SECURE
Cyber Resilience for SMEs

CRA101 : Comprendre les obligations de la législation sur la cyber-résilience (CRA)

31/03/2026

Funded by the European Union

Déclaration de financement de l'UE : Financé par l'Union européenne au titre de la subvention n° 101190325. Les points de vue et opinions exprimés n'engagent toutefois que leurs auteurs et ne reflètent pas nécessairement celles de l'Union européenne ou Centre européen de compétence en matière de cybersécurité, d'industrie, de technologie et de recherche. Ni l'Union européenne ni l'autorité de financement ne peuvent en être tenues pour responsables.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Avertissement de l'ECCC : Le projet est soutenu par le Centre européen de compétences en cybersécurité et de ses membres.

AVERTISSEMENT

Ce document fait partie du livrable D4.1 « Lignes directrices et ressources pour la conformité des SME à la législation sur la cyber-résilience (CRA)» du projet SECURE.

Le présent document est une traduction du guide original rédigé en anglais. Les abréviations sont conservées en anglais, telles qu'elles figurent dans la liste des abréviations.

Premier auteur : *Centre pour la cybersécurité de Belgique (CCB)*

Deuxième auteur : *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Table des matières

Introduction 6

Comprendre les obligations du CRA - CRA 101 7

1. Évaluation des risques liés à la cybersécurité **7**

2. Gestion des vulnérabilités et mises à jour de sécurité **8**

3. Informations destinées aux utilisateurs, instructions et point de contact unique **9**

4. Obligations de signalement : signalement des vulnérabilités et des incidents **10**

4.1. Quoi **11**

4.2. À qui **12**

4.3. Comment **13**

5. Évaluation de la conformité **14**

5.1. Procédures d'évaluation de la conformité **14**

5.2. Présomption de conformité **14**

5.3. Catégories de produits **15**

5.4. Déclaration de conformité UE (EU DoC) **17**

5.5. Marquage CE **17**

5.6. Démonstration de la conformité au moyen de la documentation technique **17**

Conclusion 19

Liste des tableaux et des figures

Tableau 1 : Signalement des vulnérabilités et des incidents 11
Tableau 2 : Procédures d'évaluation de la conformité 16

Abréviations

CE - Conformité Européenne (European Conformity)

CRA – Loi sur la cyber-résilience (Cyber Resilience Act)

CSIRT – Équipe d'intervention en cas d'incident de sécurité informatique (Computer Security Incident Response Team)

CVD – Divulgation coordonnée des vulnérabilités (Coordinated Vulnerability Disclosure)

ENISA – Agence de l'Union européenne pour la cybersécurité (European Union Agency for Cybersecurity)

EU – Union européenne (European Union)

EU DoC – Déclaration de conformité de l'Union européenne (European Union Declaration of Conformity)

NB – Organisme notifié (Notified Body)

PDE – Produit avec éléments numériques (Product with Digital Elements)

SBOM – Nomenclature logicielle (Software Bill of Materials)

SME – Petite et moyenne entreprise (Small and Medium Enterprise)

SPOC – Point de contact unique (Single Point of Contact)

Introduction

La loi sur la cyber-résilience (CRA) de l'Union européenne (UE), règlement (UE) 2024/2847, a été adoptée dans le but de renforcer la préparation et la résilience en matière de cybersécurité du marché numérique de l'UE face aux défis croissants dans ce domaine. En introduisant des règles harmonisées et des exigences minimales claires en matière de cybersécurité, le CRA vise à réduire les vulnérabilités et à protéger à la fois les consommateurs et les entreprises. Bien que ce règlement historique soit entré en vigueur en décembre 2024, il prévoit une mise en œuvre progressive, avec une période de transition et d'adaptation allant de 2024 à 2027. Concrètement, le CRA énonce les obligations des fabricants, importateurs et distributeurs de produits comportant des éléments numériques (PDE). **L'article 13 et l'annexe I** du CRA énumèrent les exigences essentielles en matière de cybersécurité auxquelles les fabricants doivent se conformer, tant lors de la mise sur le marché européen de leurs PDE que tout au long du cycle de vie de ces derniers. La partie I des exigences de l'annexe I porte sur les propriétés des PDE, tandis que la partie II porte sur la gestion des vulnérabilités. Au-delà de l'annexe I et de l'article 13 du CRA, d'autres exigences sont toutefois imposées – par exemple, en matière d'informations et de notices d'utilisation (annexe II), d'obligations de notification (articles 14 à 17) et de conformité (articles 27 à 32). Dans un premier temps visant à traduire les principales obligations légales en orientations concrètes, **le présent guide offre un aperçu simplifié[1] des obligations**, réparties en **cinq sections**, à prendre en compte **au minimum**. L'objectif est de rendre le règlement plus accessible et d'améliorer la sensibilisation et la compréhension à un niveau élémentaire, en particulier pour les petites et moyennes entreprises (PME), conformément aux objectifs **du projet SECURE**[2] . Pour des conseils techniques et des outils sur la mise en œuvre pratique de ces dispositions, d'autres ressources sont mises à disposition de manière continue sur le **référentiel ouvert SECURE**.

[1] Il s'agit d'une liste non exhaustive destinée à simplifier les obligations découlant du CRA et qui ne mentionne pas les exceptions prévues par ce dernier. Seules les obligations principales y figurent, afin d'offrir une vue d'ensemble. Elles ont été sélectionnées à la suite d'une lecture attentive du texte législatif du CRA.

[2] Le projet « Strengthening EU SMEs Cyber Resilience » (SECURE) offre un soutien financier et des conseils aux PME pour les aider à se conformer au CRA.

Calendrier du CRA :

- Entrée en vigueur : 10 décembre 2024
- Entrée en vigueur des obligations de déclaration : 11 septembre 2026
- Application intégrale des exigences du CRA : 11 décembre 2027

Comprendre les obligations du CRA - CRA 101

1. Évaluation des risques liés à la cybersécurité

Afin de respecter l'obligation de veiller à ce que votre PDE « ait été conçu, développé et fabriqué conformément aux exigences essentielles en matière de cybersécurité énoncées dans la partie I de l'annexe I »[3] – c'est-à-dire en garantissant « un niveau approprié de cybersécurité en fonction des risques »[4] – une évaluation des risques liés à la cybersécurité *doit* être réalisée. Cette évaluation doit être **documentée**[5] et **régulièrement mise à jour** tout au long de la « période de soutien »[6] .

Concrètement, l'évaluation des risques devrait, au minimum, inclure[7] :

1) Une **analyse des risques liés à la cybersécurité** tenant compte :
   - La finalité et l'utilisation prévisible du PDE ;
   - Les conditions d'utilisation (par exemple, l'environnement opérationnel, les actifs à protéger).

2) Une **clarification, une explication et/ou une justification** de
   - L'application de l'[8] de cybersécurité dès la conception – c'est-à-dire comment celle-ci est-elle appliquée ?
   - L'applicabilité (ou la non-applicabilité) des exigences de l'annexe I, partie I, au PDE – c'est-à-dire les exigences de sécurité sont-elles applicables, et de quelle manière ?

[3] Art. 13, paragraphe 1, de la CRA.
[4] Annexe I, partie I, point 1, CRA.
[5] Documentation technique : précisée au point 5.
[6] Période de soutien : précisée au point 2.
[7] Art. 13, paragraphe 3, CRA.
[8] Annexe I, partie I, point 1, CRA.

- L'application et la mise en œuvre des exigences en matière de gestion des vulnérabilités[9] – c'est-à-dire comment les exigences en matière de gestion des vulnérabilités sont-elles appliquées ?

Lorsqu'un PDE contient des composants provenant de tiers, le CRA s'attend à ce que vous fassiez preuve **de diligence raisonnable** pour garantir la cybersécurité du produit final. Cela peut signifier, par exemple, signaler une vulnérabilité que vous avez identifiée au fabricant de ce composant et prendre des mesures supplémentaires pour y remédier. Pour ce faire, une nomenclature logicielle (SBOM)[10] et une politique de divulgation coordonnée des vulnérabilités (CVD) à l'intention des fournisseurs doivent être mises en place et tenues à la disposition des autorités de surveillance du marché sur demande.

2. Gestion des vulnérabilités et mises à jour de sécurité

Comme le stipule l'article 13, paragraphe 8, les fabricants doivent veiller à ce que les vulnérabilités du PDE et de ses composants soient « gérées efficacement et conformément aux exigences essentielles énoncées à l'annexe I, partie II »[11] tout au long de la période de support.

Cela signifie, entre autres[12] :

1) **Identifier et documenter les vulnérabilités** – c'est-à-dire établir la SBOM (au moins pour les dépendances de niveau supérieur) et la tenir à disposition pour la fournir aux autorités de surveillance du marché sur demande[13] ;
2) Traiter et corriger les vulnérabilités sans délai – c'est-à-dire **fournir des mises à jour de sécurité** sans retard injustifié et gratuitement (accompagnées de messages d'avis à l'intention des utilisateurs) :

[9] Annexe I, partie II, CRA.
[10] Un registre officiel des détails et des relations au sein de la chaîne d'approvisionnement des composants inclus dans les éléments logiciels des PDE (art. 3, paragraphe 39, CRA).
[11] Art. 13, paragraphe 8, CRA.
[12] Annexe I, partie II, CRA.
[13] Le partage de ces informations avec les utilisateurs est facultatif.

- Chaque mise à jour de sécurité publiée pendant la période de support doit rester disponible pendant au moins 10 ans après sa publication, ou pendant le reste de la période de support, la durée la plus longue étant retenue[14] .

3) **Réviser et tester** régulièrement la sécurité du produit ;

4) **Partager des informations** sur les vulnérabilités corrigées (et potentielles), leurs impacts et leur gravité, les instructions destinées aux utilisateurs pour y remédier, les coordonnées pour signaler les vulnérabilités, ainsi que mettre en place et appliquer une politique de gestion des vulnérabilités (CVD).

La «période de support» mentionnée ci-dessus «reflète la durée pendant laquelle le produit est censé être utilisé»[15] et doit tenir compte de manière proportionnée des attentes des utilisateurs, de la nature (de la finalité) du PDE et du droit de l'Union applicable.

Concrètement, lorsque vous définissez votre période de support, celle-ci doit être :

- D'au moins cinq ans (à moins que la durée de vie du produit ne soit inférieure à cinq ans, auquel cas la période de support est égale à la durée de vie du produit) ;
- clairement spécifiée (date de fin : mois et année) au moment de l'achat/sur l'emballage/sous forme numérique (une fois cette date atteinte, les utilisateurs devraient idéalement en être informés)[16] .

La détermination et la définition de la période de support doivent figurer dans la documentation technique[17] .

3. Informations destinées aux utilisateurs, instructions et point de contact unique

Conformément à l'article 13, paragraphes 14 à 18, et à l'annexe II, les fabricants *doivent*, au minimum, **informer clairement les utilisateurs** en indiquant sur support papier/numérique :

- les coordonnées du fabricant (nom, dénomination sociale ou marque déposée, adresse postale, adresse électronique ou coordonnées numériques, site web) ;

[14] Art. 13, paragraphe 9, CRA.
[15] Art. 13, paragraphe 8, CRA.
[16] Art. 13, paragraphe 19, CRA.
[17] Documentation technique : précisée au point 5.

- les coordonnées du PDE (nom, type, usage prévu, environnement de sécurité et propriétés de sécurité, fonctionnalités essentielles, risques potentiels en matière de cybersécurité, assistance technique en matière de sécurité fournie, date de fin de la période de support) ;
- des instructions détaillées ou un lien vers celles-ci (concernant les mesures d'utilisation sécurisée, les effets possibles sur la sécurité des données dus à des modifications du produit, l'installation des mises à jour de sécurité, la mise hors service sécurisée et la suppression des données utilisateur, les paramètres d'installation par défaut des mises à jour de sécurité) ;
- Un point de contact unique (SPOC) doit être désigné pour permettre aux utilisateurs de:
    - Communiquer directement et rapidement avec le fabricant par le moyen de communication de son choix (sans se limiter aux outils automatisés) ;
    - Signaler les vulnérabilités ;
    - Indiquer l'emplacement de la politique CVD.
- Liens (le cas échéant) vers la politique en matière de vulnérabilités, la déclaration de conformité de l'UE (EU DoC)[18] , la SBOM (si elle est mise à la disposition des utilisateurs).

Les instructions d'utilisation doivent être disponibles dans un langage facilement compréhensible, en ligne ou sur papier, pendant au moins dix ans ou pendant la période de support (la plus longue des deux prévalant).

4. Obligations de signalement : signalement des vulnérabilités et des incidents

En ce qui concerne les obligations de signalement[19] , le tableau ci-dessous présente un aperçu de vos obligations. Vous trouverez ci-dessous des précisions supplémentaires.

[18] Déclaration de conformité UE : précisée au point 5.

[19] Art. 14-17, CRA.

Tableau 1 :

Signalement des vulnérabilités et des incidents

Signalement	Vulnérabilités	Incidents
QUOI	*Obligatoire :* « vulnérabilités activement exploitées » *Facultatif :* vulnérabilités (non activement exploitées) ; cybermenaces	*Obligatoire* : « incidents graves » *Facultatif* : incidents (non graves) ; incidents évités de justesse
À QUI	CSIRT[20] Plateforme de signalement unique (ENISA) Utilisateurs concernés	
COMMENT	1) Notification d'alerte précoce (24 h) 2) Notification de vulnérabilité (72 h) 3) Rapport final (14 jours)	1) Notification d'alerte précoce (24 h) 2) Notification d'incident (72 h) 3) Rapport final (1 mois)

4.1. Quoi

Selon les définitions énoncées à l'article 3 du CRA,

- Une « vulnérabilité activement exploitée » nécessite des preuves fiables d'exploitation par un acteur malveillant dans un système sans l'autorisation de son propriétaire[21] ;

[20] Art. 3, paragraphe 51, CRA : « CSIRT désigné comme coordinateur » désigne un CSIRT désigné comme coordinateur conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555.

[21] Art. 3, point 42, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Un incident est considéré comme « grave » lorsqu'il[22] :
    - A un impact négatif ou est susceptible d'avoir un impact sur la capacité du PDE à protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou des fonctions ; ou
    - A conduit ou peut conduire à l'introduction/l'exécution de code malveillant dans le produit ou dans le réseau et les systèmes d'information d'un utilisateur.

4.2. À qui

L'équipe d'intervention en cas d'incident de sécurité informatique (CSIRT) à laquelle l'incident doit être signalé est celle de l'État membre dans lequel le fabricant[23] :

- Possède son établissement principal ; ou, si cela ne peut être déterminé,
- possède l'établissement comptant le plus grand nombre d'employés.

Si le fabricant est situé en dehors de l'UE, une chaîne de secours peut être suivie, qui prend en compte l'établissement du mandataire du fabricant → importateur → distributeur → là où se trouve le plus grand nombre de PDE ou d'utilisateurs.

Sous réserve de quelques exceptions, toutes les notifications passeront par la plateforme de signalement unique, qui doit encore être mise en place et gérée par l'Agence de l'Union européenne chargée de la cybersécurité (ENISA), et seront diffusées aux autres CSIRT et aux autorités de surveillance du marché via un point de terminaison de notification électronique.

Les utilisateurs concernés (et, le cas échéant, tous les utilisateurs) doivent également être informés des vulnérabilités/incidents et des mesures à prendre, de préférence dans un format lisible par machine. Les CSIRT peuvent informer les utilisateurs si le fabricant ne le fait pas[24] .

[22] Art. 3, point 44, CRA ; art. 14, paragraphe 5, CRA.

[23] Le CSIRT est généralement le CERT national : Computer Emergency Response Team.

[24] Art. 14, paragraphe 8, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.3. Comment

Il existe plusieurs différences dans la notification des vulnérabilités et des incidents.

Vulnérabilités

1) **Notification d'alerte précoce** : doit être soumise au plus tard dans les 24 heures suivant la prise de connaissance et doit indiquer, le cas échéant, les États membres où le PDE est disponible.
2) **Notification de vulnérabilité** : doit être soumise au plus tard dans les 72 heures suivant la prise de connaissance et doit inclure :
    - des informations générales sur le PDE ;
    - Nature générale de la vulnérabilité ;
    - Mesures correctives ou d'atténuation prises ou pouvant être prises par les utilisateurs ;
    - Sensibilité des informations notifiées.
3) **Rapport final** : doit être soumis au plus tard **14 jours** après la mise en œuvre des mesures correctives/d'atténuation et doit inclure :
    - Description – gravité et impact ;
    - Informations sur l'acteur malveillant, le cas échéant ;
    - Détails sur la mise à jour de sécurité ou toute autre mesure corrective disponible.

Incidents

1) **Notification d'alerte précoce** : doit être soumise au plus tard dans les 24 heures suivant la prise de connaissance et doit indiquer,
    - le cas échéant, les États membres dans lesquels le PDE est disponible ;
    - s'il existe des soupçons quant à une cause liée à des actes illicites ou malveillants.
2) **Notification d'incident** : doit être soumise au plus tard dans les 72 heures suivant la prise de connaissance et doit inclure :
    - des informations générales sur la nature de l'incident ;
    - une évaluation initiale de l'incident ;

- Les mesures correctives ou d'atténuation prises ou pouvant être prises par les utilisateurs ;
- le niveau de sensibilité des informations notifiées.

3) **Rapport final** : doit être soumis dans un délai d'un mois à compter de la notification de l'incident et doit inclure :
    - Description – gravité et impact ;
    - Type de menace ou cause profonde susceptible d'avoir provoqué l'incident ;
    - Mesures d'atténuation appliquées et en cours.

5. Évaluation de la conformité

Avant la mise sur le marché d'un PDE, le fabricant doit démontrer que celui-ci est conforme aux exigences essentielles en matière de cybersécurité énoncées à l'annexe I du CRA. Cela s'effectue par le biais de **la procédure d'évaluation de la conformité** applicable à la catégorie de produit concernée.

5.1. Procédures d'évaluation de la conformité

Le CRA prévoit, entre autres :

- un contrôle interne (module A) ;
- l'examen CE de type suivi de la conformité au type (modules B + C) ;
- Assurance qualité complète (module H) ;
- Évaluation dans le cadre d'un système européen de certification en matière de cybersécurité, le cas échéant.

Les normes harmonisées et les spécifications communes ne constituent pas des procédures de conformité. Elles peuvent toutefois faciliter la démonstration de la conformité.

5.2. Présomption de conformité

Un produit qui est conforme aux

- des normes harmonisées dont les références ont été publiées au Journal officiel, ou

- des spécifications communes adoptées par la Commission européenne

est **présumé conforme**[25] aux exigences essentielles couvertes par ces normes ou spécifications.

Lorsque ces normes ou spécifications ne sont pas (entièrement) appliquées, le fabricant doit démontrer directement la conformité aux exigences de l'annexe I par le biais de la procédure d'évaluation de la conformité applicable. Le cas échéant, un certificat européen de cybersécurité peut également être utilisé pour démontrer la conformité, dans les limites prévues par l'ACR.

5.3. Catégories de produits

La procédure d'évaluation de la conformité à appliquer dépend de la classification du PDE au titre du CRA, telle que précisée aux annexes III et IV du CRA[26] . Le CRA distingue les produits par défaut, les produits importants (classes I et II) et les produits critiques.

Selon la catégorie :

- un contrôle interne peut suffire ;
- L'intervention d'un organisme notifié (ON) peut être requise ; ou
- Une évaluation dans le cadre d'un système de certification européen peut être obligatoire ou autorisée.

La classification correcte est donc déterminante pour définir la procédure applicable.

Le tableau 2 de la page ci-dessous présente un aperçu des procédures pouvant s'appliquer à chaque classe de produits.

[25] Art. 27, CRA.

[26] Art. 32, CRA ; Annexe VIII, CRA.

Tableau 2 :
Procédures d'évaluation de la conformité

	Contrôle interne (module A)	Examen de type UE suivi d'une vérification de la conformité au type (modules B + C)	Assurance qualité complète (module H)	Système européen de certification en matière de cybersécurité	Normes harmonisées/ Spécifications communes[27]
Produits par défaut	X	X	X	X	X Peut fournir une assistance en matière de conformité pour les exigences couvertes
Produits importants de classe I	X[28]	X	X	X niveau : substantiel[29]	X Peut apporter un soutien à la conformité pour les exigences couvertes
Produits importants de classe II		X	X	X niveau : substantiel[30]	X Peut apporter un soutien à la conformité pour les exigences couvertes
Produits critiques				X niveau : substantiel	X Peut fournir une assistance en matière de conformité pour les exigences couvertes

[27] Les normes harmonisées et les spécifications communes ne constituent pas des procédures, mais peuvent servir à démontrer la conformité.

[28] Le contrôle interne (module A) ne peut être utilisé que lorsque des normes harmonisées, des spécifications communes ou, le cas échéant, un système de certification pertinent sont appliqués. Si ce n'est pas le cas, les voies applicables sont l'examen de type UE suivi de la conformité au type (modules B+C) ou l'assurance qualité complète (module H).

[29] Si, en vertu de l'article 8, paragraphe 1, du CRA, un acte délégué est adopté, le système de certification cyber de l'UE peut être utilisé. Dans le cas contraire, il convient de se rabattre sur les règles relatives aux produits importants de classe II.

[30] La note de bas de page 29 s'applique.

5.4. Déclaration de conformité UE (EU DoC)

Une fois l'évaluation de la conformité réussie, le fabricant établit une **déclaration de conformité UE** (EU DoC)[31] .

Dans cette déclaration, vous confirmez que le PDE est conforme aux exigences essentielles applicables et comprend les éléments requis prévus par le CRA. La structure type figure à l'annexe V du CRA. La DoC UE simplifiée figure à l'annexe VI. Elle doit être mise à disposition dans les langues requises par l'État membre dans lequel le PDE est mis sur le marché et doit rester disponible pendant la période légalement prescrite.

5.5. Marquage CE

Afin de permettre aux consommateurs d'identifier les PDE qui satisfont aux exigences du CRA et de prendre des décisions éclairées lors de l'achat et de l'utilisation de ces PDE, un **marquage CE**[32] doit être « apposé de manière visible, lisible et indélébile »[33] avant la mise sur le marché du PDE. Cela doit être effectué sur le produit lui-même. Lorsque cela n'est pas possible en raison de la nature du produit, il doit être apposé sur l'emballage et figuré dans la déclaration de conformité UE qui l'accompagne[34] [35] . Le marquage CE indique que le produit est conforme à toute la législation de l'Union applicable exigeant le marquage CE, y compris le CRA.

5.6. Démonstration de la conformité au moyen de la documentation technique

La documentation technique est un élément clé de l'évaluation de la conformité**.** Rétablie par l'article 31 du CRA et l'annexe VII, la documentation technique concerne tous les points abordés précédemment, car elle doit être établie avant la mise sur le marché du PDE et mise à jour en continu tout au long de la période de support[36] . Regroupant la majorité des obligations du CRA, la documentation technique doit donc inclure[37] :

[31] Article 28 du CRA ; annexes V et VI du CRA.
[32] Marquage «Conformité Européenne» (CE).
[33] Article 30, paragraphe 1, du CRA.
[34] Art. 29-30, CRA.
[35] Des règles supplémentaires s'appliquent si un organisme notifié participe à l'évaluation de la conformité.
[36] Art. 31, paragraphe 2, CRA.
[37] Annexe VII, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- une description générale du PDE (usage prévu, versions logicielles ayant une incidence sur la conformité, preuves des caractéristiques externes, marquage et disposition interne pour les produits matériels, informations et instructions destinées à l'utilisateur) ;
- une description de la conception, du développement et de la production du PDE, ainsi que des processus de gestion des vulnérabilités (par exemple, description de l'architecture du système, SBOM, politique CVD, processus de surveillance, etc.) ;
- Évaluation des risques de cybersécurité ;
- Définition et clarification de la période de support ;
- Normes harmonisées appliquées (ou parties de celles-ci) ;
- Rapports d'essais de conformité et rapports de gestion des vulnérabilités ;
- Copie de la déclaration de conformité (DoC) de l'UE.

Un formulaire **simplifié de documentation technique** doit être élaboré par la Commission européenne à l'intention des micro-entreprises et des petites entreprises[38] . En outre, l'article 33 stipule que tant les États membres que la Commission européenne doivent apporter **leur soutien aux PME**, notamment sous la forme de conseils[39] et de possibilités d'aide financière.

Le **projet SECURE offre un soutien financier aux PME tenues de se conformer au CRA et fournit régulièrement des lignes directrices et des ressources destinées à aider les PME à mettre en œuvre le CRA**, comme le présent guide CRA101.

[38] Art. 33, paragraphe 5, CRA.

[39] Art. 26, CRA.

Conclusion

Afin de fournir un **aperçu accessible des principales obligations énoncées dans le CRA**, ce guide se concentre sur **cinq éléments** du CRA à prendre en compte au minimum : (1) l'évaluation des risques de cybersécurité ; (2) la gestion des vulnérabilités et les mises à jour de sécurité ; (3) les informations destinées aux utilisateurs, les instructions et le point de contact unique ; (4) Obligations de notification : notification des vulnérabilités et des incidents ; (5) Évaluation de la conformité. Il clarifie des éléments tels que la période de support, la déclaration de conformité de l'UE et le marquage CE, ainsi que la documentation technique. Dans le but **d'aider les PME à s'y retrouver dans le cadre juridique complexe**, ce guide propose un résumé des principales obligations légales qui doivent être comprises avant leur mise en œuvre. Pour des conseils pratiques sur la manière d'aborder et de mettre en œuvre ces dispositions légales, ainsi que sur des éléments particuliers du CRA (par exemple, la SBOM, la gestion des vulnérabilités, etc.), des lignes directrices techniques et des outils supplémentaires seront mis à disposition de manière continue sur le **référentiel central SECURE**, à mesure que la mise en œuvre du CRA progressera. Dans un deuxième temps, il est recommandé aux PME de consulter les autres lignes directrices disponibles sur le référentiel SECURE, telles que « **Exigences essentielles en matière de cybersécurité de la législation sur la cyber-résilience (CRA): Annexe I, Partie I et »** pour obtenir des suggestions et des recommandations pratiques sur chacune des dispositions de l'annexe I, ainsi que le **« CRA Methodological Compliance Assessment Framework »** pour disposer d'une boîte à outils et d'une liste de contrôle étape par étape sur la conformité au CRA au-delà de l'annexe I.