Cyber Resilience Act og de kommende krav til danske virksomheder

Dagens program

10:00 **Velkommen**

10:05 **Introduktion til Cyber Resilience Act**

Winn Nielsen, Digitaliseringsstyrelsen

10:30 **Hvad kommer Cyber Resilience Act til at betyde for danske virksomheder?**

Mette Peetz-Schou, Dansk Industri

10:55 **Standarder og CE-mærkning**

Jeppe Pilgaard Bjerre, Force Technology

11:20 **Spørgsmål og afrunding**

11:30 **Tak for i dag**

Om Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- Ca. 190 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:

Dansk Standards udvalg for cyber- og informationssikkerhed er med til at skrive fremtidens standarder

DANSK STANDARD

Udvalget består af 55+ medlemmer fra store danske virksomheder, smv'er, konsulenthuse, offentlige myndigheder, NGO'er, brancheorganisationer mm.

- Åbent for alle interesserede
- Beslutter den danske holdning
- Sikrer, at de danske interesser bliver varetaget på den internationale bane
- Bidrager til at definere fremtidens markedskrav

Aktuelle temaer

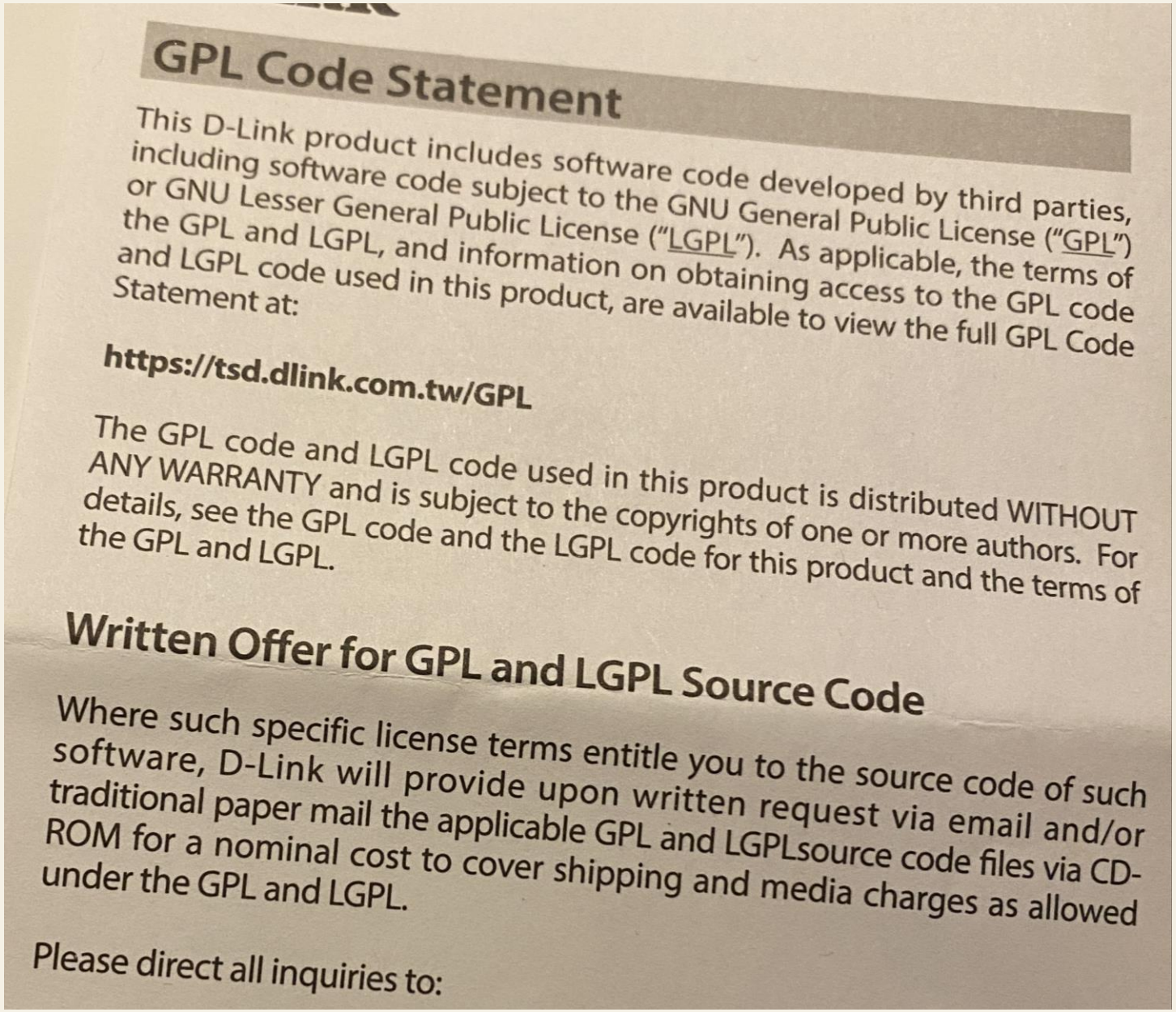
- Holde øje med udviklingen og implementeringen af relevant lovgivning på cyberområdet; fx **Cyber Resilience Act**, Cyber Security Act, Radioudstyrsdirektivet og NIS2.
- Følge aktivt med i udviklingen af de standarder, der skal udarbejdes i relation til EU lovgivning, herunder standarder under **Cyber Resilience Act** og Radioudstyrsdirektivet.
- Eventuelle revisioner af ISO/IEC 27000 serien
- Udbrede kendskabet til standarder for cyber- og informationssikkerhed gennem egne arrangementer, indlæg på eksterne arrangementer, via artikler mm.

Læs mere om udvalget på ds.dk/s-441

Digitaliseringsstyrelsen

Cyber resilience act

Winn Nielsen
Winnie@digst.dk



GPL Code Statement

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to view the full GPL Code Statement at:

https://tsd.dlink.com.tw/GPL

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

Written Offer for GPL and LGPL Source Code

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPLsource code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:

Agenda

1. Formål
2. Baggrund
3. Overblik
4. Omfattede produkter og opdeling
5. Tilgængeliggørelse
6. Væsentlig ændring
7. Krav og forpligtelser
8. Overensstemmelse
9. Standardiseringsanmodning
10. Tilsyn og håndhævelse
11. Status og tidslinje

Cyber resilence act - formål

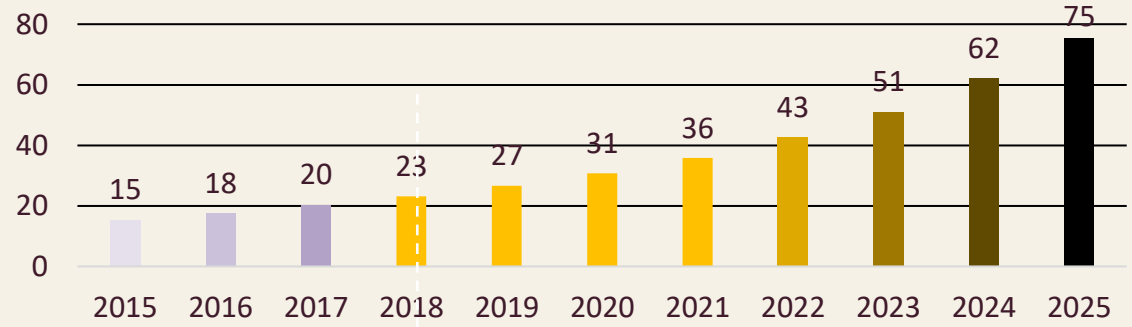
1. Strømline og supplere de eksisterende regler
2. Skabe et minimumsniveau af cybersikkerhed i produkter
3. Forhindre fragmentering af cybersikkerhedskravene til produkter på det indre marked

a) Dække alle produkter (der ikke i forvejen er dækket andre steder på samme niveau)
b) Dække alle facetter af cybersikkerhed (integritet, tilgængelighed og fortrolighed)
c) Dække hele produktets livscyklus
d) Dække alle involverede

Baggrund

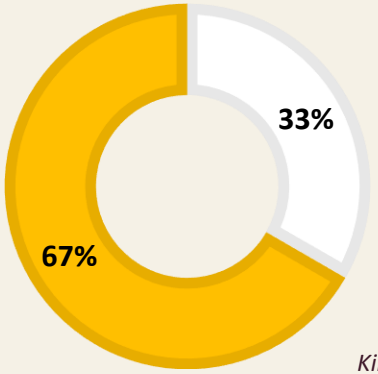
- **Stærkt stigende brug** af produkter med en digital komponent (inkl. software)
- **Lavt cybersikkerhedsniveau** (eller slet ikke eksisterende)
  - Udbredte sårbarheder og utilstrækkelig og inkonsekvent levering af sikkerhedsopdateringer til at løse dem
  - En utilstrækkelig brugerforståelse og adgang til information
- **Betydelige risici**
  - Produkterne kan anvendes som **springbræt**
  - Produkterne kan, koordineret med andre eller lignende produkter, anvendes til **storskala angreb**
- **Store konsekvenser** for borgernes sikkerhed og grundlæggende rettigheder og friheder.
- **Øgede omkostningerne** for brugerne og samfundet
  - Vellykkede cyberangreb førte i 2021 til en årlig omkostning for cyberkriminalitet på ca. **41 billioner kr.** globalt

IoT-enheder på verdensplan fra 2015 til 2025 (i mia.)



Kilde: Forbes / IHS (2021)

Årsager til cybersikkerhedshændelser i digital infrastruktur og tjenester (NIS)



Udnyttelse af sårbarheder
i IoT-produkter og software

Andre årsager
Fx phishing eller identitetstyveri

Kilde: ENISA/Gartner (2022)

Overblik

Cybersikkerhedsregler for hardware og software

Minimumsniveau for sikkerhed i produkter før de må sættes på markedet

Forpligtelser for producenter, distributører og importører

Ansvar og forpligtelser gennem hele forsyningskæden

Krav gennem produktets livscyklus

Cybersikkerhed fra design til udfasning af produktet. Fx via håndtering af sårbarheder gennem softwareopdateringer

Harmoniserede standarder

Tilbyder en vejledning for overholdelse af cybersikkerhedskravene

Vurdering af overensstemmelse

Forskellige vurderingsprocedurer baseret på produktets risikoprofil

Rapporteringsforpligtelser

Virksomheder skal rapportere om cybersikkerhedshændelser inden for bestemte tidsrammer

Markedsovervågning og håndhævelse

Værktøjer og beføjelser så myndigheder effektivt kan tage hånd om overtrædelser af cybersikkerhedsregler og sikre ensrettet tilgang nationalt og på tværs af grænser

Omfattede produkter

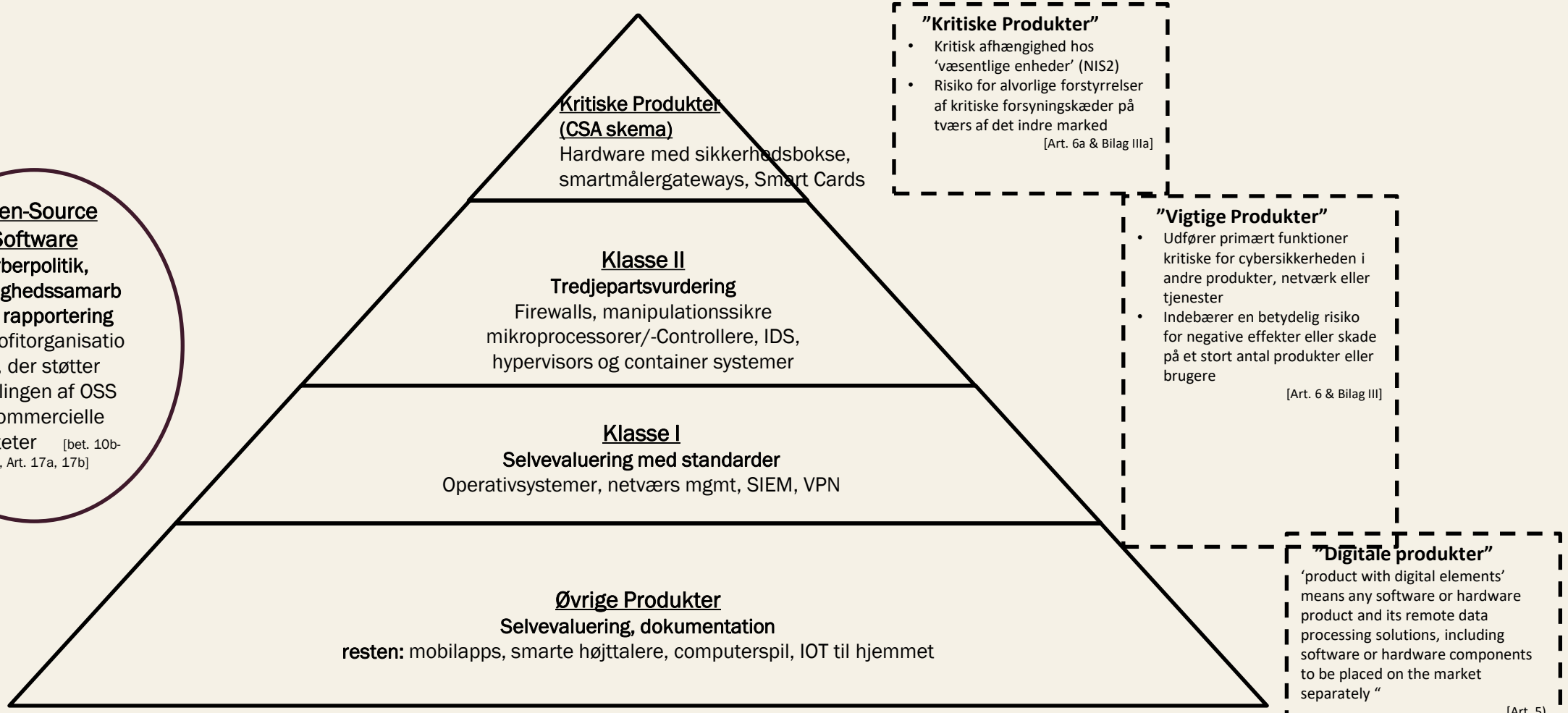
Omfattet

- Hardware produkter og komponenter, der tilgængeliggøres på markedet
  - fx bærbare computere, smarte apparater, grafikkort, bundkort og sensorer
- Software produkter og komponenter, der tilgængeliggøres på markedet separate
  - Fx operativsystemer, tekstbehandling, regneark, spil, browsere og mobilapps, plugins og browserudvidelser
- Fjerndatabehandling
  - fx Kontrolfunktion til en smart-termostat hostet i clouden; Indkøbs-app, der gemmer indkøbslisten på producentens server; Cloud-baseret tekstbehandling

Ikke omfattet

- Ikke-kommercielle produkter
  - Open Source (uden betalte tillægstjenester/support)
  - Offentlige løsninger som ikke er del af en kommerciel aktivitet
- Tjenester (fx enkeltstående Cloud / SaaS / hjemmesider) (Dækket (delvist) af NIS2)
- Særregulering, nationale kompetencer, m.fl.
- Identiske reservedele
- Produkter udelukkende udviklet eller tilpasset tbf. national sikkerhed og militære formål
- Køretøjer (2019/2144 EU)
- Medicinsk udstyr (2017/745 & 2017/746 EU)
- Certificeret luftfartsudstyr (2018/1139 EU)

Opdeling af produkter



Tilgængeliggørelse

"gøre tilgængelig på markedet": enhver levering af et produkt med digitale elementer med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed mod eller uden vederlag

Fabrikant, importør og distributør

En importør eller distributør anses for at være fabrikant når denne bringer et produkt med digitale elementer i omsætning under sit navn eller varemærke eller foretager en væsentlig ændring af et produkt med digitale elementer, der allerede er bragt i omsætning.

Væsentlig Ændring

Definition: En ændring efter produktets markedsføring, som påvirker overensstemmelsen med CRA's væsentlige krav eller ændrer produktets tiltænkte anvendelsesformål

- Ændrer det tiltænkte formål: Softwareopdateringer, der ændrer produktets tiltænkte formål, som ikke var forudset i den oprindelige risikovurdering.
- Ændrer Risikoniveauet: Opdateringer, der ændrer risikotypen eller øger risikoniveauet

- Sikkerhedsopdateringer betragtes ikke som væsentlige, hvis de ikke ændrer det tiltænkte formål, men kun foretager mindre justeringer for at mindske cybersikkerhedsrisikoen.

- Mindre Funktionalitetsopdateringer: Generelt ikke betragtet som væsentlige, f.eks. visuelle forbedringer eller nye sprog.

Forpligtelser ved Væsentlige Ændringer

- produktets overensstemmelse med CRA skal verificeres igen via passende procedure jf. risikoniveauet.
- Importører og distributører, der foretager væsentlige ændringer, anses som producenter og CRA's dertilhørende krav.

Krav til produkter

Væsentlige Krav (Bilag I)

- **Produktegenskaber (del 1)**
- Design og udvikling skal sikre et passende risikobaseret cybersikkerhedsniveau.
- Sikker-som-standard; mulighed for nulstilling til oprindelig tilstand.
- Adressering af sårbarheder via sikkerhedsopdateringer; inkl. automatisk opdatering.
- Beskyttelse mod uautoriseret adgang; kryptering af data; integritetsbeskyttelse.
- Dataminimering (produktets formål); funktionalitetssikring efter hændelser.
- Begrænsning af angrebsflader.
- Sikker sletning af brugerdata og -indstillinger; sikker dataoverførsel.

Håndtering af Sårbarheder (del 2)

- Identifikation og dokumentation af sårbarheder; softwarekomponentliste.
- Omhyggelig og rettidig håndtering af sårbarheder; sikkerhedsopdateringer adskilt fra funktionalitetsopdateringer.
- Regelmæssige sikkerhedstests og -revisioner; offentliggørelse af opdateringsinfo.
- Koordineret sårbarhedsoplysningspolitik; sikker opdateringsdistribution.
- Gratis sikkerhedsopdateringer med vejledning; fremme af sårbarhedsoplysningsdeling

Forpligtelser og supportperiode

Forpligtelser

- Produktsikkerhed fra Design til Udfasning:
  Sikre indbygget cybersikkerhed og løbende håndtering af sårbarheder.
- Risikovurdering og Compliance:
  Gennemføre regelmæssige risikovurderinger; overholde specifikke sikkerhedsstandarder.
- Rapportering af Sårbarheder:
  Etabler procedurer for hurtig identifikation og rapportering af sikkerhedshuller.
- Overvågning og Opdateringer:
  Sikre løbende overvågning og udgivelse af sikkerhedsopdateringer.
- Transparens for Brugere:
  Informer brugere om produktsikkerhed og opdateringspolitikker.
- Samarbejde med Myndigheder:
  Samarbejd med tilsynsmyndigheder om cybersikkerhedsrisici og compliance.

Supportperiode (Art. 10(6))

- Fastlægges af fabrikanten baseret på forventet brugstid.
- Mindst 5 år, eller lig med forventet brugstid hvis under 5 år.
- Skal tage højde for brugerforventninger, produktets natur og formål, samt relevant EU-lovgivning.
- Kan skelnes til lignende produkter, tilgængelighed af driftsmiljø, tredjepartskomponenters supportperiode, og vejledning fra ADCO eller Kommissionen.

Overensstemmelsesprocedure

Overensstemmelsesprocedure

- ”Alm.” produkter: selvevaluering
- Kritiske produkter:
  - Klasse 1: brug af en harmoniseret standard eller tredjepartsvurdering
  - Klasse 2: tredjepartsvurdering
- Særligt kritiske produkter: EU certificering (CSA)

Særlige hensyn

- Overensstemmelse med krav i anden lovgivning
  - Cybersikkerhedskrav i MR + AIA
  - Produktsikkerhedskrav under GPSR
  - Særlig procedure for EHR-systemer i EHDS-forordningen
- Tilpassede SMV-vurderingsgebyrer

Tilsyn og håndhævelse

Tilsyn

Værktøjer til rådighed for markedsovervågningsmyndigheder (MSA'er):

- Dokumentationskontrol, anmodninger om oplysninger, kontrolbesøg, laboratorietest
- Koordination og samarbejde mellem Kommissionen/ENISA og nationale myndigheder
- Notifikation om cybersikkerhedshændelser: nationale CSIRTs -> ENISA -> MSA'er

Håndhævelse

Ved manglende overholdelse har MSA'er beføjelser til at:

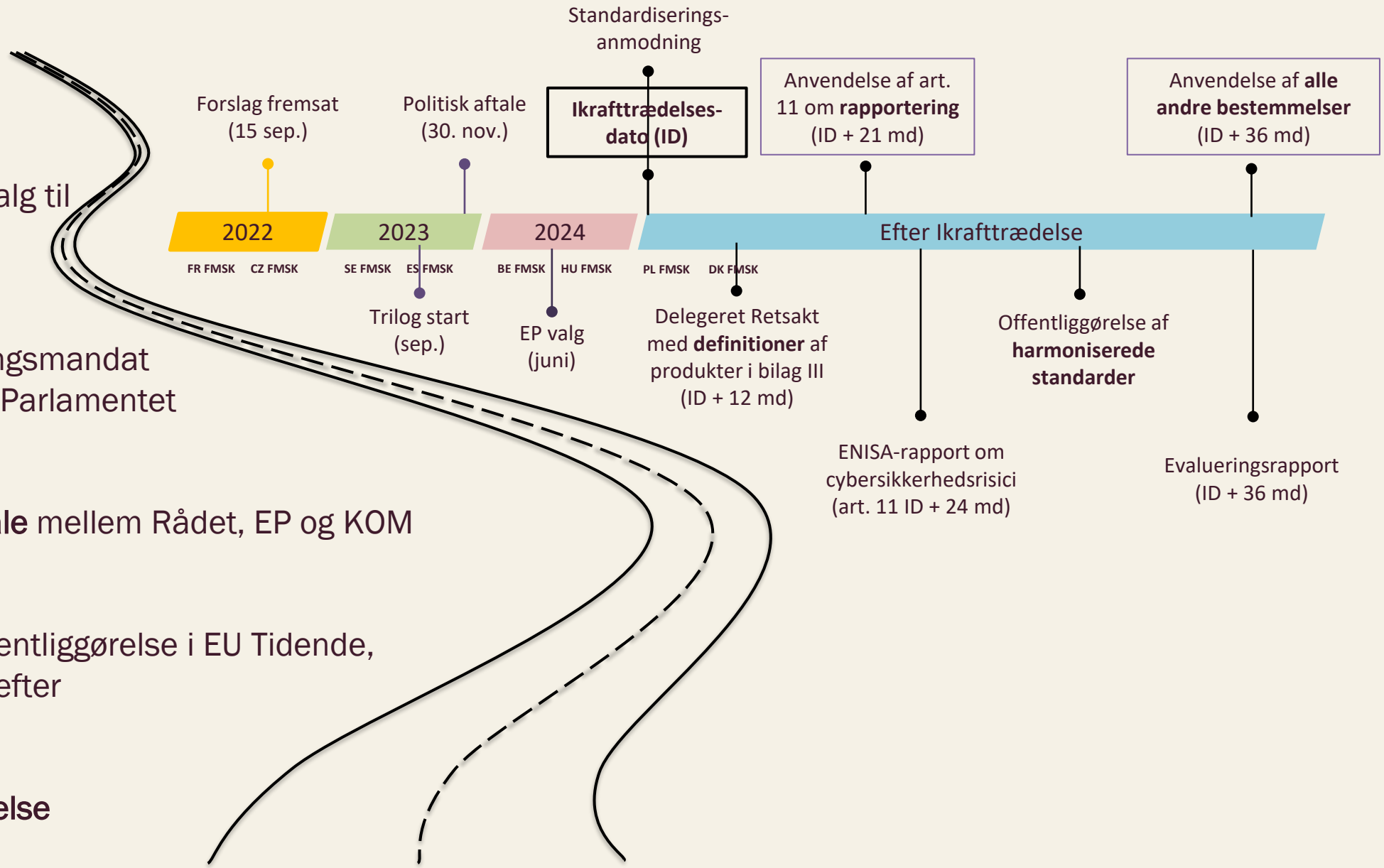
- Kræve at fabrikanter bringer manglende overholdelse til ophør og eliminerer risiko;
- Forbyde/begrænse tilgængeliggørelsen af et produkt eller at kræve, at produktet trækkes tilbage/tilbagekaldes;
- Pålægge bøder (op til 112 mio. kr. eller op til 2,5 % af global omsætning).

Under ekstraordinære omstændigheder kan Kommissionen kræve, at ENISA foretager en evaluering og, hvis det skønnes nødvendigt på EU-plan, forberede en korrigerende eller restriktiv foranstaltning, via en gennemførelsesretsakt (og efter høringer af medlemsstaterne).

Tidsplan og status

- **21. april 2023**
  Forelæggelse for Folketingets Europaudvalg til **Forhandlingsmandat**
- **19. juli 2023**
  Vedtagelse af forhandlingsmandat i både Rådet og Europe-Parlamentet
- **30. November 2023**
  Enighed om **politisk aftale** mellem Rådet, EP og KOM
- **3-4. kvartal 2024**
  Formel vedtagelse*, offentliggørelse i EU Tidende, ikrafttrædelse 20 dage efter
- **2026 / 2027**
  Reglerne finder **anvendelse**

*mulig forsinkelse pga. oversættelse



Tak for ordet

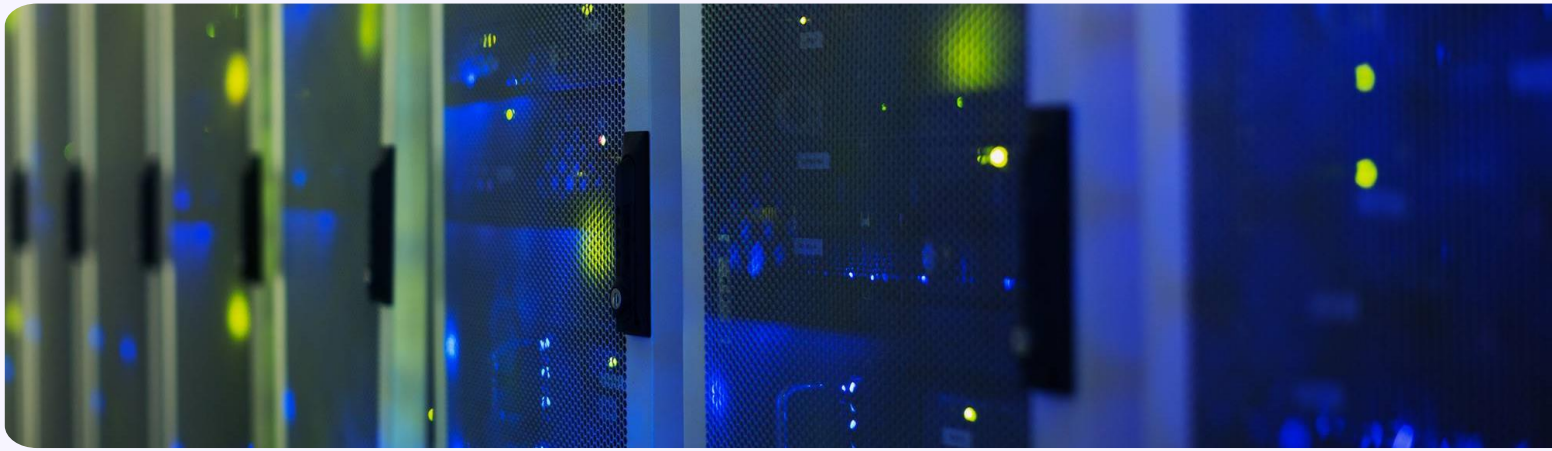
Hvad kommer Cyber Resilience Act til at betyde for danske virksomheder?

Seniorchefkonsulent, Mette Peetz-Schou, DI - Europapolitik

Dansk Industri

Tvunget fokus på cybersikkerhed

Minimumskrav på tværs af produkter



Dansk Industri

Flere krav til flere produkter

Krav til produkters cybersikkerhed på det tidspunkt, hvor de bringes i omsætning

Krav til produkter gennem hele livscyklus
- I udviklingsfasen
- Efter at de er bragt i omsætning
-
Nyt for CE-mærkede produkter

Fysiske produkter
(maskiner, radioudstyr, forbrugerprodukter)

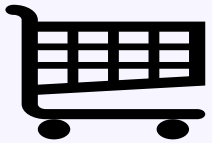
Software (indlejret/ikke indlejret)

Delvis udtagelse for open sourse software

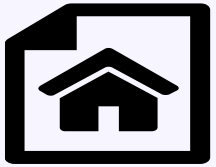
Fjerndatabehandling

Dansk Industri

Leverandør af komponenter



Kunde, der køber produkter og komponenter



Produktionsenheden (NIS2-krav)

Dansk Industri

Hvad er vigtigst nu i forhold til Cyber Resilience Act?

Dokumentér designfasen af de produkter, der er under udvikling (Q4 2027)

Gør klar til overvågning og rapportering af sårbarheder for alle produkter
–også dem, der allerede er på markedet og er indenfor produktets forventede levetid

Dansk Industri

Sæt dig ind i de generelle krav!
Husk andre krav, der kan ramme dit produkt, som evt. skal opfyldes inden!

Forbrugerprodukter (December 2024)
Radioudstyr (August 2025)
Maskiner (Januar 2027)
Kunstig intelligens (Efterår 2026)

Dansk Industri

Forpligtelser

1. **Produktsikkerhed fra Design til Udfasning:**
   Sikre indbygget cybersikkerhed og løbende håndtering af sårbarheder.
2. **Risikovurdering og Compliance:**
   Gennemføre regelmæssige risikovurderinger; overholde specifikke sikkerhedsstandarder.
3. **Rapportering af Sårbarheder:**
   Etabler procedurer for hurtig identifikation og rapportering af sikkerhedshuller.
4. **Overvågning og Opdateringer:**
   Sikre løbende overvågning og udgivelse af sikkerhedsopdateringer.
5. **Transparens for Brugere:**
   Informer brugere om produktsikkerhed og opdateringspolitikker.
6. **Samarbejde med Myndigheder:**
   Samarbejd med tilsynsmyndigheder om cybersikkerhedsrisici og compliance.

Supportperiode (Art. 10(6))

- Fastlægges af fabrikanten baseret på forventet brugstid.
- Mindst 5 år, eller lig med forventet brugstid hvis under 5 år.
- Skal tage højde for brugerforventninger, produktets natur og formål, samt relevant EU-lovgivning.
- Kan skelnes til lignende produkter, tilgængelighed af driftsmiljø, tredjepartskomponenters supportperiode, og vejledning fra ADCO eller Kommissionen.

Væsentlige Krav (Bilag I)

Produktegenskaber (del 1)

- Design og udvikling skal sikre et passende risikobaseret cybersikkerhedsniveau.
- Sikker-som-standard; mulighed for nulstilling til oprindelig tilstand.
- Adressering af sårbarheder via sikkerhedsopdateringer; inkl. automatisk opdatering.
- Beskyttelse mod uautoriseret adgang; kryptering af data; integritetsbeskyttelse.
- Dataminimering (produktets formål); funktionalitetssikring efter hændelser.
- Begrænsning af angrebsflader.
- Sikker sletning af brugerdata og -indstillinger; sikker dataoverførsel.

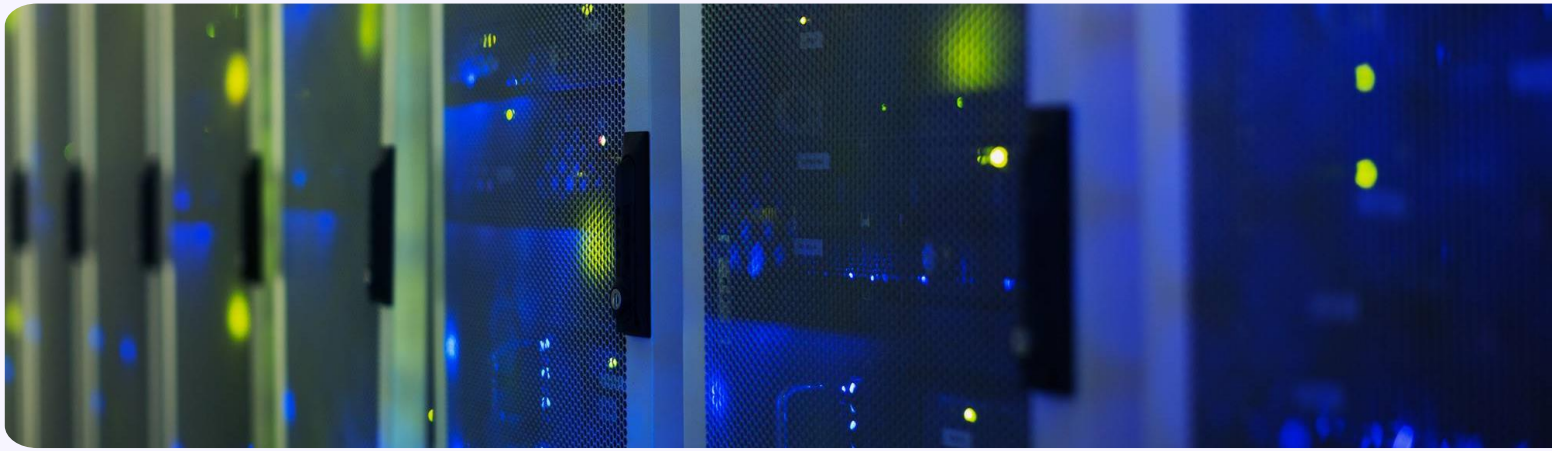
Håndtering af Sårbarheder (del 2)

- Identifikation og dokumentation af sårbarheder; softwarekomponentliste.
- Omhyggelig og rettidig håndtering af sårbarheder; sikkerhedsopdateringer adskilt fra funktionalitetsopdateringer.
- Regelmæssige sikkerhedstests og -revisioner; offentliggørelse af opdateringsinfo.
- Koordineret sårbarhedsoplysningspolitik; sikker opdateringsdistribution.
- Gratis sikkerhedsopdateringer med vejledning; fremme af sårbarhedsoplysningsdeling

digitaliserings og
ligestillingsministeriet

Løbende indfasning af regulering

Dobbelt regulering? Desværre, ja!



Dansk Industri

Benyt dig af de standarder der allerede findes

F.eks.

- EN 18031-1,-2, -3 serien (RED DA)
- Søg inspiration i DS/PAS 2600:2021 (cybersikkerhed i produkter (IoT))

Dansk Industri

Vær opmærksom på, hvis dine produkter ikke er omfattet af selvevaluering (modul A)

Kravene er de samme på tværs af produkter. Men nogle produkter kræver brug af 3. part i forbindelse med overensstemmelsesvurderingen

Definitioner af de relevante produkter er under udarbejdelse

Dansk Industri

Etablér en organisation, der kan håndtere kravene til produkterne, leverandørerne og produktionen

IT, OT, Legal, Product Compliance

Vigtigt at arbejde sammen

Dansk Industri

Leverandør af komponenter

Din virksomhed(NIS2)

Produktionsenheden

Maskine

- kan være forbundet til nettet via radio
- kan benytte kunstig intelligens
- benytter software
- (kan benyttes af en forbruger)

Kunde, der køber produkter og komponenter

Dansk Industri

Hvad skal jeg gøre nu?

Forhold dig til alle de regler der kommer!

Etabler samarbejde på tværs af organisationen

IT – OT
Legal – product compliance

Arbejd med produkternes cybersikkerhed samtidigt med cybersikkerheden af produktionsenheden (NIS2)

- Skel til Cyberrobusthedsforordningen, selvom det ikke er de regler, der skal anvendes først
  - Reglerne vedr. radioudstyr forventes at blive trukket tilbage
  - Relationen til anden cyberlovgivning er uklar
- Overvej NIS2 krav, også selvom I ikke bliver omfattet
  - Cybertruslen er reel og kan lægge jeres forretning ned
- Se om D-mærket kan hjælpe jer på vej
  - D-mærket | Mærkningsordning for it-sikkerhed og data (d-maerket.dk)

- Kom på forkant gennem deltagelse i standardisering (S-441)
- Søg inspiration i DS/PAS 2600:2021 (cybersikkerhed i produkter (IoT)) og de nye standarder under radioudstyrsdirektivet, der kommer snart☺

Anvendelsesdato for EU-lovgivning vedr. cybersikkerhed Produktionsenheder og produkter

Q4 2024
Forordning om produkters sikkerhed i almindelighed (GPSR).
Finder anvendelse 13. december 2024.

Q3 2025
Kommissions forordning under Artikel 3.3 i Radioudstyrsdirektivet (RED DA)
Forordningen finder anvendelse 1. august 2025.
(Standarder afventer final vote)

Q1 2027
Maskinforordning (MR)
Forordningen finder anvendelse 20. januar 2027.
(StRq godkendt)

Q2 2021
Forordning om cybersikkerhed (CSA)
Forordningen fandt anvendelse den 28. juni 2021.

Q4 2024
Nyt revideret direktiv om et højt fælles sikkerhedsniveau for net- og informationssystemer (NIS2)
Direktivet skal implementeres i dansk ret og finder anvendelse 18. oktober 2024.
Dansk implementering forsinket.

Q2-Q3 2026
Forordning om kunstig intelligens (AIR)
Forordningen forventes publiceret til sommer, krav indfases løbende frem til Q2 2027.
NB kun 12 måneder for general purpose AI
(StRq afventer publicering)

Q3-4 2027
Cyberrobustheds-lovgivning (CRA)
Forventes publiceret til efteråret.
Finder anvendelse 36 måneder senere.
(Sårbarhedshåndtering finder anvendelse 15 måneder tidligere)
(StRq under udarbejdelse)

Efterfulgt af tilbagetrækning af RED DA?

Dansk Industri

Hvis I har spørgsmål

Mette Peetz-Schou
Seniorchefkonsulent,
Europapolitik
Dansk Industri

Telefon: 33773022
Mobil: 40373728
Mail: meps@di.dk

Baggrund med krav fra de forskellige andre lovgivninger

Seniorchefkonsulent, Mette Peetz-Schou, DI - Europapolitik

Dansk Industri

Forordning om (forbruger)produkters sikkerhed i almindelighed (GPSR)

(EU) 2023/988

Artikel 5
Almindeligt sikkerhedskrav
Erhvervsdrivende må kun bringe sikre produkter i omsætning eller gøre sikre produkter tilgængelige på markedet.

Artikel 6
Aspekter til vurdering af produkters sikkerhed
I forbindelse med vurdering af, hvorvidt et produkt er sikkert, tages der navnlig hensyn til følgende aspekter:
…
g) når produktets art kræver det, de ***passende egenskaber hvad angår cybersikkerhed***, som er nødvendige for at beskytte produktet mod påvirkninger udefra, herunder ondsindede tredjemænd, ***hvis en sådan påvirkning kan have indflydelse på produktets sikkerhed***, herunder et muligt tab af indbyrdes sammenhæng.

Anvendelsesområde

(EU) 2023/988

Artikel 2

Anvendelsesområde

1. Denne forordning finder anvendelse på produkter, som bringes i omsætning eller gøres tilgængelige på markedet, medmindre der findes EU-ret med specifikke bestemmelser om sikkerheden ved de pågældende produkter, som har samme formål.

Når produkter er omfattet af specifikke sikkerhedskrav ifølge EU-retten, finder denne forordning kun anvendelse på de aspekter og de risici eller kategorier af risici, som ikke er omfattet af disse krav.

I denne forordning forstås ved:

1) »produkt«: ethvert produkt, som, hvad enten det har forbindelse med andre varer, der mod eller uden vederlag leveres eller gøres tilgængelige, herunder i forbindelse med levering af en tjenesteydelse, eller ej, er bestemt for forbrugerne, eller som under rimeligt forudsigelige betingelser sandsynligvis vil blive anvendt af forbrugerne, selv om det ikke er bestemt for dem

Krav til radioudstyrs cybersikkerhed

- Skal sikrer, at radioudstyr
  - Ikke skader nettet eller dets funktion eller misbruger net ressourcer på en sådan måde, at det medfører en uacceptabel forringelse af tjenesten.
  - Er i stand til at sikre, at personoplysninger om brugeren og abonnenten og disses privatliv beskyttes
  - Understøtter visse faciliteter, der sikrer beskyttelse mod svig

- Gælder for radioudstyr, der kan forbindes til internettet
  - Direkte eller indirekte kommunikation via andet udstyr
    - Legetøj, børneprodukter, kropsbåret udstyr mv. i fokus under forhandlinger (forbrugerbeskyttelse)
    - Rammer alt – også industriel anvendelse af radioudstyr

Hvad betyder det i praksis?

Harmonised standards in support of the essential requirement set out in Article 3(3), point (d/e/f), of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:

d	1.	include elements to monitor and control network traffic, including the transmission of outgoing data;
d	2.	is designed to mitigate the effects of ongoing denial of service attacks;
def	3.	implement appropriate authentication and access control mechanisms;
def	4.	are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the <d><e><f>;
def	5.	are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to <d><e><f>;
def	6.	protect the exposed attack surfaces and minimise the impact of successful attacks.
ef	7.	protect stored, transmitted or otherwise processed <e> <f> against accidental or unauthorised storage, processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability of <e> <f>;
e	8.	include functionalities to inform the user of changes that may affect data protection and privacy;
ef	9.	log the internal activity that can have an impact on <e> <f>;
e	10.	allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information;

<d> = network or its functioning or misuse of network resources, <e> = personal & location data protection and privacy, <f> = financial or monetary data

Tre standarder på vej

18031-1 (Common security)
18031-2 (dataprotection)
18031-3 (fraud)

➡ Afventer
Final vote
Citation in the OJEU

Krav om brug af notificeret organ, hvis standarderne ikke publiceres

Maskinforordningen

1.1.9. *Beskyttelse mod forvanskning*

Maskinen eller det relaterede produkt skal konstrueres og fremstilles således, at dets forbindelse til en anden anordning, ved selve den tilsluttede anordnings egenskaber eller ved enhver anordning, som er fjerntilsluttet maskinen eller det relaterede produkt, ikke fører til farlige situationer.

➡ Sikkerhed

En hardwarekomponent, som transmitterer signaler eller data, som er relevante for forbindelse eller adgang til software, der er kritisk for maskinen eller det relaterede produkts overensstemmelse med de relevante væsentlige sikkerheds- og sundhedskrav, skal fremstilles således, at den er tilstrækkeligt beskyttet mod tilsigtet eller utilsigtet forvanskning. Maskinen eller det relaterede produkt skal indsamle dokumentation for legitim eller illegitim indtrængen i denne hardwarekomponent, når det er relevant for forbindelse eller adgang til software, der er kritisk for maskinens eller det relaterede produkts overensstemmelse med kravene.

➡ Tilstrækkelig beskyttelse

Dokumentation af indtrængen

Beskyttelse og identifikation af relevant software

Software og data, der er kritisk for maskinens eller det relaterede produkts overensstemmelse med de relevante væsentlige sikkerheds- og sundhedskrav, skal identificeres som sådan og skal være tilstrækkeligt beskyttet mod tilsigtet og utilsigtet forvanskning.

Maskinen eller det relaterede produkt skal identificere softwaren, der er installeret i dem, og som er nødvendig for en sikker drift, og de skal til enhver tid være i stand til at forelægge disse oplysninger i et lettilgængeligt format.

Maskinen eller det relaterede produkt skal indsamle dokumentation for legitim og illegitim indtrængen i software, eller en ændring i den i maskinen eller det relaterede produkt installerede software eller dens konfiguration.

(EU) 2023/1230

Maskinforordningen, fortsat

1.2.1. *Styresystemernes sikkerhed og pålidelighed*

Styresystemerne skal være konstrueret og fremstillet således, at der ikke kan opstå farlige situationer.

Styresystemer skal være konstrueret og fremstillet således:

a) at de efter omstændighederne og risiciene kan modstå de tilsigtede driftspåvirkninger og tilsigtede og utilsigtede ydre påvirkninger, herunder tredjeparters ondsindede handlinger, som med rimelighed kan forudses, og som fører til en farlig situation

Standardiseringsanmodningen er accepteret af CEN/CENELEC
Mapping af mangler i eksisterende standarder i gang
Behov for opdatering og publicering under maskinforordningen

(EU) 2023/1230

Forordning om kunstig intelligens

Article 15 (chapter III, section 2)

Accuracy, robustness and cybersecurity

1. **High-risk AI systems** shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness**,** and cybersecurity, and that they perform consistently in those respects throughout their lifecycle

Article 55 (chapter V, section 3)

Obligations for providers of **general-purpose AI models** with systemic risk

(d) ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model.

CRA - STANDARDS & CE

Jeppe Pilgaard Bjerre

Art. 24 – Conformity assessment procedure

Basic products

- Module A
- Module B+C
- Module H
- EU Cybersecurity certification scheme

Important products Class I

- Module A (Full hEN)
- Module B+C
- Module H
- EU Cybersecurity certification scheme (AL Substantial)

Important products Class II

- Module B+C
- Module H
- EU Cybersecurity certification scheme (AL Substantial)

Critical products

- EU Cybersecurity certification scheme (AL >= Substantial) for the specific product type
- As Class II, if no scheme exists

Updated standardisation request – 17/04-2024

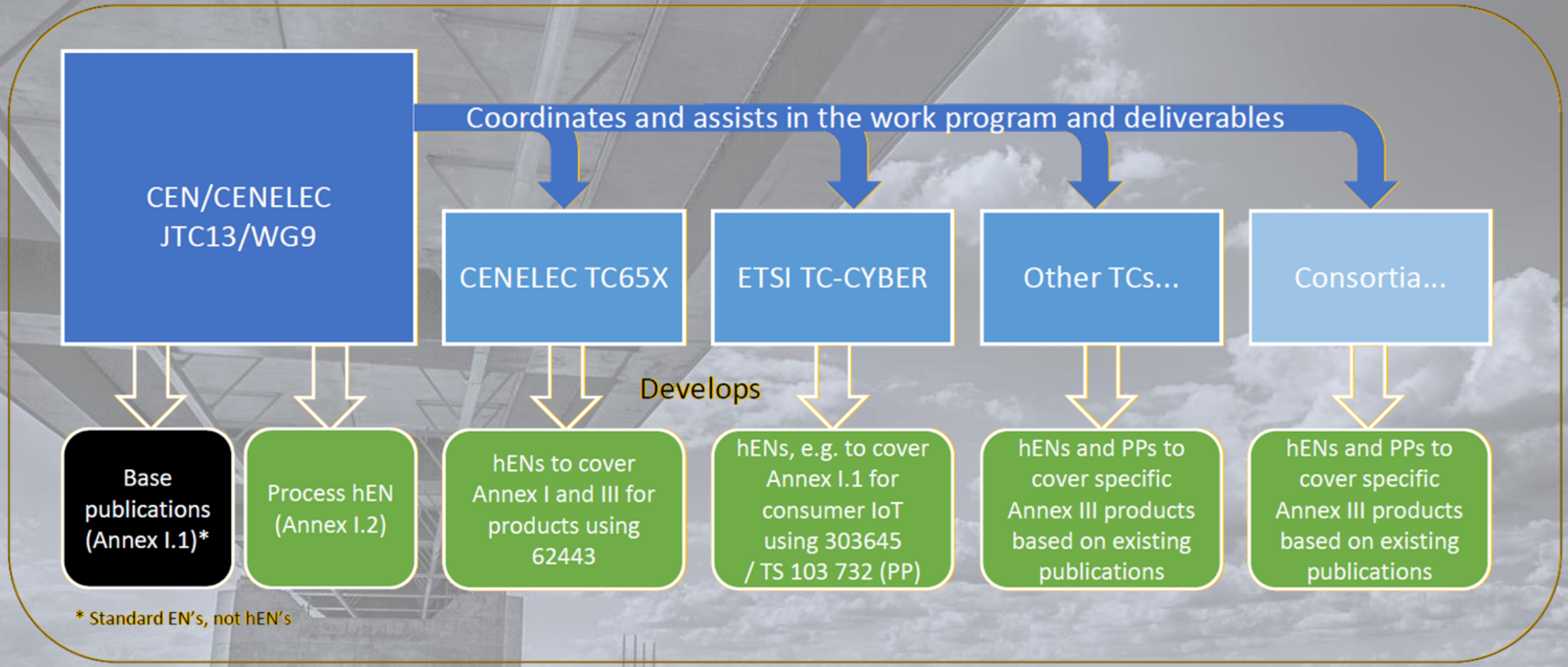
Download link:
Draft standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

Requesting 41 deliverables

- 2 horizontal proces standards by 30/08/2026
- 13 horizontal essential requirements by 30/10/2027
- 26 vertical standards by 30/10/2026

Note: the actual number of deliverables will depend on the proposed solutions by CEN/CLC which might be less (or more)

CRA framework proposal under discussion



CRA framework proposal under discussion

Horizontal

Cybersecurity requirements for products with digital elements – **General principles for cyber resilience Basic PROCESS standard** with horizontal application, guidance for common security by design considerations
Horizontal deliverable [SR.1 - 30/08/2026]

Cybersecurity requirements for products with digital elements – **Common security requirements Basic standard** with horizontal application, lists common risk mitigation requirements to address Annex I part I (multiple) *Horizontal deliverable('s) [SR.2-SR.14 - 30/10/2027], not covering specific products, reusing EN 18031*

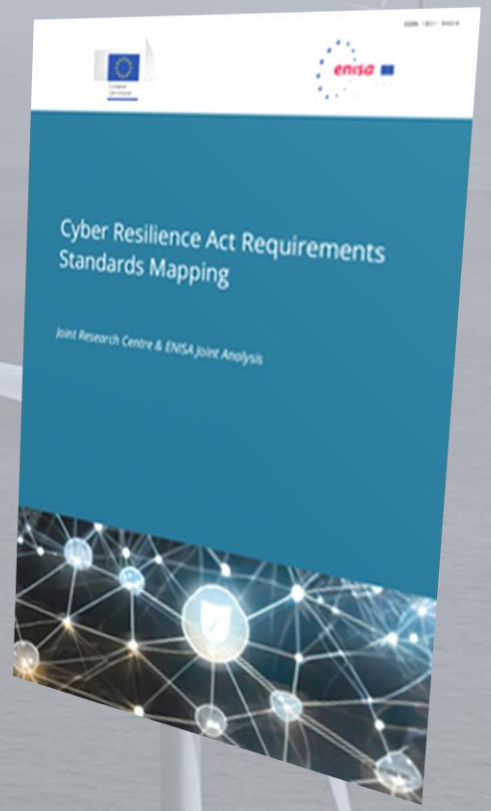
Cybersecurity requirements for products with digital elements – **Security vulnerability handling Basic PROCESS standard** with horizontal application, covers vulnerability handling as stated in Annex I part II
Horizontal deliverable [SR.15 - 30/08/2026], possibly to be cited directly or via the vertical standards

Vertical [Product(s)] Example

Cybersecurity requirements for products with digital elements – **Operational Technology Group standard** with broad application, covers essential requirements of Annex I part I for a group of products
Vertical deliverable (preferably) intended to be cited for presumption of conformity [30/10/2026]

Cybersecurity requirements for products with digital elements – **Industrial network switches Product standard** with limited application, covers essential requirements of Annex I part I for specific products
Vertical deliverable intended to be cited for presumption of conformity [SR.36? - 30/10/2026]

Standards mapping



Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis

DOWNLOAD LINK

Standards mapping (excerpt)

	Security requirements relating to the properties of products with digital elements												
Standard	1	2	3a	3b	3c	3d	3e	3f	3g	3h	3i	3j	3k
EN 303 645 V2.1.1 (2020-06)	X	X	X	X	X	X	X	X	X	X	X	X	X
EN IEC 62443-4-2:2019				X	X	X		X		X		X	X
EN IEC 62443-4-1:2018	X	X											
EN IEC 62443-3-2:2020	X												
EN ISO/IEC	X		X					X			X	X	X

	Vulnerability handling requirements							
Standard	1	2	3	4	5	6	7	8
EN 303 645 V2.1.1 (2020-06)				X	X			
EN ISO/IEC 30111:2020		X		X	X	X		X
EN IEC 62443-4-1:2018		X		X			X	X
EN ISO/IEC 29147:2020		X		X	X	X		X

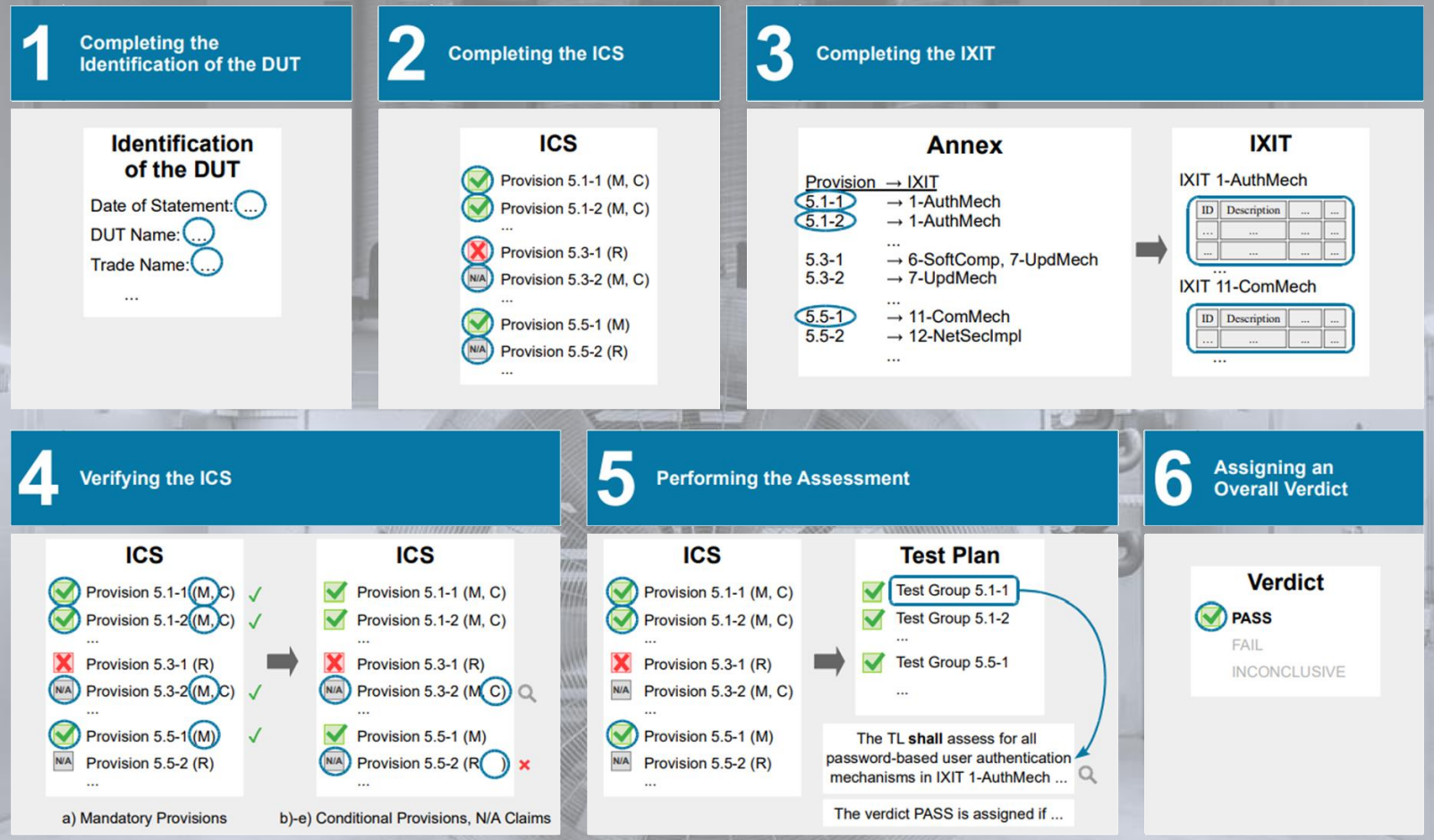
ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements

Scope

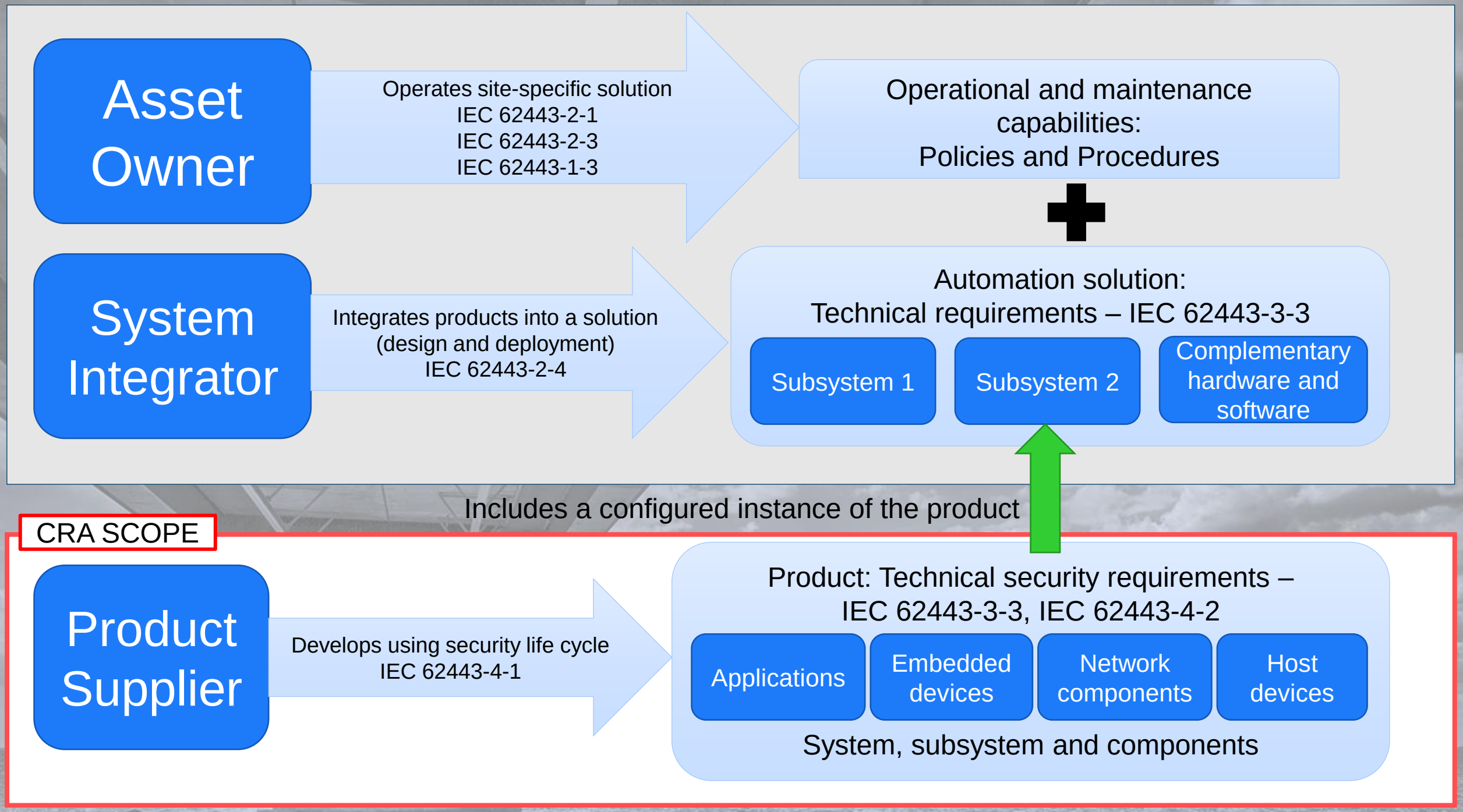
- connected children's toys and baby monitors;
- connected smoke detectors, door locks and window sensors;
- IoT gateways, base stations and hubs to which multiple devices connect;
- smart cameras, smart speakers and smart TVs together with their remote controls;
- wearable health trackers;
- connected home automation and alarm systems, especially their gateways and hubs;
- connected appliances, such as washing machines and fridges; and
- smart home assistants.

DOWNLOAD LINK - EN 303 645 V3.1.2 (2024-06)

ETSI TS 103 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements



[DOWNLOAD LINK - TS 103 701 v1.1.1 (2021-08)]


Asset Owner
Operates site-specific solution
IEC 62443-2-1
IEC 62443-2-3
IEC 62443-1-3
Operational and maintenance capabilities:
Policies and Procedures
System Integrator
Integrates products into a solution
(design and deployment)
IEC 62443-2-4
Automation solution:
Technical requirements – IEC 62443-3-3
Subsystem 1
Subsystem 2
Complementary hardware and software
Includes a configured instance of the product
CRA SCOPE
Product Supplier
Develops using security life cycle
IEC 62443-4-1
Product: Technical security requirements –
IEC 62443-3-3, IEC 62443-4-2
Applications
Embedded devices
Network components
Host devices
System, subsystem and components

NIS2 – Supplier management - Guidance

ENISA publication
[LINK]

3.5.1 Suppliers:

A supplier of products should have processes in place that provide quality products in regards of cybersecurity. As an overview, it can be summarised as follows. A supplier has the infrastructure and organisation relevant for the design, development, manufacturing and delivery of products and components managed by the requirements of ***ISO/IEC 27001***. A secure development process such as ***IEC 62443-4-1:2018*** is deployed, and technical requirements of products and components are set out in ***IEC 62443-4-2:2019***. A quality management system ***ISO 9001*** is implemented to continuously improve the quality.

NIS2 – Supplier management - Guidance

ENISA publication
LINK

3.5.2 System integrators:

A system integrator should have processes in place which ensure that cybersecurity requirements for systems are taken into consideration. As an overview, it can be summarised as follows. A system integrator has the infrastructure and organisation relevant for the design and deployment of a system managed by requirements of ***ISO/IEC 27001:2022***. A secure integrator process such as ***IEC 62443-2-4:2019*** is employed, and technical requirements of the system are reflected by ***IEC 62443-3-3***. A quality management system ISO ***9001:2015*** is implemented to continuously improve the quality.

Inspiration – DS/PAS 2600:2021

Introduction to European and international standards on product-centric cybersecurity standards for IoT products and solutions

DOWNLOAD LINK


Questions?

Consultations for manufacturers of important and critical products in the context of implementation of Cyber Resilience Act

- Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
- Standalone and embedded browsers
- Security information and event management (SIEM) systems
- Software that searches for, removes, or quarantines malicious software
- Firewalls, intrusion detection and prevention systems
- Products with digital elements with the function of virtual private network (VPN)
- Network management systems
- Boot managers
- Public key infrastructure (PKI) and digital certificate issuance software
- Physical and virtual network interfaces
- Operating systems
- Routers, modems intended for the connection to the internet, and switches
- Smart home general purpose virtual assistants
- Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
- Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council that have social interactive features (e.g. speaking or filming) or that have location tracking features
- Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply, or personal wearable products that are intended for the use by and for children
- Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
- Hardware Devices with Security Boxes
- Smartcards or similar devices, including secure elements
- Smart meter gateways within smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 of the European Parliament and of the Council and other devices for advanced security purposes, including for secure cryptoprocessing
- Microprocessors with security-related functionalities; Microcontrollers with security-related functionalities; Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities; Tamper-resistant microprocessors; and Tamper-resistant microcontrollers

Konsultationerne foregår mellem 26. juni og 17. juli. Tilmelding og mere information: https://ec.europa.eu/eusurvey/runner/CRAconsultations

Koblingen mellem lovgivning på det digitale område og standarder

Cyber Resilience Act

Cyber Resilience Act er en ny EU-forordning som stiller fælleseuropæiske cybersikkerhedskrav til produkter med digitale elementer. Med forordningen følger en række standarder, der skal hjælpe virksomhederne med at leve op til de horisonale cybersikkerhedskrav.

Cyber Security Act

Den europæiske forordning om cybersikkerhed har til formål at etablere en fælles europæisk ramme for certificering inden for cybersikkerhed, som forventes at bygge på eksisterende standarder.

Data Act

Dataforordningen (Data Act) skal skabe harmoniserede regler om fair adgang til og anvendelse af data og gøre det lettere for europæiske virksomheder at dele og anvende data.

AI Act

Forordningen om kunstig intelligens (AI Act) skal sikre fælles spilleregler for brugen og udviklingen af kunstig intelligens. Med forordningen følger en række standarder, der skal hjælpe virksomhederne med at leve op til kravene om kunstig intelligens, som forordningen stiller.

Data Governance Act

Datastyringsforordningen (Data Governance Act) har til formål at skabe tillid til datadeling til gavn for samfundet, og der skal bl.a. prioriteres tværsektorielle standarder for datadeling og interoperabilitet.

GDPR

Databeskyttelsesforordningen (GDPR) fastlægger fælleseuropæiske retningslinjer for håndteringen af personoplysninger for virksomheder, organisationer, myndigheder mm.

NIS2-direktivet

NIS2-direktivet indeholder skærpede krav til cyber- og informationssikkerhed i forhold til kritisk infrastruktur. Direktivet opfordrer til at anvende internationale, anerkendte standarder.

https://www.ds.dk/da/i-fokus/lovgivning/lovgivning-paa-det-digitale-omraade-og-standarder

DANSK STANDARD

DS CYBERDAG

3. oktober 2024

Spørgsmål?

DANSK STANDARD