EU's Cybersikkerhedskrav

MICHAEL STAUSHOLM

PRINCIPAL SECURITY ARCHITECT

Sammen kommer vi #foran**digitalt**

ALEXANDRA INSTITUTTET

EU har fået øje på cybersikkerhed

- 2018: GDPR + NIS Directive
- 2019: Cyber Security Act
- 2022: Digital Services Act + Digital Markets Act
- 2024: Product Liability Directive + General Product Safety Regulation + NIS 2 Directive + DORA + Cyber Solidarity Act + AI Act
- 2025: Radio Equipment Directive Delegated Act
- 2027: Cyber Resilience Act + Machinery Directive
- Derudover: Medico, Automobiler og anden særlovgivning

Hvordan tackler vi udfordringen?

- Stor opgave for SMV’er
  - Hvad er vi omfattet af?
  - Hvordan skal vi gribe det an?

- **Kan vi undgå GDPR lignende tilstande?**

Introducerende guide

Guide til risikostyring
Risikostyring i forhold til cyber- og informationssikkerhed for smv'er

DS/PAS 2600:2021 Cybersikkerhed i produkter (IoT)

- Giver ikke alle svar:
  - Et hurtigt overblik
  - Et bud på hvordan man kan komme igang

- 3 cases / virksomheder
  - Hvordan “typiske” virksomheder er berørt
  - … og hvordan kan arbejdet gribes an

- Fokus på NIS 2 og CRA

NIS 2

Grundlæggende IT sikkerhed for “vigtige” virksomheder

- Risikostyring
- Involvering fra ledelsen
- Generel IT-sikkerhed
- Fokus på underleverandører (!)

Mange har allerede det tekniske på plads

- Gap analyse
- Dokumentation og compliance

NIS 2 Status

Effekt (i EU) 17/10-2024

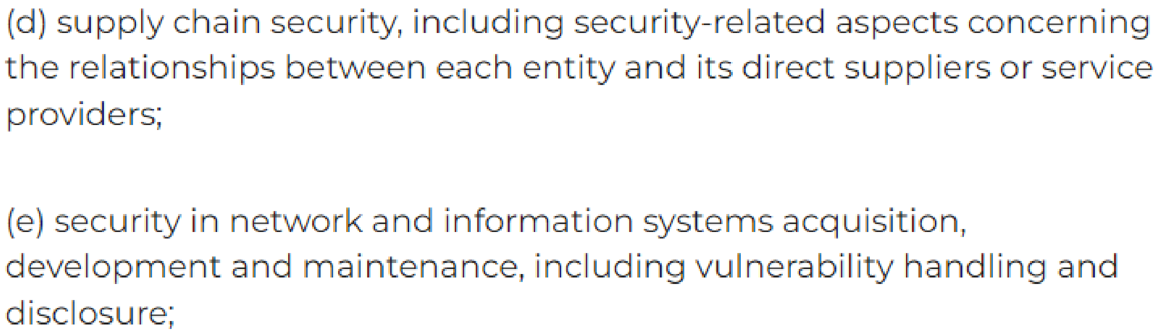
Dansk implementering har været i høring

Dansk lov pr. 1/3-2025

Nyt resort ministerium

- Måske flere forsinkelser?

Forsyningskæder



(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

- Hvilke krav skal en underleverandør leve op til?
- ENISA anbefaler: ISO 27001, IEC 62443-4-1 og ISO 9001
  - Er det realistisk?

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY

JUNE 2023

CRA - STANDARDS & CE

Jeppe Pilgaard Bjerre

FORCE TECHNOLOGY

Art. 1 - Subject matter

(a) rules for the ***making available*** on the market of products with digital elements to ensure the cybersecurity of such products

(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity

(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the ***time the product is expected to be in use***, and obligations for economic operators in relation to these processes;

(d) rules on market surveillance, ***including monitoring***, and enforcement of the above-mentioned rules and requirements.

Art. 1 - Subject matter

(a) rules for the ***making available*** on the market of products with digital elements to ensure the cybersecurity of such products

(b) essential requirements for the design, development elements, and obligations for economic operators in relat cybersecurity

‘product with digital elements’ means a software or hardware product and its remote data processing solutions, including software or hardware components ***being*** placed on the market separately;

(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the ***time the product is expected to be in use***, and obligations for economic operators in relation to these processes;

(d) rules on market surveillance, ***including monitoring***, and enforcement of the above-mentioned rules and requirements.

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*

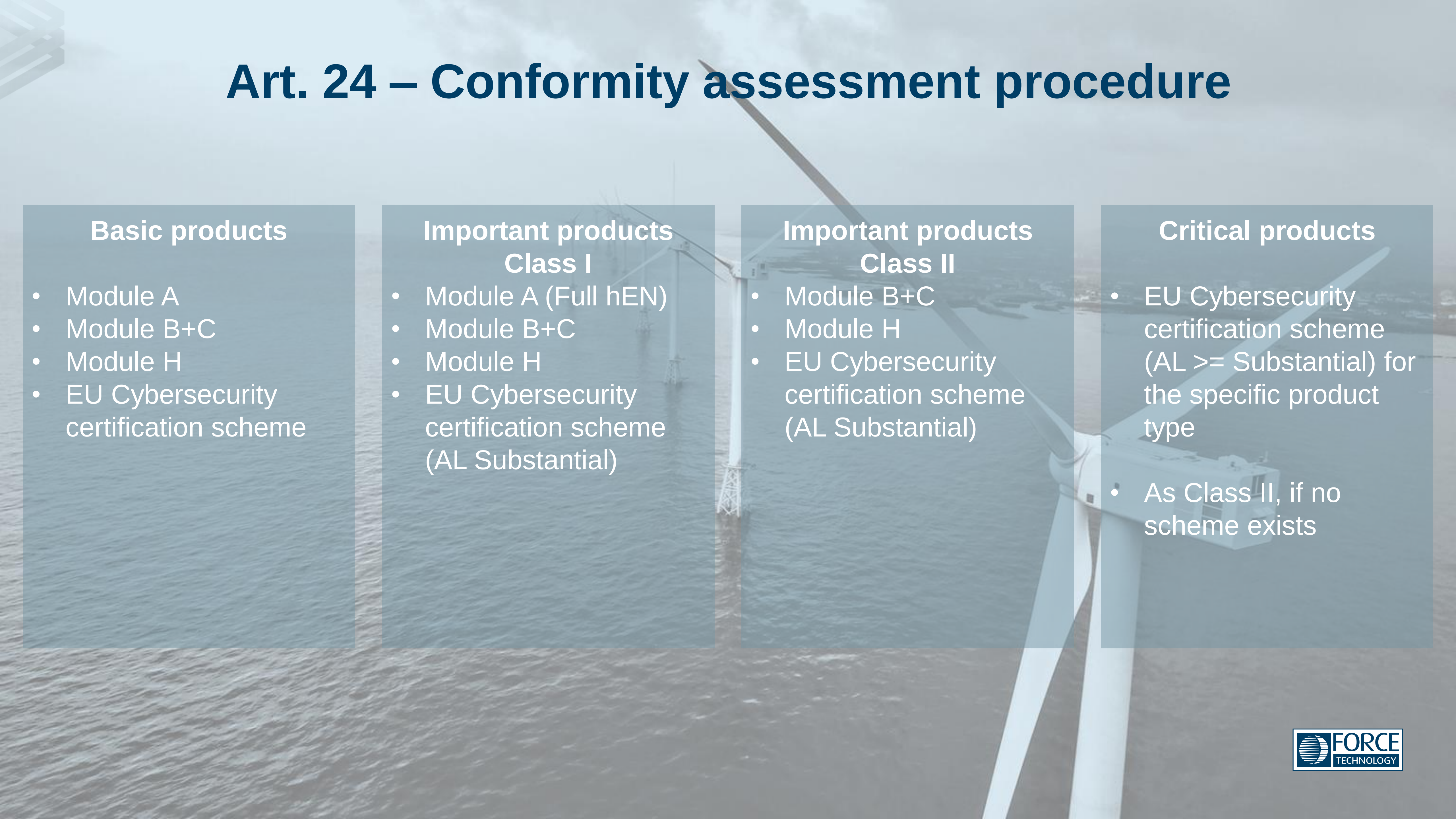
Cybersecurity requirements for products with digital elements – **Security vulnerability handling Basic PROCESS standard** with horizontal application, covers vulnerability handling as stated in Annex I part II
Horizontal deliverable [SR.15 - 30/08/2026], possibly to be cited directly or via the vertical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

FORCE TECHNOLOGY



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

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.

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY

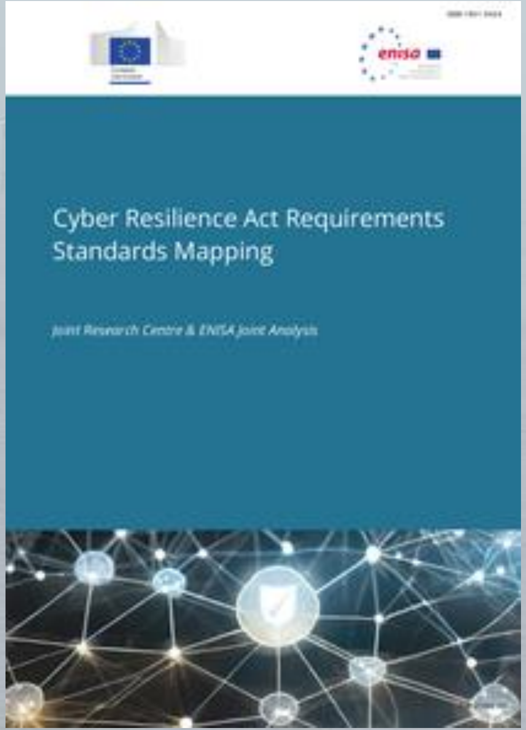
JUNE 2023

Standards inspiration

DS/PAS 2600:2021
Cybersikkerhed i
produkter (IoT)

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

DOWNLOAD LINK



Cyber Resilience Act Requirements
Standards Mapping

Joint Research Centre & ENISA Joint Analysis

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

DOWNLOAD LINK

Questions?