Kan standarder understøtte arbejdet med NIS2?

DS Cyberdag - 5. oktober 2023

Spor 1: 15.50-16.20

Det korte svar er ja…

Majken Prip
Konsulent, Dansk Standard

E: mpr@ds.dk
M: 30222330

Henriette Brandstrup
Konsulent, CyberWorks.dk

E: henriette.brandstrup@cyberworks.dk
M: 30613929

Agenda

1. NIS2 og kravene - hvad står der egentlig?
2. Baggrund for at tale standarder og NIS2
3. Hvad er ISO/IEC 27001 og ISO/IEC 27002?
4. Kobling og Compliance
5. Hvordan kan IEC 62443-serien understøtte arbejdet på OT-delen?
6. Hvordan kan man komme i gang?

NIS2 OG KRAVENE?

EU NIS2 er et, af en række af direktiver og forordninger i EU's Digitale Strategi med sigte at opbygge cybersikkerhedskapaciteter i hele EU, afbøde trusler mod net- og informationssystemer, der anvendes til at levere væsentlige tjenester og sikre kontinuiteten trods hændelser. Bidrage til EU's sikkerhed, og at økonomi og samfund kan fungere effektivt.

- Stiller krav til udvalgte sektorer, der står for samfundsmæssig infrastruktur.
- Enheder omfattet er enten væsentlige (annex 1) eller vigtige (annex 2)
- Krav til myndigheder om tilsyn
- Træder i kraft i dansk lov 18 oktober 2024

- Krav vil ledelsen om kompetencer og ansvar
- Effektiv risikostyring med risikoanalyse, foranstaltninger, kontroller, beredskab, opfølgning
- Forsyningskædesikkerhed – formentligt den mest markante forandring og der mangler ensartede måder at vurdere underleverandører på
- Hændelsesrapportering, herunder ved "nær-ved-hændelser"

NIS2 KRAVENE – HVAD STÅR DER EGENTLIG

Et par overskrifter fra NIS2 direktivet:

Ledelses- og bestyrelsesansvar for informationssikkerhed
Fokus på risikostyring og risikohåndtering
Leverandør- og forsyningssikkerhed
Implementering af effektive foranstaltninger
Uddannelse af medarbejdere og ledelse
Afrapportering af hændelser
Sanktionsmuligheder

BAGGRUND

Hvorfor overhovedet tale om standarder, når vi taler om et EU direktiv?

Artikel 25

… tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer…

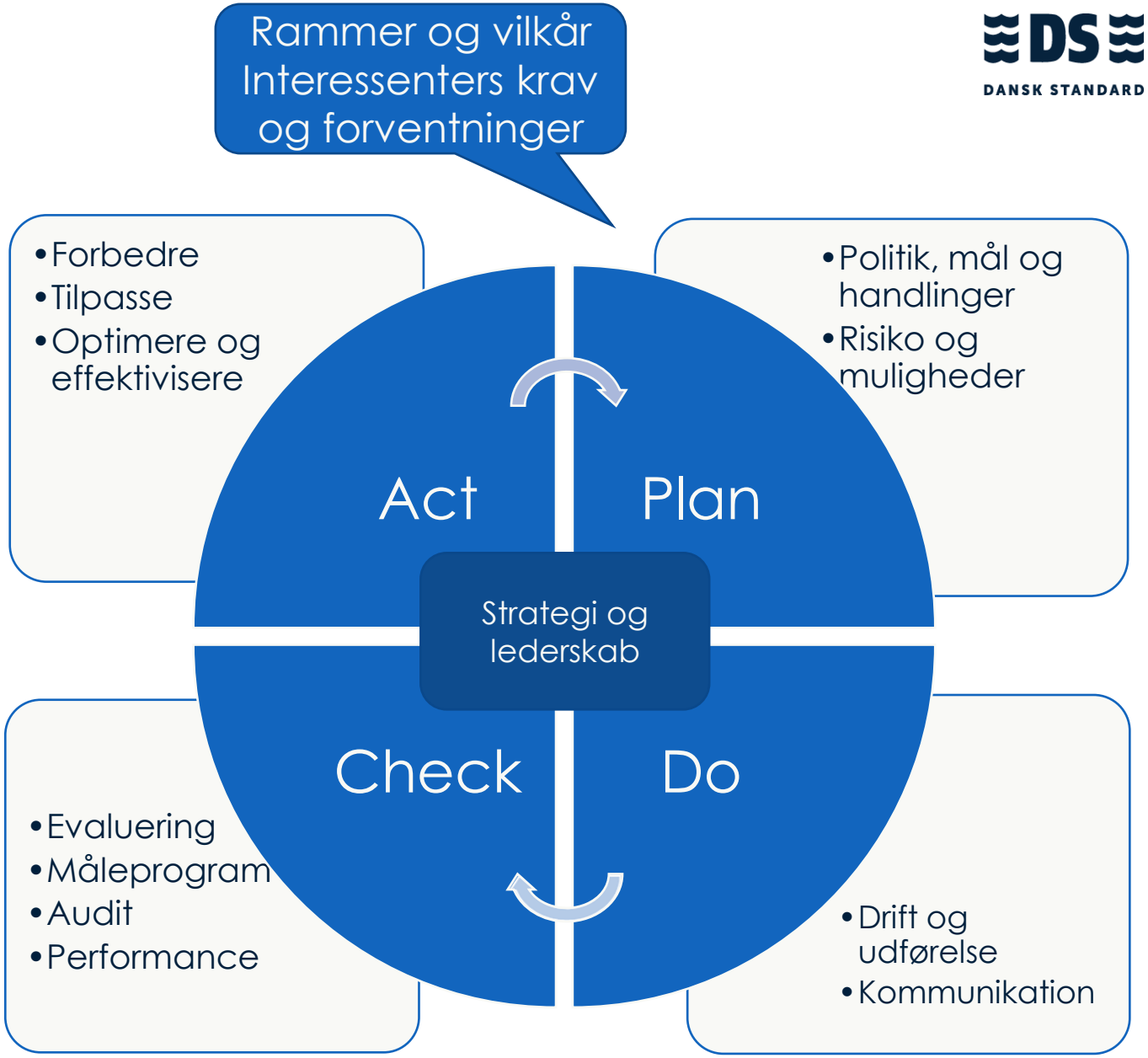
ISO/IEC 27001

Hvad er ISO 27001?

En international standard for informationssikkerhed.

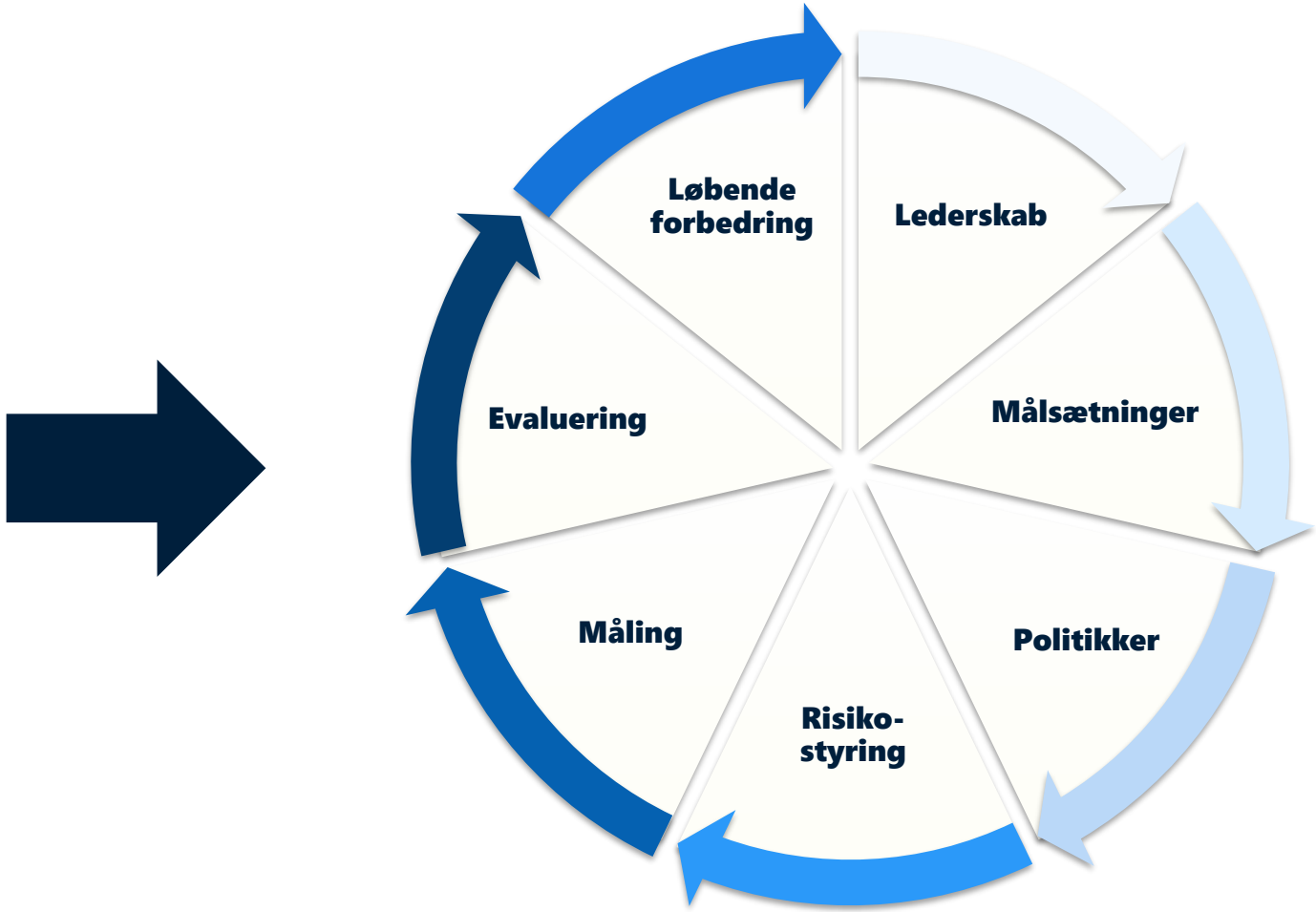
Fokus på etablering, implementering, vedligeholdelse og forbedring af et ledelsessystem for informationssikkerhed (ISMS).

Et rammeværk bestående af strukturerede processer, som skal fyldes ud og tilpasses den enkelte organisation mhp at sikre kritiske informationer mod blandt andet cybertrusler.



DE CENTRALE ELEMENTER I ISO27001

Et ledelsessystem for informationssikkerhed (ISMS) i henhold til ISO27001 omfatter processer, som indkapsler og omfatter følgende:

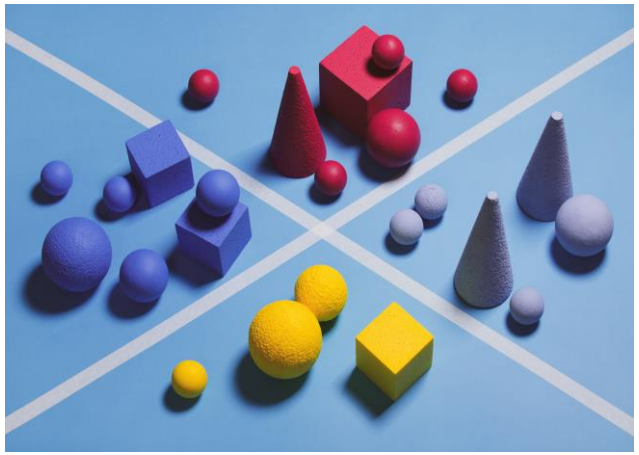


Hvad så med ISO/IEC 27002?

En komplementær standard, der giver vejledning i implementeringen af ISO 27001.

Detaljerede foranstaltninger og retningslinjer for informationssikkerhed.

UDFORMNING AF ISO/IEC 27002



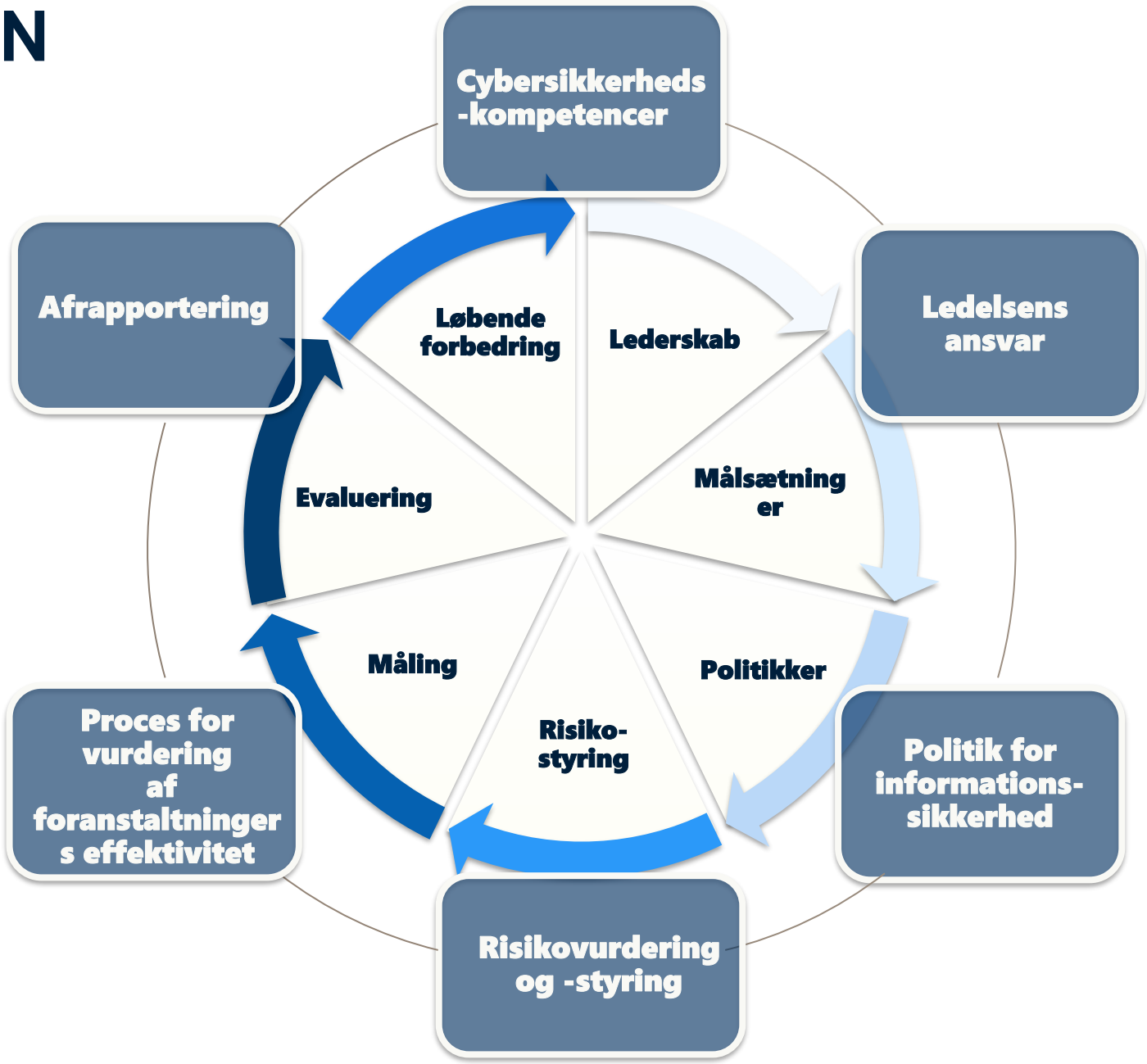
4 TEMAER

93 FORANSTALTNINGER

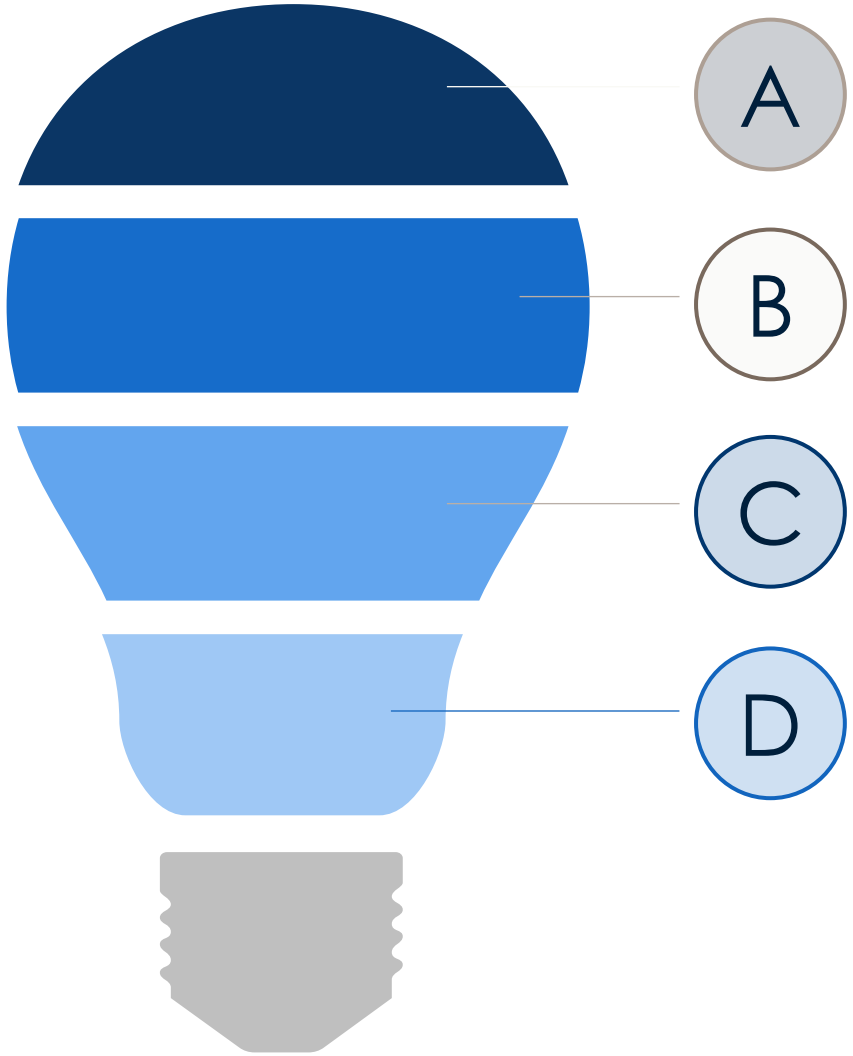
- Type af foranstaltning
- Egenskaber for informationssikkerhed
- Cybersikkerhedskoncept
- Operationelle ressourcer
- Sikkerhedsdomæner

ATTRIBUTTER

KOBLINGEN


Cybersikkerheds-kompetencer
Ledelsens ansvar
Politik for informations-sikkerhed
Risikovurdering og -styring
Proces for vurdering af foranstaltningers effektivitet
Afrapportering
Løbende forbedring
Lederskab
Målsætninger
Politikker
Risiko-styring
Måling
Evaluering

ARBEJDET MED ISO27000 SERIEN ift. NIS2



Strukturering af det løbende arbejde med informationssikkerhed

Fastlæggelse af best practices inden for informationssikkerhed

Støtte til en risikobaseret tilgang til styring af informationssikkerhed

Simpel tilpasning til fremtidige ændringer i lovgivning, samt lettere integration af lovkrav herunder NIS2 i eksisterende processer og sikkerhedsprogrammer

Hvordan kan IEC 62443-serien understøtte arbejdet på OT-delen

Art. 21,1: Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester.

Mens de fleste har et klart billede af, hvordan der kan arbejdes med risikovurdering, foranstaltninger mm for IT, er det mere uklart med OT.

OT står for **Operational Technologies** / Operationel Teknologi, og er hardware og software, som registrerer eller forårsager en handling gennem direkte overvågning og/eller kontrol af industrielt udstyr, aktiver, processer mm. SCADA, PLC, IACS (Industrial Automation Control Systems) mm er gængse termer.

Forskel på OT og IT

- OT styrer noget i den fysiske verden
- Availability, integrity, confidentiality
- Systemer har længere levetid og gamle systemer ses ofte i infrastrukturen
- Konsekvensen af tab af funktionalitet er fysisk effekt, måske HW skade
- Reparation /genopretning kan tage lang tid
- Mange interessenter har kontakt med systemer – driftsoperatører, servicefolk, installation, vedligeholdelse
- Komplekse systemer. Ofte ses smart enheder indsat i ældre infrastrukturer
- Der ses ofte distribuerede systemer

- IT systemer håndterer data
- Confidentiality, integrity, availability
- Systemer har typisk kortere levetid
- Geninstaller software og restore data

- OT-sikkerhed er ofte mindre modent end IT-sikkerhed, fordi fokus har været der på det i kortere tid. Ofte ses ingen samarbejde med IT afdelingen og topledelse fokus har været fraværende
- Bevægelse fra "island" er sket senere
- Typisk en ad hoc og reaktiv tilgang modsat threat intelligence i IT

- For mange vil kravene til OT i EU NIS2 medføre fokus på det helt basale niveau

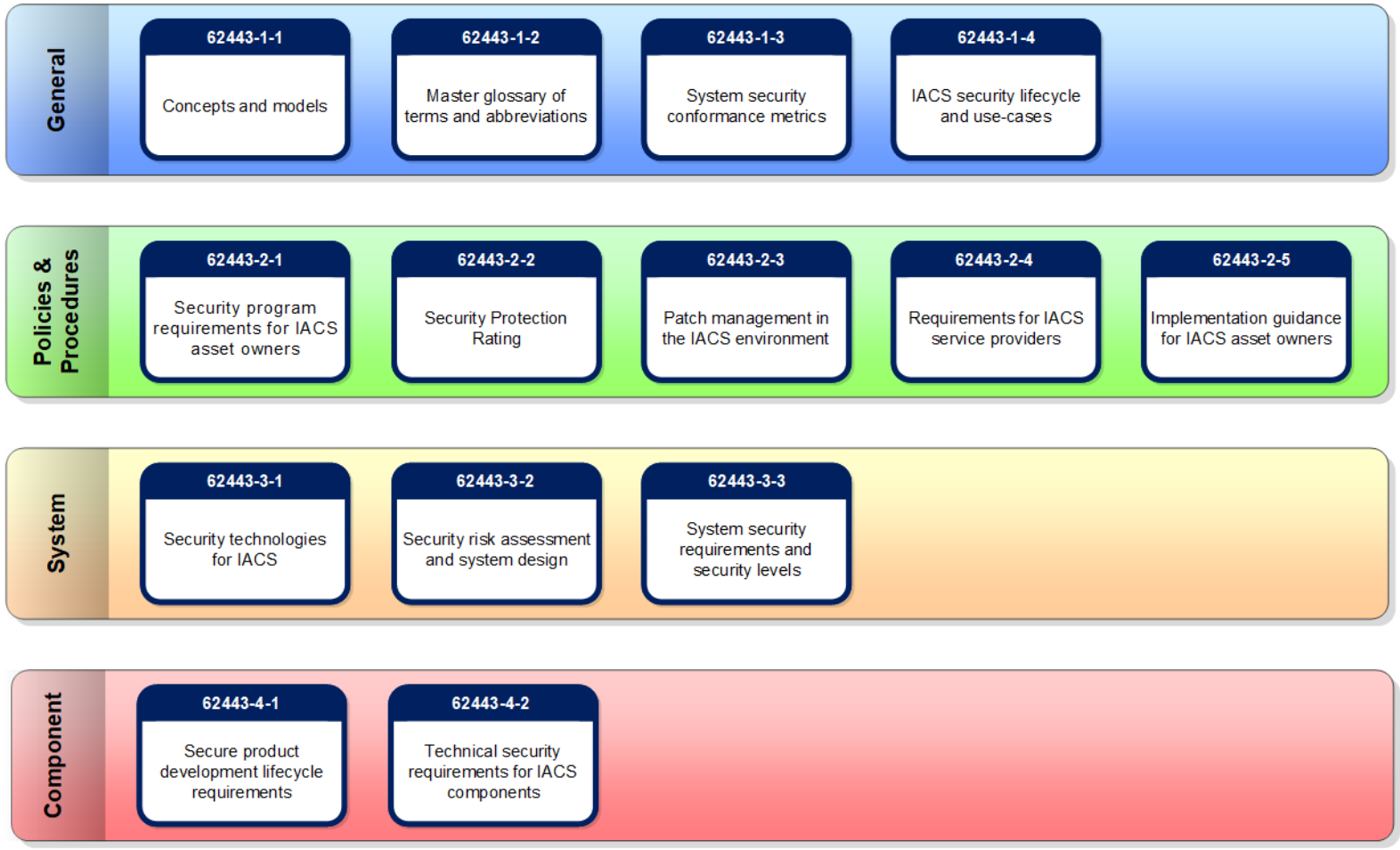
IEC62443

Forskelle på IT og OT tilsiger, at en anden tilgang må supplere fx ISO27001/2 for arbejdet for OT delen for en mere holistisk tilgang.

Her kan der plukkes i **IEC 62443-serien** til at understøtte arbejdet med kravene i EU NIS2.

Standarden adresserer behovet for sikkerhed i IACS (Industrial Automation Control Systems) og er velegnet til en bred vifte af sektorer og systemer.

OBS! Revision og tilføjelser er på vej. For visse områder.



IEC62443

IEC 62443 har forskellige features som fx ikke ses i ISO27001 fx:

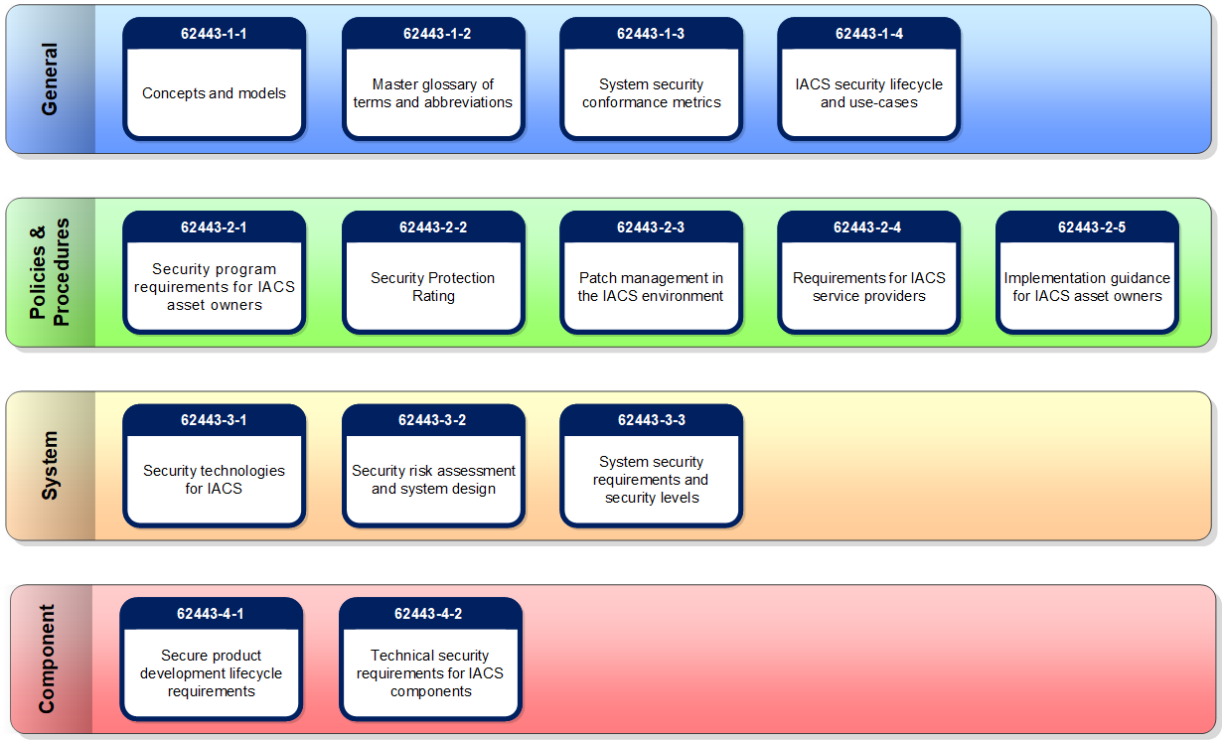
Tre pillars: people, processes, technology

Roller: Fokus for Asset Owner, Service Provider, Supplier, System/Product Vendor

Risk assessment for security eller systems design

Kravstyring, for at opnå det ønskede sikkerhedsniveau via 4 forskellige Security Levels/ ambitionsniveauer

Fundamental requirements for identification and authentification control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, ressource availaility



Hvordan kan man komme i gang? Kursus, Introduktion til OT-cybersikkerhed - for personer med IT-forståelse

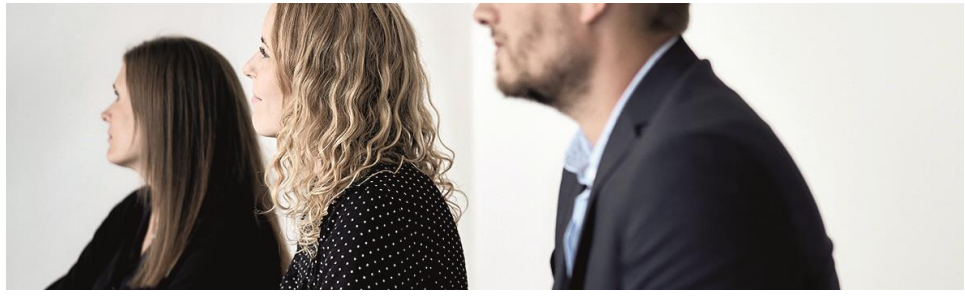
Den teknologiske udvikling, OT's øgede opkobling til internettet og fremkomst af regulatoriske krav for OT cybersikkerhed som fx EU NIS2 kalder på større fokus i organisationerne, herunder hvordan man kan styrker sin it/OT-organisation

Arbejder du med it-sikkerhed, og ser behov for at øge din viden om OT-cybersikkerhed?

Vi har et nyt kursus for personer med it-forståelse, der ønsker mere viden om OT-cybersikkerhed, om ligheder og hvordan, det adskiller sig it-området. OT står for Operational Technologies og er brugen af hardware og software til at overvåge og kontrollere fysiske processer, enheder og infrastruktur i et industrielt miljø.

https://www.ds.dk/da/ydelser/kurser/introduktion-til-ot-cybersikkerhed-for-personer-med-it-forstaaelse

11. januar 2024



På gensyn

Dansk Standard