôles et responsabilités


Les obligations en matière de CRA visent divers acteurs de la chaîne d'approvisionnement d'un produit, sans distinction de taille ou d'origine, mais en mettant l'accent sur le rôle de la personne morale ou physique par rapport au PDE concerné. Toutefois, des lignes directrices (telles que présentées dans le présent document) et des modèles simplifiés seront publiés afin de permettre notamment aux PME de remplir leurs rôles et responsabilités de manière efficace et efficiente.

Le CRA définit les rôles spécifiques et les responsabilités respectives comme suit:

## 3.1 Fabricants

Le fabricant joue un rôle majeur dans la cybersécurité des produits comportant des éléments numériques, que ce soit au stade de la conception, du développement, de la production ou du support. À ce titre, le fabricant est le principal profil d'entreprise dans le CRA, assumant l'ensemble des responsabilités (c'est-à-dire la mise en œuvre des exigences essentielles en matière de cybersécurité et des procédures d'évaluation de la conformité).

Le CRA définit un fabricant comme *« Une personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux, monétisé ou gratuit* ».

Cette définition implique que toutes les étapes de la vie d'un produit sont réalisées par un seul fabricant qui assume l'entière responsabilité de la cybersécurité du produit. Dans la pratique, comme nous le savons, la chaîne de production est toujours beaucoup plus complexe, impliquant des chaînes d'approvisionnement, des tiers et d'autres acteurs, ce qui n'entraîne toutefois pas de partage des responsabilités. À chaque étape du cycle de vie du produit

correspondent des exigences spécifiques en matière de cybersécurité pour chaque activité, étape et opération individuelle. Les responsabilités du fabricant ne s'arrêtent pas à la mise sur le marché du PDE.

Les obligations des fabricants (voir tableau 1) sont résumées dans les articles 13 et 14 du texte officiel du CRA et sont interprétées dans le présent document.

| Obligation | Activité |
|---|---|
| Mettre en œuvre les exigences essentielles de cybersécurité du CRA | Lorsqu'ils mettent sur le marché un produit comportant des éléments numériques, les fabricants doivent s'assurer qu'il a été conçu, développé et produit conformément aux exigences essentielles de cybersécurité énoncées dans la partie I de l'annexe I. |
| Évaluation régulière des risques | Réaliser et mettre à jour régulièrement des évaluations des risques liés à la cybersécurité pour les produits et la chaîne d'approvisionnement. Tenir compte des résultats de l'évaluation pour la planification, la conception, le développement, la production, la livraison et la maintenance des PDE afin de minimiser les risques liés à la cybersécurité, de prévenir les incidents et d'en minimiser l'impact, notamment en ce qui concerne la santé et la sécurité des utilisateurs. L'évaluation des risques liés à la cybersécurité doit indiquer comment les exigences essentielles en matière de cybersécurité (y compris la gestion des vulnérabilités) sont mises en œuvre. |
| Sécurité dès la conception et par défaut | Veiller à ce que les produits soient conçus de manière sécurisée et soient livrés avec des configurations par défaut sécurisées. |
| Gestion des vulnérabilités | Mettre en œuvre des processus clairs avec une tolérance zéro pour les vulnérabilités connues du public et activement exploitées. |
| Mises à jour de sécurité | Fournir des mises à jour de sécurité gratuites et en temps opportun tout au long du cycle de vie du produit, indépendamment des mises à jour des fonctionnalités. |
| Conformité et marquage CE | Effectuer une évaluation de la conformité (auto-évaluation ou évaluation par un tiers) et apposer le marquage CE. |
| Documentation et DoC | Créer et tenir à jour la documentation technique et la déclaration de conformité UE (dans les langues du marché cible). |
| Signalement | Signaler activement les vulnérabilités exploitées et les incidents importants ayant un impact sur la sécurité, simultanément au CSIRT et à l'ENISA, via la plateforme de signalement unique (UE), comme indiqué ci-dessous: |
| | - Alerte précoce: dans les 24 heures |
| | - Rapport initial: dans les 72 heures |
| | - Rapport final: dans les 14 jours (vulnérabilité) / 1 mois (incident) |
| | Informer les utilisateurs concernés du produit contenant des éléments numériques. |

*Tableau 1: Obligations des fabricants*

La section 3 du présent document détaille les exigences essentielles en matière de cybersécurité énoncées dans l'annexe I de la loi, résumées ici comme suit:

- Réaliser et documenter **une évaluation des risques liés à la cybersécurité,** y compris les risques liés à la chaîne d'approvisionnement.
- Garantir des pratiques **de sécurité dès la conception** et **par défaut.**
- Mettre en œuvre des processus **de gestion des vulnérabilités**, y compris le signalement et la tolérance zéro pour les vulnérabilités activement exploitées et connues du public.
- Fournir **des mises à jour de sécurité** pendant le cycle de vie du produit.
- Entreprendre des procédures **d'évaluation de la conformité** adaptées à la catégorie de produits.
- Créer et tenir à jour **la documentation technique, les fichiers d'information destinés aux utilisateurs, la déclaration de conformité UE** (dans les langues du pays où le produit est commercialisé, y compris les informations requises. Un modèle simplifié de déclaration de conformité est à la disposition des PME à l'annexe VI du CRA et à l'annexe I du présent document).

Les PME reconnues comme fabricants doivent être informées que le CRA introduit l'obligation de signaler les vulnérabilités activement exploitées et les incidents graves dès que le fabricant en a connaissance. Un incident est considéré comme grave lorsqu'il est causé par ou peut introduire un code malveillant ou affecte la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou de fonctions sensibles ou importantes du PDE.

Bien que les micro et petites entreprises ne soient pas soumises à des amendes administratives si elles ne respectent pas le délai d'alerte précoce de 24 heures, il leur est recommandé de le faire dès que possible. Les obligations de notification sont examinées en détail au chapitre 6.

## 3.2 Intendants de logiciels ouverts

Le rôle des intendants de logiciels ouverts est très courant dans les PME, car le concept de code libre et ouvert trouve son origine dans les PME et la société des indépendants et relève davantage d'une communauté que d'un objectif commercial. Par conséquent, il est difficile de définir les obligations des fournisseurs de logiciels ouverts lorsqu'ils font partie de la chaîne d'approvisionnement pour la fabrication d'un PDE.

La définition du intendant de logiciels ouverts qualifie leur PDE de logiciel libre et ouvert, en attendant qu'il soit systématiquement pris en charge de manière durable et en soulignant qu'il est destiné à des activités commerciales.
Les fournisseurs de logiciels ouverts ne sont pas classés comme fabricants par le CRA, sauf s'ils exercent des activités commerciales avec des logiciels ouverts, telles que la facturation du logiciel lui-même, la fourniture d'une assistance technique moyennant des frais ou la monétisation par le biais de services connexes. Cela est clairement indiqué dans le considérant

18 du règlement CRA: « *seuls les logiciels libres et ouverts mis à disposition sur le marché, donc fournis pour être distribués ou utilisés dans le cadre d'une activité commerciale, devraient relever du champ d'application du présent règlement* ».

Bien que le CRA ne prévoit pas d'amendes administratives pour les intendants de logiciels ouverts, ceux-ci sont soumis à un régime réglementaire allégé, dont les obligations sont énumérées à l'article 24 du CRA et résumées dans le tableau 2 ci-dessous.

| Obligation | Activité |
|---|---|
| Politique en matière de cybersécurité et de gestion des vulnérabilités | Mettre en place et documenter une politique de cybersécurité afin de favoriser le développement d'un PDE sécurisé ainsi qu'une gestion efficace des vulnérabilités par les développeurs de ce produit, en encourageant le signalement volontaire des vulnérabilités et le partage d'informations concernant les vulnérabilités découvertes au sein de la communauté open source. |
| Coopération | Coopérer avec les autorités de surveillance du marché, à leur demande, en vue d'atténuer les risques liés à la cybersécurité que présentent les logiciels libres et open source. |
| Notification | Informer les autorités compétentes et les utilisateurs concernés (ou tous les utilisateurs) des vulnérabilités activement exploitées (si elles sont impliquées dans le développement du produit) et des incidents graves ayant un impact sur la sécurité des produits comportant des éléments numériques, dans la mesure où ils affectent les réseaux et les systèmes d'information fournis par les intendants de logiciels open source pour le développement de ces produits. |
| | Communiquer, si nécessaire, toute mesure d'atténuation des risques et corrective que les utilisateurs peuvent mettre en œuvre pour atténuer l'impact de cette vulnérabilité ou de cet incident. |

*Tableau 2: Obligations des intendants de logiciels ouverts*

Les articles 21 et 22 du CRA traitent des cas dans lesquels les obligations des fabricants s'appliquent à d'autres parties. Ces lignes directrices sont donc également pertinentes dans ces cas.

## 3.3 Importateurs et distributeurs

Les PME peuvent également être des importateurs ou des distributeurs de produits comportant des éléments numériques. Pour ces rôles, le CRA fixe des obligations spécifiques dans les articles 19 et 20 respectivement, telles que le respect des exigences essentielles en matière de cybersécurité évoquées au chapitre 3 ci-dessous et la prise en charge de certaines des obligations du fabricant.

Un importateur est défini comme *« une personne physique ou morale établie dans l'Union qui met sur le marché un produit comportant des éléments numériques, lequel porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union ».*

Un distributeur, quant à lui, est *« une personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit comportant des éléments numériques à disposition sur le marché de l'Union sans altérer ses propriétés ».*

Bien que ces lignes directrices aient été élaborées à l'intention des fabricants, elles peuvent être utilement utilisées par les importateurs et les distributeurs, à condition que les différences entre les obligations applicables à ces groupes soient bien comprises.

Les principales obligations des importateurs (article 19) et des distributeurs (article 20) sont résumées dans le tableau 3 ci-dessous:

| Obligation | Activité | Acteur | |
|---|---|---|---|
| | | Importateur | Distributeur |
| Ne mettre sur le marché de l'UE que des produits conformes au CRA | Ne pas mettre sur le marché de l'UE des produits non conformes au CRA; | ✅ | ✅ |
| Traitez les produits non conformes | S'assurer de corriger ou de retirer/rappeler tout produit soupçonné de ne pas être conforme au CRA ou à son annexe I - Exigences essentielles en matière de cybersécurité; | ✅ | ✅ |
| Signaler | Informer le fabricant et les autorités de surveillance du marché, sans retard injustifié, en cas de risque important pour la cybersécurité posé par le PDE; | ✅ | ✅ |
| | Informer le fabricant de toute vulnérabilité du produit; | ✅ | ✅ |
| | Informer les autorités de surveillance du marché et, dans la mesure du possible, les utilisateurs, si le fabricant de ce produit a cessé ses activités et n'est donc pas en mesure de se conformer aux obligations prévues par le CRA. | ✅ | ✅ |
| S'identifier | *Indiquer ses coordonnées sur la PDE ou sur la documentation accompagnant le produit, dans une langue facilement compréhensible par les utilisateurs et les autorités de surveillance du marché.* | ✅ | |
| Conserver les documents de conformité | *Conserver une copie de la déclaration de conformité UE à la disposition des autorités de surveillance du marché pendant au moins 10 ans.* | ✅ | |
| S'assurer | Avant de mettre un produit sur le marché s'assurer: | | |
| | *(a) que les procédures d'évaluation de la conformité appropriées ont été effectuées*[10]*;* | ✅ | |
| | *(b) le fabricant a établi la documentation technique;* | ✅ | |
| | *(c) le PDE porte le marquage CE et est accompagné de la déclaration de conformité UE, ainsi que des informations et instructions destinées à l'utilisateur, telles que prévues à l'annexe II, dans une langue facilement compréhensible par les utilisateurs et les autorités de surveillance du marché*[11]*;* | ✅ | |
| | *(d) le PDE ou sa documentation comporte l'identification du produit, du* | ✅ | |

[10] *Comme prévu à l'article 32*
[11] *Comme prévu à l'article 30 et à l'article 13, paragraphe 20, en conséquence*

| | | | |
|---|---|---|---|
| | *fabricant et de la période d'assistance*[12]. | | |
| | *(e) le fabricant et l'importateur ont respecté leurs obligations et ont fourni tous les documents nécessaires au distributeur.* | | ✅ |

*Tableau 3: Obligations des importateurs et des distributeurs*

En outre, l'article 21 identifie les circonstances dans lesquelles les obligations applicables aux fabricants s'appliquent également aux importateurs et aux distributeurs. C'est le cas lorsque l'importateur ou le distributeur met un PDE sur le marché sous son nom ou sa marque commerciale ou apporte une modification substantielle à un PDE déjà mis sur le marché.

## 3.4 Autres personnes physiques ou morales (article 22)

L'article 22 traite du cas où une personne physique ou morale (autre que le fabricant, l'importateur ou le distributeur) apporte une modification substantielle à un PDE et met ce produit à disposition sur le marché. Dans ce cas, l'entité concernée est considérée comme un fabricant.

## 3.5 Mandataires

Un autre rôle dans lequel les PME peuvent être reconnues est celui de mandataire du fabricant. Il s'agit d'un dérivé du rôle du fabricant et il est défini dans un mandat spécial par lequel le fabricant nomme le mandataire. Le mandat peut inclure toutes les obligations du fabricant, à l'exception de celles spécifiées explicitement par le CRA à l'article 18, qui concernent principalement la cybersécurité pendant les phases de conception, de développement et de production. Toutefois, en ce qui concerne les exigences du CRA relatives à la conformité du produit en matière de cybersécurité lorsqu'il est mis sur le marché, le mandataire doit coopérer avec les autorités exerçant un contrôle sur le PDE qu'il représente.

Les fabricants peuvent choisir de désigner un mandataire pour accomplir des tâches en leur nom, en lui délivrant un mandat. Le mandataire est tenu de fournir une copie de ce mandat aux autorités de surveillance du marché si celles-ci le lui demandent.

Lorsque le fabricant choisit cette option, le mandat doit permettre au mandataire d'effectuer au moins les tâches suivantes:

- conserver la déclaration de conformité UE et la documentation technique (voir section 4 des présentes lignes directrices) à la disposition des autorités de surveillance du marché pendant au moins 10 ans après la mise sur le marché du PDE ou pendant la période d'assistance, la plus longue des deux périodes étant retenue;
- sur demande, fournir aux autorités de surveillance du marché toutes les informations et la documentation nécessaires pour démontrer la conformité du PDE;
- coopérer avec les autorités de surveillance du marché.

[12] *Comme prévu à l'article 13, paragraphes 15, 16 et 19*

## 3.6 Organismes d'évaluation de la conformité

Les PME pourraient également assumer le rôle d'organismes d'évaluation de la conformité (OEC), également appelés organismes notifiés dans le cadre du CRA. Il s'agit d'organismes indépendants désignés par les États membres de l'UE et notifiés à la Commission européenne pour effectuer des évaluations de conformité par des tiers. Ils évaluent si certains produits numériques sont conformes aux exigences en matière de cybersécurité avant que le marquage CE puisse être demandé.

Les OEC sont principalement chargés de réaliser des évaluations de conformité conformément aux exigences du CRA (modules B, C et H) et de vérifier la documentation technique correspondante. En cas d'évaluation positive, l'organisme notifié délivre une déclaration de conformité, qui est nécessaire pour obtenir le marquage CE.

En conséquence, les organismes d'évaluation de la conformité doivent être:

- accrédités et désignés conformément aux règles de l'UE[13];
- techniquement compétents en matière de cybersécurité et d'évaluation des produits.

Ils sont soumis à une surveillance nationale et à une coordination au niveau de l'UE.

[13] Système d'information NANDO (New Approach Notified and Designated Organisations) https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

# 4. Exigences essentielles en matière de cybersécurité

## 4.1 Relatives aux propriétés des produits

### 4.1.1 Principes de sécurité dès la conception et de sécurité par défaut

Les exigences du CRA visant à adopter le principe de sécurité dès la conception et par défaut, en y faisant référence à plusieurs reprises dans le texte:

- Le considérant 32 du CRA reconnaît que la « *protection des données dès la conception et par défaut ainsi que la cybersécurité en général sont des éléments clés du règlement (UE) 2016/679* »[14].
- Le considérant 34 stipule que *« lorsqu'il intègre des composants obtenus auprès de tiers à des produits comportant des éléments numériques au cours de la phase de conception et de développement, le fabricant devrait, pour que les produits soient conçus, développés et produits conformément aux exigences essentielles de cybersécurité énoncées dans le présent règlement* »,
- L'article 13, paragraphe 1, qui détaille les obligations des fabricants, exige que *« lorsqu'ils mettent sur le marché un produit comportant des éléments numériques, les fabricants s'assurent que ce produit a été conçu, développé et fabriqué conformément aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I* »
- L'annexe I, qui détaille les exigences essentielles en matière de cybersécurité, stipule que *« (1) les PDE sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques. »*

Pour prouver leur conformité au principe de sécurité dès la conception, les PME peuvent utiliser le plan de gestion des risques pour le développement des produits, qui comprend l'identification des risques, leur analyse et les stratégies d'atténuation pour chaque étape du développement.

Plus précisément, le point (2)b de l'annexe I prévoit une exigence explicite en matière de configuration sécurisée par défaut: *« Les PDE doivent: (b) être mis à disposition sur le marché avec une configuration de sécurité par défaut, sauf accord contraire entre le fabricant et*

14Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)

*l'entreprise utilisatrice en ce qui concerne un produit sur mesure comportant des éléments numériques, y compris la possibilité de réinitialiser le produit à son état d'origine. »*

Ces concepts ne sont pas définis dans le texte et leur signification est supposée aller de soi. Par exemple, l'autorité de régulation allemande, l'Office fédéral allemand de la sécurité informatique (BSI)[15], précise que le principe de sécurité dès la conception signifie que *« les produits connectés doivent être conçus en tenant compte de la cybersécurité, par exemple en veillant à ce que les données stockées ou transmises avec le produit soient cryptées et que la surface d'attaque soit aussi réduite que possible »* et, pour le principe de sécurité par défaut, *« les paramètres par défaut des produits connectés doivent contribuer à renforcer leur sécurité, par exemple en interdisant les mots de passe par défaut faibles, en installant automatiquement les mises à jour de sécurité, etc. ».*

En ce qui concerne les preuves acceptables de conformité au principe de sécurité par défaut, les PME devraient envisager de documenter les règles de configuration sécurisée appliquées et, si le produit est fabriqué sur mesure, de proposer un accord adéquat avec ses utilisateurs professionnels comprenant des clauses pertinentes.

Dans la pratique, l'interprétation de ces exigences doit être fondée sur l'évaluation des risques et sera laissée à la discrétion du fabricant, en fonction de la nature du produit et du contexte dans lequel il sera déployé.

### 4.1.2 Gestion des risques liés à la cybersécurité

L'évaluation des risques liés à la cybersécurité sous-tend l'ensemble de l'approche en matière de cybersécurité définie dans le CRA, en favorisant une approche proactive de la gestion des risques justifiant les mesures de cybersécurité plutôt qu'une approche de conformité[16]. L'évaluation des risques est la pierre angulaire de la sécurité des produits, car elle fournit un moyen systématique d'identifier, d'évaluer et de hiérarchiser les menaces potentielles dès les premières étapes du développement et tout au long du cycle de vie du produit. En mettant continuellement à jour l'évaluation des risques à mesure que le produit évolue, les organisations s'assurent que les mesures de sécurité restent solides et pertinentes, protégeant efficacement à la fois le produit et ses utilisateurs. Ce processus guide non seulement la sélection et la rigueur des contrôles de sécurité, mais sert également de base à toutes les évaluations et décisions de sécurité ultérieures. Le respect des bonnes pratiques établies, telles que celles décrites dans les normes ISO 31000 et ISO 14971, garantit une approche complète et reproductible. En fin de compte, l'évaluation des risques est non seulement essentielle pour créer des produits sécurisés, mais elle est également une condition préalable obligatoire pour se conformer au CRA et à toute autre réglementation européenne en matière de cybersécurité ou de sécurité. En effet, le CRA lui-même utilise des techniques d'évaluation des risques pour définir un certain

[15] BSI - Office fédéral allemand de la sécurité informatique (2025) Loi sur la cyber-résilience, disponible à l'adresse suivante: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html#:~:text=Take%20cybersecurity%20into%20account.not%20have%20to%20be%20published.. consulté le 21 juillet 2025

[16] Il est également fait référence à la gestion des risques dans les considérants 37, 38, 39, 48 et 52 (qui font référence à l'évaluation coordonnée au niveau de l'Union des risques liés à la sécurité des chaînes d'approvisionnement critiques), 53, 55, 58 et 114.

nombre de classes de produits et établir des exigences de sécurité reflétant le niveau de risque associé à chaque classe de produits. Un modèle d'évaluation des risques est disponible à l'annexe B du présent document.

De plus, l'évaluation des risques pour les PDE dans le cadre du CRA est une évaluation spécifique au produit, qui va au-delà des évaluations des risques individuels liés à un projet ou à une organisation. Pour répondre aux exigences du CRA, l'évaluation doit porter spécifiquement sur la sécurité:

- **la sécurité des utilisateurs finaux**, c'est-à-dire les informations et les instructions à fournir à l'utilisateur,
- **évaluer les risques liés à la chaîne d'approvisionnement**, y compris les vulnérabilités identifiées par le biais de la nomenclature logicielle (SBOM), notamment en établissant une nomenclature logicielle dans un format couramment utilisé et lisible par machine couvrant au minimum les dépendances de haut niveau des produits et en tenant compte de la SBOM dans les exigences de gestion des vulnérabilités discutées ci-dessous, et
- **examiner comment le PDE ou ses appareils connectés pourraient avoir un impact sur d'autres** réseaux et produits avec lesquels il interagit, c'est-à-dire les exigences de conception des produits évoquées ci-dessous.

Cette perspective globale garantit que non seulement le produit lui-même, mais aussi son écosystème et ses utilisateurs, sont protégés contre les menaces en constante évolution, et que les contrôles de sécurité sont adaptés aux risques interconnectés du monde réel.

Les références clés dans le texte du CRA sont les suivantes:

- ➔ Les articles 3(37) et 3(38) définissent respectivement les concepts de « risque de cybersécurité » et de « risque de cybersécurité important ».
- ➔ L'article 13 prévoit des exigences explicites sur la manière dont les fabricants doivent gérer les risques afin de garantir un niveau de sécurité approprié pour leurs produits, le paragraphe 13(3) énumérant les éléments qu'il doit inclure, tels que l'analyse des risques basée sur l'usage prévu et l'utilisation raisonnablement prévisible du PDE, les conditions d'utilisation telles que l'environnement opérationnel ou les actifs à protéger, et autres.
- ➔ L'annexe I (point 2) établit un certain nombre d'exigences essentielles en matière de cybersécurité *sur la base de l'évaluation des risques liés à la cybersécurité visée à l'article 13, paragraphe 2.*

### 4.1.3 Objectifs en matière de sécurité

La sécurité des produits est l'un des piliers de la législation sur la cyberrésilience (CRA), qui impose aux organisations de mettre en place des mesures de sécurité robustes tout au long du cycle de vie des produits, de la conception et du développement au déploiement et à la maintenance. Les domaines clés sont les suivants:

- **Gestion des identités et des accès:** veiller à ce que seuls les utilisateurs et les systèmes autorisés puissent accéder aux fonctions et aux données sensibles, afin de réduire le risque d'accès non autorisé et d'utilisation abusive;

- **Journalisation:** mettre en place une journalisation complète pour surveiller l'activité, détecter les anomalies et faciliter les enquêtes judiciaires en cas d'incident;
- **Sécurité et minimisation des données:** protéger les données à chaque étape et ne collecter que ce qui est strictement nécessaire, ce qui limite l'exposition et réduit les risques de non-conformité;
- **Sauvegarde et effacement sécurisé:** sauvegarder régulièrement les données critiques et garantir leur suppression sécurisée lorsqu'elles ne sont plus nécessaires, afin d'éviter toute perte de données et toute récupération non autorisée;
- **Chiffrement:** protéger les informations en transit et au repos, rendre les données illisibles pour les parties non autorisées et ainsi préserver la confidentialité.

En intégrant ces contrôles tout au long du cycle de vie du produit, les organisations peuvent répondre aux exigences du CRA, renforcer la confiance et protéger les utilisateurs contre les cybermenaces émergentes et en constante évolution.

L'annexe I du CRA, au point (2), énumère les objectifs de sécurité spécifiques qui doivent être mis en œuvre par le fabricant, mais précise que les détails de la mise en œuvre de ces mécanismes reflèteront l'évaluation des risques effectuée pour le produit. Ces mécanismes de contrôle comprennent des pratiques, des procédures et des mesures techniques - les mécanismes les plus importants sont brièvement décrits ci-dessous.

*Exigences relatives à la conception du produit*
Les produits doivent:
*(j) être conçus, développés et fabriqués de manière à limiter les surfaces d'attaque, y compris les interfaces externes;*
*(k) être conçus, développés et fabriqués de manière à réduire les répercussions d'un incident, en utilisant des mécanismes et des techniques appropriés de limitation de l'exploitation de failles.*
Ces exigences de conception doivent être considérées conjointement avec l'exigence de configuration sécurisée par défaut.

Pour prouver leur conformité aux exigences ci-dessus, les PME doivent intégrer, mettre en œuvre et surveiller des évaluations complètes des risques liés aux produits, cartographier les risques liés aux services et aux contrôles, évaluer la documentation de conception, examiner le code, garantir la séparation des environnements de production et de développement, établir et surveiller des bases de référence en matière de sécurité afin de détecter les anomalies, et effectuer des sauvegardes régulières des logiciels et des données.

*Mesures visant à détecter et à éliminer les vulnérabilités tout au long du cycle de vie du produit*
La détection et l'élimination des vulnérabilités avant la mise sur le marché du logiciel sont une exigence clé du CRA. Les PDE doivent:
*(a) être mis sur le marché sans vulnérabilités exploitables connues;*

Les vulnérabilités connues sont répertoriées dans des bases de données publiques, par exemple la base de données européenne[17] ou la base de données nationale américaine[18], ou encore dans des outils d'analyse des vulnérabilités (voir la méthodologie de test d'intrusion Confirmate pour plus de détails sur l'analyse et la gestion des vulnérabilités).
Lorsqu'une vulnérabilité est connue pour avoir déjà été exploitée dans le cadre d'une cyberattaque, le fabricant doit prendre les mesures nécessaires pour empêcher qu'elle ne soit exploitée avec succès contre le PDE avant et après sa mise sur le marché. De nombreux pirates informatiques, même sans compétences avancées, exploitent les vulnérabilités connues mais non corrigées par des exploits « zero-day ».

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

La deuxième partie des exigences essentielles en matière de sécurité est entièrement consacrée à la gestion des vulnérabilités.

Une fois qu'une vulnérabilité est identifiée, il est important de l'évaluer en fonction de sa gravité selon un cadre accepté tel que le CVSS (Common Vulnerability Scoring System). La hiérarchisation est effectuée en fonction de cette évaluation afin que les vulnérabilités critiques et activement exploitées soient traitées en urgence. La correction s'effectue généralement par la publication d'un correctif ou d'une modification de configuration.

En vertu du CRA, les fabricants ont l'obligation de fournir ces mises à jour de sécurité aux utilisateurs sans délai injustifié, en utilisant des mécanismes de mise à jour sécurisés et en les séparant des mises à jour de fonctionnalités. Les mises à jour doivent être fournies gratuitement, accompagnées de messages d'avertissement clairs et, dans la mesure du possible, activées pour une installation automatique par défaut. Cela garantit que les utilisateurs sont protégés rapidement, même s'ils n'agissent pas de manière proactive. Les meilleures pratiques du secteur recommandent des accords de niveau de service (SLA) pour la gestion des correctifs. Par exemple:

- 24 à 48 heures pour corriger les vulnérabilités critiques
- 7 jours pour les vulnérabilités élevées
- 30 jours pour les vulnérabilités moyennes
- 90 jours pour les vulnérabilités faibles

Après la correction, une surveillance continue est essentielle. Les fabricants doivent s'assurer que les correctifs ont été appliqués efficacement et surveiller toute tentative d'exploitation des vulnérabilités restantes, notamment en analysant les journaux système et en prêtant attention aux alertes de détection d'intrusion.

[17] Disponible à l'adresse: https://euvd.enisa.europa.eu/
[18] Disponible à l'adresse suivante: https://nvd.nist.gov/

Pièges à éviter:

- Retarder la correction jusqu'à la mise à jour des fonctionnalités;
- Sous-estimer la gravité des vulnérabilités;
- Ne pas informer les utilisateurs en temps utile et de manière compréhensible.

De plus, la mise en place précipitée de correctifs sans tests appropriés peut entraîner de nouveaux problèmes ou risques. Par conséquent, en combinant une correction rapide, le déploiement de correctifs et une surveillance continue, les PME peuvent mettre en place un processus solide de gestion des vulnérabilités qui répond aux exigences essentielles du CRA en matière de cybersécurité.

Outre l'élaboration et la mise en œuvre de politiques et de procédures pertinentes, les preuves recommandées pour démontrer la conformité aux exigences ci-dessus pourraient inclure des tests de pénétration (internes et par des tiers), des mécanismes de mise à jour automatique de la sécurité, des revues de code et, surtout, des mises à jour pertinentes (voire proactives) en temps opportun, dès qu'une nouvelle menace ou vulnérabilité est connue, même si elle n'a pas encore été exploitée.

*Exigences techniques*

Des exemples de mesures types permettant de satisfaire aux exigences techniques du CRA sont répertoriés dans toutes les normes de sécurité de l'information, y compris NIST SP800 ou Cyber Fundamentals (CyFun) dans leur rubrique respective: Protéger. Des exemples de mesures spécifiques sont donnés ci-dessous.

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

Les mesures recommandées par le cadre de cybersécurité du NIST comprennent:

- Exiger une authentification multifactorielle;
- Appliquer des politiques relatives à la force minimale des mots de passe, des codes PIN et des authentificateurs similaires;
- Réauthentifier périodiquement les utilisateurs, les services et le matériel en fonction du risque (par exemple, dans les architectures « zero trust »);
- Veiller à ce que le personnel autorisé puisse accéder aux comptes essentiels à la protection de la sécurité dans des situations d'urgence.

*(e) protéger la confidentialité des données stockées, transmises ou traitées de toute autre manière, qu'elles soient personnelles ou autres, par exemple en cryptant les données pertinentes au repos ou en transit à l'aide de mécanismes de pointe et en utilisant d'autres moyens techniques;*

Les mesures recommandées dans les principes fondamentaux en matière de cybersécurité comprennent:

- Envisager l'utilisation de techniques de cryptage pour le stockage, la transmission ou le transport des données (par exemple, ordinateur portable, clé USB);
- Les mécanismes de contrôle d'intégrité à la pointe de la technologie (par exemple, contrôles de parité, contrôles de redondance cyclique, hachages cryptographiques) et les outils associés peuvent surveiller automatiquement l'intégrité des systèmes d'information et des applications hébergées.

Des recommandations similaires peuvent être trouvées dans d'autres normes pertinentes:

*(f) protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, des commandes, des programmes et de la configuration contre toute manipulation ou modification non autorisée par l'utilisateur et signaler les corruptions;*
*(g) ne traiter que les données, à caractère personnel ou autres, qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité prévue du produit comportant des éléments numériques (minimisation des données);*
*(h) protéger la disponibilité des fonctions essentielles et de base, notamment après un incident, y compris par des mesures de résilience et d'atténuation face aux attaques par déni de service.*

Il est important de noter que le CRA identifie CE QUI doit être fait, mais pas COMMENT cela doit être fait. La manière dont ces exigences sont mises en œuvre est entièrement laissée à la discrétion du fabricant, même s'il est clairement attendu que les méthodes adoptées soient proportionnées au niveau de risque associé au produit.

Les PME pourraient démontrer leur conformité aux exigences ci-dessus en dotant leurs produits d'éléments numériques avec des fonctionnalités de journalisation leur permettant d'être intégrés dans l'environnement de cybersécurité de leurs utilisateurs professionnels. L'intégration doit également tenir compte de la compatibilité avec le contrôle d'accès centralisé, régulièrement testé, y compris par des tests de pénétration, et surtout, d'une cryptographie avancée.

Les mesures de sécurité spécifiques que les PME doivent au minimum envisager pour satisfaire aux exigences ci-dessus comprennent:

- Adopter des politiques et des procédures en matière d'identité, de contrôle d'accès, d'autorisation et de gestion des incidents.
- Mettre en œuvre des mesures de protection dédiées pour empêcher l'accès non autorisé, la distorsion ou la modification des données du système et des enregistrements d'audit (par exemple, droits d'accès restreints, sauvegardes quotidiennes, cryptage des données, installation d'un pare-feu).
- Mettre en œuvre des mécanismes de détection et de signalement des atteintes à l'intégrité.
- Activer l'authentification multifactorielle.
- Appliquer des politiques relatives à la force minimale des mots de passe, codes PIN et autres moyens d'authentification similaires.
- Mettre en place des mécanismes de détection et de réponse aux attaques DDoS.

*Mesures visant à minimiser l'impact sur l'environnement informatique*

Deux exigences visent à minimiser l'impact d'un incident ou d'un dysfonctionnement du produit sur son environnement, à savoir les points (i) et (k) décrits ci-dessous:

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

Cette exigence impose que les PDE soient non seulement sécurisés pour leur compte, mais qu'ils ne constituent pas non plus une menace pour la disponibilité d'autres appareils ou réseaux. Elle est similaire à la directive sur les équipements radioélectriques, selon lequel les appareils ne doivent pas « interférer avec d'autres appareils ou réseaux », ce qui exige que les équipements utilisent efficacement le spectre radioélectrique et respectent les normes de compatibilité électromagnétique, afin d'éviter toute interférence nuisible. Appliqué à la cybersécurité, nous pourrions recommander que les PDE soient conçus avec soin afin d'éviter une consommation excessive de données, de CPU ou de réseau, par exemple, et qu'ils soient dotés de points de contrôle afin d'éviter qu'ils ne soient utilisés pour une attaque par déni de service. Dans le cadre d'une attaque par déni de service, les PDE compromis pourraient entrer dans une armée de bots (appareils compromis) et attaquer simultanément un réseau, un site web ou une application, mettant hors service le produit ou le réseau visé.

*(k) être conçus, développés et produits de manière à réduire l'impact d'un incident à l'aide de mécanismes et de techniques appropriés d'atténuation des risques d'exploitation;*

Les mesures de sécurité spécifiques que les PME doivent au minimum envisager pour satisfaire aux exigences ci-dessus comprennent:

- Réaliser une évaluation complète des risques liés au produit dès sa phase de conception, en tenant compte des risques potentiels sur la disponibilité des services fournis par d'autres appareils ou réseaux en raison du PDE ou des appareils connectés, et en identifiant les mesures d'atténuation permettant de réduire l'impact ou la probabilité des risques.
- Mettre en œuvre des mesures de protection dédiées pour empêcher l'accès non autorisé, la distorsion ou la modification des données du système et des enregistrements d'audit (par exemple, droits d'accès restreints, sauvegardes quotidiennes, cryptage des données, installation d'un pare-feu).
- Mettre en œuvre des mécanismes de détection et de réponse aux attaques DDoS.

*Contrôles liés à l'utilisateur*

Deux mesures supplémentaires visent à donner à l'utilisateur les moyens de gérer sa propre sécurité et ses propres données:

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

Les techniques de détection des comportements anormaux indiquant une cyberattaque reposent principalement sur l'examen et l'analyse des journaux des produits comportant des éléments numériques afin de déterminer le type et le vecteur de l'attaque et de prendre les mesures appropriées pour y répondre. Cela se fait généralement à l'aide de logiciels de collecte et de corrélation des journaux, pour lesquels les produits comportant des éléments numériques doivent disposer de fonctionnalités permettant d'enregistrer et de surveiller leurs activités.

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

Les techniques de suppression sécurisée des données sont diverses, selon le type de support (papier, disque dur, cloud) ou le niveau de sensibilité (des données génériques à l'historique des clients).

Les mesures de sécurité spécifiques que les PME doivent envisager, au minimum, pour satisfaire aux exigences ci-dessus, comprennent:

- Intégrer des fonctionnalités de soutien pour l'enregistrement et la surveillance des activités PDE.
- Intégrer des fonctionnalités de suppression et de transfert de données sécurisées, et permettre à l'utilisateur de lancer le processus de manière simple.
- Utiliser des méthodes telles que la réécriture complète de la mémoire, l'effacement par cryptage, le remplissage à zéro, la suppression au niveau matériel ou même la destruction physique pour garantir que les données sont véritablement irrécupérables. Il est essentiel d'identifier tous les secrets stockés avant l'effacement, de vérifier que les données ont bien été supprimées et de révoquer les certificats des appareils pendant le processus.

Le CRA suppose que les personnes malveillants peuvent obtenir des informations importantes (voire confidentielles) pour planifier leurs attaques, qu'ils peuvent extraire des PDE auxquels ils ont accès après leur mise au rebut ou leur remplacement par d'autres, à moins qu'il n'existe un mécanisme sécurisé permettant de détruire les anciennes données et de nettoyer les supports de stockage abandonnés.

## 4.2 Chaînes d'approvisionnement et sécurité des tiers

Les fabricants sont responsables de la cybersécurité de l'ensemble des produits qu'ils fabriquent, y compris les composants tiers intégrés ou incorporés, tels que les bibliothèques logicielles, les modules ouverts et les micrologiciels. En particulier, les fabricants doivent évaluer et gérer les risques provenant de la chaîne d'approvisionnement et vérifier que les logiciels tiers sont conformes aux exigences du CRA.

Dans la pratique, cela signifie que toute responsabilité imposée au fabricant doit également être attendue de la chaîne d'approvisionnement correspondante si elle a un impact sur le produit final. Voici quelques exemples d'attentes, sans que cette liste soit exhaustive:

- Sécurité dès la conception et par défaut;
- Prolongation de la période d'assistance (qui doit être compatible avec celle du produit final);
- Gestion et divulgation des vulnérabilités;
- Gestion des incidents (dans la mesure où ils ont un impact sur le produit du fabricant).

En conséquence, les fabricants devront faire preuve de diligence raisonnable dans le choix des fournisseurs et autres contributeurs tiers à leurs produits.

Dans le cadre de cette activité, les fabricants doivent tenir à jour et fournir une nomenclature logicielle (SBOM) répertoriant tous les composants logiciels utilisés, y compris les dépendances tierces et logiciels ouverts. La SBOM doit être:

- Disponible sous une forme lisible par machine sur demande des clients et des autorités de surveillance du marché;
- tenue à jour et refléter toutes les modifications apportées tout au long du cycle de vie du produit.

De plus amples détails sur le format (par exemple JSON) et les éléments (informations) de la SBOM peuvent être fournis par la Commission européenne sous la forme d'un acte d'exécution.

Parallèlement, l'Agence américaine pour la cybersécurité et la sécurité des infrastructures (CISA) fournit un aperçu des meilleures pratiques et des exigences minimales dans son projet de document intitulé « Minimum Elements for a Software Bill of Materials (SBOM) » (Éléments minimaux pour une nomenclature logicielle) d'août 2025.

Pour les PME qui fabriquent des produits couverts par le CRA, ces exigences SBOM en constante évolution de la CISA éclairent les aspects techniques et les normes de maintenance SBOM. Mais les détails de la CISA introduisent également une complexité opérationnelle non négligeable.

## 4.3 Gestion des vulnérabilités

La partie II des exigences essentielles en matière de sécurité (annexe I du CRA) traite des exigences relatives à la gestion des vulnérabilités. Il existe ici un certain chevauchement avec les exigences de la partie I (par exemple, l'exigence selon laquelle les produits comportant des éléments numériques doivent être mis sur le marché sans vulnérabilités exploitables connues). Cependant, la plupart des exigences énumérées dans cette partie de l'annexe sont axées sur les politiques et les procédures et visent explicitement la gestion des vulnérabilités.

### 4.3.1 Identification et documentation

*(1) identifier et documenter les vulnérabilités et les composants contenus dans les produits comportant des éléments numériques, notamment en établissant une nomenclature des composants logiciels dans un format couramment utilisé et lisible par machine, couvrant au minimum les dépendances de haut niveau des produits;*
L'obligation de produire une nomenclature logicielle (SBOM) est obligatoire. De plus amples informations sur le lien entre le concept de SBOM et le CRA figurent aux considérants 77 et 118 et à l'article 13, paragraphe 24, du CRA.
Comme indiqué ci-dessus, à l'heure où nous rédigeons le présent document, il n'existe pas de format imposé pour un tel document, ni d'ailleurs de format standard accepté, bien que l'article 13, paragraphe 24, permette à la Commission, au moyen d'actes d'exécution tenant compte des normes et des meilleures pratiques européennes ou internationales, de préciser le format et les éléments de la SBOM.
En outre, les fabricants doivent *(3) effectuer des tests et des examens efficaces et réguliers de la sécurité du produit comportant des éléments numériques;*
Il est important de noter ici que l'exigence (3) consiste à mettre en place un processus complet et périodique de tests et d'examens, tant pour les vulnérabilités techniques et organisationnelles que pour les erreurs de configuration, qu'une vulnérabilité ait été découverte ou non.

### 4.3.2 Remédiation

Les vulnérabilités PDE doivent être traitées ou corrigées sans délai. Cela est nécessaire pour garantir que le produit reste sécurisé sur le marché de l'UE. En outre, le CRA a précisé que, dans la mesure du possible, les nouvelles mises à jour de sécurité doivent être fournies séparément des mises à jour fonctionnelles. Cela pourrait contribuer à réduire le décalage entre le développement du produit et la maintenance de la sécurité.

### 4.3.3 Divulgation des vulnérabilités et partage d'informations

Il existe trois exigences clés dans ce domaine pour les fabricants des PDE:
*4) dès la publication d'une mise à jour de sécurité, communiquent sur les vulnérabilités corrigées, en publiant notamment une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit comportant des éléments numérique concerné, les conséquences de ces vulnérabilités, leur gravité et des informations claires et accessibles aidant les utilisateurs à y remédier; dans des cas dûment justifiés, lorsque les fabricants considèrent que les risques pour la sécurité liés à la publication l'emportent sur les avantages en matière de sécurité, ils peuvent retarder la publication des informations relatives à une vulnérabilité corrigée jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif adapté;*
*5) mettent en place et appliquent une politique de divulgation coordonnée des vulnérabilités;*
*6) prennent des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits comportant des éléments numériques ainsi que des composants tiers contenus dans ces produits, y compris en fournissant une adresse de contact pour le signalement des vulnérabilités découvertes dans les produits concernés;*

L'exigence (5) fait référence à la divulgation coordonnée des vulnérabilités, qui a une signification spécifique dans ce contexte. Le concept de divulgation coordonnée des vulnérabilités (CVD) est décrit en détail par l'ENISA[19]. En substance, la CVD est un ensemble de règles (par exemple, une politique) publiées par un fabricant qui permet à des experts en sécurité externes bien intentionnés (il peut s'agir de « hackers éthiques » ou de services d'analyse des vulnérabilités) d'identifier les vulnérabilités potentielles de ses systèmes ou produits, et qui prévoit une procédure (formulaire, canal, contacts) pour signaler les failles de sécurité identifiées au fabricant. La CVD définit généralement les systèmes concernés et les conditions dans lesquelles l'identification peut être effectuée (aucune loi n'est enfreinte, aucun préjudice n'est causé, aucune donnée n'est divulguée).

### 4.3.4 Gestion des mises à jour de sécurité

Les dernières exigences de la partie II concernent la gestion des mises à jour de sécurité, garantissant que les mesures correctives (mises à jour de sécurité) évoquées ci-dessus sont réalisables grâce à *des mécanismes permettant de distribuer en toute sécurité les mises à jour* pour les PDE.

*En outre, les mises à jour de sécurité doivent être gratuites et accompagnées de messages consultatifs fournissant aux utilisateurs les informations pertinentes, y compris sur les mesures potentielles à prendre.* Tout cela dans le but de permettre aux utilisateurs de PDE de sécuriser leurs produits et de prendre les mesures nécessaires pour atténuer les risques, le cas échéant.

# 5. Évaluation de la conformité

## 5.1 Procédures d'évaluation de la conformité

Les procédures d'évaluation de la conformité adoptées par le CRA sont basées sur le NLF[20] et s'articulent autour du principe « risque élevé = assurance élevée ». À savoir, les catégories par défaut (non spécifiquement mentionnées dans le règlement) sont soumises à des procédures d'auto-évaluation, la catégorie « Important I » est basée sur une norme harmonisée ou une évaluation par un tiers, les catégories « Important II » et « Produit critique » sont soumises à une évaluation et à une certification par un tiers en conséquence. Les exigences spécifiques pour chaque catégorie de produits sont résumées dans le tableau suivant. Une description détaillée des procédures d'évaluation de la conformité est disponible dans le chapitre « Processus de

[19] https://www.enisa.europa.eu/topics/vulnerability-disclosure

[20] Le NLF (nouveau cadre législatif) clarifie l'utilisation du marquage CE et crée une boîte à outils de mesures à utiliser dans la législation sur les produits. Le NLF comprend: le règlement (CE) n° 765/2008 fixant les exigences en matière d'accréditation et de surveillance du marché des produits, la décision n° 768/2008 relative à un cadre commun pour la commercialisation des produits, qui comprend des dispositions de référence à intégrer dans les révisions de la législation sur les produits. Il s'agit en fait d'un modèle pour la future législation sur l'harmonisation des produits, le règlement (UE) 2019/1020 relatif à la surveillance du marché et à la conformité des produits. Pour plus de détails, veuillez consulter le site web de la Commission européenne: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_fr

conformité CRA » du document **CONFIRMATE D3.1 – Architecture pour l'évaluation automatisée de la conformité CRA,** dans le processus de conformité au CRA. Les exigences sont énoncées à l'article 32 de la loi. L'annexe VIII fournit une description détaillée des procédures d'évaluation de la conformité elles-mêmes.

Le CRA reconnaît et s'appuie sur les procédures de conformité présentées ci-dessous.

**5.1.1 Normes harmonisées**. Il s'agit de normes européennes officiellement reconnues qui confèrent une présomption de conformité avec des exigences légales spécifiques de la législation européenne. Elles servent de références normatives et vérifiables pour la gestion des risques, le développement sécurisé et la sécurité opérationnelle.

Ces normes doivent encore être élaborées et reconnues officiellement pour présumer la conformité aux exigences essentielles en matière de cybersécurité. En février 2025, la Commission européenne a chargé les organismes européens de normalisation (CEN, CENELEC, ETSI) d'élaborer 41 normes: 15 normes horizontales, qui s'appliquent de manière générale à tous les PDE, et 25 normes verticales, qui sont adaptées à des types de produits et à des classes de risque spécifiques. Les normes horizontales traitent des exigences générales en matière de sécurité (type A) et de vulnérabilité (type B), tandis que les normes verticales fournissent des orientations détaillées pour des produits spécifiques, par exemples navigateurs, les appareils IoT (type C), influençant la possibilité pour les fabricants de procéder à une auto-évaluation ou d'exiger la conformité d'un tiers, les normes les plus sensibles étant élaborées dans des conditions restreintes. La liste complète des normes est disponible sur le site web du CEN/CENELEC[21].

Il est prévu de publier les normes de type A et les normes de type B relatives à la gestion des vulnérabilités d'ici le 30 août 2026, toutes les normes de type C d'ici le 30 octobre 2026 et les normes de type B restantes d'ici le 30 octobre 2027.

Outre les normes harmonisées qui soutiennent directement la conformité au CRA, les fabricants sont encouragés à utiliser les principales normes industrielles lors de la mise en œuvre des exigences CRA. Des exemples notables sont répertoriés à l'annexe C.

**5.1.2 Les spécifications communes** (adoptées par l'acte d'exécution de la CE) sont des lignes directrices détaillées et pratiques de la Commission européenne destinées à aider les fabricants à satisfaire des exigences spécifiques en matière de cybersécurité, en l'absence de normes harmonisées ou pour les domaines qui ne sont pas suffisamment couverts par une norme harmonisée publiée, et qui servent de solution de repli dans de tels cas.

**5.1.3 Certificats** délivrés dans le cadre d'un système européen de certification de la cybersécurité.

[21] Disponible à l'adresse suivante: https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf

Le principal système de certification de l'UE qui soutiendra la conformité au CRA est l'EUCC (European Common Criteria). L'EUCC est un système de certification de cybersécurité volontaire à l'échelle européenne qui permet la certification de produits TIC tels que les composants technologiques (puces, cartes à puce), le matériel et les logiciels. S'appuyant sur le cadre d'évaluation des critères communs SOG-IS existant depuis plus de vingt ans, il sert de prolongement et d'extension (de 17 États membres de l'UE actuellement à l'ensemble des 27 qui l'adoptent). Il propose deux niveaux d'assurance basés sur le niveau de risque associé à l'utilisation prévue du produit, du service ou du processus, en termes de probabilité et d'impact d'un accident.
La Commission européenne a centralisé tous les documents et orientations liés à l'EUCC[22]. Opter pour une certification européenne en matière de cybersécurité comme procédure d'évaluation de la conformité présente l'avantage d'une présomption de conformité avec le CRA, même pour les catégories à haut risque, et renforce la crédibilité du marché et la confiance des clients.

La loi européenne sur la cybersécurité (UE 2019/881) établit un cadre commun pour la certification de la cybersécurité dans toute l'UE. En vertu de la législation sur la cyberrésilience (CRA), ce cadre revêt une importance particulière pour les produits présentant des risques plus élevés, ceux classés comme **importants de classe II** ou **critiques** dans l'annexe VIII. Pour ces classes de produits, la certification peut servir de preuve formelle du respect des niveaux d'assurance « substantiels » ou « élevés ».

## 5.2 Procédures minimales requises pour l'évaluation de la conformité

Les PME doivent au moins respecter les procédures minimales requises définies dans le CRA pour leur catégorie de produits, comme expliqué dans le document CONFIRMATE D3.1 – Architecture for Automated CRA Conformance Assessment (Architecture pour l'évaluation automatisée de la conformité au CRA)[23] **OU** toute autre procédure plus exigeante. Plus la procédure d'évaluation choisie est exigeante, plus le PDE apparaît sûr et fiable sur le marché, ce qui peut constituer un avantage concurrentiel significatif. Par exemple, si le PDE appartient à la catégorie par défaut, la procédure minimale requise est le module A, mais la PME peut choisir l'une des autres procédures plus exigeantes ci-dessous. Si un PDE appartient à la classe importante I, la PME qui le fabrique peut procéder à une auto-évaluation par rapport aux normes harmonisées pour son type de produit, si elles sont disponibles, ou, si elles ne le sont pas, choisir la procédure la plus exigeante suivante: le module B+C ou le module H. Si un PDE est répertorié dans la classe importante II, les procédures minimales requises sont au nombre de deux: le « module B+C » ou le module H, qui exigent tous deux une évaluation par un tiers.

[22] Disponible ici: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_fr
[23] Disponible ici: https://confirmate-project.eu/materials/

Les options de procédure pour des produits spécifiques sont résumées dans le tableau ci-dessous, chaque coche indiquant une option pour la catégorie donnée:

| Type / catégorie de produit | Par défaut | Classe I importante | Classe importante II | Critique |
|---|---|---|---|---|
| Auto-évaluation (Module A – Contrôle interne) | ✅ | | | |
| Auto-évaluation par rapport à la norme harmonisée de l'UE, spécifications communes (Module A – Contrôle interne) | ✅ | ✅ | | |
| Évaluation CAB de la conception + Auto-évaluation de la production (modules B+C) | ✅ | ✅ | ✅ | |
| Assurance qualité CAB complète (Module H) | ✅ | ✅ | ✅ | |
| Certificat européen de cybersécurité (CSA) de niveau « substantiel » ou « élevé » | ✅ | ✅ | ✅ | ✅ |

Une exception est faite pour les logiciels ouverts: *« Les fabricants de produits importants comportant des éléments numériques répondant aux critères de logiciels libres et ouverts devraient pouvoir suivre la procédure de contrôle interne basée sur le module A, à condition de mettre la documentation technique à la disposition du public »* (considérant 91 du CRA).

## 5.3 Marquage CE et documentation technique

### 5.3.1 Marquage CE

Le marquage CE est défini dans le CRA comme « *le marquage par lequel un fabricant indique qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant sont conformes aux exigences essentielles de cybersécurité énoncées à l'annexe I et à toute autre législation d'harmonisation de l'Union applicable prévoyant son apposition ».*
En général, le marquage CE est requis pour attester qu'un produit satisfait à toutes les exigences applicables de l'UE en matière de cybersécurité et de sécurité. Dans le contexte du CRA, le marquage CE ne doit être apposé qu'après (a) avoir achevé la procédure d'évaluation de la conformité pertinente et (b) avoir rédigé et signé la déclaration de conformité UE.
Le marquage CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) n° 765/2008. Le marquage CE doit être apposé de manière visible, lisible et indélébile sur le produit et son emballage ou sur la documentation qui l'accompagne (si le marquage physique n'est pas possible).

***NB:*** *tous les produits ne doivent pas nécessairement porter le marquage CE. Celui-ci n'est obligatoire que pour la plupart des produits couverts par les directives « nouvelle approche ». Il est interdit d'apposer le marquage CE sur d'autres produits. Veuillez noter que le marquage CE n'indique pas qu'un*

*produit a été approuvé comme sûr par l'UE ou par une autre autorité. Il n'indique pas non plus l'origine d'un produit*[24].

### 5.3.2 Documentation technique

Les fabricants sont tenus de préparer et de conserver une documentation technique (conformément à l'annexe VII du CRA) démontrant la conformité du produit. Cette obligation s'applique tant à l'auto-évaluation qu'à l'évaluation par un tiers.

Cette documentation doit inclure:

- Une description générale du produit
- Une description de la conception, du développement et de la production du produit
- Les évaluations initiales et actualisées des risques
- Les informations qui ont été prises en compte pour déterminer la période d'assistance
- Une liste des normes harmonisées appliquées en tout ou en partie au produit
- Les rapports d'essai, résultats d'inspection et normes appliquées
- Une description de la procédure d'évaluation de la conformité utilisée
- Une copie de la déclaration de conformité UE
- Le cas échéant, la nomenclature du logiciel

Pour les PME, une option permettant de simplifier la documentation technique sera disponible dans un règlement d'exécution de la Commission qui n'était pas encore publié au moment de la rédaction du présent guide.

## 5.4 Déclaration de conformité

La déclaration de conformité (DoC) est un document juridique attestant qu'un produit satisfait aux exigences essentielles applicables en matière de cybersécurité énoncées à l'annexe I du CRA. Elle est rédigée par le fabricant après avoir mené à bien les procédures d'évaluation de la conformité appropriées, doit être signée par un représentant autorisé et mise à la disposition des autorités nationales de surveillance du marché. Le DoC doit contenir:

- Le nom et l'adresse du fabricant
- L'identification du produit
- Une déclaration de conformité au CRA
- Une liste des normes pertinentes et des procédures de conformité utilisées
- La référence à l'examen UE de type (le cas échéant)
- La signature, la date et les coordonnées de la personne responsable

Le contenu de la déclaration de conformité est indiqué dans les annexes V et VI du CRA.

[24] *Voir le texte intégral et toutes les options de format du marquage CE sur le site web de la Commission européenne: https://single-market-economy.ec.europa.eu/single-market/goods/ce-marking_fr*

# 6. Obligations en matière de notification et après la mise sur le marché

## 6.1 Obligations de notification

Conformément à l'article 14, les PME sont tenues de signaler à la fois les « vulnérabilités activement exploitées » et les « incidents graves ». Ceux-ci sont définis comme suit:

- Une vulnérabilité activement exploitée est une faille de sécurité déjà utilisée ou faisant l'objet d'une attaque malveillante active.
- Un incident grave est un événement ayant un impact sur la confidentialité, l'intégrité ou la disponibilité du produit, y compris l'introduction d'un logiciel malveillant.

L'article 14 du CRA décrit en outre un incident grave comme un incident qui (a) affecte négativement ou est susceptible d'affecter négativement la capacité d'un PDE à protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou de fonctions sensibles ou importantes, OU (b) a conduit ou est susceptible de conduire à l'introduction ou à l'exécution d'un code malveillant dans un PDE ou dans les systèmes d'information et les réseaux d'un utilisateur du produit.
Les exigences en matière de notification pour ces deux types d'événements diffèrent, comme expliqué dans les sections suivantes. Vous trouverez plus de détails à ce sujet à l'article 14 du CRA.

Outre la notification obligatoire de toute vulnérabilité activement exploitée et de tout incident grave, le CRA prévoit également la notification volontaire de tout autre incident ou menace pesant sur le PDE. La même procédure de notification simultanée au CSIRT et à l'ENISA via la plateforme de notification unique s'applique.

## 6.2 Procédure de notification

Toutes les notifications obligatoires doivent être soumises via la future plateforme unique de notification[25] à l'ENISA et simultanément au CSIRT de l'établissement principal du fabricant dans l'UE. Une fois que la plateforme unique de notification (voir ci-dessous) sera disponible, cela se fera par le biais d'une notification unique à la plateforme.

*Vulnérabilités activement exploitées*

La notification des vulnérabilités activement exploitées se déroule en trois étapes distinctes:

- Étape 1: alerte précoce dans **les 24 heures** suivant la prise de connaissance. Le cas échéant, les États membres dans lesquels le produit a été mis à disposition doivent être identifiés à ce stade.
- Étape 2: Rapport initial sur la vulnérabilité dans **les 72 heures** suivant la prise de connaissance, comprenant:

[25] Voir l'article 16 du CRA: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

    - *des informations générales sur le produit, la nature générale de l'exploitation et de la vulnérabilité concernée;*
    - *Toute mesure corrective ou d'atténuation prise, ainsi que les mesures correctives ou d'atténuation que les utilisateurs peuvent prendre.*
    - Une évaluation par le fabricant du niveau de sensibilité des informations notifiées.
- Étape 3: Rapport final au plus tard **14 jours** après la mise à disposition d'un correctif, comprenant:
    - *Une description de la vulnérabilité, y compris de sa gravité et de ses répercussions;*
    - *Le cas échéant, des informations concernant tout acteur malveillant ayant exploité ou exploitant la vulnérabilité;*
    - *Des précisions concernant la mise à jour de sécurité ou les autres mesures correctives qui ont été mises en place pour remédier à la vulnérabilité.*

*Incidents de sécurité graves*

Le signalement des incidents de sécurité graves se déroule également en trois étapes distinctes, la différence essentielle résidant dans la dernière étape.

- Étape 1: Alerte précoce dans **les 24 heures** suivant la prise de connaissance, comprenant:
    - Un avis indiquant si l'incident est soupçonné d'être causé par des actes illégaux ou malveillants, qui doit également préciser.
    - Le cas échéant, les États membres dans lesquels le produit a été mis à disposition.
- Étape 2: notification de l'incident dans **les 72 heures** suivant sa détection, comprenant:
    - La nature de l'incident
    - Une évaluation initiale de l'incident
    - Toute mesure corrective ou d'atténuation prise, ainsi que les mesures correctives ou d'atténuation que les utilisateurs peuvent prendre
    - Une évaluation par le fabricant du niveau de sensibilité des informations notifiées.
- Étape 3: Rapport final dans un délai **d'un mois** après la notification dans les 72 heures, comprenant:
    - *Une description détaillée de l'incident, y compris de sa gravité et de ses répercussions;*
    - *Le type de menace ou la cause profonde qui a probablement déclenché l'incident*
    - *Les mesures d'atténuation appliquées et en cours.*

*Notification aux utilisateurs*

Pour les deux types d'incidents, dès qu'ils ont connaissance d'une vulnérabilité ou d'un incident, les fabricants doivent en informer sans délai les utilisateurs concernés (et, le cas échéant, tous les utilisateurs), en leur fournissant des conseils d'atténuation des risques dans un format facilement automatisable et lisible par machine. Si les fabricants ne procèdent pas à cette notification, le CSIRT peut intervenir pour informer les utilisateurs.

*Signalement volontaire*

En dehors du champ d'application de leurs obligations de notification, conformément à l'article 15, les fabricants sont encouragés à signaler volontairement toute vulnérabilité et menace susceptible d'affecter la cybersécurité d'un PDE. De même, la notification des incidents qui ne sont pas graves est également volontaire.

Ce mécanisme de notification volontaire pourrait introduire une bonne pratique pour les PME, avec un effet positif indirect pour le fabricant et ses clients, en augmentant la visibilité sur la menace et en prévenant ainsi d'autres incidents. En outre, lorsqu'il est difficile d'évaluer avec précision si une vulnérabilité particulière est activement exploitée ou si un incident est grave, la notification volontaire semble être l'option la plus sûre.

## 6.3 Coopération avec les autorités européennes et nationales

### 6.3.1 L'ENISA et les CSIRT en matière de gestion des vulnérabilités

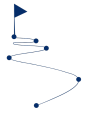
Les fabricants signalent les vulnérabilités activement exploitées et les incidents graves à l'ENISA et au CSIRT national conformément aux dispositions de l'article 14 de la loi. Les exigences applicables au fabricant sont présentées à la section 5.2 des présentes lignes directrices.

### 6.3.2 Autorités nationales de surveillance du marché

Les autorités de surveillance du marché sont chargées de faire respecter les obligations prévues par le CRA dans chaque pays. La manière dont cela s'applique au CRA est expliquée au chapitre V du CRA.

Les conséquences pour les fabricants sont les suivantes: ils sont tenus de

- coopérer lors des enquêtes, des audits et des inspections;
- fournir des documents (par exemple, SBOM, évaluations des risques, dossiers techniques) sur demande;
- d'informer les autorités nationales de surveillance du marché des cas de non-conformité et des mesures correctives, le cas échéant.



# 7. Les étapes à suivre par les PME pour mettre en œuvre le CRA

## 7.1 Évaluation initiale de la portée et des lacunes

La première étape vers la conformité au CRA consiste à bien comprendre quels produits entrent dans le champ d'application du CRA, quel est le rôle de l'organisation par rapport aux produits concernés et quelles sont les exigences auxquelles les produits sont conformes et non conformes. Pour ce faire, il convient de procéder à une évaluation de la portée et des lacunes.

Le présent document, ainsi que les outils fournis par le projet CONFIRMATE, ont pour but de faciliter l'analyse initiale: champ d'application, identification des rôles, évaluation des lacunes et suivi des améliorations au fil du temps à mesure que l'organisation remédie aux exigences non respectées. En ce sens, l'évaluation des lacunes doit être considérée comme un « document vivant », c'est-à-dire qu'elle doit être mise à jour régulièrement afin de refléter les progrès réalisés. De cette manière, l'évaluation reflétera fidèlement la situation de l'organisation en matière de conformité à tout moment.

## 7.2 Élaboration d'un plan de mise en œuvre

Le plan de mise en œuvre peut être élaboré une fois que l'évaluation initiale des lacunes a été effectuée. Tout comme l'évaluation elle-même, le plan doit être considéré comme un document qui évolue avec le temps et tient compte des enseignements tirés au fur et à mesure de l'avancement du projet de mise en œuvre.

En matière de planification, il est recommandé de suivre une approche « par vagues successives », dans laquelle les activités des trois prochains mois sont planifiées de manière très détaillée et les activités au-delà de cette période sont estimées au mieux. Il peut être contre-productif d'entrer trop dans les détails dans des plans qui s'étendent dans un futur lointain, car les activités à long terme ont tendance à être modifiées pour tenir compte des enseignements tirés au cours des premières phases d'un projet.

Dans tous les cas, si elle n'existe pas, la réalisation d'une évaluation des risques doit être considérée comme prioritaire, car les résultats de cette évaluation justifieront les mesures prévues et mises en œuvre et permettront à l'organisation de hiérarchiser les risques de la manière la plus efficace possible.

En ce qui concerne la planification à court terme, il est recommandé de simplifier les activités, de définir des résultats clairs pour chaque tâche et de réduire au maximum la durée allouée à chaque activité. Cela permet d'éviter le problème des tâches qui sont toujours terminées à 90 %, mais qui ne semblent jamais atteindre les 100 %.

Enfin, les PME peuvent tirer pleinement parti des ressources développées spécifiquement pour les aider à se conformer au CRA dans le cadre du programme « Europe numérique (Digital Europe)»: nos outils du projet CONFIRMATE, mentionnés à l'annexe E, et d'autres projets, énumérés à l'annexe F, ainsi que les ressources d'aide européennes et nationales destinées aux PME, énumérées à l'annexe D.

## 7.3 Formation et sensibilisation du personnel

Les programmes de formation et de sensibilisation sont un élément clé du plan visant à assurer la conformité. Bien que tout ait été mis en œuvre pour simplifier les exigences du CRA dans les présentes lignes directrices et dans les outils qui les accompagnent, il est extrêmement important que le personnel acquière et maintienne une compréhension approfondie du CRA et des politiques connexes.

D'autres conseils, outils et modèles que les PME pourraient utiliser pour mettre en œuvre les exigences de sécurité essentielles et se conformer aux exigences en matière de documentation sont énumérés dans les annexes. L'utilisation de ces ressources n'est pas obligatoire, à l'exception de l'exemple de déclaration de conformité, mais doit être envisagée dans le cadre d'un plan à l'échelle de l'organisation.

# 8. Calendriers et périodes de transition

Les dates clés du calendrier de mise en œuvre du CRA sont les suivantes:

| Date | Événement |
|---|---|
| 11.12.24 | Entrée en vigueur du CRA |
| 11.06.26 | Obligations applicables aux organismes d'évaluation de la conformité en matière de notification[26] |
| 30.08.26 | Date limite pour les normes de type A et les normes harmonisées de type B relatives au traitement des vulnérabilités |
| 11.09.26 | Les obligations de notification des vulnérabilités et des incidents de sécurité deviennent applicables. |
| 30.10.27 | Date limite pour les normes harmonisées de type B restantes. |
| 11.12.27 | Application intégrale du CRA |

[26] Il s'agit d'une obligation qui incombe aux États membres et non aux fabricants.

## Annexe A: Déclaration UE de conformité simplifiée

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

> … [nom du fabricant] déclare que le produit comportant des éléments numériques de type … [désignation du type de produit comportant un élément numérique] est conforme au règlement (UE) 2024/2847 (1).
>
> Le texte complet de la déclaration UE de conformité est disponible à l'adresse internet suivante: …

---

(1) JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

## Annexe B: Modèle d'évaluation des risques

La boîte à outils interopérable de l'ENISA pour la gestion des risques dans l'UE fournit une méthodologie harmonisée et reconnue par l'UE à cette fin. Elle est conçue pour soutenir la mise en œuvre cohérente de la gestion des risques dans toute l'UE, en intégrant la norme ISO/IEC 27005, la directive NIS2 et les pratiques spécifiques au secteur. Il convient toutefois de noter que cette boîte à outils n'a pas été spécialement conçue pour répondre aux exigences du CRA, mais doit être considérée comme un outil à usage général couvrant de nombreux domaines d'application différents.

La boîte à outils comprend des modèles standardisés et des conseils pour:

- L'identification et l'évaluation des actifs
- l'analyse des menaces et des vulnérabilités
- L'estimation et l'évaluation des risques
- Définition des mesures de traitement et d'atténuation des risques
- L'intégration avec les contrôles de sécurité requis en vertu de l'annexe I du CRA[27]

Il prend en charge les évaluations qualitatives et semi-quantitatives et est interopérable avec les méthodologies nationales et internationales. L'utilisation de cette boîte à outils permet d'assurer la cohérence, l'auditabilité et la traçabilité complète des décisions en matière de sécurité à l'appui des évaluations de conformité et de la documentation technique en vertu du CRA.

[27] Notez qu'il ne s'agit pas d'une correspondance explicite avec les contrôles du CRA.

## Annexe C: Normes pertinentes

- Les annexes B et C de la norme ETSI TS 103 701 peuvent être utilisées pour structurer la documentation technique prête à être auditée à l'aide des modèles ICS/IXIT.
- **ISO/IEC 27001** - Système de gestion de la sécurité de l'information (SGSI)
- **ISO/IEC 27701** - Système de gestion des informations confidentielles (PIMS)
- **ETSI EN 303 645** - Exigences de sécurité de base pour l'IoT grand public, dont les clauses 4 et 5 peuvent être utilisées pour définir les exigences de sécurité de base
- **OWASP ASVS** – Norme de vérification de la sécurité des applications
- **CIS Benchmarks** - Directives de configuration sécurisée
- **Directives de la Fondation pour la sécurité de l'IoT** – Meilleures pratiques en matière de sécurité des appareils IoT
- **NIST SP 800-53** - **Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations.**
- **NIST SP 800-37** - Cadre de gestion des risques (RMF), fournissant un processus qui intègre les activités de gestion des risques liés à la sécurité, à la confidentialité et à la chaîne d'approvisionnement cybernétique dans le cycle de vie du développement des systèmes.
- **Cadre de cybersécurité du NIST (CSF)**, fournissant des conseils sur la gestion des risques liés à la cybersécurité
- **IEC 62443 / ISA-62443** - Normes de sécurité pour les systèmes d'automatisation et de contrôle industriels
- **ISO 9001** - Système de gestion de la qualité
- **CMMC** - Certification du modèle de maturité en matière de cybersécurité
- **RGPD** - Règlement général sur la protection des données

# Annexe D: Ressources européennes et nationales d'aide aux PME

La Commission européenne, l'Agence européenne de cybersécurité (ENISA) et le Centre européen de compétences en matière de cybersécurité (ECCC) publient tous des rapports sur la cybersécurité, dont beaucoup fournissent des lignes directrices qui pourraient être utiles aux PME mettant en œuvre le CRA.

En particulier, les lignes directrices pour la sécurisation de l'Internet des objets (IoT)[28] définissent l'ensemble des exigences de sécurité tout au long du cycle de vie, depuis les exigences et la conception jusqu'à la livraison et la maintenance pour l'utilisation finale, en passant par l'élimination. Cette étude a été spécialement conçue pour aider les fabricants, les développeurs, les intégrateurs et toutes les parties prenantes impliquées dans la chaîne d'approvisionnement de l'IoT à prendre de meilleures décisions en matière de sécurité lors de la conception, du déploiement ou de l'évaluation des technologies IoT.

En outre, le guide de l'ENISA sur la cybersécurité des PME est un guide sur mesure destiné à améliorer la cybersécurité des petites organisations, y compris les fabricants.

**Au niveau national,** la mission des centres nationaux de compétences en matière de cybersécurité est de stimuler l'excellence de la recherche et la compétitivité de l'Union dans le domaine de la cybersécurité. Une liste des centres a été publiée par l'ECCC[29].

Outre les centres de compétences, de nombreux États membres de l'UE ont créé une agence nationale de cybersécurité. Alors que les centres de compétences se concentrent sur la recherche et l'innovation, les centres de cybersécurité ont tendance à couvrir tous les aspects de la cybersécurité (bien que leurs mandats détaillés diffèrent d'un État membre à l'autre). En voici quelques exemples:

- **Belgique:** CCB - Centre pour la cybersécurité Belgique
- **Allemagne:** BSI – Office fédéral de la sécurité informatique
- **France:** ANSSI – Agence nationale de la sécurité des systèmes d'information
- **Italie:** ACN – Agenzia per la Cybersicurezza Nazionale
- **Roumanie:** DNSC – Directoratul Național de Securitate Cibernetică

Enfin, les organisations professionnelles et industrielles créent des ressources pour aider leurs membres à comprendre et à se conformer au CRA. Par exemple, la Digital SME Alliance, l'ECSO (au niveau de l'UE) et Agoria,

[28]Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
[29]Disponible à l'adresse suivante: https://cybersecurity-centre.europa.eu/nccs-0_fr

## Annexe E: Outils CONFIRMATE

Vous trouverez ci-dessous un bref aperçu des autres guides, formations, outils et documents accompagnant le présent document. Tous les documents relatifs au projet sont disponibles sur www.CONFIRMATE-project.eu/materials.

## Partie 1 Conseils et méthodologies

Méthodologie de test d'intrusion: document élaboré et évalué par des pairs qui vise à aider les PME à se préparer et à réaliser un test d'intrusion PDE efficace, conforme aux exigences de la loi sur la cyber-résilience (CRA). Basé sur les normes industrielles, il vise à résumer et à fournir un guide essentiel sur ce qui est nécessaire et sur ce qui peut être attendu comme résultat d'un test d'intrusion de produit, en tenant compte des produits spécifiques relevant d'une série de catégories CRA.

D3.1 - Architecture pour l'évaluation automatisée de la conformité au CRA: aperçu détaillé et complet du cadre CONFIRMATE, décrivant clairement et méthodiquement ses fonctionnalités et sa structure prévues. Le document présente et définit clairement le processus d'évaluation de la conformité tel que stipulé par le CRA, offrant aux lecteurs un contexte fondamental sur les exigences réglementaires. Par la suite, le livrable illustre précisément comment les utilisateurs finaux interagiront avec le cadre CONFIRMATE et en tireront profit tout au long du processus d'évaluation de la conformité au CRA.
À la suite de la description orientée utilisateur, le livrable précise l' architecture logicielle envisagée, en détaillant les éléments essentiels tels que les composants clés, les divisions modulaires et les interactions entre ces éléments.

D2.2 - Modèle de données probantes: une base pour la collecte et l'évaluation automatiques des données probantes techniques dans toutes les technologies, garantissant que les informations nécessaires sont efficacement saisies et organisées. En tirant parti des formats lisibles par machine, le modèle facilite l'intégration des données probantes dans les outils de conformité automatisés, réduisant ainsi les efforts manuels nécessaires à la documentation et améliorant la précision des évaluations de conformité. Il convient toutefois de noter que cette approche ne garantit pas une conformité totale avec le CRA, car certaines exigences ne sont pas transposables dans des méthodes de collecte automatique de données. Le modèle de données probantes permet également la création de mesures respectives, dérivées des exigences essentielles du CRA, et s'aligne sur celles-ci. Ces mesures fournissent des indicateurs quantifiables de conformité.

## Partie 2 Logiciel ouvert d'évaluation automatisée de la conformité

CONFIRMATE propose un logiciel ouvert qui rationalise l'évaluation de la conformité aux exigences essentielles du CRA en matière de cybersécurité en répertoriant toutes les exigences et mesures essentielles en matière de cybersécurité, en comparant automatiquement les paramètres de sécurité avec les spécifications du CRA et en déterminant les mesures

individuelles à prendre. Ses tableaux de bord intuitifs et ses fonctionnalités structurées aident les organisations à identifier rapidement les exigences essentielles du CRA en matière de cybersécurité qui sont mises en œuvre et celles qui doivent être évaluées ou mises en œuvre, ce qui permet de gagner un temps précieux dans les contrôles de conformité tout en fournissant des informations claires et exploitables pour une conformité et une amélioration continues.

En outre, des documents d'information tels que:

- D2.2 – Modèle de données probantes, qui permettent d'automatiser la vérification de la conformité grâce à une approche structurée de la collecte et de l'évaluation des preuves.
- D3.1 – Architecture pour l'évaluation automatisée de la conformité CRA, un document fournissant un aperçu détaillé et complet du cadre CONFIRMATE, décrivant ses fonctionnalités et sa structure prévues, présentant le processus d'évaluation de la conformité et illustrant comment les utilisateurs finaux interagiront avec CONFIRMATE et en tireront parti dans le processus d'évaluation de la conformité CRA.

## Partie 3 Formations et ateliers CONFIRMATE

Cette liste est un document évolutif, qui comprend une série de formations et d'ateliers prévus jusqu'en juillet 2026.

**Introduction à la conformité CRA:** tout ce que vous devez savoir sur la loi européenne sur la cyber-résilience (CRA)[30] est un aperçu complet des principes et obligations clés du CRA. La vidéo explique l'impact du CRA sur les fabricants, les importateurs, les distributeurs et les intendants de logiciels ouverts en décrivant les rôles et les responsabilités, les classifications des produits en fonction des risques (par défaut, important et critique), ainsi que les exigences de sécurité, le marquage CE et les évaluations de conformité. Elle aborde également des sujets cruciaux tels que la divulgation des vulnérabilités, le signalement des incidents, la nomenclature des composants logiciels (SBOM), les délais d'application et les sanctions en cas de non-conformité.

**Explication de la méthodologie de test d'intrusion[31]**

Dans le cadre de la série de formations sur la conformité à la loi sur la cyber-résilience (CRA), ce module fournit un guide complet et détaillé sur la méthodologie des tests d'intrusion pour les produits comportant des éléments numériques. Il est destiné aux fabricants, aux PME et aux équipes de cybersécurité qui souhaitent se conformer de manière efficace et efficiente aux exigences du CRA. La formation couvre les cinq phases clés des tests d'intrusion conformes au CRA et explique comment planifier, mener et rendre compte des tests conformément aux normes CRA. Elle clarifie également les exigences de conformité pour les produits de classe I importante, de classe II importante et de catégorie par défaut.

[30] Disponible sur YouTube https://youtu.be/-QbPIFVobNw
[31] Disponible sur YouTube: https://youtu.be/wpJluHL9IIQ

## Annexe F: Outils d'autres projets de l'UE

Parallèlement à CONFIRMATE, une série de projets européens supplémentaires visant à aider les PME à se conformer au CRA ont été lancés. Chaque projet a un angle d'approche différent, provient d'un ensemble de pays différents et crée des ressources et des outils complémentaires. La liste des projets en cours pour la période 2025-2026, compilée par CyberStandEU[32], est la suivante:

1. CRA-AI: le projet CRA-AI développe une plateforme alimentée par l'IA pour aider les PME à se conformer et à rester conformes à la loi européenne sur la cyber-résilience, en réunissant des experts en cybersécurité de six pays de l'UE.
2. CURIUM: CURIUM développe le Compliance Continuum, un ensemble d'outils visant à automatiser et à simplifier la conformité à la loi européenne sur la cyber-résilience (CRA). En proposant des évaluations de cybersécurité, une gestion des risques et des tests de vulnérabilité, il aide les PME à réduire leurs coûts, à accélérer la certification et à renforcer l'écosystème européen de sécurité numérique.
3. OSCRAT: OSCRAT développe des outils gratuits et ouverts pour aider les PME européennes, les décideurs politiques et les associations industrielles à se conformer à la loi sur la cyber-résilience (CRA) et à renforcer leurs pratiques en matière de cybersécurité.
4. OCCTET: OCCTET est un projet financé par l'UE qui développe une boîte à outils ouverts pour aider les PME à automatiser la conformité à la loi sur la cyber-résilience (le CRA) pour les logiciels ouverts. La boîte à outils comprend une liste de contrôle de conformité, des outils d'évaluation automatisés, une base de données fédérée, des outils d'analyse des dépendances et des ressources de reporting.
5. CYBERFORT: CYBERFORT aide les PME à répondre aux exigences de la loi sur la cyber-résilience (CRA) en leur proposant des outils sur mesure, des conseils d'experts et des formations. Grâce à une plateforme ouverte et à la collaboration avec des entreprises de cybersécurité, des autorités et des acteurs industriels, il renforce la cyber-résilience et la sensibilisation à travers l'Europe.
6. TRUSTBOOST: TrustBoost est un projet financé par l'UE (accord de subvention n° 101158687) soutenu par le Centre européen de compétence en matière de cybersécurité. Sa mission est de renforcer la cybersécurité, la résilience et la conformité dans toute l'UE en encourageant la collaboration en matière de certification et de respect des principales législations européennes.
7. CRACoWi: CRACoWi (Cyber Resilience Act Compliance Wizard) est un projet de l'UE visant à créer un assistant numérique pour aider les PME, les fabricants, les distributeurs et les importateurs à respecter les normes de la loi sur la cyber-résilience (le CRA), garantissant la sécurité des produits depuis leur conception jusqu'à leur commercialisation.
8. CRACY: CRACY (CRA made Easy) aide les PME européennes à satisfaire aux exigences de la loi sur la cyber-résilience (CRA) en simplifiant la conformité des produits comportant des éléments numériques, en promouvant les meilleures pratiques et en favorisant des produits et services plus sûrs.

[32] Disponible à l'adresse: https://cyberstand.eu/events/impacting-CRA-defining-standards-future

# Annexe G: Relation avec d'autres législations de l'UE

Bien qu'il ne soit pas possible de présenter dans ce document une analyse complète des relations entre le CRA et d'autres législations de l'UE, certains des liens les plus importants sont mentionnés ci-dessous:

1. *Le nouveau cadre législatif (CE/2008/765 et CE:2008/768):* le CRA s'appuie sur le NLF et étend essentiellement le cadre aux produits comportant des éléments numériques. Ceci est décrit en détail dans la section 4.1 des présentes lignes directrices.
2. *Cyber-résilience:* la directive NIS2 et le règlement DORA visent tous deux à améliorer la cyber-résilience dans l'ensemble de l'UE. Ils définissent la gestion des risques liés à la cybersécurité et la notification des incidents par les entités en rapport avec leurs services essentiels. Le CRA complète ces initiatives en imposant des exigences de sécurité relatives aux produits comportant des éléments numériques, qui s'inscrivent dans le cadre réglementaire de l'UE en matière de produits.
3. *La directive sur les équipements radioélectriques (RED) (directive 2014/53/UE)* se concentre sur la sécurité, la compatibilité électromagnétique et l'interopérabilité des produits équipés de radio. Le CRA se concentre sur la cybersécurité et couvre un champ d'application plus large (y compris les logiciels, et pas seulement l'IoT). Elle remplace l'acte délégué RED pour la cybersécurité.
4. *Le règlement sur les machines (règlement (UE) 2023/1230)* couvre la santé et la sécurité lors de l'utilisation de machines. Il complète le CRA, qui s'applique aux composants numériques des machines. Les deux règlements s'appliquent simultanément.
5. *RGPD de l'UE:* le CRA s'appuie sur le RGPD, qui exige la protection et la minimisation de toutes les données (à caractère personnel ou non) traitées par les produits comportant des éléments numériques mis sur le marché de l'UE.
6. *La loi sur l'IA* (règlement (UE) 2024/1689) réglemente la fiabilité et la sécurité des systèmes (d'IA). Elle s'applique aux fonctionnalités d'IA à haut risque, tandis que le CRA s'applique à la cybersécurité du produit lui-même. Un système d'IA à haut risque doit être conforme à la fois à la loi sur l'IA et aux exigences de cybersécurité du CRA.
7. *La loi européenne sur les services numériques (DSA) et la loi européenne sur les marchés numériques (DMA)* imposent la responsabilité des plateformes et la modération des contenus (DSA) ainsi que l'équité du marché pour les gardiens (DMA). Le CRA ne recoupe pas directement ces réglementations, mais elle s'applique aux logiciels utilisés par les plateformes et les systèmes backend.
8. *Loi sur la cybersécurité (CSA)* (règlement (UE) 2019/881): le CRA fait référence aux systèmes de certification développés dans le cadre de la CSA au titre des exigences d'évaluation de la conformité (voir la section 4 des présentes lignes directrices pour plus de détails).