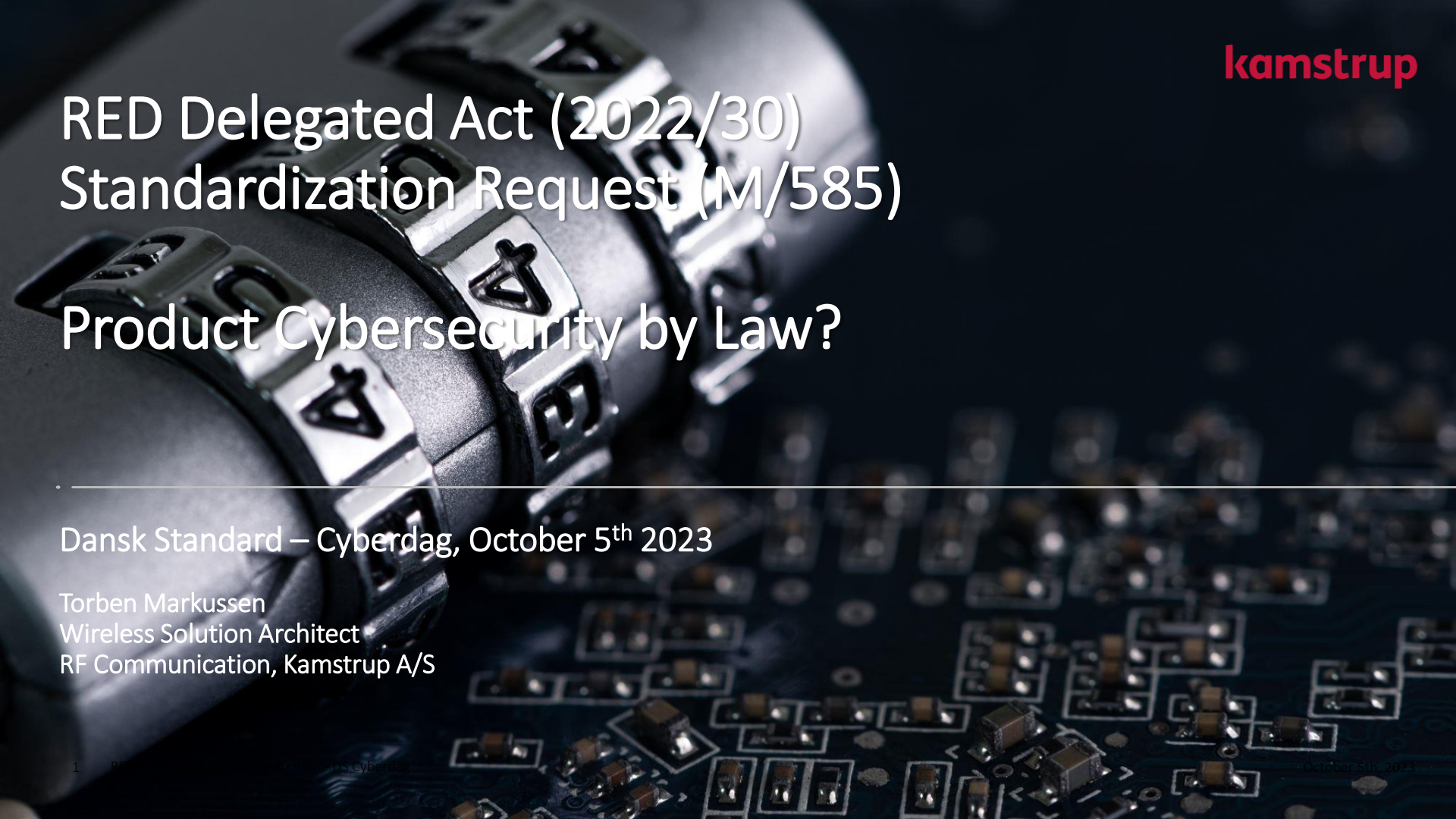


kamstrup

RED Delegated Act (2022/30) Standardization Request (M/585)

Product Cybersecurity by Law?

Dansk Standard – Cyberdag, October 5th 2023

Torben Markussen
Wireless Solution Architect
RF Communication, Kamstrup A/S

… Who am I and why are we involved in this work?

- Cybersecurity on products by law
- Radio Equipment Directive (RED)
- The Standardisation Request
- How does this affect a manufacturer?
- Introduction to the harmonised standards

Cybersecurity Recommendations

- Cybersecurity Standards
- Sector Specific Regulations
- National Provisions
- EU Regulations
- Customer Requirements

Voluntary?

ISO 27000 series

IEC 62443-X

CEM v3.1 (ISO 15408)
(certification)

EN 303 645

Bundesamt
für Sicherheit in der
Informationstechnik

NIST SP 1800 series

When does Radio Equipment Directive apply to a product?

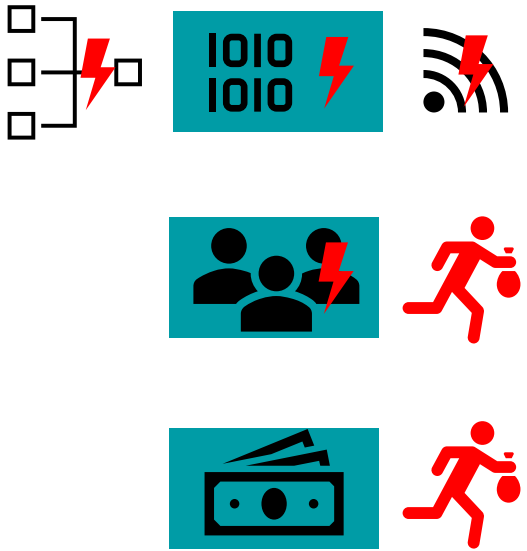
- Radio equipment into the EU market
- Radio function within the product
  - Transmitters
  - Receivers
  - Transceivers
- Frequency range of up to 3000 GHz

Essential requirements scope

Product Safety Article 3.1.a	EMC Performance Article 3.1.b	Radio Performance Article 3.2	Other categories Article 3.3

RED Delegated Regulation (2022/30) activates RED requirements 3.3.(d)(e)(f)

- 3.3 (d) “radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”
- 3.3 (e) “radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected”
- 3.3 (f) “radio equipment supports certain features ensuring protection from fraud”



kamstrup

Scope of Regulation 2022/30

- Internet connected

- OR childcare, toys or wearables

3.3 (e)

Applicability date

- Enters into force 1st August 2025

- All products “placed on the market” after this date must comply

kamstrup

What is a harmonized European Norm (standard)?

- Harmonized standards (hENs) enable self-assessment, ***IF***

Manufacturer has fully applied (tested against)
- Harmonised Standards
- Listed in the OJEU
- For RED Articles 3.2 and 3.3

- A tool to demonstrate ***Presumption of Conformity*** with the essential requirements of the directive

Standardization Request (M/585)

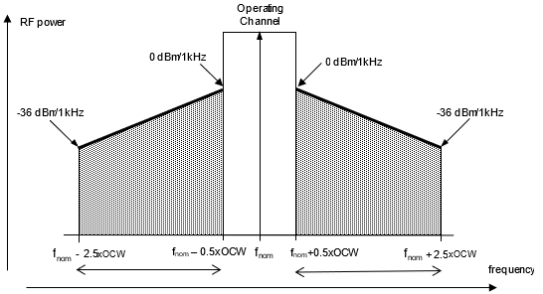
- 3 Generic harmonized standards
  - Covering 3.3 (d) + 3.3 (e) + 3.3 (f)
  - Applicable to all products in scope

- Mandated to CEN CENELEC JTC13 / WG8

Challenges

Most of the current (200+) RED harmonized standards have a very specific scope

- Test limits are regulated and static over time
- Test equipment is specified
- Test methods are defined
- PASS / FAILURE criteria is clearly defined
- Measurable, objectively verifiable criteria leading to assessment verdict

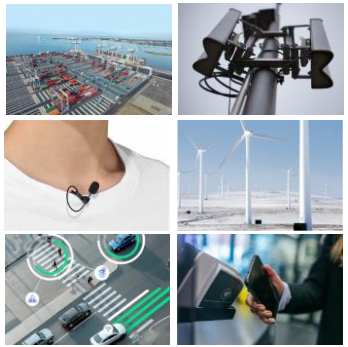


Cyber risks / vulnerabilities are a moving target

Address all products using various technologies in scope of (EU) 2022/30

Horizontal scope includes a huge variety of equipment for very different use environments (risk)

The security protection levels that should be achieved are different across various sectors (assets)



Many appropriate solutions

Introduction to the Harmonized Standards

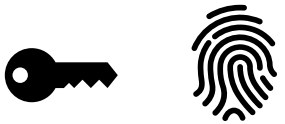
Requirement	prEN 18031-1 3.3.(d)	prEN 18031-2 3.3.(e)	prEN 18031-3 3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

Introduction to the Harmonized Standards

Requirement	prEN 18031-1 3.3.(d)	prEN 18031-2 3.3.(e)	prEN 18031-3 3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

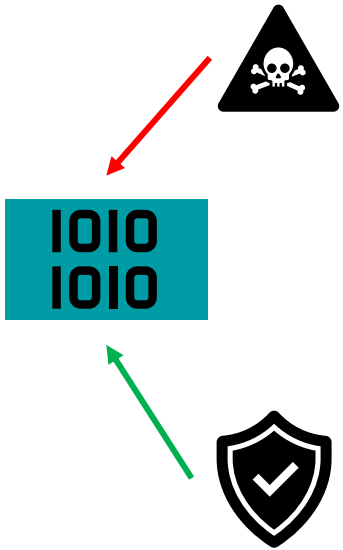
Introduction to the Harmonized Standards

Requirement	prEN 18031-1 3.3.(d)	prEN 18031-2 3.3.(e)	prEN 18031-3 3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓



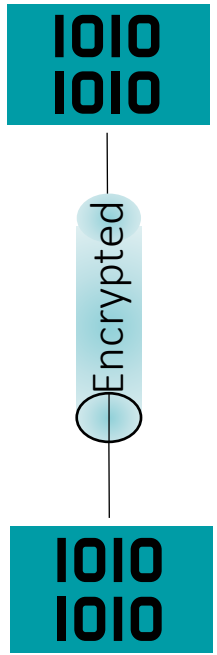
Introduction to the Harmonized Standards

Requirement	prEN 18031-1 3.3.(d)	prEN 18031-2 3.3.(e)	prEN 18031-3 3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓



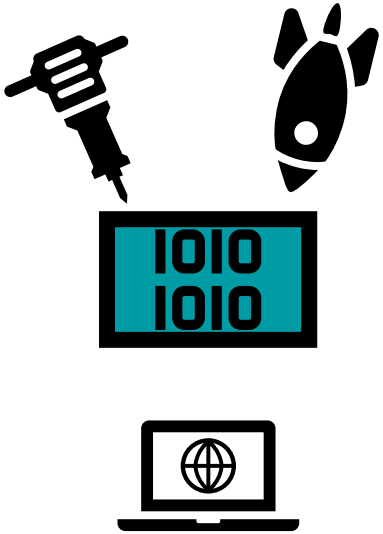
Introduction to the Harmonized Standards

Requirement	prEN 18031-1 3.3.(d)	prEN 18031-2 3.3.(e)	prEN 18031-3 3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓



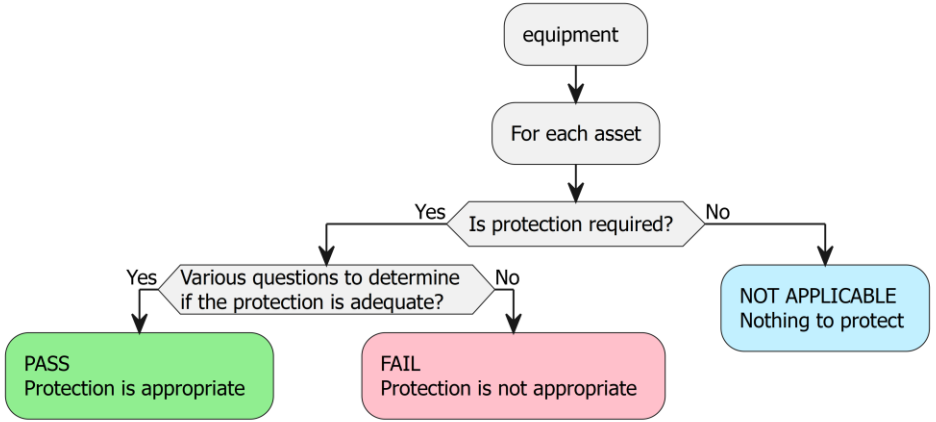
Introduction to the Harmonized Standards

Requirement	prEN 18031-1 3.3.(d)	prEN 18031-2 3.3.(e)	prEN 18031-3 3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

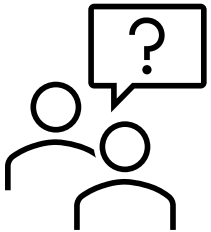


Decision trees

- A harmonized standard shall be applied in its **entirety** for presumption of conformity
- The standards provide **decision trees**, to assess
  - if a specific requirement ***applies*** to a specific product
  - if a specific product is ***sufficiently*** protected
- All paths through decision trees shall be documented in detail



Example requirement – Applicability (3.3.d)



5 Requirements

5.1 [ACM] Access control mechanism

5.1.1 [ACM-1] Applicability of access control mechanisms

5.1.1.1 Requirement

The equipment shall use access control mechanisms to manage entities access to security assets and network assets, unless for security or network assets where:

— Its full public accessibility is the "equipment's reasonably foreseeable and intended use"; or

— the "foreseeable and intended operational environment of use" ensures that its accessibility is limited to authorized entities.

5.1.1.2 Rationale

Security and network assets are exposed to unauthorized access attempts. Access control mechanisms limit the ability of any unauthorized entity to access these assets.

Assessments

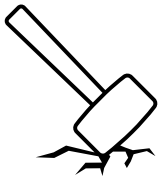
Assessments are conducted by examining the assessment cases, not all assessment cases might be provided for every mechanism:

- Conceptual assessment
  Examine if the provided documentation and rationale adequately provides the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface)

- Functional completeness assessment
  Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)

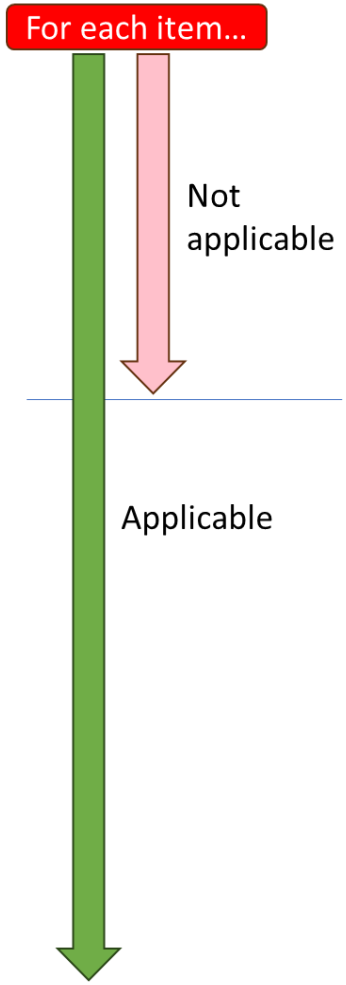
$A = A$?

- Functional sufficiency assessment
  Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data)



Structure (Clause 4)

Clause #	Title	Description on how to apply the standard
5.x	XXX **Mechanism**	Mechanism for each specific item (e.g., external interface or security asset)
5.x.1	XXX-1 **Applicability** of mechanisms	Applicability of the mechanism
5.x.1.1	Requirement	For each specific item determine and assess if the mechanism is required. Note: A mechanism might combine applicability and appropriateness in a single requirement.
5.x.1.2	Rationale	
5.x.1.3	Guidance	
5.x.1.4	Assessment criteria	
5.x.1.4.1	Assessment objective	
5.x.1.4.2	Required information	
5.x.1.4.3	Conceptual assessment	
5.x.1.4.4	Functional completeness assessment	
5.x.1.4.5	Functional sufficiency assessment	
5.x.2	XXX-2 **Appropriate** mechanisms	Appropriateness of the mechanism
5.x.2.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the mechanism is implemented sufficiently. Note: A mechanism might have multiple appropriateness sub-clauses to focus on specific properties.
5.x.2.2	Rationale	
5.x.2.3	Guidance	
5.x.2.4	Assessment criteria	
5.x.2.4.1	Assessment objective	
5.x.2.4.2	Required information	
5.x.2.4.3	Conceptual assessment	
5.x.2.4.4	Functional completeness assessment	
5.x.2.4.5	Functional sufficiency assessment	
5.x.y	XXX-# **Supporting** Requirements	Applicability and appropriateness of supporting requirements for the mechanism
5.x.y.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the supporting requirement needs to be implemented (there might be specific conditions, for instance if the equipment is a toy) and if it needs to be implemented, whether it is implemented sufficiently.
5.x.y.2	Rationale	
5.x.y.3	Guidance	
5.x.y.4	Assessment criteria	
5.x.y.4.1	Assessment objective	
5.x.y.4.2	Required information	
5.x.y.4.3	Conceptual assessment	
5.x.y.4.4	Functional completeness assessment	
5.x.y.4.5	Functional sufficiency assessment	



kamstrup
Confidential

Closing Remarks

- Prepare for coming regulations in EU and DK (and UK)
- Assess your own products in scope of RED Delegated Regulation (2022/30)
  - Familiarize with the content of the hEN's for RED
  - Optionally, participate in the public enquiry (Contact DS before November 1st)
- Determine if other security frameworks you already use, cover some of the essential requirements already – do a gap analysis
- Be aware of the scope changes with upcoming Cyber Resilience Act (CRA) – not limited to "internet connected"

Thank you!

toma@kamstrup.com