

EN 40000-serien

Cyber resilience gennem hele produktets
levetid

Jeppe Pilgaard Bjerre

1 oktober 2026

EN 40000-serien i ét billede

Horisontale standarder, som understøtter CRA for produkter med digitale elementer



1-2 etablerer modellen. 1-3 operationaliserer sikkerhedsvedligeholdelsen.

EN 40000-1-2: Cyberresilience-systemet

Risikobaseret styring gennem hele produktets livscyklus

Risikobaseret tilgang

Produktkontekst
Risikoacceptkriterier
Risikovurdering og behandling

Security by design

Least privilege
Attack surface minimization
Defence in depth

Secure by default

Sikker standardkonfiguration
Sikre opdateringer
Beskyttelse af brugeren

Output: dokumenterede beslutninger, krav og evidens

Hvad skal 1-2 kunne efterlade som evidens?

Det afgørende er sporbarhed fra produktkontekst og risiko til beslutning, implementering og test.

01	Produktkontekst	Intended purpose, brugere, miljø, afhængigheder
02	Risikobillede	Aktiver, trusler, konsekvenser og antagelser
03	Behandlingsbeslutninger	Valgte foranstaltninger samt begrundede fravalg
04	Verifikation	Testresultater og objektiv evidens
05	Vedligeholdelse	Triggerpunkter for revurdering og opdatering

Spørgsmålet er ikke kun:

“Hvad har vi gjort?”

men også:

“Hvorfor er det tilstrækkeligt?”

EN 40000-1-3: sårbarheder skal håndteres som en drift

Standarden organiserer producentens aktiviteter i seks sammenhængende faser gennem produktets supportperiode.

FORBEREDELSE | Politikker · roller · CVD · komponentoverblik/SBOM · testplan · sikker opdateringskanal



Nye fund, ændringer og erfaringer føres tilbage til politikker, risikovurdering, komponentdata og testplan.

Kernen: Sårbarheden behandles efter dens faktiske risiko for produktet, ikke kun efter en generisk severity-score.

1-2 og 1-3 hænger sammen gennem produktets levetid

1-2 styrer risikobeslutningerne. 1-3 leverer operationelle signaler, rettelser og læring tilbage.



Tre ting at tage med

Den korte version

01

Cybersecurity er en livscyklusaktivitet

Sikkerheden skal etableres, vedligeholdes og revurderes.

02

Vulnerability handling er en formaliseret proces

Politikker, komponentdata, monitorering, remediation og kommunikation skal hænge sammen.

03

1-2 og 1-3 udgør én operationel model

Risikostyringen fra 1-2 driver beslutningerne i 1-3.

1-2 bygger cyberresilience. 1-3 holder sikkerheden aktuel efter release.

Fra CRA-overblik til praktisk implementering

Kursus hos Dansk Standard: Cyber Resilience Act

Et naturligt næste skridt

01

FORSTÅ

CRA's struktur, roller og centrale forpligtelser

02

OMSÆT

kravene til produktets udvikling, dokumentation og support

03

PLANLÆG

en praktisk vej mod compliance i egen organisation

Målet: at kunne omsætte CRA fra lovtekst til konkrete aktiviteter og evidens.

21. oktober 2026

kl. 9:00 - 16:00

Cyber Resilience Act – krav og standarder i praksis

● Få pladser tilbage

Dansk Standard, 12 etage, Lokale O

Göteborg Plads 1

2150

Nordhavn

**Læs
kursusbeskrivelsen og
se aktuelle datoer**

Scan QR-koden



Thank you



Jeppe Pilgaard Bjerre
Specialist
+4543251548
jpbj@forcetechnology.com

