SECURE
Cyber Resilience for SMEs

Methodologisch beoordelingskader voor CRA-naleving

20/10/2025

Funded by the European Union

EU-financieringsverklaring: Gefinancierd door de Europese Unie onder Grant Agreement nr. 101190325. De geuite standpunten en meningen zijn echter uitsluitend die van de auteur(s) en geven niet noodzakelijkerwijs de standpunten en meningen van de Europese Unie of het European Cybersecurity Industrial, Technology and Research Competence Centre weer. Noch de Europese Unie, noch de subsidieverstrekkende instantie kan hiervoor verantwoordelijk worden gehouden.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC-disclaimer: Het project wordt ondersteund door het European Cybersecurity Competence Centre en zijn leden.

DISCLAIMER

Dit document maakt deel uit van Deliverable D4.1 'Guidelines and Materials for SMEs CRA Compliance' van het SECURE-project.

Dit document is een vertaalde versie van de oorspronkelijk Engelstalige richtlijn. Afkortingen worden in het Engels behouden, zoals terug te vinden in de lijst met Afkortingen.

Inhoudsopgave

Lijst met tabellen en figuren

Afkortingen

AES – Advanced Encryption Standard

API – Application Programming Interface

CI/CD – Continue integratie en continue levering/implementatie (Continuous Integrations and Delivery/Deployment)

CIS – Centre for Internet Security

CRA – Cyber Resilience Act

CSIRT – Computer Security Incident Response Team

CVD – Gecoördineerde bekendmaking van kwetsbaarheden (Coordinated Vulnerability Disclosure)

CVE – Gemeenschappelijke kwetsbaarheden en blootstellingen (Common Vulnerabilities and Exposures)

CVSS – Gemeenschappelijk kwetsbaarheidsscoresysteem (Common Vulnerability Scoring System)

CWS – Common Weakness Enumeration

DDoS – Distributed Denial of Service

DMS – Documentbeheersysteem

DPIA – Gegevensbeschermingseffectbeoordeling

ECDSA – Elliptic Curve Digital Signature Algorithm

ENISA – Agentschap van de Europese Unie voor cyberbeveiliging

ETSI – European Technical Standards Institute

EU – Europese Unie

EUDoC– Conformiteitsverklaring van de Europese Unie

EUCS – EU-cloudbeveiliging

FTP – File Transfer Protocol

GDPR/AVG – Algemene Verordening Gegevensbescherming

IDS – Inbraakdetectiesysteem (Intrusion Detection System)

IEC – International Electrotechnical Commission

IoT – Internet of Things

IPS – Inbraakpreventiesysteem (Intrusion Prevention System)

ISO – International Standards Organisation

KMO – Kleine en Middelgrote Onderneming

MFA – Multi-factor authenticatie

NB – Aangemelde instantie (Notified Body)

NIST – National Institute of Standards and Technology (Verenigde Staten)

NIST NVD – NIST National Vulnerability Database

OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation

OTA – Over The Air

OWASP – Open Worldwide Application Security Project

OWASP ESAPI – OWASP Enterprise Security API

OWASP SAMM – OWASP Software Assurance Maturity Model

OWASP ZAP – OWASP Zed Attack Proxy

PASTA – Process for Attack Simulation and Threat Analysis

PDE – Product met digitale elementen

PSIRT – Product Security Incident Response Team

RBAC – Role-Based Access Control

SBOM – Software Bill of Materials

SDLC – Software Development Lifecycle

SIEM – Security Information and Event Management

SNMP – Simple Network Management Protocol

SPDX – System Package Data Exchange

SQL – Structured Query Language

SSL – Secure Sockets Layer

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

TLS – Transport Layer Security

UPnP – Universal Plug and Play

VPN – Virtual Private Network

XSS – Cross-site scripting

Inleiding

De **Cyber Resilience Act (CRA)** van de Europese Unie, Verordening (EU) 2024/2847, stelt een uitgebreid kader vast om te waarborgen dat producten met digitale elementen (PDE's) gedurende hun gehele levenscyclus, van ontwerp tot het einde van de levensduur, veilig zijn. Om **kleine en middelgrote ondernemingen (kmo's) te helpen bij het evalueren en verbeteren van hun nalevingsstatus ten aanzien van de CRA**, biedt dit document een methodologisch kader voor zelfbeoordeling van de naleving. Het maakt deel uit van het materiaal dat wordt aangeboden door het **SECURE-project**[1] , dat tot doel heeft kmo's te ondersteunen bij de implementatie van de CRA. Aan de hand van een zeer gedetailleerd kader worden **vijf belangrijke criteria** nader toegelicht: (1) Naleving van essentiële cyberbeveiligingseisen, (2) certificering van producten met digitale elementen, (3) classificatie van producten als klasse I of klasse II en bijbehorende maatregelen, (4) volledigheid van de technische documentatie, en (5) algemene conformiteitsbeoordelingsprocedures. Elk hoofdstuk is verrijkt met richtlijnen, praktische voorbeelden, case studies, checklists, verwijzingen naar sjablonen, hulpmiddelen en normen, zodat kmo's effectief kunnen omgaan met de CRA-verplichtingen aan de hand van uitvoerbare strategieën die zijn afgestemd op hun beperkte middelen. Ze zijn echter louter **suggestief** en bieden aanbevelingen op basis van erkende benaderingen en beste praktijken om kmo's te ondersteunen bij het nalevingstraject. Verwijzingen naar bestaande hulpmiddelen en kaders moeten als illustratief worden beschouwd. Deze richtlijn kan worden bijgewerkt naarmate het wetgevingskader van de CRA zich verder ontwikkelt.

[1] Het project "Strengthening EU SMEs Cyber Resilience" (SECURE) biedt financiële steun en begeleiding aan kmo's om aan de CRA te voldoen.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Methodologisch beoordelingskader voor CRA-naleving

1. Naleving van essentiële cyberbeveiligingsvereisten

De **naleving van de essentiële cyberbeveiligingsvereisten** vormt de hoeksteen van de naleving van de CRA en waarborgt dat producten met digitale elementen voldoen aan strenge cyberbeveiligingsnormen om op de EU-markt te mogen worden gebracht. Bijlage I van de CRA specificeert 13 **cyberbeveiligingseisen voor producten** en 8 **eisen voor de respons op kwetsbaarheden**, in totaal 21 essentiële eisen. Dit hoofdstuk zet een uitgebreide methodologie uiteen voor kmo's om de naleving te beoordelen, bewijsmateriaal te documenteren, hiaten te identificeren en herstelplannen te ontwikkelen. Het bevat gedetailleerde uitleg, praktische hulpmiddelen, case studies, sjablonen en stapsgewijze begeleiding om een grondige evaluatie en naleving te waarborgen.

1.1. Eisen inzake product-cyberbeveiliging

De vereisten inzake product-cyberbeveiliging schrijven voor dat producten worden ontworpen en ontwikkeld met beveiliging als kernprincipe ("secure by design and by default"). Deze vereisten waarborgen dat producten vrij zijn van bekende misbruikbare kwetsbaarheden, veilige standaardconfiguraties hebben, tijdige beveiligingsupdates ondersteunen en de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens beschermen. Hieronder volgt een uitgebreide toelichting op de vereisten[2] , met gedetailleerde richtlijnen, voorbeelden, hulpmiddelen en methodologieën.

1.1.1. Geen bekende uitbuitbare kwetsbaarheden

Fabrikanten moeten ervoor zorgen dat producten bij de release vrij zijn van bekende kwetsbaarheden die kunnen worden uitgebuit. Dit vereist grondige tests vóór de release, waaronder kwetsbaarheidsscans, penetratietests en code reviews. Kleine en middelgrote ondernemingen (kmo's), die vaak over beperkte middelen beschikken, kunnen gebruikmaken van kosteneffectieve beveiligingstest- en scantools (bijvoorbeeld een dynamische scanner voor webapplicaties, een netwerkkwetsbaarheidsscanner, een tool voor statische applicatiebeveiligingstests en een containerimage-scanner) om problemen op te sporen. Een

[2] Sommige van de overlappende vereisten uit bijlage I van de CRA zijn in deze richtlijn gegroepeerd, met als resultaat een lijst van acht concrete verplichtingen.

fabrikant van slimme sloten moet bijvoorbeeld testen op Bluetooth-kwetsbaarheden, zoals zwakke koppelingsprotocollen of replay-aanvallen, en de maatregelen ter verhelping daarvan vastleggen in een kwetsbaarheidsbeheerslog. Het testen moet aansluiten bij standaarden zoals **de OWASP Top 10** of **de CWE/SANS Top 25** om veelvoorkomende kwetsbaarheden te dekken.

Gedetailleerde richtlijnen:

- **Kwetsbaarheidsscans**: Gebruik OpenVAS of Nessus om te scannen op CVE's, waarbij scans tijdens de ontwikkeling tweewekelijks worden gepland. KMO's hebben toegang tot gratis versies van tools zoals Trivy voor container-based applicaties.
- **Penetratietesten**: Voer handmatige of geautomatiseerde tests uit met tools zoals Metasploit of schakel externe dienstverleners in voor driemaandelijkse beoordelingen. Richt je op risicovolle gebieden zoals authenticatie of netwerkinterfaces.
- **Code reviews**: Gebruik SonarQube om kwetsbaarheden op codeniveau op te sporen, zoals SQL-injectie of cross-site scripting (XSS). Voer peer reviews uit voor kritieke componenten.
- **Documentatie**: Houd een log bij voor kwetsbaarheidsbeheer met kolommen voor CVE-ID, CVSS-score, getroffen component, herstelmaatregel en status. Gebruik tools zoals Jira of Trello voor het bijhouden hiervan.
- **Herstelplan**: Stel voor niet-gepatchte kwetsbaarheden prioriteiten vast op basis van CVSS-scores (bijv. >7.0 als kritiek) en stel termijnen voor herstel vast (bijv. 30 dagen voor kritieke problemen).

Case study: Een kmo die een slimme thermostaat ontwikkelt, voert een kwetsbaarheidsscan uit met Nessus en identificeert daarbij een zwak versleutelingsprotocol (TLS 1.1). Het bedrijf upgradet naar TLS 1.3, test de oplossing met OWASP ZAP en documenteert het proces in een log, inclusief CVSS-scores en testrapporten. De zelfbeoordeling bevestigt dat er geen bekende kwetsbaarheden meer zijn, ondersteund door een penetratietestrapport van een externe leverancier.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 1 :
Sjabloon kwetsbaarheidsbeheerslog

CVE-ID	CVSS-score	Component	Beschrijving	Herstelmaatregel	Status	Datum opgelost
CVE-2025-1234	8.5	TLS 1.1	Zwakke versleuteling	Upgrade naar TLS 1.3	Opgelost	15 juni 2025

1.1.2. Veilige standaardconfiguraties

Producten moeten worden geleverd met versterkte standaardinstellingen om risico's tot een minimum te beperken, zoals het uitschakelen van onnodige diensten, het gebruik van sterke wachtwoorden en het sluiten van open poorten. KMO's moeten zich houden aan **ETSI EN 303 645**, dat IoT-specifieke richtlijnen biedt, of aan **CIS-benchmarks** voor specifieke technologieën (bijv. Linux, Docker). Een slimme thuiscamera moet bijvoorbeeld standaard externe toegang uitschakelen, unieke wachtwoorden vereisen en ongebruikte poorten zoals Telnet sluiten.

Gedetailleerde richtlijnen:

- **Configuratiecontrole**: Stel een checklist op basis van ETSI EN 303 645 op, waarmee instellingen worden gecontroleerd zoals uitgeschakelde debug-modi, het ontbreken van standaard inloggegevens en gesloten poorten. Gebruik tools die controles uitvoeren op de beveiliging van het systeem.
- **Poortscanning**: Gebruik **Nmap** om open poorten en services te identificeren, zodat alleen de noodzakelijke actief zijn. Schakel bijvoorbeeld FTP uit als dit niet nodig is.
- **Wachtwoordbeleid**: Implementeer sterke standaardwachtwoorden of dwing gebruikers deze tijdens de installatie in te stellen. Gebruik tools om de sterkte van wachtwoorden te controleren.
- **Documentatie**: Neem configuratie-instellingen op in het technische dossier, met verwijzing naar normen zoals CIS Benchmarks. Documenteer afwijkingen en de redenen daarvoor.
- **Gebruikersbegeleiding**: Geef installatie-instructies in gebruikershandleidingen, waarin wordt uitgelegd hoe veilige configuraties kunnen worden gehandhaafd (bijvoorbeeld het uitschakelen van gast-wifi).

Case study: Een kmo die wifi-routers produceert, zorgt ervoor dat UPnP en Telnet standaard zijn uitgeschakeld en gebruikt Nmap om te controleren of de poorten gesloten zijn. De checklist voor zelfbeoordeling bevestigt de naleving van ETSI EN 303 645, paragraaf 5.1, ondersteund door een configuratierapport en instructies in de gebruikershandleiding.

Tabel 2 :
Sjabloon configuratiechecklist

Instelling	Vereiste	Status	Bewijs	Opmerkingen
UPnP	Uitgeschakeld	Conform	Nmap-scanrapport	Geverifieerd 10-06-2025

1.1.3. Onmiddellijke beveiligingsupdates

Producten moeten automatische beveiligingsupdates ondersteunen, waarbij gebruikers de mogelijkheid hebben om zich hiervoor af te melden. KMO's kunnen gebruikmaken van **OTA-updatemechanismen** (Over-the-Air) via platforms zoals **Mender.io, AWS IoT Device Management** of **Balena**. Updates moeten worden ondertekend en geverifieerd met behulp van tools zoals **OpenSSL** om manipulatie te voorkomen. Een fabrikant van draagbare apparaten moet er bijvoorbeeld voor zorgen dat firmware-updates kwetsbaarheden binnen 30 dagen na ontdekking verhelpen, met duidelijke meldingen aan de gebruiker.

Gedetailleerde richtlijnen:

- **Update-infrastructuur**: Stel een OTA-updateserver in of maak gebruik van cloudgebaseerde oplossingen. Zorg ervoor dat updates zijn ondertekend met RSA-2048 of ECDSA.
- **Updates testen**: Controleer of updates worden geïnstalleerd zonder de functionaliteit te verstoren, met behulp van testomgevingen zoals **Docker**. Voer regressietests uit om de compatibiliteit te waarborgen.
- **Gebruikersmeldingen**: Gebruik e-mail, in-app-meldingen of LED-indicatoren om gebruikers op de hoogte te brengen van updates. Vermeld instructies voor het afmelden in de gebruikershandleidingen.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Documentatie**: Neem de updatefrequentie, ondertekeningsmechanismen en procedures voor gebruikersmeldingen op in het technisch dossier. Registreer de updategeschiedenis met tijdstempels en de aangepakte CVE's.
- **Nalevingsstatistieken**: Houd de implementatietijd van updates bij (bijv. <30 dagen voor kritieke patches) en de acceptatiegraad onder gebruikers.

Case study: Een kmo die slimme luidsprekers maakt, gebruikt Mender.io om ondertekende firmware-updates te pushen, waarmee een CVE binnen 25 dagen wordt verholpen. De zelfbeoordeling documenteert het OTA-proces, de gebruikersmelding via e-mail en de resultaten van de regressietests, waardoor naleving van de CRA-vereisten wordt gewaarborgd.

Tabel 3 :
Sjabloon voor updatelog

Update-ID	Verholpen CVE	Releasedatum	Implementatietijd	Gebruikersmelding	Status
V2.1.3	CVE 2025-5678	1 juli 2025	25 dagen	E-mail verzonden op 30-06-2025	Geïmplementeerd

1.1.4. Bescherming tegen ongeoorloofde toegang

Sterke authenticatiemechanismen, zoals **multi-factor authenticatie (MFA)**, **OAuth 2.0** of **OpenID Connect**, zijn essentieel om ongeoorloofde toegang te voorkomen. KMO's kunnen **JSON Web Tokens (JWT)** gebruiken voor API-beveiliging en **role-based access control (RBAC)** om rechten te beperken. Tools zoals **Burp Suite** of **Postman** kunnen aanvallen simuleren om toegangscontroles te testen. Een met de cloud verbonden IoT-apparaat moet bijvoorbeeld MFA vereisen voor gebruikersaccounts en JWT gebruiken voor API-eindpunten.

Gedetailleerde richtlijnen:

- **Authenticatie implementeren**: Gebruik MFA-bibliotheken zoals **Auth0** of **Okta** voor gebruikersaccounts. Implementeer JWT voor API's volgens RFC 7519.

- **Toegangscontroles testen**: Voer penetratietests uit met Burp Suite om brute-force- of sessiekapingaanvallen te simuleren. Gebruik tools zoals **Wireshark** om het netwerkverkeer te monitoren.
- **Beleid documenteren**: Neem authenticatie- en toegangscontrolebeleid op in het technische dossier, met gedetailleerde informatie over protocollen (bijv. OAuth 2.0) en RBAC-configuraties.
- **Toegang monitoren**: Schakel het loggen van toegangspogingen in met **Syslog** of **ELK Stack**, met waarschuwingen voor verdachte activiteiten (bijv. meerdere mislukte inlogpogingen).
- **Regelmatige audits**: Plan driemaandelijkse audits van de toegangscontroles, met behulp van tools zoals **HashiCorp Vault** voor het beheer van inloggegevens.

Case study: Een kmo die een slimme deurbel ontwikkelt, implementeert MFA met behulp van Auth0 en test dit met Burp Suite, waarbij een fout in het sessiebeheer wordt geïdentificeerd en verholpen. De zelfbeoordeling omvat authenticatiebeleid, testrapporten en logconfiguraties.

Tabel 4 :
Sjabloon voor toegangsbeheerbeleid

Component	Authenticatie	Toegangscontrole	Testmethode	Bewijs	Status
Gebruikers-aanmelding	MFA (Auth0)	RBAC (beheerder/gebruiker)	Burp Suite	Testrapport 20-06-2025	Voldoet

1.1.5. Vertrouwelijkheid, integriteit en beschikbaarheid van gegevens

Versleuteling is van cruciaal belang voor de bescherming van gegevens. KMO's moeten **AES-256** implementeren voor gegevens in rust en **TLS 1.3** voor gegevens in transit, in overeenstemming met **NIST SP 800-52**. Invoervalidatie moet injectieaanvallen voorkomen, met behulp van bibliotheken zoals **OWASP ESAPI**. Een apparaat voor gezondheidsmonitoring moet bijvoorbeeld patiëntgegevens versleutelen om te voldoen aan de AVG (GDPR) en CRA, waarbij vertrouwelijkheid en integriteit worden gewaarborgd.

Gedetailleerde richtlijnen:

- **Kies versleutelingsstandaarden**: Gebruik AES-256 voor opslag en TLS 1.3 voor communicatie. Implementeer sleutelbeheer met **AWS KMS** of **HashiCorp Vault**.
- **Versleuteling testen**: Voer penetratietests uit met Metasploit om de gegevensbescherming te controleren. Gebruik tools zoals **SSL Labs** om TLS-configuraties te beoordelen.
- **Valideer invoer**: Implementeer invoervalidatie met behulp van ESAPI of vergelijkbare bibliotheken om SQL-injectie of XSS te voorkomen.
- **Versleuteling documenteren**: Neem versleutelingsprotocollen, beleidsregels voor sleutelbeheer en testresultaten op in het technische dossier.
- **Beschikbaarheid bewaken**: Gebruik monitoringtools zoals **Nagios** om de uptime van het systeem en de weerbaarheid tegen DDoS-aanvallen te waarborgen.

Case study: Een kmo in medische hulpmiddelen versleutelt patiëntgegevens met AES-256 en TLS 1.3, voert tests uit met Metasploit en documenteert de naleving in het technisch dossier. Validatie van invoer voorkomt SQL-injectie, geverifieerd door middel van OWASP ZAP-scans.

Tabel 5 :
Sjabloon voor naleving van versleutelingsvoorschriften

Gegevenstype	Versleuteling	Sleutelbeheer	Testmethode	Bewijs	Status
Patiëntgegevens	AES-256	AWS KMS	Metasploit	Testrapport 25-06-2025	Conform

1.1.6. Gegevensminimalisatie en vermindering van het aanvalsoppervlak

Producten mogen alleen noodzakelijke gegevens verzamelen en moeten het aantal open interfaces tot een minimum beperken. KMO's kunnen **Nmap** gebruiken om te scannen op open poorten en **OWASP Dependency-Check** om ongebruikte afhankelijkheden te identificeren. Een **Data Protection Impact Assessment (DPIA)**, in overeenstemming met de AVG, moet de gegevensverzameling

rechtvaardigen. Een fitnesstracker moet bijvoorbeeld de gegevens beperken tot hartslag en aantal stappen, en ongebruikte Bluetooth-diensten uitschakelen.

Gedetailleerde richtlijnen:

- **Breng gegevensstromen in kaart**: Voer een DPIA uit om het verzamelen, verwerken en opslaan van gegevens te documenteren. Gebruik tools zoals **OneTrust** voor het automatiseren van de DPIA.
- **Beperk het aantal interfaces**: Gebruik Nmap om onnodige poorten of API's te identificeren en te sluiten. Schakel ongebruikte protocollen zoals SNMP of FTP uit.
- **Verwijder afhankelijkheden**: Gebruik Dependency-Check om ongebruikte bibliotheken te identificeren en te verwijderen.
- **Minimalisatie documenteren**: Neem de resultaten van de DPIA en de interfaceconfiguraties op in het technisch dossier.
- **Regelmatige evaluaties**: Plan driemaandelijkse DPIA-updates om productwijzigingen weer te geven.

Case study: Een kmo die fitnesstrackers produceert, voert een DPIA uit, beperkt de gegevensverzameling tot essentiële statistieken en schakelt ongebruikte Bluetooth-diensten uit. Nmap-scans bevestigen een minimaal aanvalsoppervlak, gedocumenteerd in de zelfbeoordeling.

Tabel 6:
Sjabloon DPIA-samenvatting

Gegevenstype	Doel	Noodzaak	Maatregelen ter beperking	Bewijs	Status
Hartslag	Gezondheidsmonitoring	Essentieel	Locatietracking uitgeschakeld	DPIA-rapport 30-06-2025	Voldoet

1.1.7. Beperking en registratie van incidenten

Producten moeten mechanismen bevatten om schade door incidenten te beperken, zoals rate-limiting of inbraakdetectie, en veilige logregistratie mogelijk maken. KMO's kunnen tools voor logregistratie gebruiken, waarbij ze zorgen voor tamper-proof storage. Een netwerkrouter moet bijvoorbeeld pogingen tot ongeoorloofde toegang registreren en rate-limiting toepassen om brute-force-aanvallen te voorkomen.

Gedetailleerde richtlijnen:

- **Beperk de schade**: Gebruik rate-limiting (bijv. via **NGINX**) en inbraakdetectiesystemen zoals Snort.
- **Logregistratie inschakelen**: Configureer Syslog of ELK Stack voor veilige, versleutelde logregistratie. Stel bewaartermijnen in (bijv. 6 maanden).
- **Test de risicobeperkende maatregelen**: Simuleer aanvallen met tools zoals **hping3** om de effectiviteit van rate-limiting en IDS te controleren.
- **Documenteer logbestanden**: Neem logformaten, bewaarbeleid en testresultaten op in het technische dossier.
- **Logbestanden beoordelen**: Plan maandelijkse beoordelingen van logbestanden in om afwijkingen te identificeren, met behulp van tools zoals **Splunk** voor analyse.

Case study: Een router-KMO implementeert rate-limiting met NGINX en logt toegangspogingen met ELK Stack. Penetratietests met hping3 bevestigen de beveiligingsmaatregelen, gedocumenteerd in de zelfbeoordeling.

Tabel 7 :
Sjabloon configuratie logregistratie

Gebeurtenistype	Log formaat	Opslag	Bewaarperiode	Testmethode	Bewijs	Status
Toegangspogingen	Syslog	Versleuteld	6 maanden	hping3	Testrapport 01-07-2025	Voldoet

1.1.8. Verwijdering van gebruikersgegevens

Producten moeten gebruikers in staat stellen om persoonlijke gegevens veilig te verwijderen met behulp van cryptografische wismethoden. Een slimme luidspreker moet bijvoorbeeld een optie voor het terugzetten naar de fabrieksinstellingen bieden, waarbij gebruikersgegevens worden overschreven met behulp van tools, zoals **een cryptografische bibliotheek voor veilig wissen**. KMO's moeten de effectiviteit van het verwijderen controleren met forensische tools.

Gedetailleerde richtlijnen:

- **Verwijdering implementeren**: Bied een veilige resetoptie aan, waarbij gebruik wordt gemaakt van cryptografische wisprocedures (bijv. OpenSSL s_random).
- **Verwijdering testen**: Gebruik forensische tools om te controleren of de gegevens onherstelbaar zijn.
- **Documenteer het proces**: Neem instructies voor het wissen en testresultaten op in het technisch dossier.
- **Gebruikersrichtlijnen**: Geef duidelijke instructies in gebruikershandleidingen, met online ondersteuning voor het oplossen van problemen.
- **Regelmatige tests**: Plan jaarlijkse tests om te garanderen dat de verwijderingsmechanismen effectief blijven.

Case study: Een kmo die slimme luidsprekers produceert, implementeert een fabrieksreset met cryptografische wisprocedure, getest met Autopsy. De zelfbeoordeling omvat instructies in de gebruikershandleiding en testrapporten.

Tabel 8 :
Sjabloon voor verificatie van gegevensverwijdering

Component	Verwijderingsmethode	Testtool	Bewijs	Status
Gebruikersgegevens	Cryptografisch wissen	Autopsie	Testrapport 5 juli 2025	Voldoet

1.2. Vereisten voor de respons op kwetsbaarheden

De 8 vereisten voor de respons op kwetsbaarheden zorgen voor continu beveiligingsbeheer na de release en vereisen processen voor het identificeren, verhelpen en openbaar maken van kwetsbaarheden. Hieronder volgt een gedetailleerde toelichting op de vereisten[3] .

1.2.1. Software Bill of Materials (SBOM)

Fabrikanten moeten een machinaal leesbare SBOM bijhouden in formaten zoals **CycloneDX** of **SPDX**. Tools zoals **Snyk**, **Dependabot** of **Trivy** kunnen het genereren van een SBOM automatiseren. Een kmo bezig met webapplicaties gebruikt bijvoorbeeld Dependabot om afhankelijkheden bij te houden en een SBOM te genereren, waardoor transparantie voor componenten van derden wordt gewaarborgd.

Gedetailleerde richtlijnen:

- **SBOM genereren**: Gebruik Snyk of Trivy om een SBOM aan te maken, inclusief versienummers en licenties.
- **SBOM bijwerken**: Plan maandelijkse updates in om nieuwe componenten of patches weer te geven.
- **Componenten controleren**: Controleer op kwetsbaarheden met behulp van de NVD van NIST of de database van Snyk.
- **SBOM documenteren**: Neem de SBOM op in het technische dossier, samen met een changelog voor updates.
- **Integreer met CI/CD**: Gebruik tools zoals **GitHub Actions** om het genereren van de SBOM in ontwikkelingspijplijnen te automatiseren.

Case study: Een kmo die clouddiensten aanbiedt, genereert een SBOM met CycloneDX en ontdekt daarbij een kwetsbare bibliotheek (Log4j). Het bedrijf past de bibliotheek aan, werkt de SBOM bij en legt het proces vast in de zelfbeoordeling.

[3] Zoals hierboven vermeld, zijn sommige vereisten opnieuw gegroepeerd om overlap te voorkomen, met als resultaat een lijst van zes verplichtingen.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 9 :
Sjabloon SBOM-overzicht

Component	Versie	Licentie	Kwetsbaarheid	Actie	Status
Log4j	2.16.0	Apache 2.0	CVE-2021-44228	Gepatcht naar 2.17.1	Opgelost

1.2.2. Tijdige verhelping van kwetsbaarheden

Kwetsbaarheden moeten zonder onnodige vertraging worden aangepakt, waarbij kritieke problemen prioriteit krijgen op basis van **CVSS-scores**. KMO's moeten binnen 30 dagen patches uitbrengen voor kritieke kwetsbaarheden en binnen 60 dagen voor overige kwetsbaarheden. Een kmo die slimme camera's maakt, brengt bijvoorbeeld binnen 25 dagen een patch uit voor een CVE en stelt gebruikers hiervan per e-mail op de hoogte.

Gedetailleerde richtlijnen:

- **Kwetsbaarheden monitoren**: Gebruik Snyk, NIST's NVD of **VulnDB** om CVE's bij te houden.
- **Prioriteit toekennen aan patches**: Gebruik CVSS-scores om prioriteiten te stellen (bijv. >7,0 als kritiek, 4,0-6,9 als gemiddeld).
- **Patches testen**: Voer regressietests uit in een sandbox-omgeving om de stabiliteit te waarborgen.
- **Gebruikers op de hoogte brengen**: Gebruik e-mail, in-app-meldingen of adviezen op de website om gebruikers te informeren.
- **Documenteer de herstelmaatregelen**: neem patch-tijdlijnen, testresultaten en gebruikersmeldingen op in het technische dossier.

Case study: Een kmo die slimme sloten maakt, identificeert een kritieke CVE (CVSS 8,8) en brengt binnen 20 dagen een patch uit, waarbij het proces en de gebruikersmelding in de zelfbeoordeling worden gedocumenteerd.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 10 :
Sjabloon voor log van kwetsbaarheidsoplossingen

CVE-ID	CVSS-score	Component	Datum patch	Meldingsmethode	Status
CVE-2025-5678	8.8	Firmware	1 juli 2025	E-mail	Opgelost

1.2.3. Regelmatige beveiligingstests

Periodieke tests, waaronder penetratietests, kwetsbaarheidsscans en code reviews, zijn vereist. KMO's kunnen **OpenVAS**, **Nessus** of externe dienstverleners gebruiken voor kosteneffectieve audits, waarbij driemaandelijkse scans en jaarlijkse penetratietests worden gepland.

Gedetailleerde richtlijnen:

- **Tests plannen**: Plan driemaandelijkse kwetsbaarheidsscans en jaarlijkse penetratietests, in overeenstemming met **ISO 27001 Bijlage A.12.6.1**.
- **Gebruik tools**: Gebruik OpenVAS voor scans, Burp Suite voor webapplicaties of Metasploit voor penetratietests.
- **Resultaten documenteren**: Neem testrapporten, bevindingen en herstelplannen op in het technische dossier.
- **Herstel bevindingen**: Stel prioriteiten op basis van ernst en stel tijdschema's voor herstelmaatregelen vast.
- **Testen automatiseren**: Integreer tools zoals **Snyk** in CI/CD-pijplijnen voor continue scans.

Case study: Een kmo die slimme apparaten voor thuisgebruik produceert, voert elk kwartaal OpenVAS-scans uit en laat jaarlijks een penetratietest uitvoeren door een externe dienstverlener, waarbij de resultaten en herstelplannen in de zelfbeoordeling worden vastgelegd.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 11 :
Sjabloon voor beveiligingstesten

Test-type	Frequentie	Tool	Laatst uitgevoerd	Bevindingen	Status van de herstelmaatregelen
Kwetsbaarheidsscan	Per kwartaal	OpenVAS	30-06-2025	2 CVE's	Opgelost

1.2.4. Transparantie bij het bekendmaken van kwetsbaarheden

Fabrikanten moeten details over kwetsbaarheden en corrigerende updates openbaar maken zodra er patches beschikbaar zijn. KMO's moeten op hun website beveiligingsadviezen publiceren waarin de ernst, de impact, de getroffen versies, de risicobeperkende maatregelen/tijdelijke oplossingen en de tijdschema's worden beschreven, in overeenstemming met erkende normen en best pracitces voor het bekendmaken van kwetsbaarheden (bijvoorbeeld ISO/IEC 29147 en ISO/IEC 30111, de CVD-richtlijnen van ENISA, de FIRST multiparty coordination guidance, of een gelijkwaardig intern beleid dat hiermee overeenkomt).

Gedetailleerde richtlijnen:

- **Maak een sjabloon voor bekendmaking**: ontwikkel een standaardformaat voor beveiligingsadviezen, inclusief CVE-ID, CVSS-score, impact en details over de patch.
- **Advisories publiceren**: Plaats deze op de bedrijfswebsite, blog of het beveiligingsportaal.
- **Gebruikers op de hoogte brengen**: Gebruik e-mail, in-app-meldingen of sociale media om gebruikers te informeren.
- **Documentatie van bekendmakingen**: Voeg een link of DMS path toe naar uw openbare adviesarchief, de interne wijzigingslog voor het advies en bewijs van gebruikersmeldingen (lijsten, tijdstempels en kanalen).
- **Betrek coördinatoren**: Deel beveiligingsadviezen waar nodig met relevante nationale CSIRT's/PSIRT's of kwetsbaarheidscoördinatie-communities en archieven om bekendheid te bevorderen (gebruik neutrale kanalen; een specifiek merk is niet vereist).
- **Vermeld uw basis:** Noem in uw openbaar beleid de richtlijn waaraan u zich houdt (bijv. ISO/IEC 29147 en ISO/IEC 30111 of de ENISA CVD best practices) en vermeld dat

functioneel gelijkwaardige processen worden geaccepteerd. Vermeld de versie en datum van het beleid en herzie het jaarlijks.

Case study: Een kmo die smart-tv's produceert, publiceert een beveiligingsadvies voor een CVE, waarin de patch en de gevolgen gedetailleerd worden beschreven. De zelfbeoordeling omvat het advies en de registraties van gebruikersmeldingen.

Tabel 12 :
Sjabloon beveiligingsadvies

CVE-ID	CVSS-score	Gevolgen	Patchdetails	Publicatiedatum	Meldingsmethode
CVE-2025-1234	7,5	Datalek	Firmware v2.1.3	01-07-2025	Website, e-mail

Er kunnen andere kolommen worden toegevoegd, zoals Getroffen Versies/Builds; Mitigaties/Tijdelijke Oplossingen (indien er nog geen patch beschikbaar is); Tijdlijn van de Bekendmaking (melding ontvangen – bevestigd – gepatcht – gepubliceerd); Vermeldingen (onderzoeker/CSIRT, indien van toepassing).

1.2.5. Beleid inzake gecoördineerde bekendmaking van kwetsbaarheden (CVD)

KMO's moeten een duidelijk kanaal bieden voor het melden van kwetsbaarheden, zoals een speciaal e-mailadres of webportaal. Platforms zoals HackerOne of Bugcrowd kunnen CVD faciliteren via bugbounty-programma's, waarmee ethische hackers worden aangemoedigd om problemen te melden.

Gedetailleerde richtlijnen:

- **Stel een CVD-beleid op**: Stel een beleid op met een speciaal e-mailadres (bijv.security@company.com) of portaal, volgens de richtlijnen **van ISO 29147**.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Meldingen stimuleren**: Maak het beleid bekend op de bedrijfswebsite en op ontwikkelaarsforums.
- **Reageer snel**: Bevestig meldingen binnen 7 dagen en geef binnen 30 dagen updates.
- **Beleid documenteren**: Neem het CVD-beleid, responsstatistieken en gemelde kwetsbaarheden op in het technische dossier.
- **Beloon melders**: Overweeg bugbounties om het melden te stimuleren, met behulp van platforms zoals HackerOne.

Case study: Een kmo zet een CVD-portaal op HackerOne op en ontvangt en lost een gemelde kwetsbaarheid binnen 25 dagen op. In de zelfbeoordeling worden het beleid en de responsstatistieken vastgelegd.

Tabel 13 :
Sjabloon CVD-beleid

Kanaal	Reactietijd	Gemelde kwetsbaarheden	Bewijs	Status
security@company.com	7 dagen	3 CVE's	HackerOne-rapport	Opgelost

1.2.6. Gratis beveiligingsupdates

Updates moeten gedurende een vastgestelde ondersteuningsperiode kosteloos worden aangeboden (bijvoorbeeld minimaal 5 jaar voor IoT-apparaten of gedurende de levensduur van het product). KMO's moeten ervoor zorgen dat updates eenvoudig te installeren zijn, bij voorkeur automatisch, via OTA-mechanismen.

Gedetailleerde richtlijnen:

- **Bepaal de ondersteuningsperiode (CRA art. 13, lid 8):** Stel een ondersteuningsperiode vast die aansluit bij de verwachte gebruiksduur van het product; deze mag niet korter zijn dan 5 jaar, tenzij redelijkerwijs kan worden verwacht dat het product minder dan 5 jaar zal worden gebruikt, in welk geval de ondersteuningsperiode gelijk is aan die kortere levensduur. Als

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

het product naar verwachting langer dan 5 jaar zal worden gebruikt, stel dan een langere ondersteuningsperiode vast**.**

- **Automatiseer updates**: Gebruik OTA-platforms zoals Mender.io of Balena voor naadloze updates.
- **Updates testen**: Controleer de installatie en functionaliteit van updates in een testomgeving.
- **Ondersteuning documenteren**: Neem ondersteuningsbeleid, updatelog en gebruikersinstructies op in het technisch dossier.
- **Controleer de naleving**: Houd de implementatie van updates en de acceptatiegraad bij gebruikers bij, en zorg ervoor dat er geen kosten in rekening worden gebracht.

Volgens de CRA-vereisten moet de fabrikant ervoor zorgen dat elke beveiligingsupdate voor gebruikers beschikbaar blijft gedurende een periode van ten minste 10 jaar vanaf de uitgifte ervan of gedurende de resterende looptijd van de ondersteuningsperiode, afhankelijk van welke periode het langst is. In de praktijk moeten kmo's een archief met beveiligingspatches bijhouden (bijvoorbeeld op de website of updateserver) dat ook na het einde van de officiële ondersteuning toegankelijk is voor klanten. Ook als het product door middel van grote softwareversies evolueert, moet de fabrikant gebruikers de nieuwe versies kosteloos aanbieden, zonder extra hardware- of softwarekosten op te leggen om van de beveiligingsoplossingen te kunnen profiteren (in overeenstemming met art. 13, lid 10, CRA). Al deze aspecten worden gedocumenteerd in het technisch dossier, met inbegrip van de motivering voor de ondersteuningsperiode (minimaal 5 jaar) en de wijze waarop gebruikers worden geïnformeerd over het einde van de ondersteuning of de beschikbaarheid van beveiligingsupdates op lange termijn.

Case study: Een kmo die slimme thermostaten produceert, verbindt zich tot 5 jaar gratis updates via Mender.io en documenteert het beleid en het OTA-mechanisme in de zelfbeoordeling.

Tabel 14 :
Sjabloon ondersteuningsbeleid

Product	Ondersteuningsperiode	Updatemechanisme	Laatste update	Bewijs	Status
Thermostaat	5 jaar	OTA (Mender.io)	01-07-2025	Update-log	Voldoet

1.3. Aanbevolen checklist voor zelfbeoordeling

Om te voldoen aan de verplichtingen van de CRA inzake technische documentatie en conformiteitsbeoordeling, kan het bijhouden van een gestructureerde checklist voor zelfbeoordeling een sterke ondersteuning bieden. Wij raden één enkele checklist aan die alle 21 vereisten van Bijlage I omvat, om de status, het bewijsmateriaal en de goedkeuring gedurende de levenscyclus van het product bij te houden. De kolommen voor een dergelijke zelfbeoordeling kunnen als volgt zijn:

- **Referentie bijlage I / ID van de verplichting (bijv. 1.1.9 Secure Boot)**
- **Product / Versie (incl. firmware-/softwareversie)**
- **Conformiteitsverklaring (Ja / Gedeeltelijk / Nee)**
- **Objectief bewijs (link/path) (testrapport, beleid, configuratie, SBOM, advies)**
- **Test-/beoordelingsdatum**
- **Verantwoordelijke / Eigenaar**
- **Afwijkingen en compenserende maatregelen (indien van toepassing)**
- **Resterend risico en motivering**
- **Volgende actie / Uiterste datum**
- **Goedkeuring / Ondertekening (naam, datum)**
- **Verwijzing naar technische documentatie (waar dit te vinden is in de index van de technische documentatie)**

KMO's kunnen een compliance-dashboard gebruiken in tools zoals **Confluence**, **Notion** of **Excel** om de voortgang in beeld te brengen, naar bewijsmateriaal te linken en corrigerende maatregelen bij te houden.

Deze checklist is een intern controle-instrument dat bedoeld is om de naleving van de CRA-voorschriften te ondersteunen (technische documentatie, conformiteitsbeoordeling en monitoring na het op de markt brengen van het product). De checklist vervangt op zichzelf geen enkele CRA-verplichting, maar biedt structuur aan het bewijsmateriaal dat u toch al moet aanleveren en bijhouden.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.4. Case study

Een kmo die een slimme deurbel ontwikkelt, voert een zelfbeoordeling uit:

- **Productvereisten**: Gebruikt OWASP ZAP om te controleren of er geen kwetsbaarheden zijn, implementeert TLS 1.3 en schakelt ongebruikte poorten uit. Penetratietests bevestigen de naleving.
- **Respons op kwetsbaarheden**: genereert een SBOM met CycloneDX, voert driemaandelijkse OpenVAS-scans uit en publiceert een CVD-beleid op HackerOne.
- **Resultaat**: Voldoet volledig aan 18 vereisten, identificeert hiaten in automatische updates en plant herstelmaatregelen binnen 3 maanden, gedocumenteerd in een dashboard.

1.5. Tools en hulpmiddelen

De voorbeelden en mogelijkheden die in dit document worden genoemd, zijn tool-onafhankelijk. Ze beschrijven wat een tool moet doen, niet welk merk moet worden gebruikt. Teams mogen elke gelijkwaardige oplossing gebruiken die de genoemde mogelijkheden en bewijzen biedt.

- **Kwetsbaarheidsscans**: OpenVAS, Nessus, Trivy.
- **Penetratietesten**: Metasploit, Burp Suite.
- **Codeanalyse**: SonarQube, OWASP Dependency-Check.
- **Logregistratie**: Syslog, ELK Stack, Graylog.
- **SBOM-generatie**: Snyk, CycloneDX, SPDX.
- **Standaarden**: ETSI EN 303 645, NIST SP 800-53, ISO 27001.

Dit hoofdstuk biedt kmo's een robuuste, gedetailleerde methodologie aan om naleving van alle essentiële vereisten te realiseren en te documenteren, ondersteund door praktische tools, sjablonen en case studies.

2. Certificering van producten die digitale elementen bevatten

Het criterium **Certificering van producten die digitale elementen bevatten** maakt gebruik van Europese cyberbeveiligingscertificeringsregelingen om naleving van de CRA aan te tonen, in overeenstemming met de **Cyberbeveiligingsverordening (EU) 2019/881**. Er bestaan EU-certificeringsregelingen voor cyberbeveiliging in het kader van de Cyberbeveiligingsverordening

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

(bijvoorbeeld EUCC voor ICT-producten), maar hun rol voor het vermoeden van conformiteit met de CRA zal nog moeten gespecificeerd worden door gedelegeerde handelingen van de Commissie krachtens artikel 27, lid 9.

Vermoeden van conformiteit (CRA art. 27, leden 8 en 9): wanneer de Commissie via een gedelegeerde handeling krachtens de CRA toepasselijke Europese certificeringsregelingen voor cyberbeveiliging vaststelt, wordt aangenomen dat producten met een EU-conformiteitsverklaring (EUDoC) of -certificaat in het kader van een dergelijke regeling uitsluitend voldoen aan de vereisten van bijlage I die onder dat certificaat vallen. Dit hoofdstuk biedt een uitgebreide methodologie voor kmo's om de toepasbaarheid van certificering te beoordelen, de CRA-eisen aan normen te koppelen en certificeringen in de zelfbeoordeling te integreren, met gedetailleerde richtlijnen, case studies en sjablonen.

2.1. Certificeringsregelingen en normen

De CRA stimuleert certificeringen **zoals Common Criteria (ISO/IEC 15408)**, **EUCS (EU Cloud Security), ETSI EN 303 645** (voor IoT) en **IEC 62443** (voor industriële systemen). KMO's moeten nagaan of hun productcategorie onder een bestaand schema valt, met behulp van bronnen zoals **de lijsten met kandidaat-certificeringschema's van ENISA.**

Belangrijke normen:

- **ETSI EN 303 645**: Heeft betrekking op IoT-beveiliging, waaronder veilige configuraties, gegevensbescherming en het melden van kwetsbaarheden.
- **Common Criteria**: Biedt zekerheidsniveaus (EAL1-EAL7) voor IT-producten, geschikt voor kritieke systemen zoals firewalls.
- **ISO 27001**: Richt zich op beveiligingsprocessen binnen organisaties, relevant voor de respons op kwetsbaarheden.
- **IEC 62443**: Richt zich op het industriële IoT en omvat veilige ontwikkeling en exploitatie.
- **NIST SP 800-53**: Biedt technische beveiligingsmaatregelen die aansluiten bij de CRA-vereisten.

2.2. Methodologie voor zelfbeoordeling

De zelfbeoordeling moet een gedetailleerde checklist bevatten:

1. **Bestaande certificeringen**: Beschikt het product over een cyberbeveiligingscertificering? Een smart home-apparaat dat bijvoorbeeld is gecertificeerd volgens ETSI EN 303 645 voldoet aan veel CRA-vereisten.
2. **Toepasselijkheid**: Komt het product in aanmerking voor een Europees certificeringsprogramma? Raadpleeg de lijsten van ENISA of de aangemelde instanties (NB).
3. **Afstemming op normen**: Breng de CRA-vereisten in kaart ten opzichte van normen en identificeer overlappingen. Zo heeft ISO 27001 A.12.6.1 betrekking op de respons op kwetsbaarheden.
4. **Certificeringsplanning**: Beoordeel de haalbaarheid van het nastreven van certificering, rekening houdend met kosten, tijdschema's en voordelen.
5. **Gedeeltelijke naleving**: Leg naleving van de normen vast, ook zonder volledige certificering, om aan te tonen dat de nodige zorgvuldigheid is betracht.

Tabel 15 :
Voorbeeld van een Mapping

CRA-vereiste	Norm	Clausule	Bewijs
Veilige standaardconfiguraties	ETSI EN 303 645	Paragraaf 5.1	Configuratierapport
Bekendmaking van kwetsbaarheden	ISO 27001	A.12.6.1	CVD-beleid

2.3. Praktische stappen voor kmo's

1. **Identificeer relevante normen**: Gebruik de website van ENISA of raadpleeg aangemelde instanties om de toepasselijke normen te vinden. Een kmo die slimme meters levert, zou bijvoorbeeld IEC 62443 moeten raadplegen.
2. **Naleving documenteren**: Houd een administratie bij van de naleving van normen, zoals ISO 27001-auditrapporten of ETSI EN 303 645-testresultaten.

3. **Schakel certificeringsinstanties in**: Neem contact op met door ENISA vermelde geaccrediteerde instanties voor certificeringsprocessen.
4. **Maak gebruik van gedeeltelijke naleving**: Documenteer gedeeltelijke naleving van normen om de reikwijdte van de CRA-beoordeling te beperken.
5. **Stel een certificeringsroadmap op**: Plan tijdschema's, budgetten en middelen voor certificering. Zo kan een Common Criteria-certificering bijvoorbeeld 6-12 maanden duren en €50.000-€100.000 kosten.

2.4. Case study

Een kmo die een cloudgebaseerd IoT-platform ontwikkelt, streeft naar EUCS-certificering:

- **Beoordeling**: Brengt de CRA-vereisten in kaart ten opzichte van EUCS en identificeert overlappingen op het gebied van gegevensbescherming, versleuteling en de respons op kwetsbaarheden.
- **Actie**: Schakelt een aangemelde instantie in, dient testrapporten in (bijv. penetratietests, SBOM) en documenteert de naleving van de EUCS-bepalingen.
- **Resultaat**: Behaalt de certificering binnen 9 maanden, waardoor de naleving van de CRA-vereisten wordt gestroomlijnd en het vertrouwen van de markt wordt versterkt. De zelfbeoordeling omvat een afstemmingstabel en een certificeringsrapport.

2.5. Sjabloon voor certificeringsroutekaart

Tabel 16 :
Sjabloon certificeringsroadmap

Certificering	Tijdschema	Kosten	Verantwoordelijke	Bewijs	Status
EUCS	9 maanden (1 maart 2025 tot 1 december 2025)	€ 75.000	Beveiligingsteam	Testrapporten	In uitvoering

2.6. Hulpmiddelen en bronnen

- **ENISA**: Lijsten met kandidaat-certificeringschema's en overzichten van aangemelde instanties.
- **Normen**: ETSI EN 303 645, ISO 27001, IEC 62443, Common Criteria.
- **Hulpmiddelen**: Confluence voor documentatie, Snyk voor het genereren van SBOM's, OWASP ZAP voor het uitvoeren van tests.

Dit gedeelte zorgt ervoor dat kmo's gebruik kunnen maken van certificeringen om de naleving van de CRA te vereenvoudigen, met gedetailleerde richtlijnen, sjablonen en case studies.

3. Productclassificatie: nalevingstrajecten

Het criterium **Productclassificatie** bepaalt het juiste nalevingstraject op basis van de risico-gebaseerde classificatie van producten door de CRA in de categorieën Standaard, Belangrijk - Klasse I (Bijlage III), Belangrijk - Klasse II (Bijlage III) en Kritiek (Bijlage IV). Dit hoofdstuk biedt een uitgebreide methodologie waarmee kmo's producten kunnen classificeren, hun nalevingsverplichtingen kunnen begrijpen en de classificatie kunnen integreren in de zelfbeoordeling, met gedetailleerde richtlijnen, methodologieën voor risicobeoordeling en case studies.

3.1. Inzicht in productclassificatie

De CRA classificeert producten op basis van hun potentiële cyberbeveiligingsrisico, zoals gedefinieerd in bijlage III en bijlage IV:

- **Standaard – Niet opgenomen in bijlage III/IV.**
- **Belangrijk – Klasse I (bijlage III) —** bijv. besturingssystemen, browsers, VPN, SIEM, routers/modems.
- **Belangrijk – Klasse II (bijlage III) —** bijv. hypervisors, container-runtimes, firewalls, IDS/IPS.
- **Kritiek (bijlage IV) –** bijv. hardware-apparaten met beveiligingsboxen, gateways voor slimme meters, smartcards/beveiligingselementen.

De classificatie is gebaseerd op het gebruiksscenario van het product, de gevoeligheid van de gegevens en de potentiële impact op kritieke infrastructuur of de veiligheid van gebruikers.

3.2. Methodologie voor zelfbeoordeling

De zelfbeoordeling moet een gedetailleerde beslissingsboom bevatten:

1. **Raadpleeg de bijlagen bij de CRA**: Bekijk bijlage III en IV voor productcategorieën. Zo vallen slimme thuiscamera's onder klasse I, terwijl VPN-software tot klasse II behoort.
2. **Beoordeel de impact van risico's**: Voer een risicobeoordeling uit met behulp van **ISO 27005**, **NIST SP 800-30** of **OCTAVE Allegro** om de impact van een cyberaanval te evalueren.
3. **Classificatie documenteren**: Leg de classificatie, de resultaten van de risicobeoordeling en de motivering vast in het technisch dossier.
4. **Controleer het nalevingstraject**: Zorg ervoor dat de juiste beoordelingsmodule (interne controle, EU-typeonderzoek) wordt gevolgd op basis van de classificatie.

Tabel 17 :
Voorbeeld van een beslissingsboom

Vraag	Antwoord	Actie
Staat het product in bijlage III of IV?	Ja (klasse II)	Schakel een aangemelde instantie in voor het EU-typeonderzoek
Zou een storing gevolgen kunnen hebben voor kritieke infrastructuur?	Nee	Classificeren als standaard of klasse I, gebruik interne controle

3.3. Conformiteitstrajecten

- **Standaardproducten** – Module A (Interne controle). De fabrikant beoordeelt zelf of aan alle 21 eisen van bijlage I wordt voldaan en bewaart de volledige technische documentatie.
- **Belangrijk – Klasse I –** Module A alleen indien geharmoniseerde normen/gemeenschappelijke specificaties of een toepasselijk EU-certificatiesysteem voor

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

cyberbeveiliging (zekerheidsniveau ≥ "substantieel") worden toegepast; anders is een beoordeling door een derde partij (modules B + C of H) vereist voor de niet-gedekte eisen.

- **Belangrijk – Klasse II** – Beoordeling door een derde partij is verplicht (modules B + C of H) of een toepasselijk EU-certificatiesysteem voor cyberbeveiliging (zekerheidsniveau ≥ "substantieel"); module A is niet toegestaan.
- **Kritiek (bijlage IV)** – Indien aangewezen door een gedelegeerde handeling, is EU-cyberbeveiligingscertificering verplicht (garantieniveau zoals gespecificeerd). Totdat een dergelijke aanwijzing plaatsvindt, is artikel 32, lid 3, van toepassing (dezelfde opties als bij "Belangrijk – Klasse II").

3.4. Praktische stappen voor kmo's

1. **Classificatiechecklist**: Stel een checklist op om te controleren of het product voldoet aan de criteria van klasse I of II, inclusief vragen over de gevoeligheid van gegevens, de impact op de infrastructuur en vermeldingen in de bijlagen.
2. **Risicobeoordeling**: Gebruik OCTAVE Allegro of NIST SP 800-30 om risico's te beoordelen, met de nadruk op waarschijnlijkheid en impact. Beoordeel bijvoorbeeld risico's zoals datalekken of manipulatie van apparaten.
3. **Nalevingsplanning**: Identificeer voor Klasse II aangemelde instanties (bijv. via ENISA) en reserveer middelen voor audits (€50.000-€150.000). Plan voor de standaardproducten/Klasse I interne audits.
4. **Documentatie**: Neem classificatierapporten, risicobeoordelingen en nalevingsplannen op in het technisch dossier.
5. **Regelmatige herzieningen**: Beoordeel de classificatie jaarlijks opnieuw om rekening te houden met productupdates of nieuwe CRA-richtlijnen.

Tabel 18 :
Sjabloon risicobeoordeling

Bedreiging	Waarschijnlijkheid	Gevolgen	Risiconiveau	Beperkende maatregelen	Bewijs
Ongeautoriseerde toegang	Medium	Hoog	Hoog	MFA	Testrapport 1 juli 2025

3.5. Case study

Een kmo die een wachtwoordbeheerder (Klasse I) ontwikkelt, classificeert deze op basis van Bijlage III, voert een NIST SP 800-30-risicobeoordeling uit (waarbij risico's zoals diefstal van inloggegevens worden geïdentificeerd) en schakelt een aangemelde instantie in voor een EU-typeonderzoek. De zelfbeoordeling documenteert de classificatie, de risicobeoordeling en de voorbereiding op de audit, waardoor naleving van de CRA-vereisten wordt gewaarborgd.

3.6. Hulpmiddelen en bronnen

- **Risicobeoordeling**: OCTAVE Allegro, NIST SP 800-30, ISO 27005.
- **Documentatie**: Confluence, SharePoint.
- **Aangemelde instanties**: ENISA-lijst.

Dit hoofdstuk stelt een praktische, tool-onafhankelijke workflow voor die kmo's kunnen gebruiken om producten te classificeren en een geschikt CRA-conformiteitsbeoordelingstraject te kiezen. Het is één optie om naleving te ondersteunen; organisaties mogen een gelijkwaardige workflow gebruiken als deze tot dezelfde beslissingen en hetzelfde bewijsmateriaal leidt. De bovenstaande stappen en artefacten zijn aanbevelingen, geen door-de-CRA-voorgeschreven methoden. Wanneer in dit document sprake is van een "risicobeoordelingstool", moet dit worden opgevat als elke methode die de genoemde capaciteitsresultaten oplevert (bijvoorbeeld een kwalitatieve risicomatrix of een eenvoudig scoreformulier).

Deze richtlijn zal worden bijgewerkt naarmate de uitvoerings- en gedelegeerde handelingen van de EU en de certificeringsregelingen worden afgerond. Beschouw de bovenstaande workflows tot die tijd als **illustratieve opties** om de interne classificatie en het verzamelen van bewijsmateriaal te structureren.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4. Technische documentatie en risicobeoordeling

Het criterium **Technische documentatie en risicobeoordeling** zorgt ervoor dat kmo's uitgebreide documentatie opstellen om aan te tonen dat ze aan de CRA voldoen. De CRA vereist een technisch dossier voor elk product, met onder meer productbeschrijvingen, risicobeoordelingen, beveiligingsmaatregelen, testrapporten en gebruikersrichtlijnen. Dit hoofdstuk biedt een uitgebreide methodologie voor het samenstellen en beoordelen van documentatie, met gedetailleerde richtlijnen, sjablonen en case studies.

4.1. Documentatievereisten

Het technisch dossier moet het volgende bevatten:

1. **Productbeschrijving**: Gedetailleerde specificaties, functionaliteit en beoogd gebruik.
2. **Risicobeoordeling**: Uitgebreide analyse van bedreigingen en risicobeperkende maatregelen, in overeenstemming met **ISO 27005** of **NIST SP 800-30**.
3. **Naleving van essentiële eisen**: Bewijs van naleving van alle 21 eisen, inclusief testrapporten en beleidsregels.
4. **Testrapporten**: Resultaten van kwetsbaarheidsscans, penetratietests en code reviews.
5. **Secure Development Lifecycle (SDLC)**: Beleid voor veilig coderen, testen en beoordelen, in overeenstemming met **OWASP SAMM** of **Microsoft SDL**.
6. **Gebruikershandleiding**: Handleidingen of online help-secties waarin cyberbeveiligings-functies worden uitgelegd, zoals het installeren van updates en het melden van kwetsbaarheden.

4.2. Methodologie voor zelfbeoordeling

1. **Checklist voor documentatie**: Controleer of alle vereiste documenten aanwezig zijn, waaronder productbeschrijvingen, risicobeoordelingen en testrapporten.
2. **Risicobeoordelingsproces**: Gebruik **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) of **PASTA** (Process for Attack Simulation and Threat Analysis) om bedreigingen te identificeren.
3. **Bewijs verzamelen**: Verzamel testrapporten (bijv. Nessus, Metasploit), SBOM's en SDLC-beleidsregels.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4. **Technisch dossier organiseren**: Gebruik documentbeheersystemen zoals **Confluence**, **SharePoint** of **Notion** voor toegankelijkheid en auditgereedheid.
5. **Regelmatige updates**: Plan driemaandelijkse evaluaties om de documentatie bij te werken, zodat productwijzigingen of nieuwe kwetsbaarheden worden weergegeven.

Tabel 19 :
Sjabloon voor documentatiechecklist

Document	Vereist	Status	Bewijs	Tekortkomingen	Actie
Productbeschrijving	Ja	Voltooid	Specificatie V1.2	Geen	N.v.t.
Risicobeoordeling	Ja	Gedeeltelijk	STRIDE-rapport	Gegevens over risicobeperkende maatregelen ontbreken	Voltooien vóór 01-08-2025

4.3. Praktische stappen voor kmo's

1. **Stel een productbeschrijving op**: beschrijf hardware, software, connectiviteit en gebruiksscenario's in detail. Een beschrijving van een slimme thermostaat omvat bijvoorbeeld Wi-Fi-protocollen en gegevensverwerking.
2. **Voer een risicobeoordeling uit**: gebruik STRIDE om bedreigingen zoals ongeoorloofde toegang of gegevensmanipulatie te identificeren. Documenteer risicobeperkende maatregelen zoals versleuteling of toegangscontroles.
3. **Bewijsmateriaal verzamelen**: Stel testrapporten samen met behulp van tools zoals Nessus, OWASP ZAP of SonarQube. Neem SBOM's en SDLC-beleidsregels op.
4. **Organiseer de documentatie**: gebruik Confluence om een gestructureerd technisch dossier aan te maken, met mappen voor beschrijvingen, beoordelingen en rapporten.
5. **Gebruikersrichtlijnen verstrekken**: Stel handleidingen op met duidelijke instructies voor cyberbeveiliging, met behulp van sjablonen uit **ETSI EN 303 645**.

4.4. Case study

Een kmo die slimme camera's produceert, stelt een technisch dossier samen:

- **Productbeschrijving**: Bevat details over de specificaties van de camera, Wi-Fi-connectiviteit en cloudopslag.
- **Risicobeoordeling**: Gebruikt STRIDE om bedreigingen zoals ongeautoriseerde streaming te identificeren, die worden beperkt met TLS 1.3 en MFA.
- **Testrapporten**: Bevat Nessus-scanresultaten en penetratietestrapporten.
- **SDLC**: past OWASP SAMM toe en documenteert veilige programmeerpraktijken.
- **Gebruikershandleiding**: Bevat een handleiding met update-instructies en een CVD-e-mail.
- **Resultaat**: De zelfbeoordeling controleert de volledigheid, identificeert hiaten in de SDLC-documentatie en plant corrigerende maatregelen binnen 6 maanden.

4.5. Hulpmiddelen en bronnen

- **Risicobeoordeling**: STRIDE, PASTA, NIST SP 800-30.
- **Testen**: Nessus, OWASP ZAP, Metasploit.
- **Documentatie**: Confluence, SharePoint, Notion.
- **Normen**: OWASP SAMM, Microsoft SDL, ETSI EN 303 645.

Dit hoofdstuk zorgt ervoor dat kmo's beschikken over een volledig, auditklaar technisch dossier, met gedetailleerde methodologieën en sjablonen.

5. Conformiteitsbeoordelingsproces en EU-conformiteitsverklaring

Het criterium **Conformiteitsbeoordelingsproces en EU-conformiteitsverklaring** rondt de naleving van de CRA af en zorgt ervoor dat kmo's de juiste beoordelingsmodule volgen en een geldige conformiteitsverklaring afgeven. Dit hoofdstuk biedt een uitgebreide methodologie om dit proces te doorlopen, verplichtingen na het op de market brengen van het product aan te pakken en de verklaring voor te bereiden, met gedetailleerde richtlijnen, sjablonen en case studies.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.1. Conformiteitsbeoordelingsmodules

De CRA past de volgende modules van bijlage VIII toe:

- **Module A** – Interne controle. De fabrikant beoordeelt zelf of aan alle 21 eisen wordt voldaan; hij houdt technische documentatie en een conformiteitsverklaring bij. (Wordt gebruikt voor standaardproducten; voor klasse I alleen onder de voorwaarden in punt 3.3.)
- **Module B** – EU-typeonderzoek. Een aangemelde instantie beoordeelt een representatief product "type" aan de hand van de toepasselijke eisen.
- **Module C** – Conformiteit met het EU-type op basis van interne productiecontrole. De fabrikant zorgt ervoor dat de productie in overeenstemming is met het in module B goedgekeurde "type".
- **Module H** – Volledige kwaliteitsborging. Een aangemelde instantie beoordeelt en controleert het volledige kwaliteitssysteem van de fabrikant (ontwerp en productie) aan de hand van de toepasselijke eisen.

Zoals samengevat in punt 3.3 betekent dit, wanneer toegepast op de verschillende productklassen:

- **Standaardproducten**: Module A.
- **Belangrijk – Klasse I**: Module A alleen indien geharmoniseerde normen/gemeenschappelijke specificaties of een toepasselijk EU-certificeringssysteem (≥ "substantieel") worden toegepast; anders B + C of H.
- **Belangrijk – Klasse II**: B + C of H, of een toepasselijk EU-certificeringssysteem (≥ "substantieel"); module A is niet toegestaan.
- **Kritiek (bijlage IV):** EU-certificering verplicht wanneer dit bij gedelegeerde handeling wordt vastgesteld; tot die tijd geldt artikel 32, lid 3 (hetzelfde als "Belangrijk - Klasse II").

5.2. Methodologie voor zelfbeoordeling

1. **Bepaal de module**: Bepaal de vereiste module op basis van de classificatie (standaard, klasse I of klasse II).
2. **Interne beoordelingen uitvoeren**: Controleer voor standaardproducten en klasse I of aan alle eisen is voldaan aan de hand van de checklist voor zelfbeoordeling.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3. **Schakel aangemelde instanties in**: Voor klasse II dient u het technisch dossier in bij een aangemelde instantie en pakt u de bevindingen van de audit aan.
4. **Vervul verplichtingen na het op de markt brengen**: Houd kwetsbaarheden in de gaten, breng updates uit en houd de documentatie bij gedurende de gehele levenscyclus van het product.
5. **Verklaring afgeven**: Onderteken de EU-conformiteitsverklaring, waarmee u bevestigt dat aan de CRA-vereisten is voldaan.

Tabel 20 :
Sjabloon EU-conformiteitsverklaring

EU-conformiteitsverklaring
Product: [Productnaam] Fabrikant: [Bedrijfsnaam, adres] Hierbij verklaren wij dat het bovengenoemde product voldoet aan Verordening (EU) 2024/2847 (Cyber Resilience Act). Essentiële eisen: Volledig in overeenstemming met bijlage I. Conformiteitsbeoordeling: [Module, bijv. interne controle] Toegepaste normen: [bijv. ETSI EN 303 645, ISO 27001] Datum: [JJJJ-MM-DD] Ondertekend door: [Naam, functie]

5.3. Praktische stappen voor kmo's

1. **Controleer de classificatie**: Bepaal de klasse van het product om de beoordelingsmodule vast te stellen.
2. **Voer interne audits uit**: Gebruik de checklist voor zelfbeoordeling om de naleving te controleren, ondersteund door testrapporten en documentatie.

3. **Schakel aangemelde instanties in**: Neem voor klasse II contact op met geaccrediteerde instanties (bijv. via ENISA), dien het technisch dossier in en bereid u voor op audits.
4. **Monitoring na het op de markt brengen**: Gebruik tools zoals Snyk of de NVD van NIST om kwetsbaarheden op te sporen en breng indien nodig patches uit.
5. **Verklaring afgeven**: Stel de conformiteitsverklaring op, onderteken deze en neem deze op in het technisch dossier.

5.4. Case study

Een kmo die slim speelgoed van klasse I ontwikkelt, voert een interne audit uit en controleert aan de hand van Nessus- en OWASP ZAP-rapporten of aan alle 21 eisen is voldaan. De zelfbeoordeling bevestigt dat de documentatie volledig is, wat leidt tot een ondertekende conformiteitsverklaring. Voor een firewall van klasse II schakelt de kmo een aangemelde instantie in, dient testrapporten in en pakt de bevindingen van de audit binnen drie maanden aan, waarbij het proces wordt gedocumenteerd.

5.5. Hulpmiddelen en bronnen

- **Auditeren**: Confluence voor het bijhouden van audits, Nessus voor het testen.
- **Aangemelde instanties**: ENISA-lijst.
- **Normen**: ETSI EN 303 645, ISO 27001.

Dit gedeelte zorgt ervoor dat KMO's het conformiteitsbeoordelingsproces voltooien en aan de voorschriften blijven voldoen, met gedetailleerde methodologieën en sjablonen.

Conclusie

Dit methodologische beoordelingskader voor CRA-naleving biedt **ondersteuning aan kmo's bij de implementatie van de Cyber Resilience Act** (CRA), door middel van diepgaande begeleiding, praktische voorbeelden, case studies en hulpmiddelen met betrekking tot **vijf belangrijke criteria** van de CRA: (1) Naleving van essentiële cyberbeveiligingseisen, (2) Certificering van producten met digitale elementen, (3) Indeling van producten in klasse I of klasse II en bijbehorende maatregelen, (4) Volledigheid van de technische documentatie, en (5) Algemene conformiteitsbeoordelingsprocedures. In lijn met de doelstellingen van het **SECURE-project** is de richtlijn erop gericht de CRA-verplichtingen concreet te maken door middel van aanbevelingen die zijn gebaseerd op erkende benaderingen en best practices op cybergebied; deze aanbevelingen blijven echter suggestief. Afhankelijk van toekomstige ontwikkelingen in de juridische context van de CRA kan de richtlijn worden aangepast. Als volgende stappen voor kmo's wordt aanbevolen om aanvullende richtlijnen in de **SECURE-databank** te raadplegen, zoals **De essentiële cyberbeveiligingsvereisten van de CRA: Bijlage I, Deel I** voor praktische suggesties en aanbevelingen voor elk van de bepalingen in Bijlage I, evenals **CRA 101: Inzicht in CRA-verplichtingen** voor een beknopt overzicht van de wettelijke verplichtingen in het kader van de CRA.