SECURE
Cyber Resilience for SMEs

CRA101: Inzicht in de CRA-verplichtingen

31/03/2026

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.

Eerste auteur: *Centrum voor Cyberveiligheid België (CCB)*

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

Inhoudsopgave

Lijst van tabellen en figuren

Afkortingen

CE - Conformité Européenne (European Conformity)

CRA – Cyber Resilience Act

CSIRT – Computer Security Incident Response Team

CVD – Gecoördineerde openbaarmaking van kwetsbaarheden (Coordinated Vulnerability Disclosure)

ENISA – Agentschap van de Europese Unie voor Cyberbeveiliging

EU – Europese Unie

EU DoC – EU-Conformiteitsverklaring

KMO – Kleine en Middelgrote Onderneming

NB – Aangemelde Instantie (Notified Body)

PDE – Product met Digitale Elementen

SBOM – Software Bill of Materials

SPOC – Centraal contactpunt (Single Point of Contact)

Inleiding

De **Cyber Resilience Act** (CRA) van de Europese Unie (EU), Verordening (EU) 2024/2847, is aangenomen met als doel de cyberweerbaarheid en veerkracht van de Europese digitale markt te verbeteren gezien de toenemende uitdagingen op het gebied van cyberbeveiliging. Door geharmoniseerde regels en een duidelijk minimum aan cyberbeveiliginseisen in te voeren, beoogt de CRA kwetsbaarheden te verminderen en zowel consumenten als bedrijven te beschermen. Hoewel deze verordening in december 2024 in werking is getreden, werd er gekozen voor een gefaseerde implementatie, waardoor er een overgangs- en aanpassingsperiode is van 2024 tot 2027. Concreet introduceert de CRA verplichtingen voor fabrikanten, importeurs en distributeurs van producten met digitale elementen (PDE's). **Artikel 13 en bijlage I** van de CRA sommen de essentiële cyberbeveiligingseisen op waaraan fabrikanten moeten voldoen, zowel bij het op de EU-markt brengen van hun PDE's als gedurende de gehele levenscyclus van het PDE. Deel I van de eisen in bijlage I richt zich op de eigenschappen van de PDE's, deel II richt zich op de respons op kwetsbaarheden. Naast bijlage I en artikel 13 van de CRA worden echter nog andere vereisten opgelegd – bijvoorbeeld met betrekking tot informatie en instructies voor de gebruiker (bijlage II), rapportageverplichtingen (artikel 14-17) en conformiteit (artikel 27-32). In een eerste poging om de belangrijkste wettelijke verplichtingen te vertalen naar concrete richtlijnen, biedt deze gids **een vereenvoudigd overzicht[1] van de verplichtingen**, onderverdeeld in **vijf componenten**, die **minimaal** in acht moeten worden genomen. Het doel is om de toegankelijkheid van de verordening te vergroten en het bewustzijn en begrip op basisniveau te verbeteren, in het bijzonder voor kleine en middelgrote ondernemingen (kmo's), in lijn met de doelstellingen van het **SECURE-project**[2] . Voor technische handleidingen en hulpmiddelen voor de praktische uitvoering van deze bepalingen wordt op doorlopende basis aanvullend materiaal beschikbaar gesteld in de **SECURE open repository**.

[1] Dit is een niet-uitputtend overzicht dat bedoeld is om de verplichtingen van de CRA te verduidelijken en bevat niet alle uitzonderingen die in de CRA worden overwogen. Om een overzicht te geven, zijn alleen de belangrijkste verplichtingen opgenomen. Deze zijn geselecteerd op basis van een grondige bestudering van de wettekst van de CRA.

[2] 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

Tijdlijn van de CRA:

- Inwerkingtreding: 10 december 2024
- Rapportageverplichtingen van toepassing: 11 september 2026
- Volledige toepassing van de CRA-vereisten: 11 december 2027

Inzicht in CRA-verplichtingen - CRA 101

1. Beoordeling van de cyberbeveiliginsrisico's

Om te voldoen aan de verplichting dat je PDE is "ontworpen, ontwikkeld en geproduceerd overeenkomstig de essentiële cyberbeveiligingsvereisten van deel I van bijlage I"[3] – d.w.z. het waarborgen van "een passend cyberbeveiligingsniveau op basis van de risico's"[4] – *moet* een cyberbeveiligingsrisicobeoordeling worden uitgevoerd. Deze beoordeling moet worden **gedocumenteerd**[5] en gedurende de zogenaamde "ondersteuningsperiode"[6] **regelmatig worden bijgewerkt**.

Concreet moet de risicobeoordeling ten minste het volgende omvatten[7] :

1) Een **analyse van de cyberbeveiligingsrisico's**, rekening houdend met:
   - Het beoogde doel en het voorzienbaar gebruik van het PDE;
   - Gebruiksvoorwaarden (bijv. operationele omgeving, te beschermen activa).

2) Een **verduidelijking, uitleg en/of rechtvaardiging** van
   - De toepassing van cybersecurity by design[8] – d.w.z. hoe wordt dit toegepast?
   - De toepasbaarheid (of niet-toepasbaarheid) van de eisen in bijlage I, deel I, op het PDE – d.w.z. zijn de beveiligingseisen van toepassing en op welke manier?

[3] Art. 13, lid 1, CRA.
[4] Bijlage I, deel I, punt 1, CRA.
[5] Technische documentatie: toegelicht in punt 5.
[6] Ondersteuningsperiode: toegelicht in punt 2.
[7] Art. 13, lid 3, CRA.
[8] Bijlage I, deel I, punt 1, CRA.

- De toepassing en implementatie van de vereisten inzake de respons op kwetsbaarheden[9] – d.w.z. hoe worden de vereisten inzake de respons op kwetsbaarheden toegepast?

Wanneer een PDE componenten bevat die afkomstig zijn van derden, verwacht de CRA dat je met **passende zorgvuldigheid** handelt om de cyberbeveiliging van het eindproduct te waarborgen. Dit kan bijvoorbeeld betekenen dat je een kwetsbaarheid die je hebt vastgesteld, meldt aan de fabrikant van die component en dat je deze verder aanpakt. Om dit te kunnen doen, moeten een Software Bill of Materials (SBOM)[10] en een beleid voor de gecoördineerde openbaarmaking van kwetsbaarheden (CVD) voor leveranciers worden bijgehouden en op verzoek ter beschikking worden gesteld aan markttoezichtautoriteiten.

2. Respons op kwetsbaarheden en beveiligingsupdates

Zoals vermeld in artikel 13, lid 8, moeten fabrikanten ervoor zorgen dat de kwetsbaarheden van het PDE en de componenten daarvan – "doeltreffend en in overeenstemming met de essentiële cyberbeveiligingsvereisten van deel II van bijlage I worden aangepakt"[11] gedurende de gehele ondersteuningsperiode.

Dit houdt onder meer in[12] :

1) Het **identificeren en documenteren van kwetsbaarheden** – d.w.z. het opstellen van de SBOM (minstens voor de afhankelijkheden op het hoogste niveau) en deze beschikbaar houden om op verzoek aan markttoezichtautoriteiten te verstrekken[13] ;
2) Het onverwijld aanpakken en verhelpen van kwetsbaarheden – d.w.z. het zonder onnodige vertraging en kosteloos **verstrekken van beveiligingsupdates** (met adviezen voor gebruikers):

[9] Bijlage I, deel II, CRA.
[10] De SBOM of "softwarestuklijst" is een formeel overzicht van de details en de relaties in de toeleveringsketen van componenten die zijn opgenomen in software-elementen van PDE's (art. 3, lid 39, CRA).
[11] Art. 13, lid 8, CRA.
[12] Bijlage I, deel II, CRA.
[13] Het delen ervan met gebruikers is optioneel.

- Elke beveiligingsupdate die tijdens de ondersteuningsperiode wordt uitgebracht, moet ten minste 10 jaar na de uitbreng beschikbaar blijven, of voor de rest van de ondersteuningsperiode, indien deze langer is[14] .

3) Het regelmatig **evalueren en testen** van de productbeveiliging;

4) Het **delen van informatie** over verholpen (en potentiële) kwetsbaarheden, de gevolgen en ernst ervan, instructies voor gebruikers om deze te verhelpen, contactadressen voor de melding van kwetsbaarheden, evenals het invoeren en handhaven van een CVD-beleid.

De hierboven genoemde "**ondersteuningsperiode**" weerspiegelt "de verwachte gebruiksduur van het product"[15] en moet in verhouding rekening houden met de verwachtingen van de gebruiker, de aard (het doel) van het PDE en het relevante Unierecht.

Concreet betekent dit dat bij het vaststellen van uw ondersteuningsperiode, deze:

- ten minste vijf jaar moet bedragen (tenzij de levensduur van het product korter is dan vijf jaar; in dat geval is de ondersteuningsperiode gelijk aan de levensduur van het product);
- duidelijk gespecificeerd moet worden (einddatum: maand en jaar) op het moment van aankoop/op de verpakking/in digitale vorm (wanneer deze datum is bereikt, moeten gebruikers idealiter hiervan op de hoogte worden gesteld)[16] .

De vaststelling en definitie van de ondersteuningsperiode moeten worden opgenomen in de technische documentatie[17] .

3. Gebruikersinformatie, -instructies en centraal contactpunt

Overeenkomstig artikel 13, leden 14-18, en bijlage II *moeten* fabrikanten **gebruikers duidelijk informeren** door op papier/digitaal het volgende op te nemen:

- Gegevens van de fabrikant (naam, geregistreerde handelsnaam of merk, postadres, e-mailadres of digitaal contact, website);

[14] Art. 13, lid 9, CRA.
[15] Art. 13, lid 8, CRA.
[16] Art. 13, lid 19, CRA.
[17] Technische documentatie: verduidelijkt in punt 5.

- Gegevens van het PDE (naam, type, beoogd doel, beveiligingsomgeving en beveiligingseigenschappen, essentiële functionaliteiten, mogelijke cyberbeveiligings-risico's, aangeboden technische beveiligingsondersteuning, einddatum van de ondersteuningsperiode);
- Gedetailleerde instructies of een internetadres daartoe (met betrekking tot maatregelen voor veilig gebruik, mogelijke invloeden op de gegevensbeveiliging als gevolg van productwijzigingen, het installeren van beveiligingsupdates, veilige buitenbedrijfstelling en verwijdering van gebruikersgegevens, standaardinstellingen voor de installatie van beveiligingsupdates);
- Er moet een centraal contactpunt (SPOC) worden aangewezen om gebruikers in staat te stellen:
    - rechtstreeks en snel te communiceren met de fabrikant via het door hen gewenste communicatiemiddel (niet beperkt tot geautomatiseerde hulpmiddelen);
    - kwetsbaarheden te melden;
    - CVD-beleid op te zoeken.
- Links (indien van toepassing) naar het CVD-beleid, de EU-conformiteitsverklaring (EU DoC)[18] en de SBOM (indien beschikbaar voor gebruikers).

De informatie en instructies moeten in een gemakkelijk te begrijpen taal beschikbaar zijn, in elektronische vorm of op papier, gedurende ten minste tien jaar of de ondersteuningsperiode (afhankelijk van welke periode langer is).

4. Rapportageverplichtingen: het melden van kwetsbaarheden en incidenten

Wat betreft de rapportage[19] geeft de onderstaande tabel een overzicht van je verplichtingen. Daaronder vind je verdere toelichting.

[18] EU-conformiteitsverklaring: toegelicht in punt 5.

[19] Art. 14-17, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 1 :

Melding van kwetsbaarheden en incidenten

Melding	Kwetsbaarheden	Incidenten
WAT	*Moet:* 'actief uitgebuite kwetsbaarheden' *Mag:* kwetsbaarheden (niet actief uitgebuit); cyberdreigingen	*Moet*: 'ernstige incidenten' *Mag*: incidenten (niet-ernstig); bijna-incidenten
AAN WIE	CSIRT[20] Centraal meldingsplatform (ENISA) Getroffen gebruikers	
HOE	1) Vroegtijdige waarschuwing (24 uur) 2) Kwetsbaarheidsmelding (72 uur) 3) Eindverslag (14 dagen)	1) Vroegtijdige waarschuwing (24 uur) 2) Incidentmelding (72 uur) 3) Eindverslag (1 maand)

4.1. Wat

Volgens de definities in artikel 3 van de CRA geldt dat:

- Een 'actief uitgebuite kwetsbaarheid' betrouwbaar bewijs vereist van uitbuiting door een kwaadwillende actor in een systeem zonder toestemming van de systeemeigenaar[21] ;

[20] Art. 3, lid 51, CRA: "als coördinator aangewezen CSIRT" betekent een CSIRT dat als coördinator is aangewezen overeenkomstig artikel 12, lid 1, van Richtlijn (EU) 2022/2555.

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

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Een incident als 'ernstig' wordt beschouwd wanneer het[22] :
    - negatieve gevolgen heeft of kan hebben op het vermogen van het PDE om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of functies te beschermen; of
    - heeft geleid of kan leiden tot de invoering/uitvoering van kwaadwillige code in het product of in de netwerk- en informatiesystemen van een gebruiker.

4.2. Aan Wie

Het Computer Security Incident Response Team (CSIRT) waaraan moet worden gemeld, is dat van de lidstaat waar de fabrikant[23] :

- zijn hoofdvestiging heeft; of, indien dit niet vast te stellen is,
- de vestiging heeft met het grootste aantal werknemers.

Indien de hoofdvestiging buiten de EU is, kan een keten worden gevolgd die rekening houdt met de vestiging van de gemachtigde vertegenwoordiger van de fabrikant → importeur → distributeur → de lidstaat waar het grootste aantal gebruikers zich bevindt.

Afgezien van enkele uitzonderingen zullen alle meldingen via het centrale meldingsplatform verlopen dat moet worden opgezet en onderhouden door het Europees Agentschap voor cyberbeveiliging (ENISA), en zullen ze via een elektronische endpoints worden verspreid naar andere CSIRT's en markttoezichtautoriteiten.

Getroffen gebruikers (en, indien van toepassing, alle gebruikers) moeten ook worden geïnformeerd over kwetsbaarheden/incidenten en corrigerende maatregelen, bij voorkeur in een machinaal leesbaar formaat. CSIRT's kunnen gebruikers informeren als de fabrikant dit nalaat[24] .

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

[23] Het CSIRT is doorgaans het nationale CERT: Computer Emergency Response Team.

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

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.3. Hoe

Er zijn meerdere verschillen in de rapportage over kwetsbaarheden en incidenten.

Kwetsbaarheden

1) **Vroegtijdige waarschuwing**: moet uiterlijk binnen 24 uur na constatering worden ingediend en moet, in voorkomend geval, aangeven in welke lidstaten het PDE beschikbaar is.
2) **Kwetsbaarheidsmelding**: moet uiterlijk binnen 72 uur na constatering worden ingediend en moet het volgende bevatten:
    - Algemene informatie over het PDE;
    - Algemene aard van de uitbuiting en de kwetsbaarheid;
    - Correctieve of risicobeperkende maatregelen die zijn genomen en die door gebruikers kunnen worden genomen;
    - Gevoeligheid van de gemelde informatie.
3) **Eindrapport**: dient uiterlijk **14 dagen** na de corrigerende/risicobeperkende maatregel te worden ingediend en moet het volgende bevatten:
    - Beschrijving – ernst en gevolgen;
    - Informatie over kwaadwillige actoren, indien van toepassing;
    - Details over de beschikbare beveiligingsupdate of andere corrigerende maatregelen.

Incidenten

1) **Vroegtijdige waarschuwing**: moet uiterlijk binnen 24 uur na het constateren worden ingediend en moet het volgende vermelden:
    - In voorkomend geval, de lidstaten waar het PDE beschikbaar is;
    - Of er een vermoeden bestaat dat het incident is veroorzaakt door onwettige of kwaadwillige handelingen.
2) **Incidentmelding**: moet uiterlijk binnen 72 uur na constatering worden ingediend en moet het volgende bevatten:
    - Algemene informatie over de aard van het incident;
    - Een eerste beoordeling van het incident;

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Correctieve of beperkende maatregelen die zijn genomen en die door gebruikers kunnen worden genomen;
- De gevoeligheid van de gemelde informatie.

3) **Eindrapport**: moet binnen **één maand** na indiening van de incidentmelding worden ingediend en moet het volgende bevatten:
    - Beschrijving – ernst en gevolgen;
    - Soort bedreiging of grondoorzaak die het incident waarschijnlijk heeft veroorzaakt;
    - Toegepaste en lopende beperkende maatregelen.

5. Conformiteitsbeoordeling

Voordat een PDE op de markt wordt gebracht, moet de fabrikant aantonen dat het voldoet aan de essentiële cyberbeveiligingseisen zoals vastgelegd in bijlage I van de CRA. Dit gebeurt via de **conformiteitsbeoordelingsprocedure** die van toepassing is op de betreffende productcategorie.

5.1. Conformiteitsbeoordelingsprocedures

De CRA voorziet de volgende procedures:

- Interne controle (module A);
- EU-typeonderzoek gevolgd door conformiteit met het EU-type op basis van interne productiecontrole (modules B + C);
- Volledige kwaliteitsborging (module H);
- Beoordeling binnen een Europees cyberbeveiligingscertificeringsregeling, indien van toepassing.

Geharmoniseerde normen en gemeenschappelijke specificaties zijn geen conformiteitsprocedures. Zij kunnen echter wel het aantonen van de conformiteit ondersteunen.

5.2. Vermoeden van conformiteit

Een product dat voldoet aan

- geharmoniseerde normen waarvan de referenties in het Publicatieblad van de Europese Unie zijn bekendgemaakt, of
- gemeenschappelijke specificaties die door de Europese Commissie zijn vastgesteld

wordt **geacht te voldoen**[25] aan de essentiële cyberbeveiligingseisen die onder die normen of specificaties vallen.

Wanneer dergelijke normen of specificaties niet (volledig) worden toegepast, moet de fabrikant rechtstreeks aantonen dat aan de eisen van bijlage I wordt voldaan via de toepasselijke conformiteitsbeoordelingsprocedure. Indien relevant kan ook een Europees cyberbeveiligingscertificaat worden gebruikt om conformiteit aan te tonen, binnen de door de CRA gestelde grenzen.

5.3. Productcategorieën

De toe te passen conformiteitsbeoordelingsprocedure hangt af van de classificatie van het PDE volgens de CRA, zoals gespecificeerd in bijlage III en IV van de CRA[26] . De CRA maakt onderscheid tussen standaardproducten, belangrijke producten (klasse I en II) en kritieke producten.

Afhankelijk van de categorie:

- kan interne controle voldoende zijn;
- kan de betrokkenheid van een aangemelde instantie (NB) vereist zijn; of
- kan beoordeling binnen een Europees cyberbeveiligingscertificeringsregeling verplicht of toegestaan zijn.

De **juiste classificatie** is daarom bepalend voor de vaststelling van de toepasselijke procedure.

Een overzicht van welke procedure per productklasse kan worden toegepast is te vinden in tabel 2 op de onderstaande pagina.

[25] Art. 27, CRA.

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

Tabel 2 :
Conformiteitsbeoordelingsprocedures

	Interne controle (module A)	EU-typeonderzoek + conformiteit o.b.v. interne productiecontrole (modules B + C)	Volledige kwaliteits-borging (module H)	Europese certificerings-regeling	Geharmoniseerde normen/ Gemeenschappelijke specificaties[27]
Standaard-producten	**X**	**X**	**X**	**X**	**X** Kan conformiteits-ondersteuning bieden voor de betreffende eisen
Belangrijke producten Klasse I	**X**[28]	**X**	**X**	**X** niveau: substantieel[29]	**X** Kan conformiteits-ondersteuning bieden voor de betreffende eisen
Belangrijke producten Klasse II		**X**	**X**	**X** niveau: substantieel[30]	**X** Kan conformiteits-ondersteuning bieden voor de betreffende eisen
Kritieke producten				**X** niveau: substantieel	**X** Kan conformiteits-ondersteuning bieden voor de betreffende eisen

[27] Geharmoniseerde normen en gemeenschappelijke specificaties zijn geen procedures, maar kunnen het aantonen van conformiteit ondersteunen.

[28] Interne controle (module A) mag alleen worden gebruikt wanneer geharmoniseerde normen, gemeenschappelijke specificaties of, indien van toepassing, een relevante certificeringsregeling worden toegepast. Wanneer dit niet het geval is, zijn de toepasselijke routes de EU-typeonderzoek gevolgd door conformiteit met het EU-type op basis van interne productiecontrole (modules B+C) of volledige kwaliteitsborging (module H).

[29] Indien krachtens art. 8, lid 1, van de CRA een gedelegeerde handeling wordt vastgesteld, kan de EU-cybercertificeringsregeling worden gebruikt. Zo niet, dan valt men terug op de regels voor Belangrijke Producten, Klasse II.

[30] Voetnoot 29 is van toepassing.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.4. EU-conformiteitsverklaring (EU DoC)

Na een succesvolle conformiteitsbeoordeling stelt de fabrikant een **EU-conformiteitsverklaring** (EU DoC) op[31] .

In deze verklaring bevestig je dat het PDE voldoet aan de toepasselijke essentiële cyberbeveiligingseisen en de vereiste elementen bevat zoals bepaald in de CRA. De modelstructuur is te vinden in bijlage V van de CRA. De vereenvoudigde EU DoC is te vinden in bijlage VI. Deze moet beschikbaar worden gesteld in de talen die voorgeschreven zijn door de lidstaat waarin het PDE op de markt wordt gebracht en moet beschikbaar blijven gedurende de wettelijk voorgeschreven periode.

5.5. CE-markering

Om consumenten in staat te stellen PDE's te herkennen die aan de CRA-eisen voldoen en weloverwogen beslissingen te nemen bij de aankoop en het gebruik van dergelijke PDE's, moet een **CE-markering**[32] "zichtbaar, leesbaar en onuitwisbaar"[33] worden aangebracht voordat het PDE in de handel wordt gebracht. Dit moet op het product zelf gebeuren. Wanneer dit vanwege de aard van het product niet mogelijk is, moet de markering op de verpakking worden aangebracht en worden opgenomen in de bijbehorende EU-conformiteitsverklaring[34] [35] . De CE-markering geeft aan dat het product voldoet aan alle toepasselijke EU-wetgeving die CE-markering vereist, inclusief de CRA.

5.6. Aantonen van conformiteit door middel van technische documentatie

Een belangrijk onderdeel van conformiteit is de **technische documentatie.** Zoals voorgeschreven in artikel 31 van de CRA en bijlage VII, is de technische documentatie relevant voor alle eerder besproken punten, aangezien deze moet worden opgesteld voordat het PDE in de handel wordt gebracht en gedurende de ondersteuningsperiode voortdurend moet worden bijgewerkt[36].

[31] Art. 28, CRA; bijlage V-VI, CRA.
[32] Conformité Européenne (European Conformity).
[33] Art. 30, lid 1, CRA.
[34] Art. 29-30, CRA.
[35] Er gelden aanvullende regels indien een aangemelde instantie bij de conformiteitsbeoordeling betrokken is.
[36] Art. 31, lid 2, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

De technische documentatie brengt de meeste CRA-verplichtingen tezamen en moet daarom het volgende bevatten[37] :

- Algemene beschrijving van het PDE (beoogd doel, softwareversies die van invloed zijn op de naleving, bewijs van externe kenmerken, markering en interne lay-out voor hardware producten, gebruikersinformatie en -instructies);
- Beschrijving van het ontwerp, de ontwikkeling en de productie van het PDE, en de procedures inzake de respons op kwetsbaarheden (bijv. beschrijving van de systeemarchitectuur, SBOM, CVD-beleid, monitoringprocessen, enz.);
- Beoordeling van cyberbeveiligingsrisico's;
- Definitie en verduidelijking van de ondersteuningsperiode;
- Toegepaste geharmoniseerde normen (of delen daarvan);
- Conformiteits- en testverslagen en verslagen over de respons op kwetsbaarheden;
- Exemplaar van de EU-conformiteitsverklaring.

De Europese Commissie zal een **vereenvoudigd formulier** voor **technische documentatie** ontwikkelen voor micro- en kleine ondernemingen[38] . Bovendien bepaalt artikel 33 dat zowel de lidstaten als de Europese Commissie **ondersteuning** moeten bieden aan kmo's – onder andere in de vorm van richtsnoeren[39] en mogelijkheden voor financiële steun.

Het SECURE-project **biedt financiële steun aan kmo's die aan de CRA moeten voldoen en verstrekt doorlopend richtlijnen en materiaal om kmo's te helpen bij de implementatie van de CRA**, zoals deze CRA101-richtlijn.

[37] Bijlage VII, CRA.
[38] Art. 33, lid 5, CRA.
[39] Art. 26, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusie

Om een **toegankelijk overzicht** te bieden **van de belangrijkste verplichtingen die in de CRA zijn vastgelegd**, richt deze richtlijn zich op **vijf onderdelen** van de CRA die minimaal overwogen moeten worden: (1) Beoordeling van cyberbeveiligingsrisico's; (2) Respons op kwetsbaarheden en beveiligingsupdates; (3) Gebruikersinformatie, -instructies en Centraal contactpunt; (4) Rapportageverplichtingen: rapportage van kwetsbaarheden en incidenten; (5) Conformiteitsbeoordeling. De richtlijn verduidelijkt elementen zoals de ondersteuningsperiode, de EU-conformiteitsverklaring en CE-markering, en de technische documentatie. Met het oog op **het ondersteunen van kmo's bij hun navigatie doorheen dit complexe wettelijke kader**, biedt deze richtlijn een samenvatting van de belangrijkste wettelijke verplichtingen die moeten worden begrepen vóór de implementatie ervan. Voor praktische begeleiding over hoe deze wettelijke bepalingen verder moeten worden benaderd en geïmplementeerd, evenals over specifieke elementen van de CRA (bijv. SBOM, kwetsbaarheidsbeheer, enz.), zullen er naarmate de implementatie van de CRA vordert, op doorlopende basis aanvullende technische richtsnoeren en hulpmiddelen beschikbaar komen in de SECURE central repository. Als volgende stappen voor kmo's wordt aanbevolen om de andere richtlijnen in de SECURE-repository te raadplegen, zoals de **CRA's Essential Cybersecurity Requirements: Annex I, Part I** voor praktische suggesties en aanbevelingen over de bepalingen van bijlage I, evenals het **CRA Methodological Compliance Assessment Framework** voor een stapsgewijze toolkit en checklist voor naleving van de gehele CRA.