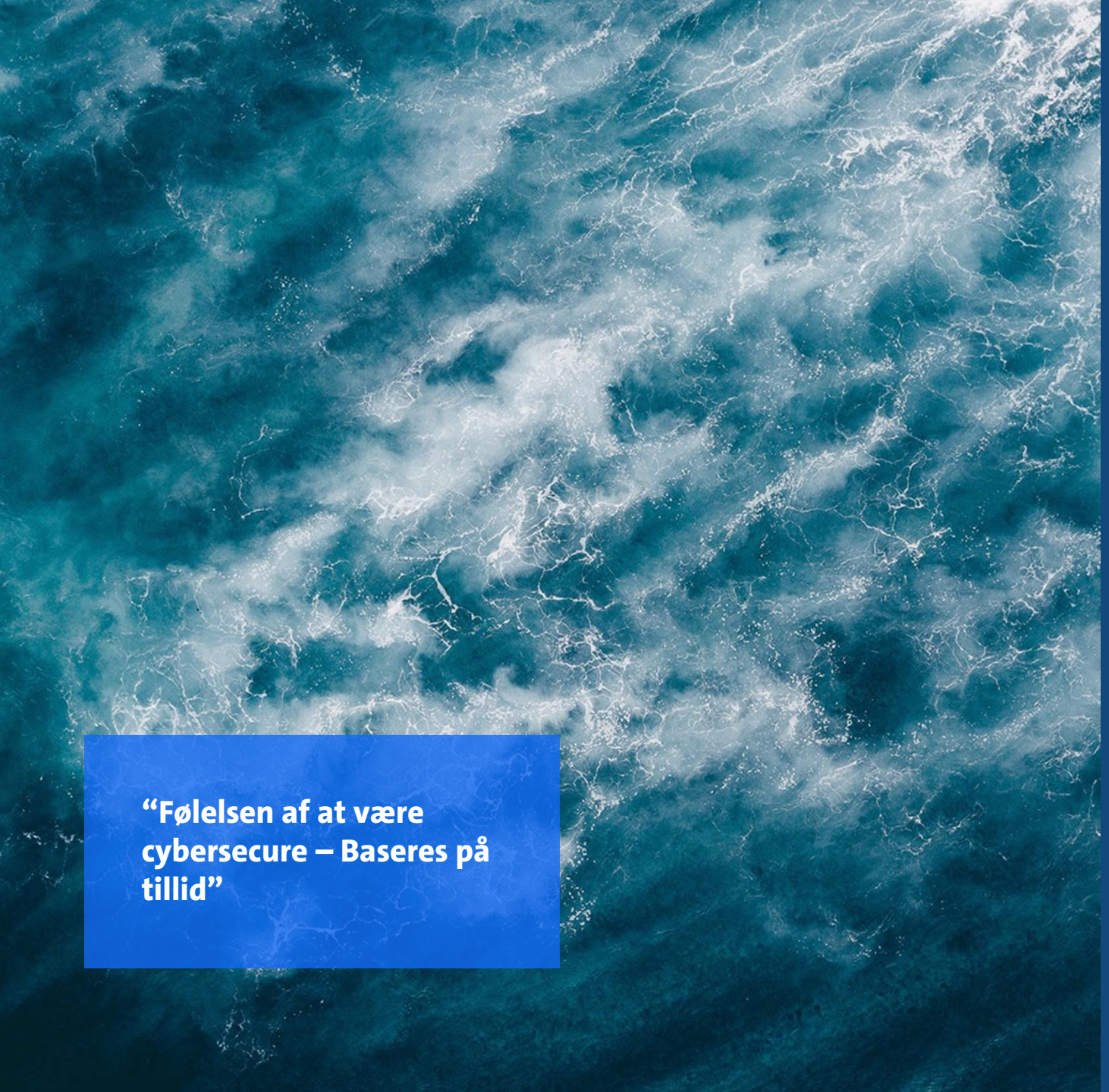
At arbejde med standarder

- På vejen mod opfyldelse af de kommende EU krav på Cybersecurity

Kristian Baasch Thomsen, Lead Digital Compliance Specialist, Grundfos.

GRUNDFOS

Possibility in every drop



“Følelsen af at være cybersecure – Baseres på tillid”

Indhold

- Hvor kommer kravene fra?
- Info – ERFA & oplysning
- Bidrage til fremtiden
- Forbered Politikker – Kultur – Processer
- Cybersecurity review – IoTSF
- Brug af standarder

Hvor kommer kravene fra?

Sikkert produkt

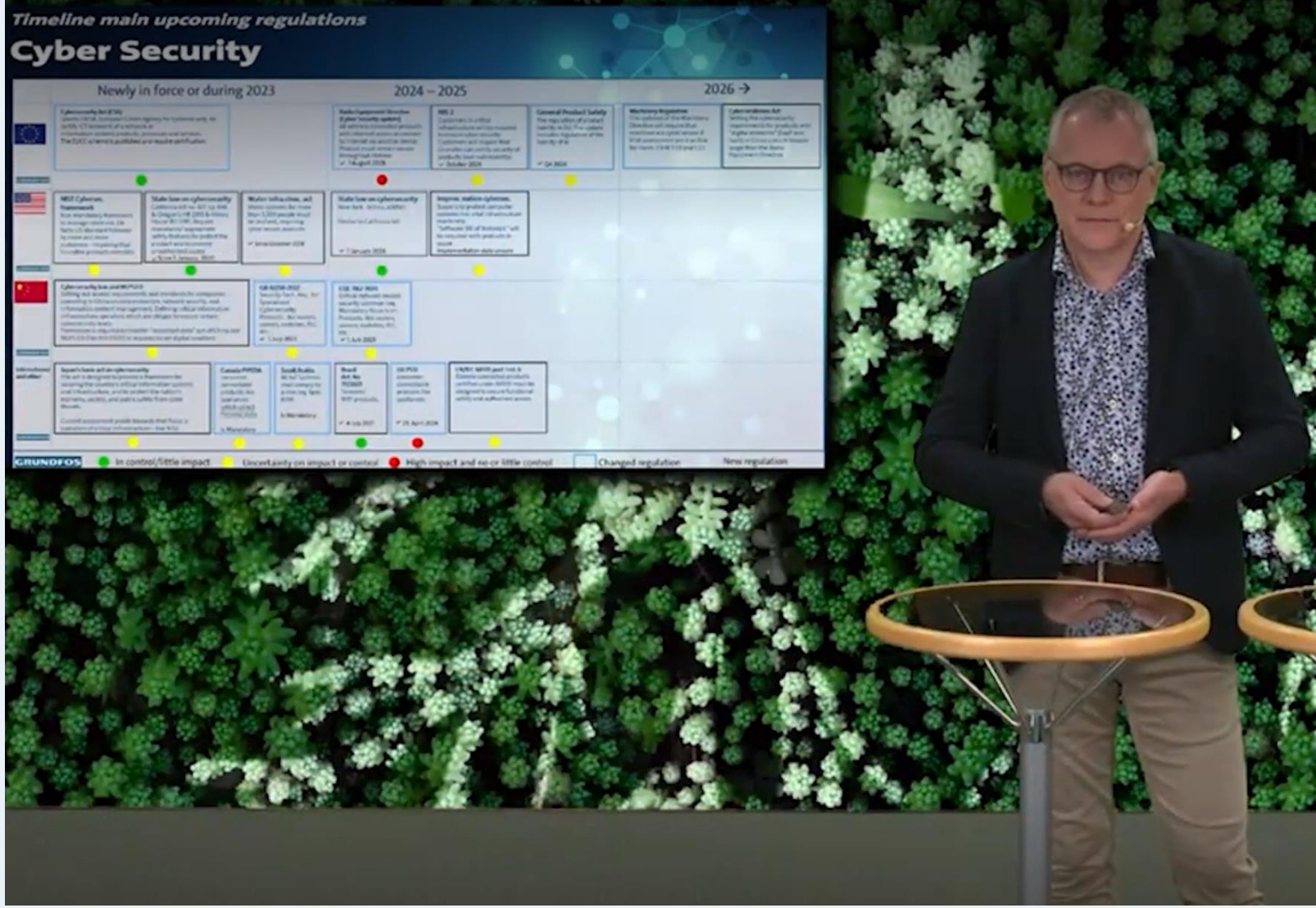
Produktrelateret lovgivning.
Defineret af tilsigtet anvendelse eller brugen af teknologi

Sikker aplikation

"Systems of systems" relatede krav. F.eks som sættes til operatører af services eller infrastruktur.

Info - ERFA & oplysning

- Application Security Team
- Lunch n´ Learn
- Boot camp - vidensdeling og læring
- Cybersecurity Forum - ERFA
- Regulatory Outlook
- Yammer posts
- Obligation Summary



GRUNDFOS

Possibility in every drop

Bidrage til fremtiden

Cybersecure IOT in Danish Industry
CIDI Netværket

DI's ekspertpanel for det indre marked

Forbered Politikker – Kultur - Processer

Nye/Skærpede krav:

- UK PSTI – senest 29. april 2024
- EU: RED DA – senest 1. august 2025
- Cybersecurity en del af risikoanalysen
- Krav til organisationen sikrer cybersecurity på produkter, efter ibrugtagning (UK/CRA).
- Krav til operatører af kritisk production, services og infrastrukturer, NIS2 – senest 24. oktober 2024.

Handlinger:

- Sikre at Governance og organisering er på plads rettidigt (Roller og ansvar på tværs af virksomheden).
- Sikre at politikker og processer er tilstede som grundlag til at opfylde lovkravene.
- Cybersecurity i udviklingskravet
- Modne organisationen til at levere på "Secure Development Lifecycle – SDL"
- Bliv certificeret, hvis giver værdi.
- Følg med og ret rettidigt

Cybersecurity review kultur

- Forbedre opmærksomhed på cybersecurity
- Sigte mod cybersecurity excellence i relation til brugerscenarier
- Opbyg et grundlag for opfyldelse af fremtidige regulatoriske krav
- Vurdere IoT produkternes cybersecurity level
- Grundlag for GAP analyser

Primary Keyword	Description	Secondary keyword	Description
System	The requirement is applicable to the technical elements of the device/ product or service	***Software***	The requirement is directly applicable to the software of the device or service
		Hardware	The requirement is directly applicable to the electronics of the device/service hardware (PCB, processor, components etc.)
		Physical	The requirement is directly applicable to mechanical aspects of the device such as the casing, form factor etc.
Business	A business requirement not directly related to the operational function of the device/ product or service	***Process***	A flow of activities that indirectly contributes to the security characteristics of a device or service
		Policy	The instructions and guidelines that indirectly contribute to the security characteristics of a device or service
		Responsibility	A role or responsibility that indirectly contributes to the security characteristics of a device or service

Table 3: Keyword Categories

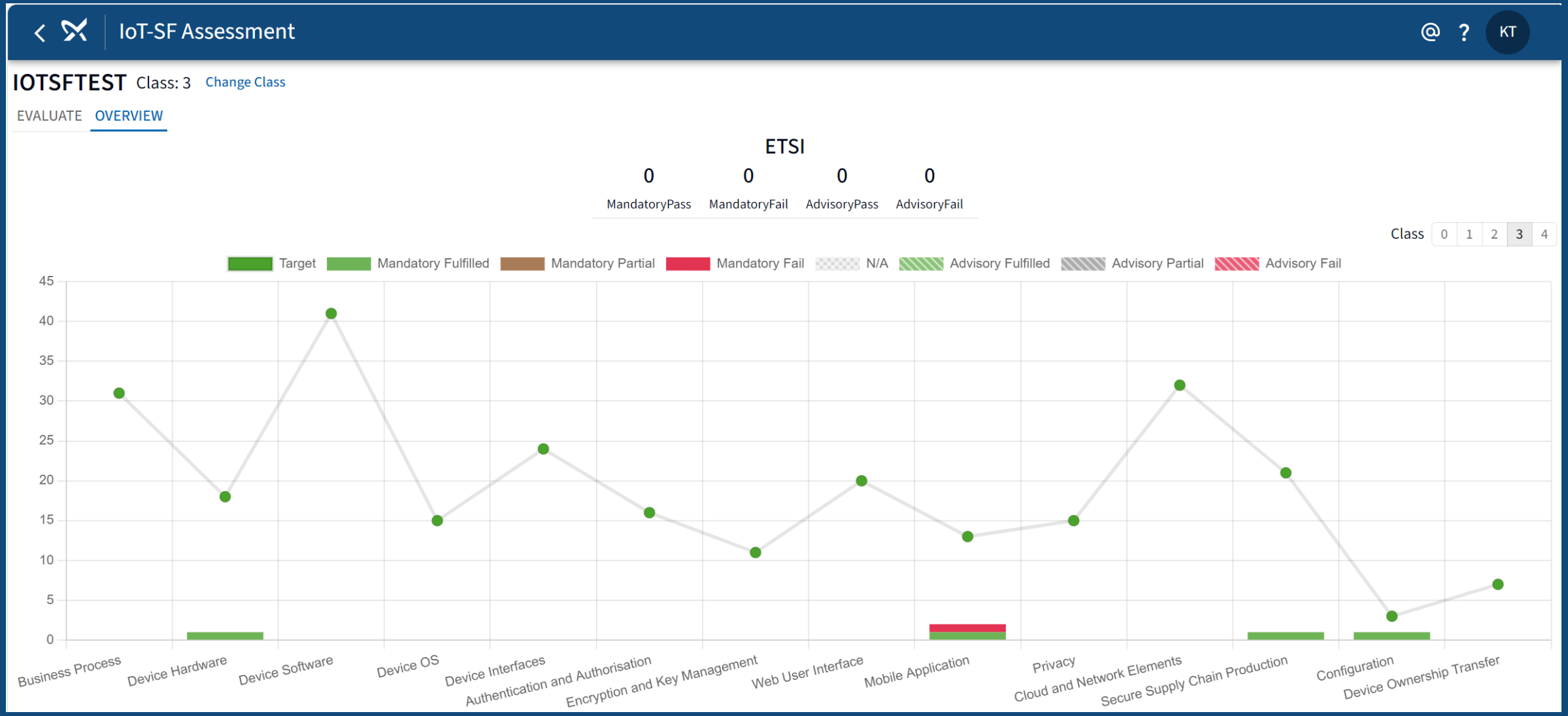
IoTSF IoT Security Assurance Framework Release 3.0 Nov 2021 (iotsecurityfoundation.org)

>290 review spørgsmål til eftertanke

GRUNDFOS

Possibility in every drop

Cybersecurity review kultur



Eksempel på brug af standarder

Krav UK PSTI - som eksempel:

- Passwords skal være unikke per device eller indstilles af brugeren ved ibrugtagning. Password skal være "stærkt". Krav om information til, hvordan brugeren skifter password.
  (ETSI EN 303 645 Provision 5.1-2)
- "Vulnerability disclosure policy" skal være offentligt tilgængelig og der er krav om information til brugeren.
  (ETSI EN 303 645 Provision 5.2-1)
- Offentliggørelse af den definerede support periode, hvor fabrikanten stiller security opdateringer rettidigt tilgængeligt.
  (ETSI EN 303 645 Provision 5.3-13)

2.4.7.7	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device.	Mandatory for all classes	Business	Process
2.4.7.8	Where using initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret.	Mandatory for Class 1 and above	System	Software

2.4.3.14	As part of the Security Policy, publish the organisation's conflict resolution process for Vulnerability Disclosures.	Mandatory for Class 1 and above	Business	Process

2.4.3.9.1	There is a minimum support period during which security updates will be made available to all stakeholders.	Mandatory for all classes	Business	Process

Brug af standarder

- til opfyldelse af kundekrav

- NIS2 krav til operatører stiller krav til produkterne.
- Kunderne stiller krav i købsprocessen
- Kundekrav “overhaler” lovkravene
- Brug af standarder, som f.eks. IEC 62443-4-x eller EN 303 645 skaber et fundament
- Certificeringer skaber tillid og hurtigere købsproces

GRUNDFOS

Possibility in every drop

“Følelsen af at være cybersecure baseres på tillid”

GRUNDFOS

Possibility in every drop

“Standarder er en aftalt måde at gøre ting på”

GRUNDFOS

Possibility in every drop

Possibility in every drop