SECURE
Cyber Resilience for SMEs

Cadre méthodologique pour l'évaluation de la conformité au CRA.

20/10/2025

Funded by the European Union

Déclaration de financement de l'UE : Financé par l'Union européenne sous le numéro GA n° 101190325.
Les points de vue et opinions exprimés ne reflètent toutefois que celles de l'auteur ou des auteurs et ne reflètent pas nécessairement celles de l'Union européenne ou du Centre européen de compétences pour la cybersécurité industrielle, technologique et de recherche. Ni l'Union européenne ni l'autorité qui octroie le financement ne peuvent en être tenues responsables..

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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

AVERTISSEMENT

Table des matières

Introduction 9

Cadre méthodologique pour l'évaluation de la conformité au CRA 10

1. Conformité aux exigences essentielles en matière de cybersécurité 10

1.1. Exigences en matière de cybersécurité des produits 10

1.1.1. Absence de vulnérabilités exploitables connues 10

1.1.2. Configurations par défaut sécurisées 12

1.1.3. Mises à jour de sécurité rapides 13

1.1.4. Protection contre les accès non autorisés 14

1.1.5. Confidentialité, intégrité et disponibilité des données 15

1.1.6. Minimisation des données et réduction de la surface d'attaque 16

1.1.7. Atténuation des incidents et journalisation 17

1.1.8. Suppression des données utilisateur 18

1.2. Exigences en matière de gestion des vulnérabilités 19

1.2.1. Nomenclature logicielle (SBOM) 19

1.2.2. Correction rapide des vulnérabilités 20

1.2.3. Tests de sécurité réguliers 21

1.2.4. Transparence dans la divulgation des vulnérabilités 22

1.2.5. Politique de divulgation coordonnée des vulnérabilités (CVD) 23

1.2.6. Mises à jour de sécurité gratuites 24

1.3. Liste de contrôle recommandée pour l'auto-évaluation 25

1.4. Étude de cas 26

1.5. Outils et ressources 27

2. Certification des produits contenant des éléments numériques 28

2.1. Systèmes de certification et normes 28

2.2. Méthodologie d'auto-évaluation 29

2.3. Mesures pratiques pour les PME 29

2.4. Étude de cas 30

2.5. Modèle de feuille de route de certification 30
2.6. Outils et ressources 30
3. Classification des produits : parcours de mise en conformité 32
3.1. Comprendre la classification des produits 32
3.2. Méthodologie d'auto-évaluation 32
3.3. Voies de mise en conformité 33
3.4. Mesures pratiques pour les PME 34
3.5. Étude de cas 34
3.6. Outils et ressources 35
4. Documentation technique et évaluation des risques 36
4.1. Exigences en matière de documentation 36
4.2. Méthodologie d'auto-évaluation 36
4.3. Mesures concrètes pour les PME 37
4.4. Étude de cas 38
4.5. Outils et ressources 38
5. Processus d'évaluation de la conformité et déclaration de conformité UE 39
5.1. Modules d'évaluation de la conformité 39
5.2. Méthodologie d'auto-évaluation 40
5.3. Étapes pratiques pour les PME 41
5.4. Étude de cas 41
5.5. Outils et ressources 41
Conclusion 42

Liste des tableaux et figures

Tableau 1 : Modèle de registre de gestion des vulnérabilités 11
Tableau 2 : Modèle de liste de contrôle de configuration 133
Tableau 3 : Modèle de journal des mises à jour 14
Tableau 4 : Politique de contrôle d'accès aux modèles 15
Tableau 5 : Conformité au chiffrement des modèles 166
Tableau 6 : Résumé de l'AIPD du modèle 17
Tableau 7 : Configuration de la journalisation des modèles 18
Tableau 8 : Vérification de la suppression des données du modèle 19
Tableau 9 : Résumé de la SBOM du modèle 20
Tableau 10 : Modèle de journal de correction des vulnérabilités 21
Tableau 11 : Modèle de calendrier des tests de sécurité 222
Tableau 12 : Modèle d'avis de sécurité 233
Tableau 13 : Modèle de politique CVD 244
Tableau 14 : Modèle de politique de support 25
Tableau 15 : Exemple de mise en correspondance 29
Tableau 16 : Modèle de feuille de route de certification 30
Tableau 17 : Exemple d'arbre de décision 333
Tableau 18 : Modèle d'évaluation des risques 344
Tableau 19 : Modèle de liste de contrôle de la documentation 377
Tableau 20 : Modèle de déclaration de conformité (DoC) de l'UE 40

Abréviations

AES – Norme de chiffrement avancée (Advanced Encryption Standard)

API – Interface de programmation d'application (Application Programming Interface

CI/CD – Intégration continue et livraison/déploiement continus (Continuous Integrations and Delivery/Deployment)

CIS – Centre for Internet Security

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)

CVE – Vulnérabilités et expositions communes (Common Vulnerabilities and Exposures)

CVSS – Système commun d'évaluation des vulnérabilités (Common Vulnerability Scoring System)

CWS – Énumération commune des faiblesses (Common Weakness Enumeration)

DDoS – Déni de service distribué (Denial of Service)

DMS – Système de gestion documentaire (Document Management System)

DPIA – Analyse d'impact relative à la protection des données (Data Protection Impact Assessment)

ECDSA – Algorithme de signature numérique à courbe elliptique (Elliptic Curve Digital Signature Algorithm)

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

ETSI – Institut européen de normalisation technique (European Technical Standards Institute)

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

EUCS – Sécurité du cloud de l'UE (EU Cloud Security)

FTP – Protocole de transfert de fichiers (File Transfer Protocol)

GDPR – Règlement général sur la protection des données (General Data Protection Regulation)

IDS – Système de détection d'intrusion (Intrusion Detection System)

IEC – Commission électrotechnique internationale (International Electrotechnical Commission)

IoT – Internet des objets (Internet of Things)

IPS – Système de prévention des intrusions (Intrusion Prevention System)

ISO – Organisation internationale de normalisation (International Standards Organisation)

MFA – Authentification multifactorielle (Multi-factor authentication)

NB – Organisme notifié (Notified Body)

NIST – Institut national des normes et des technologies (États-Unis) (National Institute of Standards and Technology)

NIST NVD – Base de données nationale des vulnérabilités du NIST (NIST National Vulnerability Database)

OCTAVE – Évaluation des menaces, des actifs et des vulnérabilités critiques sur le plan opérationnel (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OTA – A distance (Over The Air)

OWASP – Projet mondial ouvert sur la sécurité des applications (Open Worldwide Application Security Project)

OWASP ESAPI – API de sécurité d'entreprise de l'OWASP (OWASP Enterprise Security API)

OWASP SAMM – Modèle de maturité de l'assurance logicielle de l'OWASP (OWASP Software Assurance Maturity Model)

OWASP ZAP – Proxy d'attaque OWASP Zed (OWASP Zed Attack Proxy)

PASTA – Processus de simulation d'attaques et d'analyse des menaces (Process for Attack Simulation and Threat Analysis)

PDE – Produit comportant des éléments numériques (Product with Digital Elements)

PSIRT – Équipe d'intervention en cas d'incident de sécurité des produits (Product Security Incident Response Team)

RBAC – Contrôle d'accès basé sur les rôles (Role-Based Access Control)

SBOM – Nomenclature logicielle (Software Bill of Materials)

SDLC – Cycle de vie du développement sécurisé (Secure Software Development Lifecycle)

SIEM – Gestion des informations et des événements de sécurité (Security Information and Event Management)

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

SNMP – Protocole simple de gestion de réseau (Simple Network Management Protocol)

SPDX – Échange de données sur les paquets système (System Package Data Exchange)

SQL – Langage de requêtes structurées (Structured Query Language)

SSL – Couche de sockets sécurisés (Secure Sockets Layer)

STRIDE – Usurpation d'identité, altération, répudiation, divulgation d'informations, déni de service, élévation de privilèges (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)

TLS – Sécurité de la couche de transport (Transport Layer Security)

UPnP – Plug-and-Play universel (Universal Plug and Play)

VPN – Réseau privé virtuel (Virtual Private Network)

XSS – Cross-site Scripting

Introduction

La loi sur la cyber-résilience (CRA) de l'Union européenne, le règlement (UE) n° 2024/2847, établit un cadre complet visant à garantir la sécurité des produits comportant des éléments numériques (PDE) tout au long de leur cycle de vie, de leur conception à leur mise au rebut. Afin **d'aider les petites et moyennes entreprises (PME) à évaluer et à améliorer leur niveau de conformité au CRA**, le présent document propose un cadre méthodologique d'auto-évaluation de la conformité. Il fait partie des ressources fournies par le **projet SECURE**[1] , qui vise à accompagner les PME dans la mise en œuvre de la CRA. À travers un cadre très détaillé, **cinq critères clés** sont développés : (1) la conformité aux exigences essentielles en matière de cybersécurité, (2) certification des produits comportant des éléments numériques, (3) classification des produits en classe I ou classe II et mesures correspondantes, (4) exhaustivité de la documentation technique, et (5) procédures globales d'évaluation de la conformité. Chaque section est enrichie de conseils approfondis, d'exemples pratiques, d'études de cas, de listes de contrôle, ainsi que de références à des modèles, des outils et des normes, garantissant ainsi que les PME puissent s'acquitter efficacement de leurs obligations au titre de la CRA grâce à des stratégies concrètes adaptées à leurs contraintes en matière de ressources. Toutefois, ces éléments restent tous de **nature suggestive**, proposant des recommandations fondées sur des approches reconnues et des bonnes pratiques afin d'accompagner les PME dans leur démarche de mise en conformité. Les références aux outils et cadres existants doivent être considérées à titre d'illustration. Le présent guide est susceptible d'être mis à jour à mesure que le cadre législatif du CRA évolue.

[1] Le projet « Renforcement de la cyber-résilience des PME de l'UE » (SECURE) propose un soutien financier et des conseils aux PME afin de les aider à se conformer au CRA.

Cadre méthodologique pour l'évaluation de la conformité au CRA

1. Conformité aux exigences essentielles en matière de cybersécurité

Le critère **de conformité aux exigences essentielles en matière de cybersécurité** constitue la pierre angulaire de la conformité au CRA ; il garantit que les produits comportant des éléments numériques répondent à des normes strictes de cybersécurité pour pouvoir être mis sur le marché de l'UE. L'annexe I du règlement CRA spécifie 13 **exigences de cybersécurité applicables aux produits** et 8 **exigences relatives à la gestion des vulnérabilités**, soit un total de 21 exigences essentielles. Cette section fournit une méthodologie exhaustive permettant aux PME d'évaluer leur conformité, de documenter leurs preuves, d'identifier les lacunes et d'élaborer des plans de remédiation. Elle comprend des explications détaillées, des outils pratiques, des études de cas, des modèles et des instructions étape par étape afin de garantir une évaluation et une conformité rigoureuses.

1.1. Exigences en matière de cybersécurité des produits

Les exigences en matière de cybersécurité des produits imposent que ceux-ci soient conçus et développés en plaçant la sécurité au cœur de leur conception («sécurisé dès la conception et par défaut»). Ces exigences garantissent que les produits sont exempts de vulnérabilités exploitables connues, disposent de configurations par défaut sécurisées, prennent en charge les mises à jour de sécurité en temps opportun et protègent la confidentialité, l'intégrité et la disponibilité des données. Vous trouverez ci-dessous une analyse complète des exigences[2] , accompagnée de conseils détaillés, d'exemples, d'outils et de méthodologies.

1.1.1. Absence de vulnérabilités exploitables connues

Les fabricants doivent s'assurer que leurs produits ne présentent aucune vulnérabilité exploitable connue au moment de leur mise sur le marché, ce qui nécessite des tests rigoureux avant la mise sur le marché, notamment des analyses de vulnérabilité, des tests d'intrusion et des revues de code. Les PME, souvent limitées en ressources, peuvent tirer parti d'outils de test et d'analyse de sécurité rentables (par exemple, un scanner dynamique d'applications web, un scanner de vulnérabilités réseau, un outil de test de sécurité statique des applications et un scanner d'images de conteneurs) pour identifier les problèmes. Par exemple, un fabricant de serrures intelligentes doit tester les vulnérabilités Bluetooth, telles que les protocoles d'appairage faibles ou les attaques par rejeu, et

[2] Certaines des exigences de l'annexe I du CRA qui se recoupent ont été regroupées dans la présente ligne directrice, ce qui a donné lieu à une liste de huit obligations concrètes.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

consigner les mesures correctives dans un journal de gestion des vulnérabilités. Les tests doivent s'aligner sur des normes telles que **l'OWASP Top 10** ou **le CWE/SANS Top 25** afin de couvrir les vulnérabilités courantes.

Conseils détaillés :

- **Analyse des vulnérabilités** : utilisez OpenVAS ou Nessus pour rechercher les CVE, en programmant des analyses toutes les deux semaines pendant la phase de développement. Les PME peuvent accéder à des versions gratuites d'outils tels que Trivy pour les applications basées sur des conteneurs.
- **Tests d'intrusion** : effectuez des tests manuels ou automatisés à l'aide d'outils tels que Metasploit ou faites appel à des prestataires tiers pour des évaluations trimestrielles. Concentrez-vous sur les domaines à haut risque tels que l'authentification ou les interfaces réseau.
- **Révisions de code** : utilisez SonarQube pour détecter les vulnérabilités au niveau du code, telles que les injections SQL ou les attaques de type « cross-site scripting » (XSS). Mettez en place des révisions par les pairs pour les composants critiques.
- **Documentation** : tenez à jour un journal de gestion des vulnérabilités comportant des colonnes pour l'identifiant CVE, le score CVSS, le composant affecté, la mesure corrective et le statut. Utilisez des outils tels que Jira ou Trello pour le suivi.
- **Plan de correction** : pour les vulnérabilités non corrigées, établissez des priorités en fonction des scores CVSS (par exemple, > 7,0 pour les vulnérabilités critiques) et fixez des délais de correction (par exemple, 30 jours pour les problèmes critiques).

Étude de cas : Une PME développant un thermostat intelligent effectue un scan de vulnérabilités à l'aide de Nessus, identifiant un protocole de chiffrement faible (TLS 1.1). La PME passe à TLS 1.3, teste la correction avec OWASP ZAP et documente le processus dans un journal, en incluant les scores CVSS et les rapports de test. L'auto-évaluation confirme qu'il ne reste aucune vulnérabilité connue, ce qui est corroboré par un rapport de test d'intrusion réalisé par un prestataire tiers.

Tableau 1 :
Modèle de journal de gestion des vulnérabilités

Identifiant CVE	Score CVSS	Composant	Description	Mesure corrective	Statut	Date de résolution

CVE-2025-1234	8.5	TLS 1.1	Chiffrement faible	Mise à niveau vers TLS 1.3	Résolu	15 juin 2025

1.1.2. Configurations par défaut sécurisées

Les produits doivent être livrés avec des paramètres par défaut renforcés afin de minimiser les risques, par exemple en désactivant les services inutiles, en utilisant des mots de passe forts et en fermant les ports ouverts. Les PME doivent se conformer à **la norme ETSI EN 303 645**, qui fournit des lignes directrices spécifiques à l'IoT, ou **aux benchmarks CIS** pour des technologies spécifiques (par exemple, Linux, Docker). Par exemple, une caméra domestique connectée devrait désactiver l'accès à distance par défaut, exiger des mots de passe uniques et fermer les ports inutilisés tels que Telnet.

Conseils détaillés :

- **Vérification de la configuration** : élaborez une liste de contrôle basée sur la norme ETSI EN 303 645, afin de vérifier des paramètres tels que la désactivation des modes de débogage, l'absence d'identifiants par défaut et la fermeture des ports. Utilisez des outils permettant d'effectuer des contrôles de renforcement de la sécurité du système.
- **Analyse des ports** : utilisez **Nmap** pour identifier les ports et services ouverts, en veillant à ce que seuls ceux qui sont nécessaires soient actifs. Par exemple, désactivez le protocole FTP s'il n'est pas requis.
- **Politiques en matière de mots de passe** : mettez en place des mots de passe par défaut forts ou obligez les utilisateurs à en définir lors de la configuration. Utilisez des outils de vérification de la force des mots de passe.
- **Documentation** : incluez les paramètres de configuration dans le dossier technique, en faisant référence à des normes telles que les benchmarks CIS. Documentez les écarts et leurs justifications.
- **Conseils aux utilisateurs** : fournissez des instructions de configuration dans les manuels d'utilisation, en expliquant comment maintenir des configurations sécurisées (par exemple, en désactivant le Wi-Fi invité).

Étude de cas : une PME fabriquant des routeurs Wi-Fi s'assure que les paramètres par défaut désactivent l'UPnP et Telnet, en utilisant Nmap pour vérifier que les ports sont fermés. La liste de

contrôle d'auto-évaluation confirme la conformité à la norme ETSI EN 303 645, clause 5.1, étayée par un rapport de configuration et les instructions du manuel d'utilisation.

Tableau 2 :
Modèle de liste de contrôle de configuration

Paramètre	Exigence	Statut	Justificatif	Remarques
UPnP	Désactivé	Conforme	Rapport d'analyse Nmap	Vérifié 10/06/2025

1.1.3. Mises à jour de sécurité rapides

Les produits doivent prendre en charge les mises à jour de sécurité automatiques avec des options permettant à l'utilisateur de se désinscrire. Les PME peuvent utiliser des mécanismes de mise à jour **par liaison radio (OTA)** via des plateformes telles que **Mender.io, AWS IoT Device Management** ou **Balena**. Les mises à jour doivent être signées et vérifiées à l'aide d'outils tels **qu'OpenSSL** afin d'empêcher toute altération. Par exemple, un fabricant d'appareils portables doit s'assurer que les mises à jour du micrologiciel corrigent les vulnérabilités dans les 30 jours suivant leur découverte, avec des notifications claires à l'intention des utilisateurs.

Conseils détaillés :

- **Infrastructure de mise à jour** : mettez en place un serveur de mise à jour OTA ou utilisez des solutions basées sur le cloud. Assurez-vous que les mises à jour sont signées avec RSA-2048 ou ECDSA.
- **Test des mises à jour** : vérifiez que les mises à jour s'installent sans perturber le fonctionnement, à l'aide d'environnements de test tels que **Docker**. Effectuez des tests de régression pour garantir la compatibilité.
- **Notification des utilisateurs** : utilisez des e-mails, des notifications intégrées à l'application ou des voyants LED pour informer les utilisateurs des mises à jour. Fournissez des instructions de désactivation dans les manuels d'utilisation.
- **Documentation** : inclure la fréquence des mises à jour, les mécanismes de signature et les procédures de notification des utilisateurs dans le dossier technique. Consigner l'historique des mises à jour avec les horodatages et les CVE corrigés.

- **Indicateurs de conformité** : Suivez les délais de déploiement des mises à jour (par exemple, < 30 jours pour les correctifs critiques) et les taux d'adoption par les utilisateurs.

Étude de cas : une PME spécialisée dans les enceintes connectées utilise Mender.io pour déployer des mises à jour de micrologiciel signées, corrigeant un CVE en moins de 25 jours. L'auto-évaluation documente le processus OTA, la notification des utilisateurs par e-mail et les résultats des tests de régression, garantissant ainsi la conformité aux exigences du CRA.

Tableau 3 :
Modèle de journal des mises à jour

ID de mise à jour	CVE corrigé	Date de publication	Heure de déploiement	Notification aux utilisateurs	Statut
V2.1.3	CVE 2025-5678	01/07/2025	25 jours	E-mail envoyé le 30 juin 2025	Déployé

1.1.4. Protection contre les accès non autorisés

Des mécanismes d'authentification forts, tels que **l'authentification multifactorielle (MFA)**, **OAuth 2.0** ou **OpenID Connect**, sont essentiels pour empêcher tout accès non autorisé. Les PME peuvent utiliser **les jetons Web JSON (JWT)** pour sécuriser leurs API et **le contrôle d'accès basé sur les rôles (RBAC)** pour limiter les autorisations. Des outils tels que **Burp Suite** ou **Postman** permettent de simuler des attaques afin de tester les contrôles d'accès. Par exemple, un appareil IoT connecté au cloud devrait exiger l'authentification multifactorielle (MFA) pour les comptes utilisateurs et utiliser des jetons JWT pour les points de terminaison des API.

Conseils détaillés :

- **Mettre en place l'authentification** : utilisez des bibliothèques d'authentification multifactorielle telles **qu'Auth0** ou **Okta** pour les comptes utilisateurs. Mettez en place les JWT pour les API, conformément à la norme RFC 7519.
- **Tester les contrôles d'accès** : réaliser des tests d'intrusion avec Burp Suite pour simuler des attaques par force brute ou par détournement de session. Utiliser des outils tels que **Wireshark** pour surveiller le trafic réseau.
- **Documenter les politiques** : inclure les politiques d'authentification et de contrôle d'accès dans le dossier technique, en détaillant les protocoles (par exemple, OAuth 2.0) et les configurations RBAC.

- **Surveiller les accès** : activez la journalisation des tentatives d'accès à l'aide de **Syslog** ou **de la pile ELK**, avec des alertes en cas d'activité suspecte (par exemple, plusieurs échecs de connexion).
- **Audits réguliers** : planifiez des audits trimestriels des contrôles d'accès, à l'aide d'outils tels que **HashiCorp Vault** pour la gestion des identifiants.

Étude de cas : une PME développant une sonnette connectée met en œuvre l'authentification multifactorielle (MFA) à l'aide d'Auth0 et la teste avec Burp Suite, ce qui lui permet d'identifier et de corriger une faille dans la gestion des sessions. L'auto-évaluation inclut les politiques d'authentification, les rapports de test et les configurations des journaux.

Tableau 4 :
Modèle de politique de contrôle d'accès

Composant	Authentification	Contrôle d'accès	Méthode de test	Preuve	Statut
Connexion utilisateur	MFA (Auth0)	RBAC (Admin/Utilisateur)	Burp Suite	Rapport de test du 20 juin 2025	Conforme

1.1.5. Confidentialité, intégrité et disponibilité des données

Le chiffrement est essentiel pour protéger les données. Les PME doivent mettre en œuvre **le chiffrement AES-256** pour les données au repos et **le protocole TLS 1.3** pour les données en transit, conformément à **la norme NIST SP 800-52**. La validation des entrées doit empêcher les attaques par injection, à l'aide de bibliothèques telles que **OWASP ESAPI**. Par exemple, un appareil de surveillance médicale doit chiffrer les données des patients pour se conformer au RGPD et au CRA, garantissant ainsi leur confidentialité et leur intégrité.

Recommandations détaillées :

- **Choisissez des normes de chiffrement** : utilisez l'AES-256 pour le stockage et le TLS 1.3 pour les communications. Mettez en place une gestion des clés avec **AWS KMS** ou **HashiCorp Vault**.
- **Tester le chiffrement** : effectuez des tests d'intrusion avec Metasploit pour vérifier la protection des données. Utilisez des outils tels que **SSL Labs** pour évaluer les configurations TLS.

- **Valider les données d'entrée** : mettez en œuvre la validation des données d'entrée à l'aide d'ESAPI ou de bibliothèques similaires afin de prévenir les injections SQL ou les attaques XSS.
- **Documenter le chiffrement** : inclure les protocoles de chiffrement, les politiques de gestion des clés et les résultats des tests dans le dossier technique.
- **Surveillez la disponibilité** : utilisez des outils de surveillance tels que **Nagios** pour garantir la disponibilité du système et sa résilience face aux attaques DDoS.

Étude de cas : une PME spécialisée dans les dispositifs médicaux chiffre les données des patients à l'aide des normes AES-256 et TLS 1.3, effectue des tests avec Metasploit et consigne sa conformité dans le dossier technique. La validation des entrées empêche les injections SQL, comme l'ont confirmé les analyses OWASP ZAP.

Tableau 5 :
Modèle de conformité en matière de chiffrement

Type de données	Chiffrement	Gestion des clés	Méthode de test	Preuves	Statut
Données des patients	AES-256	AWS KMS	Metasploit	Rapport de test du 25 juin 2025	Conforme

1.1.6. Minimisation des données et réduction de la surface d'attaque

Les produits ne doivent collecter que les données nécessaires et réduire au minimum les interfaces ouvertes. Les PME peuvent utiliser **Nmap** pour rechercher les ports ouverts et **OWASP Dependency-Check** pour identifier les dépendances inutilisées. Une **analyse d'impact relative à la protection des données (AIPD)** , conforme au RGPD, doit justifier la collecte de données. Par exemple, un bracelet connecté de fitness doit limiter les données à la fréquence cardiaque et au nombre de pas, en désactivant les services Bluetooth inutilisés.

Conseils détaillés :

- **Cartographier les flux de données** : réaliser une AIPD pour documenter la collecte, le traitement et le stockage des données. Utiliser des outils tels que **OneTrust** pour automatiser l'AIPD.
- **Réduire au minimum les interfaces** : utilisez Nmap pour identifier et fermer les ports ou API inutiles. Désactivez les protocoles inutilisés tels que SNMP ou FTP.

- **Supprimer les dépendances** : utilisez Dependency-Check pour identifier et supprimer les bibliothèques inutilisées.
- **Documentation de la minimisation** : incluez les résultats de l'AIPD et les configurations d'interface dans le dossier technique.
- **Révisions régulières** : planifiez des mises à jour trimestrielles de l'AIPD afin de refléter les modifications apportées au produit.

Étude de cas : une PME spécialisée dans les trackers d'activité physique réalise une AIPD, limite la collecte de données aux indicateurs essentiels et désactive les services Bluetooth inutilisés. Les analyses Nmap confirment une surface d'attaque minimale, documentée dans l'auto-évaluation.

Tableau 3 :
Modèle de résumé de l'AIPD

Type de données	Finalité	Nécessité	Mesure de minimisation	Justification	Statut
Fréquence cardiaque	Suivi de la santé	Essentiel	Suivi de localisation désactivé	Rapport d'AIPD du 30 juin 2025	Conforme

1.1.7. Atténuation des incidents et journalisation

Les produits doivent intégrer des mécanismes visant à limiter les dommages causés par les incidents, tels que la limitation de débit ou la détection d'intrusion, et permettre une journalisation sécurisée. Les PME peuvent utiliser des outils de journalisation garantissant un stockage inviolable. Par exemple, un routeur réseau doit consigner les tentatives d'accès non autorisées et mettre en œuvre une limitation de débit afin de prévenir les attaques par force brute.

Conseils détaillés :

- **Mettre en œuvre des mesures d'atténuation** : utiliser la limitation de débit (par exemple via **NGINX**) et des systèmes de détection d'intrusion tels que Snort.
- **Activer la journalisation** : configurez Syslog ou ELK Stack pour une journalisation sécurisée et chiffrée. Définissez des politiques de conservation (par exemple, 6 mois).
- **Tester les mesures d'atténuation** : simulez des attaques à l'aide d'outils tels que **hping3** afin de vérifier l'efficacité de la limitation de débit et des IDS.
- **Documenter les journaux** : inclure les formats de journaux, les politiques de conservation et les résultats des tests dans le dossier technique.

- **Examiner les journaux** : planifier des examens mensuels des journaux pour identifier les anomalies, à l'aide d'outils tels que **Splunk** pour l'analyse.

Étude de cas : une PME spécialisée dans les routeurs met en œuvre la limitation de débit avec NGINX et consigne les tentatives d'accès à l'aide de la pile ELK. Des tests d'intrusion réalisés avec hping3 confirment l'efficacité des mesures d'atténuation, ce qui est documenté dans l'auto-évaluation.

Tableau 7 :
Configuration de la journalisation des modèles

Type d'événement	Format du journal	Stockage	Conservation	Méthode de test	Preuve	Statut
Tentatives d'accès	Syslog	Chiffré	6 mois	hping3	Rapport de test 01/07/2025	Conforme

1.1.8. Suppression des données utilisateur

Les produits doivent permettre aux utilisateurs de supprimer en toute sécurité leurs données personnelles, à l'aide de techniques d'effacement cryptographique. Par exemple, une enceinte connectée doit proposer une option de réinitialisation aux paramètres d'usine qui écrase les données utilisateur à l'aide d'outils d' , tels **qu'une bibliothèque cryptographique permettant un effacement sécurisé**. Les PME doivent vérifier l'efficacité de la suppression à l'aide d'outils d'analyse numérique.

Consignes détaillées :

- **Mise en œuvre de la suppression** : proposer une option de réinitialisation sécurisée, utilisant l'effacement cryptographique (par exemple, OpenSSL s_random).
- **Tester la suppression** : utiliser des outils d'analyse numérique pour vérifier que les données sont irrécupérables.
- **Documenter le processus** : inclure les instructions de suppression et les résultats des tests dans le dossier technique.
- **Conseils aux utilisateurs** : fournir des instructions claires dans les manuels d'utilisation, avec une assistance en ligne pour le dépannage.

- **Tests réguliers** : planifier des tests annuels pour s'assurer que les mécanismes de suppression restent efficaces.

Étude de cas : une PME spécialisée dans les enceintes connectées met en œuvre une réinitialisation d'usine avec effacement cryptographique, testée à l'aide d'Autopsy. L'auto-évaluation comprend les instructions du manuel d'utilisation et les rapports de test.

Tableau 8 :
Modèle de vérification de la suppression des données

Composant	Méthode de suppression	Outil de test	Preuve	Statut
Données utilisateur	Effacement cryptographique	Autopsie	Rapport d'essai du 05/07/2025	Conforme

1.2. Exigences en matière de gestion des vulnérabilités

Les 8 exigences relatives à la gestion des vulnérabilités garantissent une gestion continue de la sécurité après la mise en production, en imposant des processus d'identification, de correction et de divulgation des vulnérabilités. Vous trouverez ci-dessous une analyse détaillée de ces exigences[3]

1.2.1. Nomenclature logicielle (SBOM)

Les éditeurs doivent tenir à jour une nomenclature logicielle (SBOM) lisible par machine, dans des formats tels que **CycloneDX** ou **SPDX**. Des outils tels que **Snyk**, **Dependabot** ou **Trivy** permettent d'automatiser la génération de la SBOM. Par exemple, une PME spécialisée dans les applications web utilise Dependabot pour suivre les dépendances et générer une SBOM, garantissant ainsi la transparence des composants tiers.

Consignes détaillées :

- **Générer une SBOM** : utilisez Snyk ou Trivy pour créer une SBOM, en incluant les numéros de version et les licences.
- **Mettre à jour la SBOM** : planifiez des mises à jour mensuelles pour intégrer les nouveaux composants ou correctifs.

[3] Comme indiqué ci-dessus, afin d'éviter les chevauchements, certaines exigences ont été regroupées, ce qui a donné lieu à une liste de six obligations.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Vérifier les composants** : recherchez les vulnérabilités à l'aide du NVD du NIST ou de la base de données de Snyk.
- **Documenter la SBOM** : inclure la SBOM dans le dossier technique, avec un journal des modifications pour les mises à jour.
- **Intégration à la CI/CD** : utilisez des outils tels que **GitHub Actions** pour automatiser la génération de la SBOM dans les pipelines de développement.

Étude de cas : une PME proposant des services cloud génère une SBOM à l'aide de CycloneDX, ce qui lui permet d'identifier une bibliothèque vulnérable (Log4j). La PME applique un correctif à la bibliothèque, met à jour la SBOM et documente le processus dans son auto-évaluation.

Tableau 4 :
Modèle de résumé de la SBOM

Composant	Version	Licence	Vulnérabilité	Action	Statut
Log4j	2.16.0	Apache 2.0	CVE-2021-44228	Correctif appliqué à la version 2.17.1	Résolue

1.2.2. Correction rapide des vulnérabilités

Les vulnérabilités doivent être corrigées sans délai injustifié, en accordant la priorité aux problèmes critiques en fonction **des scores CVSS**. Les PME doivent publier des correctifs dans un délai de 30 jours pour les vulnérabilités critiques et de 60 jours pour les autres. Par exemple, une PME spécialisée dans les caméras intelligentes corrige une vulnérabilité CVE dans un délai de 25 jours et en informe les utilisateurs par e-mail.

Conseils détaillés :

- **Surveiller les vulnérabilités** : utilisez Snyk, le NVD du NIST ou **VulnDB** pour suivre les CVE.
- **Hiérarchiser les correctifs** : utilisez les scores CVSS pour établir un ordre de priorité (par exemple, > 7,0 pour les vulnérabilités critiques, 4,0 à 6,9 pour les vulnérabilités moyennes).
- **Tester les correctifs** : effectuez des tests de régression dans un environnement sandbox pour garantir la stabilité.
- **Informer les utilisateurs** : utilisez des e-mails, des notifications dans l'application ou des avis sur le site web pour informer les utilisateurs.

- **Documenter les mesures correctives** : inclure les calendriers de correction, les résultats des tests et les notifications aux utilisateurs dans le dossier technique.

Étude de cas : une PME spécialisée dans les serrures intelligentes identifie une faille CVE critique (CVSS 8,8) et publie un correctif dans les 20 jours, en documentant le processus et la notification des utilisateurs dans son auto-évaluation.

Tableau 5 :
Modèle de journal de correction des vulnérabilités

ID CVE	Score CVSS	Composant	Date du correctif	Méthode de notification	Statut
CVE-2025-5678	8.8	Micrologiciel	01/07/2025	E-mail	Résolu

1.2.3. Tests de sécurité réguliers

Des tests périodiques, notamment des tests d'intrusion, des analyses de vulnérabilité et des revues de code, sont obligatoires. Les PME peuvent utiliser **OpenVAS**, **Nessus** ou faire appel à des prestataires tiers pour réaliser des audits à moindre coût, en programmant des analyses trimestrielles et des tests d'intrusion annuels.

Consignes détaillées :

- **Planifier les tests** : prévoir des analyses de vulnérabilité trimestrielles et des tests d'intrusion annuels, conformément à **la norme ISO 27001, annexe A.12.6.1**.
- **Utilisation d'outils** : utilisez OpenVAS pour les analyses, Burp Suite pour les applications web ou Metasploit pour les tests d'intrusion.
- **Documenter les résultats** : inclure les rapports de test, les conclusions et les plans de correction dans le dossier technique.
- **Corrigez les failles identifiées** : hiérarchisez les problèmes en fonction de leur gravité et fixez des délais de correction.
- **Automatisation des tests** : intégrez des outils tels que **Snyk** dans les pipelines CI/CD pour assurer des analyses continues.

Étude de cas : une PME spécialisée dans les appareils domotiques effectue des analyses OpenVAS trimestrielles et un test d'intrusion annuel avec un prestataire tiers, en consignant les résultats et les plans de correction dans l'auto-évaluation.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tableau 6 :
Modèle de calendrier des tests de sécurité

Type de test	Fréquence	Outil	Dernier test effectué	Résultats	État de la correction
Analyse de vulnérabilité	Trimestriel	OpenVAS	30/06/2025	2 CVE	Résolues

1.2.4. Transparence dans la divulgation des vulnérabilités

Les fabricants doivent divulguer publiquement les détails des vulnérabilités et les mises à jour correctives dès que des correctifs sont disponibles. Les PME doivent publier sur leur site web des avis de sécurité détaillant la gravité, l'impact, les versions concernées, les mesures d'atténuation/solutions de contournement et les délais, conformément aux normes et bonnes pratiques reconnues en matière de divulgation des vulnérabilités (par exemple, les normes ISO/IEC 29147 et ISO/IEC 30111, les lignes directrices de l'ENISA sur le CVD, les lignes directrices de FIRST sur la coordination multipartite, ou une politique interne équivalente qui s'aligne sur celles-ci).

Recommandations détaillées :

- **Créer un modèle de divulgation** : élaborer un format standard pour les avis, comprenant l'identifiant CVE, le score CVSS, l'impact et les détails du correctif.
- **Publier les avis de sécurité** : Publiez-les sur le site web de l'entreprise, sur le blog ou sur le portail de sécurité.
- **Informer les utilisateurs** : utilisez les e-mails, les notifications intégrées à l'application ou les réseaux sociaux pour informer les utilisateurs.
- **Documenter les divulgations** : inclure un lien ou un chemin d'accès au système de gestion documentaire (DMS) vers vos archives publiques d'avis de sécurité, le journal des modifications interne du texte de l'avis, ainsi que la preuve des notifications aux utilisateurs (listes, horodatages et canaux).
- **Impliquer** les coordinateurs : le cas échéant, partagez les avis de sécurité avec les CSIRT/PSIRT nationaux concernés ou les communautés et archives de coordination des vulnérabilités afin de favoriser une large sensibilisation (utilisez des canaux neutres ; aucune marque spécifique n'est requise).
- **Précisez votre référence :** dans votre politique publique, citez la norme à laquelle vous vous conformez (par exemple, ISO/IEC 29147 et ISO/IEC 30111 ou les bonnes pratiques CVD de

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

l'ENISA) et indiquez que des processus fonctionnellement équivalents sont acceptés. Consignez la version et la date de la politique et réexaminez-la chaque année.

Étude de cas : une PME spécialisée dans les téléviseurs connectés publie un avis de sécurité concernant un CVE, détaillant le correctif et l'impact. L'auto-évaluation inclut l'avis ainsi que les enregistrements relatifs aux notifications aux utilisateurs.

Tableau 7 :
Modèle d'avis de sécurité

ID CVE	Score CVSS	Impact	Détails du correctif	Date de publication	Méthode de notification
CVE-2025-1234	7,5	Fuite de données	Micrologiciel v2.1.3	01/07/2025	Site web, e-mail

D'autres colonnes peuvent être ajoutées, telles que « Versions/builds concernées » ; « Mesures d'atténuation/solutions de contournement » (si aucun correctif n'est encore disponible) ; « Chronologie de la divulgation » (rapport reçu – accusé de réception – correctif appliqué – publication) ; « Remerciements » (chercheur/CSIRT, le cas échéant).

1.2.5. Politique de divulgation coordonnée des vulnérabilités (CVD)

Les PME doivent mettre en place un canal clair pour signaler les vulnérabilités, tel qu'une adresse e-mail dédiée ou un portail web. Des plateformes comme HackerOne ou Bugcrowd peuvent faciliter la CVD grâce à des programmes de prime aux bogues, encourageant les hackers éthiques à signaler les problèmes.

Conseils détaillés :

- **Mettre en place une politique de CVD** : élaborez une politique prévoyant une adresse e-mail dédiée (par exemple,security@company.com) ou un portail, conformément aux directives **de la norme ISO 29147**.
- **Encourager les signalements** : publiez la politique sur le site web de l'entreprise et sur les forums de développeurs.
- **Répondre rapidement** : accuser réception des signalements dans un délai de 7 jours et fournir des mises à jour dans un délai de 30 jours.

- **Documenter la politique** : inclure la politique en matière de CVD, les indicateurs de réponse et les vulnérabilités signalées dans le dossier technique.
- **Récompensez les signalants** : envisagez de mettre en place des programmes de prime aux bogues pour encourager les signalements, en utilisant des plateformes telles que HackerOne.

Étude de cas : une PME met en place un portail CVD sur HackerOne, où elle reçoit et résout un signalement de vulnérabilité en 25 jours. L'auto-évaluation rend compte de la politique mise en place et des indicateurs de réponse.

Tableau 8 :
Modèle de politique CVD

Canal	Délai de réponse	Vulnérabilités signalées	Preuves	Statut
security@company.com	7 jours	3 CVE	Rapport HackerOne	Résolu

1.2.6. Mises à jour de sécurité gratuites

Les mises à jour doivent être fournies gratuitement pendant une période de support définie (par exemple, au moins 5 ans pour les appareils IoT ou pendant toute la durée de vie du produit). Les PME doivent veiller à ce que les mises à jour soient faciles à installer, de préférence automatiquement, à l'aide de mécanismes OTA.

Recommandations détaillées :

- **Définir la période de support (art. 13, paragraphe 8, du CRA) :** fixez une période de support qui reflète la durée d'utilisation prévue du produit ; elle ne peut être inférieure à 5 ans, sauf si l'on peut raisonnablement s'attendre à ce que le produit soit utilisé pendant moins de 5 ans, auquel cas la période de support correspond à cette durée de vie plus courte. Si le produit est censé être utilisé pendant plus de 5 ans, fixez une période de support plus longue**.**
- **Automatisez les mises à jour** : utilisez des plateformes OTA telles que Mender.io ou Balena pour des mises à jour transparentes.
- **Tester les mises à jour** : vérifiez l'installation et le bon fonctionnement des mises à jour dans un environnement de test.

- **Documentation relative au support** : incluez les politiques de support, les journaux de mise à jour et les instructions d'utilisation dans le dossier technique.
- **Surveiller la conformité** : suivez le déploiement des mises à jour et les taux d'adoption par les utilisateurs, en veillant à ce qu'aucun coût ne leur soit imposé.

Conformément aux exigences du CRA, le fabricant doit veiller à ce que chaque mise à jour de sécurité reste à la disposition des utilisateurs pendant une période d'au moins 10 ans à compter de sa publication ou pendant la durée restante de la période de support, la plus longue des deux prévalant. Dans la pratique, les PME doivent maintenir un référentiel d'archives des correctifs de sécurité (par exemple sur leur site web ou sur un serveur de mises à jour) accessible aux clients même après la fin du support officiel. De plus, si le produit évolue au fil de versions logicielles majeures, le fabricant doit proposer gratuitement aux utilisateurs les nouvelles versions, sans leur imposer de coûts matériels ou logiciels supplémentaires pour bénéficier des correctifs de sécurité (conformément à l'article 13, paragraphe 10, du CRA). Tous ces aspects seront documentés dans le dossier technique, y compris la justification de la durée de la période de support (5 ans au minimum) et la manière dont les utilisateurs sont informés de la fin du support ou de la disponibilité de mises à jour de sécurité à long terme.

Étude de cas : une PME spécialisée dans les thermostats intelligents s'engage à fournir 5 ans de mises à jour gratuites via Mender.io, en documentant cette politique et le mécanisme OTA dans son auto-évaluation.

Tableau 9 :
Modèle de politique de support

Produit	Durée du support	Mécanisme de mise à jour	Dernière mise à jour	Justificatif	Statut
Thermostat	5 ans	OTA (Mender.io)	01/07/2025	Journal des mises à jour	Conforme

1.3. Liste de contrôle recommandée pour l'auto-évaluation

Pour respecter les obligations du CRA en matière de documentation technique et d'évaluation de la conformité, la mise en place d'une liste de contrôle d'auto-évaluation structurée peut constituer un soutien précieux. Nous recommandons une liste de contrôle unique couvrant l'ensemble des 21 exigences de l'annexe I afin de suivre l'état d'avancement, les preuves et les validations tout au long

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

du cycle de vie du produit. Les colonnes de cette liste de contrôle d'auto-évaluation peuvent être les suivantes :

- **Référence de l'annexe I / ID de l'exigence (par exemple, 1.1.9 Démarrage sécurisé)**
- **Produit / Version (y compris version du micrologiciel/logiciel)**
- **Déclaration de conformité (Oui / Partielle / Non)**
- **Preuve objective (lien/chemin d'accès) (rapport de test, politique, configuration, SBOM, avis)**
- **Date du test/de la révision**
- **Rôle responsable / Propriétaire**
- **Écarts et contrôles compensatoires (le cas échéant)**
- **Risque résiduel et justification**
- **Action suivante / Date d'échéance**
- **Approbation / Signature (nom, date)**
- **Référence de la documentation technique (emplacement dans l'index de la documentation technique)**

Les PME peuvent utiliser un tableau de bord de conformité dans des outils tels que **Confluence**, **Notion** ou **Excel** pour visualiser l'avancement, créer des liens vers les pièces justificatives et suivre les mesures correctives.

Cette liste de contrôle est un outil de contrôle interne destiné à faciliter la mise en conformité avec les exigences du CRA (documentation technique, évaluation de la conformité et surveillance post-commercialisation). Elle ne remplace pas en soi les obligations imposées par le CRA ; elle sert plutôt à organiser les justificatifs que vous devez déjà produire et conserver.

1.4. Étude de cas

Une PME développant une sonnette connectée réalise une auto-évaluation :

- **Exigences produit** : utilise OWASP ZAP pour vérifier l'absence de vulnérabilités, met en œuvre TLS 1.3 et désactive les ports inutilisés. Des tests d'intrusion confirment la conformité.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Gestion des vulnérabilités** : génère une SBOM avec CycloneDX, effectue des analyses OpenVAS trimestrielles et publie une politique CVD sur HackerOne.
- **Résultat** : obtient la conformité totale à 18 exigences, identifie des lacunes dans les mises à jour automatiques et planifie des mesures correctives dans un délai de 3 mois, le tout documenté dans un tableau de bord.

1.5. Outils et ressources

Les exemples et fonctionnalités répertoriés dans ce document sont indépendants des outils. Ils décrivent ce qu'un outil doit faire, et non la marque à utiliser. Les équipes peuvent utiliser n'importe quelle solution équivalente offrant les fonctionnalités et les preuves indiquées.

- **Analyse des vulnérabilités** : OpenVAS, Nessus, Trivy.
- **Tests d'intrusion** : Metasploit, Burp Suite.
- **Analyse de code** : SonarQube, OWASP Dependency-Check.
- **Journalisation** : Syslog, ELK Stack, Graylog.
- **Génération de SBOM** : Snyk, CycloneDX, SPDX.
- **Normes** : ETSI EN 303 645, NIST SP 800-53, ISO 27001.

Cette section fournit aux PME une méthodologie solide et détaillée pour atteindre et documenter la conformité à toutes les exigences essentielles, s'appuyant sur des outils pratiques, des modèles et des études de cas.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2. Certification des produits contenant des éléments numériques

Le critère de **« certification des produits contenant des éléments numériques »** s'appuie sur les systèmes européens de certification en matière de cybersécurité pour démontrer la conformité au CRA, conformément à la **loi sur la cybersécurité (UE) 2019/881**. Des systèmes de certification européens en matière de cybersécurité existent en vertu de la loi sur la cybersécurité (par exemple, l'EUCC pour les produits TIC), mais leur rôle dans la présomption de conformité au CRA sera précisé par des actes délégués de la Commission en vertu de l'article 27, paragraphe 9.

Présomption de conformité (article 27, paragraphes 8 et 9, du CRA) : lorsque la Commission précise, par voie d'actes délégués au titre du CRA, les systèmes européens de certification en matière de cybersécurité applicables, les produits titulaires d'une déclaration de conformité de l'UE ou d'un certificat délivré dans le cadre d'un tel système sont présumés conformes uniquement aux exigences de l'annexe I couvertes par ce certificat. Cette section fournit une méthodologie exhaustive permettant aux PME d'évaluer l'applicabilité de la certification, de mettre en correspondance les exigences du CRA avec les normes et d'intégrer les certifications dans l'auto-évaluation, avec des orientations détaillées, des études de cas et des modèles.

2.1. Systèmes de certification et normes

Le CRA encourage les certifications **telles que les Critères communs (ISO/IEC 15408)**, **l'EUCS (sécurité du cloud de l'UE), la norme ETSI EN 303 645** (pour l'IoT) et **la norme CEI 62443** (pour les systèmes industriels). Les PME doivent évaluer si leur catégorie de produits est couverte par un système existant, en utilisant des ressources telles que **les listes de candidats à la certification de l'ENISA.**

Normes clés :

- **ETSI EN 303 645** : couvre la sécurité de l'IoT, y compris les configurations sécurisées, la protection des données et la divulgation des vulnérabilités.
- **Critères communs** : fournit des niveaux d'assurance (EAL1 à EAL7) pour les produits informatiques, adaptés aux systèmes critiques tels que les pare-feu.
- **ISO 27001** : met l'accent sur les processus de sécurité organisationnels, pertinents pour la gestion des vulnérabilités.
- **IEC 62443** : traite de l'IoT industriel, en couvrant le développement et l'exploitation sécurisés.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **NIST SP 800-53** : fournit des contrôles techniques de sécurité, en correspondance avec les exigences de l'évaluation des risques (CRA).

2.2. Méthodologie d'auto-évaluation

L'auto-évaluation doit inclure une liste de contrôle détaillée :

1. **Certifications existantes** : le produit dispose-t-il d'une certification en matière de cybersécurité ? Par exemple, un appareil domestique intelligent certifié selon la norme ETSI EN 303 645 répond à de nombreuses exigences du CRA.
2. **Applicabilité** : le produit est-il éligible à un schéma de certification européen ? Consultez les listes de l'ENISA ou les organismes notifiés.
3. **Alignement sur les normes** : mettez en correspondance les exigences du CRA avec les normes, en identifiant les recoupements. Par exemple, la clause A.12.6.1 de la norme ISO 27001 couvre la gestion des vulnérabilités.
4. **Planification de la certification** : évaluer la faisabilité d'une démarche de certification, en tenant compte des coûts, des délais et des avantages.
5. **Conformité partielle** : documenter le respect des normes, même en l'absence de certification complète, afin de démontrer la diligence requise.

Tableau 15 :
Exemple de mise en correspondance

Exigence du CRA	Norme	Clause	Justificatif
Configurations par défaut sécurisées	ETSI EN 303 645	Clause 5.1	Rapport de configuration
Divulgation des vulnérabilités	ISO 27001	A.12.6.1	Politique en matière de CVD

2.3. Mesures pratiques pour les PME

1. **Identifier les normes pertinentes** : utiliser le site web de l'ENISA ou consulter les organismes notifiés pour trouver les normes applicables. Par exemple, une PME spécialisée dans les compteurs intelligents devrait se référer à la norme CEI 62443.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2. **Documenter la conformité** : conserver les traces de la conformité aux normes, telles que les rapports d'audit ISO 27001 ou les résultats des essais ETSI EN 303 645.
3. **Faire appel à des organismes de certification** : contactez les organismes accrédités répertoriés par l'ENISA pour les procédures de certification.
4. **Tirer parti de la conformité partielle** : documenter la conformité partielle aux normes afin de réduire le périmètre de l'évaluation du CRA.
5. **Élaborer une feuille de route pour la certification** : planifier les délais, les budgets et les ressources nécessaires à la certification. Par exemple, la certification selon les Critères communs peut prendre entre 6 et 12 mois et coûter entre 50 000 et 100 000 €.

2.4. Étude de cas

Une PME développant une plateforme IoT basée sur le cloud vise la certification EUCS :

- **Évaluation** : elle met en correspondance les exigences du CRA avec celles de l'EUCS, en identifiant les recoupements en matière de protection des données, de chiffrement et de gestion des vulnérabilités.
- **Action** : faire appel à un organisme notifié (ON), soumettre des rapports de test (par exemple, tests d'intrusion, SBOM) et documenter la conformité aux clauses de l'EUCS.
- **Résultat** : obtient la certification en 9 mois, ce qui rationalise la conformité au CRA et renforce la confiance du marché. L'auto-évaluation comprend un tableau de correspondance et un rapport de certification.

2.5. Modèle de feuille de route de certification

Tableau 16 :
Modèle de feuille de route de certification

Certification	Calendrier	Estimation des coûts	Responsable	Justificatifs	Statut
EUCS	9 mois (du 01/03/2025 au 01/12/2025)	75 000 €	Équipe de sécurité	Rapports d'essais	En cours

2.6. Outils et ressources

- **ENISA** : listes des candidats à la certification et répertoires des organismes notifiés.
- **Normes** : ETSI EN 303 645, ISO 27001, CEI 62443, Critères communs.
- **Outils** : Confluence pour la documentation, Snyk pour la génération de SBOM, OWASP ZAP pour les tests.

Cette section permet aux PME de tirer parti des certifications pour simplifier la mise en conformité avec le CRA, grâce à des conseils détaillés, des modèles et des études de cas.

3. Classification des produits : parcours de mise en conformité

Le critère **de classification des produits** détermine la voie de conformité appropriée en fonction de la classification des produits par le CRA, basée sur les risques, en quatre catégories : « Par défaut », « Important — Classe I » (annexe III), « Important — Classe II » (annexe III) et « Critique » (annexe IV). Cette section fournit une méthodologie exhaustive permettant aux PME de classer leurs produits, de comprendre leurs obligations de conformité et d'intégrer cette classification dans leur auto-évaluation, grâce à des conseils détaillés, des méthodologies d'évaluation des risques et des études de cas.

3.1. Comprendre la classification des produits

L'ARC classe les produits en fonction de leur risque potentiel en matière de cybersécurité, tel que défini dans l'annexe III et l'annexe IV :

- **Par défaut — Non répertorié dans les annexes III/IV.**
- **Important — Classe I (annexe III) —** par exemple, systèmes d'exploitation, navigateurs, VPN, SIEM, routeurs/modems.
- **Important — Classe II (annexe III) —** par exemple, hyperviseurs, environnements d'exécution de conteneurs, pare-feu, IDS/IPS.
- **Critique (annexe IV) —** par exemple, périphériques matériels équipés de boîtiers de sécurité, passerelles de compteurs intelligents, cartes à puce/éléments sécurisés.

La classification repose sur le cas d'utilisation du produit, la sensibilité des données et l'impact potentiel sur les infrastructures critiques ou la sécurité des utilisateurs.

3.2. Méthodologie d'auto-évaluation

L'auto-évaluation doit inclure un arbre de décision détaillé :

1. **Consulter les annexes du CRA** : passer en revue les annexes III et IV pour connaître les catégories de produits. Par exemple, les caméras domestiques connectées relèvent de la classe I, tandis que les logiciels VPN relèvent de la classe II.

2. **Évaluer l'impact des risques** : Réalisez une évaluation des risques à l'aide de **la norme ISO 27005**, de la spécification **NIST SP 800-30** ou de la méthode **OCTAVE Allegro** afin d'évaluer l'impact d'une cyberattaque.
3. **Classification du document** : consignez la classification, les résultats de l'évaluation des risques et la justification dans le dossier technique.
4. **Vérifier la voie de conformité** : s'assurer que le module d'évaluation approprié (contrôle interne, examen de type UE) est suivi en fonction de la classification.

Tableau17 :
Exemple d'arbre de décision

Question	Réponse	Action
Le produit figure-t-il à l'annexe III ou IV ?	Oui (classe II)	Faire appel à un organisme notifié pour l'examen de type UE
Un dysfonctionnement pourrait-il avoir un impact sur une infrastructure critique ?	Non	Le classer comme « par défaut » ou en classe I, et recourir au contrôle interne

3.3. Voies de mise en conformité

- **Produits par défaut** — Module A (contrôle interne de la production). Le fabricant évalue lui-même la conformité aux 21 exigences de l'annexe I et conserve l'intégralité de la documentation technique.
- **Important — Classe I —** Module A uniquement si des normes harmonisées/spécifications communes ou un système de certification de cybersécurité de l'UE applicable (niveau d'assurance ≥ « substantiel ») sont appliqués ; dans le cas contraire, une évaluation par un tiers (modules B + C ou H) est requise pour les exigences non couvertes.
- **Important — Classe II** — Évaluation par un tiers obligatoire (modules B + C ou H) ou un système de certification de cybersécurité de l'UE applicable (niveau d'assurance ≥ « substantiel ») ; le module A n'est pas autorisé.
- **Critique (annexe IV)** — Lorsque cela est désigné par un acte délégué, la certification de cybersécurité de l'UE est obligatoire (niveau d'assurance tel que spécifié). Jusqu'à cette

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

désignation, appliquer l'article 32, paragraphe 3 (mêmes options que pour « Important — Classe II »).

3.4. Mesures pratiques pour les PME

1. **Liste de contrôle de classification** : élaborez une liste de contrôle pour vérifier si le produit répond aux critères de la classe I ou II, en incluant des questions sur la sensibilité des données, l'impact sur l'infrastructure et les listes de l'annexe.
2. **Évaluation des risques** : utilisez OCTAVE Allegro ou la norme NIST SP 800-30 pour évaluer les risques, en mettant l'accent sur la probabilité et l'impact. Évaluez par exemple des risques tels que les violations de données ou la manipulation frauduleuse des appareils.
3. **Planification de la conformité** : pour la classe II, identifiez les organismes notifiés (par exemple via l'ENISA) et prévoyez un budget pour les audits (entre 50 000 et 150 000 €). Pour la classe par défaut/classe I, programmez des audits internes.
4. **Documentation** : inclure les rapports de classification, les évaluations des risques et les plans de conformité dans le dossier technique.
5. **Révisions régulières** : réévaluez la classification chaque année afin de tenir compte des mises à jour du produit ou des nouvelles recommandations du CRA.

Tableau 10 :
Modèle d'évaluation des risques

Menace	Probabilité	Impact	Niveau de risque	Mesures d'atténuation	Preuve
Accès non autorisé	Moyen	Élevé	Élevé	MFA	Rapport d'essai 01/07/2025

3.5. Étude de cas

Une PME développant un gestionnaire de mots de passe (classe I) le classe conformément à l'annexe III, réalise une évaluation des risques selon la norme NIST SP 800-30 (en identifiant des risques tels que le vol d'identifiants) et fait appel à un organisme notifié pour l'examen de type de l'UE. L'auto-évaluation consigne la classification, l'évaluation des risques et la préparation de l'audit, garantissant ainsi la conformité aux exigences du CRA.

3.6. Outils et ressources

- **Évaluation des risques** : OCTAVE Allegro, NIST SP 800-30, ISO 27005.
- **Documentation** : Confluence, SharePoint.
- **Organismes notifiés** : répertoire de l'ENISA.

Cette section propose un processus pratique, indépendant des outils, que les PME peuvent utiliser pour classer leurs produits et choisir une voie d'évaluation de la conformité au CRA appropriée. Il s'agit d'une option parmi d'autres pour faciliter la mise en conformité ; les organisations peuvent utiliser un processus équivalent s'il aboutit aux mêmes décisions et fournit les mêmes preuves. Les étapes et les documents mentionnés ci-dessus constituent des recommandations et non des méthodes imposées par le CRA. Lorsque le présent document fait référence à un « outil d'évaluation des risques », il s'agit d'un terme générique désignant toute méthode permettant d'obtenir les résultats attendus en matière de capacités (par exemple, une matrice de risques qualitative ou une grille d'évaluation simplifiée).

Ces lignes directrices seront mises à jour à mesure que les actes d'exécution et délégués de l'UE ainsi que les systèmes de certification seront finalisés. D'ici là, considérez les processus décrits ci-dessus comme **des options à titre d'exemple** pour structurer la classification interne et la collecte de preuves.

4. Documentation technique et évaluation des risques

Le critère **«Documentation technique et évaluation des risques»** garantit que les PME produisent une documentation exhaustive pour démontrer leur conformité au CRA. Le CRA exige un dossier technique pour chaque produit, comprenant des descriptions de produit, des évaluations des risques, des mesures de sécurité, des rapports d'essais et des guides d'utilisation. Cette section fournit une méthodologie exhaustive pour la compilation et l'évaluation de la documentation, avec des conseils détaillés, des modèles et des études de cas.

4.1. Exigences en matière de documentation

Le dossier technique doit inclure :

1. **Description du produit** : spécifications détaillées, fonctionnalités et utilisation prévue.
2. **Évaluation des risques** : analyse complète des menaces et des mesures d'atténuation, conforme à la **norme ISO 27005** ou à la spécification **NIST SP 800-30**.
3. **Conformité aux exigences essentielles** : preuves de conformité aux 21 exigences, y compris les rapports de test et les politiques.
4. **Rapports de test** : résultats des analyses de vulnérabilité, des tests d'intrusion et des revues de code.
5. **Cycle de vie de développement sécurisé (SDLC)** : politiques de codage, de test et de révision sécurisés, conformes à **l'OWASP SAMM** ou **au SDL de Microsoft**.
6. **Guides d'utilisation** : manuels ou sections d'aide en ligne expliquant les fonctionnalités de cybersécurité, telles que l'installation des mises à jour et le signalement des vulnérabilités.

4.2. Méthodologie d'auto-évaluation

1. **Liste de contrôle de la documentation** : vérifier la présence de tous les documents requis, y compris les descriptions de produits, les évaluations des risques et les rapports de test.
2. **Processus d'évaluation des risques** : utiliser **STRIDE** (usurpation d'identité, altération, répudiation, divulgation d'informations, déni de service, élévation de privilèges) ou **PASTA** (Process for Attack Simulation and Threat Analysis) pour identifier les menaces.
3. **Collecte des preuves** : rassemblez les rapports de test (par exemple, Nessus, Metasploit), les SBOM et les politiques relatives au cycle de vie du développement logiciel (SDLC).

4. **Organisation du dossier technique** : utilisez des systèmes de gestion de documents tels que **Confluence**, **SharePoint** ou **Notion** pour garantir l'accessibilité et la préparation aux audits.
5. **Mises à jour régulières** : planifier des revues trimestrielles pour mettre à jour la documentation, en tenant compte des modifications apportées aux produits ou des nouvelles vulnérabilités.

Tableau19 :
Modèle de liste de contrôle pour la documentation

Document	Obligatoire	Statut	Justificatif	Lacunes	Action
Description du produit	Oui	Spécifications complètes	Spécifications V1.2	Aucune	N/A
Évaluation des risques	Oui	Partielle	Rapport STRIDE	Détails des mesures d'atténuation manquants	À compléter avant le 01/08/2025

4.3. Mesures concrètes pour les PME

1. **Élaborer une description du produit** : détailler le matériel, les logiciels, la connectivité et les cas d'utilisation. Par exemple, la description d'un thermostat intelligent inclut les protocoles Wi-Fi et le traitement des données.
2. **Réaliser une évaluation des risques** : utiliser STRIDE pour identifier les menaces telles que l'accès non autorisé ou la falsification de données. Documenter les mesures d'atténuation telles que le chiffrement ou les contrôles d'accès.
3. **Recueillir des preuves** : compiler les rapports de test issus d'outils tels que Nessus, OWASP ZAP ou SonarQube. Inclure les SBOM et les politiques SDLC.
4. **Organiser la documentation** : utiliser Confluence pour créer un dossier technique structuré, avec des dossiers dédiés aux descriptions, aux évaluations et aux rapports.
5. **Fournir des consignes aux utilisateurs** : élaborez des manuels contenant des instructions claires en matière de cybersécurité, à l'aide des modèles de la norme **ETSI EN 303 645**.

4.4. Étude de cas

Une PME fabriquant une caméra intelligente établit un dossier technique :

- **Description du produit** : détaille les spécifications de la caméra, la connectivité Wi-Fi et le stockage dans le cloud.
- **Évaluation des risques** : utilise la méthode STRIDE pour identifier les menaces telles que la diffusion non autorisée, atténuées par le protocole TLS 1.3 et l'authentification multifactorielle (MFA).
- **Rapports de test** : inclut les résultats des analyses Nessus et les rapports de tests d'intrusion.
- **Cycle de vie du développement logiciel (SDLC)** : Adopte le modèle OWASP SAMM, en documentant les pratiques de codage sécurisé.
- **Guide de l'utilisateur** : fournit un manuel contenant les instructions de mise à jour et un e-mail CVD.
- **Résultat** : L'auto-évaluation vérifie l'exhaustivité, identifie les lacunes dans la documentation du cycle de développement logiciel (SDLC) et planifie des mesures correctives dans un délai de 6 mois.

4.5. Outils et ressources

- **Évaluation des risques** : STRIDE, PASTA, NIST SP 800-30.
- **Tests** : Nessus, OWASP ZAP, Metasploit.
- **Documentation** : Confluence, SharePoint, Notion.
- **Normes** : OWASP SAMM, Microsoft SDL, ETSI EN 303 645.

Cette section garantit que les PME disposent d'un dossier technique complet et prêt pour l'audit, comprenant des méthodologies détaillées et des modèles.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5. Processus d'évaluation de la conformité et déclaration de conformité UE

Le critère « **Processus d'évaluation de la conformité et déclaration de conformité UE »** finalise la mise en conformité avec le CRA, en garantissant que les PME suivent le module d'évaluation approprié et émettent une déclaration de conformité valide. Cette section fournit une méthodologie exhaustive pour mener à bien ce processus, répondre aux obligations post-commercialisation et préparer la déclaration, avec des conseils détaillés, des modèles et des études de cas.

5.1. Modules d'évaluation de la conformité

Le CRA applique les modules suivants de l'annexe VIII :

- **Module A** — Contrôle interne de la production. Le fabricant évalue lui-même la conformité à l'ensemble des 21 exigences ; il tient à jour la documentation technique et une déclaration de conformité. (Utilisé par défaut ; pour la classe I uniquement dans les conditions prévues au point 3.3.)
- **Module B** — Examen de type UE. Un organisme notifié évalue un « type » de produit représentatif au regard des exigences applicables.
- **Module C** — Conformité au type sur la base d'un contrôle interne de la production. Le fabricant veille à ce que la production soit conforme au «type» approuvé dans le cadre du module B.
- **Module H** — Assurance qualité complète. Un organisme notifié évalue et surveille l'ensemble du système de qualité du fabricant (conception et production) au regard des exigences applicables.

Comme résumé au point 3.3, cela signifie, lorsqu'il s'agit des différentes classes de produits :

- **Par défaut** : module A.
- **Important — Classe I** : module A uniquement si des normes harmonisées/spécifications communes ou un système de certification de l'UE applicable (≥ « substantiel ») sont appliqués ; sinon, B + C ou H.
- **Important — Classe II** : B + C ou H, ou un système de certification de l'UE applicable (≥ « substantiel ») ; le module A n'est pas autorisé.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Critique (annexe IV) :** certification de l'UE obligatoire lorsqu'elle est désignée par un acte délégué ; d'ici là, suivre l'article 32, paragraphe 3 (identique à « Important — Classe II »).

5.2. Méthodologie d'auto-évaluation

1. **Déterminer le module** : identifier le module requis en fonction de la classification (par défaut, classe I ou classe II).
2. **Réaliser des évaluations internes** : pour les dispositifs par défaut et de classe I, vérifier la conformité à toutes les exigences à l'aide de la liste de contrôle d'auto-évaluation.
3. **Faire appel à des organismes notifiés** : pour la classe II, soumettre le dossier technique à un organisme notifié et donner suite aux conclusions de l'audit.
4. **Respecter les obligations après la mise sur le marché** : surveiller les vulnérabilités, publier des mises à jour et tenir à jour la documentation tout au long du cycle de vie du produit.
5. **Émettre la déclaration** : signer la déclaration de conformité UE, attestant de la conformité aux exigences du CRA.

Tableau20 :
Modèle de déclaration de conformité de l'UE

Déclaration de conformité UE
Produit : [Nom du produit] Fabricant : [Nom et adresse de l'entreprise] Par la présente, nous déclarons que le produit susmentionné est conforme au règlement (UE) 2024/2847 (loi sur la cyber-résilience). Exigences essentielles : Conformité totale à l'annexe I. Évaluation de la conformité : [Module, par exemple, contrôle interne de la production] Normes appliquées : [par exemple, ETSI EN 303 645, ISO 27001] Date : [AAAA-MM-JJ] Signé : [Nom, fonction]

5.3. Étapes pratiques pour les PME

1. **Vérifier la classification** : confirmer la classe du produit afin de déterminer le module d'évaluation.
2. **Réaliser des audits internes** : utiliser la liste de contrôle d'auto-évaluation pour vérifier la conformité, en s'appuyant sur les rapports d'essais et la documentation.
3. **Faire appel à des organismes notifiés** : pour la classe II, contactez des organismes accrédités (par exemple via l'ENISA), soumettez le dossier technique et préparez-vous aux audits.
4. **Assurer la surveillance après la mise sur le marché** : utiliser des outils tels que Snyk ou le NVD du NIST pour suivre les vulnérabilités et publier des correctifs si nécessaire.
5. **Émettre la déclaration** : rédiger et signer la déclaration de conformité, puis l'inclure dans le dossier technique.

5.4. Étude de cas

Une PME développant un jouet connecté de classe I réalise un audit interne afin de vérifier la conformité à l'ensemble des 21 exigences à l'aide des rapports Nessus et OWASP ZAP. L'auto-évaluation confirme l'exhaustivité de la documentation, ce qui aboutit à la signature d'une déclaration de conformité. Pour un pare-feu de classe II, la PME fait appel à un organisme notifié, soumet des rapports d'essais et donne suite aux constatations de l'audit dans un délai de 3 mois, en documentant le processus.

5.5. Outils et ressources

- **Audit** : Confluence pour le suivi des audits, Nessus pour les tests.
- **Organismes notifiés** : annuaire de l'ENISA.
- **Normes** : ETSI EN 303 645, ISO 27001.

Cette section permet aux PME de mener à bien le processus d'évaluation de la conformité et de maintenir cette conformité, grâce à des méthodologies et des modèles détaillés.

Conclusion

Ce cadre méthodologique pour l'évaluation de la conformité **aide les PME à mettre en œuvre la loi européenne sur la cyber-résilience** (CRA), grâce à des conseils approfondis, des exemples pratiques, des études de cas et des outils portant sur **cinq critères clés** du CRA : (1) la conformité aux exigences essentielles en matière de cybersécurité, (2) la certification des produits comportant des éléments numériques, (3) la classification des produits en classe I ou classe II et les mesures correspondantes, (4) l'exhaustivité de la documentation technique, et (5) les procédures globales d'évaluation de la conformité. Conformément aux objectifs du **projet SECURE**, ces orientations visent à rendre tangibles les obligations du CRA grâce à des recommandations fondées sur des approches reconnues et les meilleures pratiques dans le domaine de la cybersécurité ; elles restent toutefois à titre indicatif. En fonction des évolutions futures du contexte juridique du CRA, ces orientations sont susceptibles d'être modifiées. Il est recommandé aux PME de consulter d'autres lignes directrices disponibles dans le **référentiel SECURE**, telles que « **Les exigences essentielles de cybersécurité du CRA : Annexe I, Partie I »** pour obtenir des suggestions et des recommandations pratiques concernant chacune des dispositions de l'annexe I, ainsi que « **CRA 101 : Comprendre les obligations de la législation sur la cyber-résilience (CRA) »** pour un aperçu synthétique de vos obligations légales liées au CRA.