

Procedurer for overensstemmelse

Cyber Resilience Act (CRA) stiller krav om, at alle produkter med digitale elementer skal gennemgå en **overensstemmelsesprocedure**, der dokumenterer, at de opfylder de væsentlige cybersikkerhedskrav i **Bilag I**.

Valget af procedure afhænger primært af produktets **klassificering** (almindeligt, vigtigt eller kritisk) og om der anvendes **harmoniserede standarder**.

Hvad er en overensstemmelsesprocedure?

Overensstemmelsesproceduren beskriver, **hvordan fabrikanten skal dokumentere**, at produktet er cybersikkert og lever op til kravene. Det er denne proces, der gør CE-mærkningen lovlig.

CRA foreskriver fire forskellige procedurer (Modul A, B, C og H), der kan anvendes:

- ▢ *Modul* er en fælles EU-betegnelse for forskellige procedurer til overensstemmelsesvurdering.
- ▢ *Notified Body* (bemyndiget organ) er en uafhængig og godkendt instans, som vurderer overensstemmelse på vegne af EU.

Oversigt over procedurerne

Modul	Navn	Hvem udfører vurderingen?	Typisk brugt til
Modul A	Intern kontrol	Fabrikanten selv	Almindelige produkter, evt. Klasse I
Modul B	EU-typeafprøvning	Bemyndiget organ	Del 1 af vurdering for Klasse II
Modul C	Typeoverensstemmelse (med produktionskontrol)	Fabrikanten	Del 2 – bruges sammen med B

Modul	Navn	Hvem udfører vurderingen?	Typisk brugt til
Modul H	Fuld kvalitetssikring	Bemyndiget organ + løbende kontrol	Klasse II-produkter, høj kompleksitet

▮ **Modul B og C skal anvendes sammen:** Først vurderer et eksternt organ design og sårbarhedshåndtering (Modul B), derefter sikrer fabrikanten, at produktet produceres i overensstemmelse hermed (Modul C).

Hvornår anvendes hvilke procedurer?

CRA angiver følgende overordnede retningslinjer:

Produktklasse	Anvendt procedure
Almindelige produkter	Modul A (intern kontrol)
Vigtige produkter – Klasse I	Modul A , hvis harmoniseret standard følges
Vigtige produkter – Klasse II	Modul B + C eller Modul H (altid tredjepart)
Kritiske produkter	Modul B + C , Modul H eller cybersikkerhedscertificering

▮ *Gratis open source-software*, der klassificeres som vigtigt produkt, **kan bruge Modul A**, hvis kildekode og dokumentation er offentligt tilgængelige ved markedsføringstidspunktet.

Harmoniserede standarder og formodet overensstemmelse

Hvis en fabrikant vælger at følge en **harmoniseret standard**, opnås der såkaldt *formodning om overensstemmelse*. Det betyder, at myndighederne går ud fra, at kravene i CRA er opfyldt.

▮ Eksempel: **EN 303 645** – en standard for cybersikkerhed i IoT-produkter.

Dette gør CE-mærkning og dokumentation lettere, især for små og mellemstore virksomheder.

Dokumentationskrav

Uanset hvilken procedure der vælges, skal følgende overholdes:

- Fabrikanten skal udarbejde og opbevare **teknisk dokumentation** i henhold til **Bilag VII**
- Dokumentation skal vise, hvordan produktet opfylder kravene i Bilag I
- Den skal være tilgængelig for **markedsovervågningsmyndighederne**
- **Opbevaringspligt:** Mindst **10 år** eller så længe som produktets **supportperiode** varer – alt efter hvad der er længst

▮ Produkter uden korrekt dokumentation eller procedure betragtes som **ikke-overensstemmende**, og kan **fjernes fra markedet** af myndighederne (jf. artikel 58 og 64)

Hurtig tommelfingerregel

- Almindeligt produkt? → Modul A
- Klasse I og anvender standard? → Modul A
- Klasse I uden standard, eller Klasse II? → Modul B + C eller H
- Kritisk produkt? → Certificering eller tredjepartsvurdering

▮ Se også: [07_klassificering_af_produkter.md](#) for at forstå betydningen af produktklassificering i CRA

Last update: 2025-10-30 12:07:19