Fire byggeblokke til cybersikkerhed

SKAB FÆLLES RETNING FOR CYBERSIKKERHED
I DIGITALE ENHEDER OG SYSTEMER

CyPro ■ CYBERSIKKER PRODUKTION

Opbyg IoT-cybersikkerhed – trin for trin

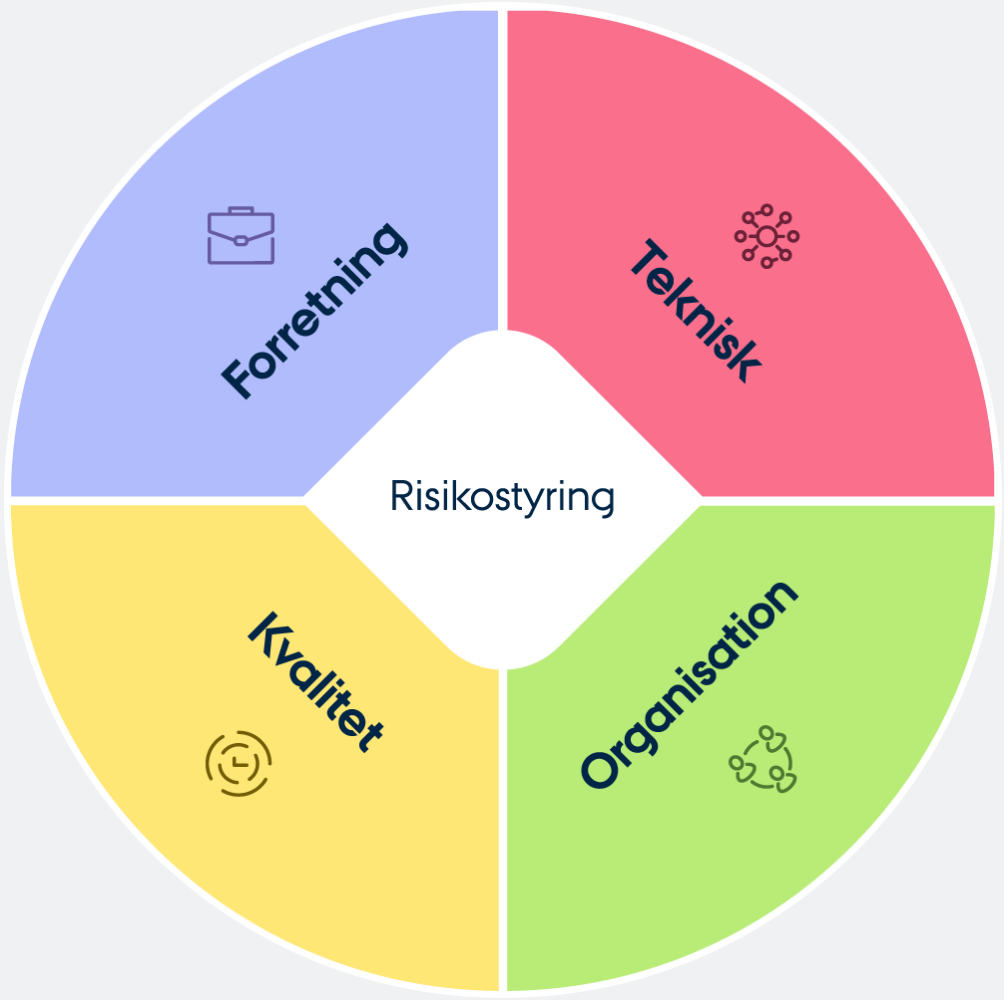
IoT-cybersikkerhed er ikke blot et teknisk anliggende – det er en fælles opgave, som går på tværs af virksomheden.

I denne vejledning præsenterer vi en **modenhedsmodel** for IoT-cybersikkerhed, der understøtter virksomheders fælles indsats for IoT-cybersikkerhed. Modellen beskriver de **fire byggeblokke**, der skal arbejdes med for at skabe IoT-cybersikkerhed. Hver byggeblok peger på en vigtig opgave og indeholder forskellige aktiviteter, der handler om mennesker, teknologi og arbejdsgange.

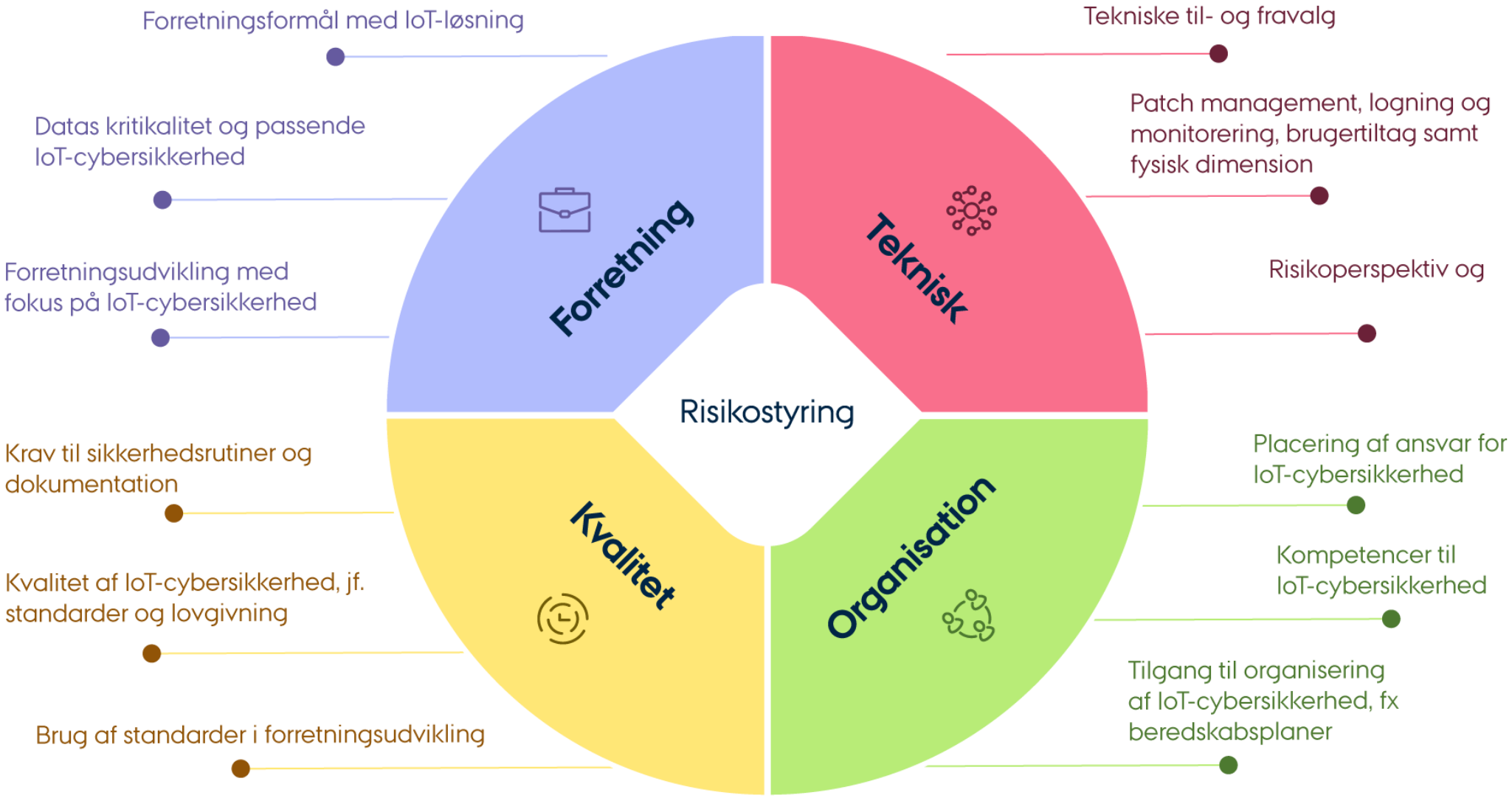
De fire byggeblokke:

- **Tekniske forhold**
- **Organisatorisk forankring**
- **Forretning**
- **Kvalitet**

Gennem jeres drøftelser i modenhedsdialogen kan I sammen definere den nuværende modenhed af hver byggeblok. På det grundlag bygger I sikkerhedsindsatsen op trin for trin i jeres eget tempo og med afsæt i virksomhedens virkelighed og risici.



Indhold i de fire byggeblokke



De fire byggeblokke

TEKNISKE ARBEJDSOPGAVER rettet imod at opbygge tekniske processer for IoT-cybersikkerhed i produkter og produktionsapparat, fx test af IoT-cybersikkerhed, patching, monitorering, kryptering.

Ambitionen i byggeblokken er at bevæge sig fra en ad hoc-tilgang med fokus på enkelte systemenheder mod en risiko-baseret tilgang, der med tiden omfatter alle IoT-systemer og løsninger i virksomheder (og evt. hos samarbejdspartnere).

ORGANISATORISKE ARBEJDSOPGAVER rettet imod, hvordan virksomheden konkret arbejder med at opbygge og forankre IoT-cybersikkerhed igennem organisering, fx forankring af arbejdet med risikovurdering og placering af ansvar for IoT-cybersikkerhed.

Ambitionen i byggeblokken er at udbrede forståelsen af IoT-cybersikkerhed, så den ikke lever i små grupper i virksomheden (fx hos bestyrelsen eller it-folk og -udviklere) men bliver et fælles anliggende for medarbejdere, ledere og bestyrelse.

FORRETNINGSMÆSSIGE ARBEJDSOPGAVER rettet imod, hvordan virksomheden arbejder med samspillet mellem sikkerhed og værdien af virksomhedens IoT-løsninger for forretningen.

Ambitionen inden for denne byggeblok er, at sikkerhedsniveauet tilpasses efter, hvor kritiske data og systemer er for forretningen. Vurdering af konsekvenserne af et cyberangreb på virksomhedens IoT-løsninger er en forretningsmæssig risikovurdering – en afvejning af sikkerhedsinvestering overfor indtjening.

KVALITETSMÆSSIGE OPGAVER rettet imod, hvordan virksomheden arbejder med at sikre og vurdere kvaliteten af IoT-cybersikkerheden ud fra lovgivning og standarder.

Ambitionen i byggeblokken er at opbygge en proaktiv tilgang til IoT-cybersikkerhed baseret på fastlagte procedurer og overblik over kvaliteten. Procedurerne skal baseres på lovgivning og/eller standarder fremfor en reaktiv tilgang til IoT-cybersikkerhed, hvor kvalitet afgøres af kundekrav. Den indbyggede risikovurdering handler om den forretningsmæssige risiko i lovgivningen og vurderingen af, om forretningen kan bevare sin værdi uden overblik og struktur baseret på en relevant standard.

Modenhedsmodellen

Nøglen til at tale om virksomhedens modenhed for IoT-cybersikkerhed er at tale om modenheden for hver af de fire byggeblokke – én efter én. På den baggrund kan I opstille mål for videreudvikling af cybersikkerheden på den måde og i det tempo, der passer til jer.

Hver fase i modenhedsmodellen er karakteriseret ved et mål om, at IoT-cybersikkerhed bliver en fælles opgave på tværs af fagligheder og funktioner i virksomheden. Målet i fase 3 er en fælles struktur, som danner grundlaget for robust IoT-cybersikkerhed.

Afhængigt af jeres afsæt kan det realistiske mål for byggeblokken variere. Målet er ikke at opnå maksimal sikkerhed overalt men at opnå den rette sikkerhed baseret på risikovurdering, forretningskritikalitet og teknologisk kontekst.

Ad hoc indsats, isolerede handlinger, behov for fælles opmærksomhed

Med afsæt i fælles opmærksomhed kan der udvikles en fælles praksis …

… som over tid kan blive til en fælles struktur af rutiner, processer og dokumentation

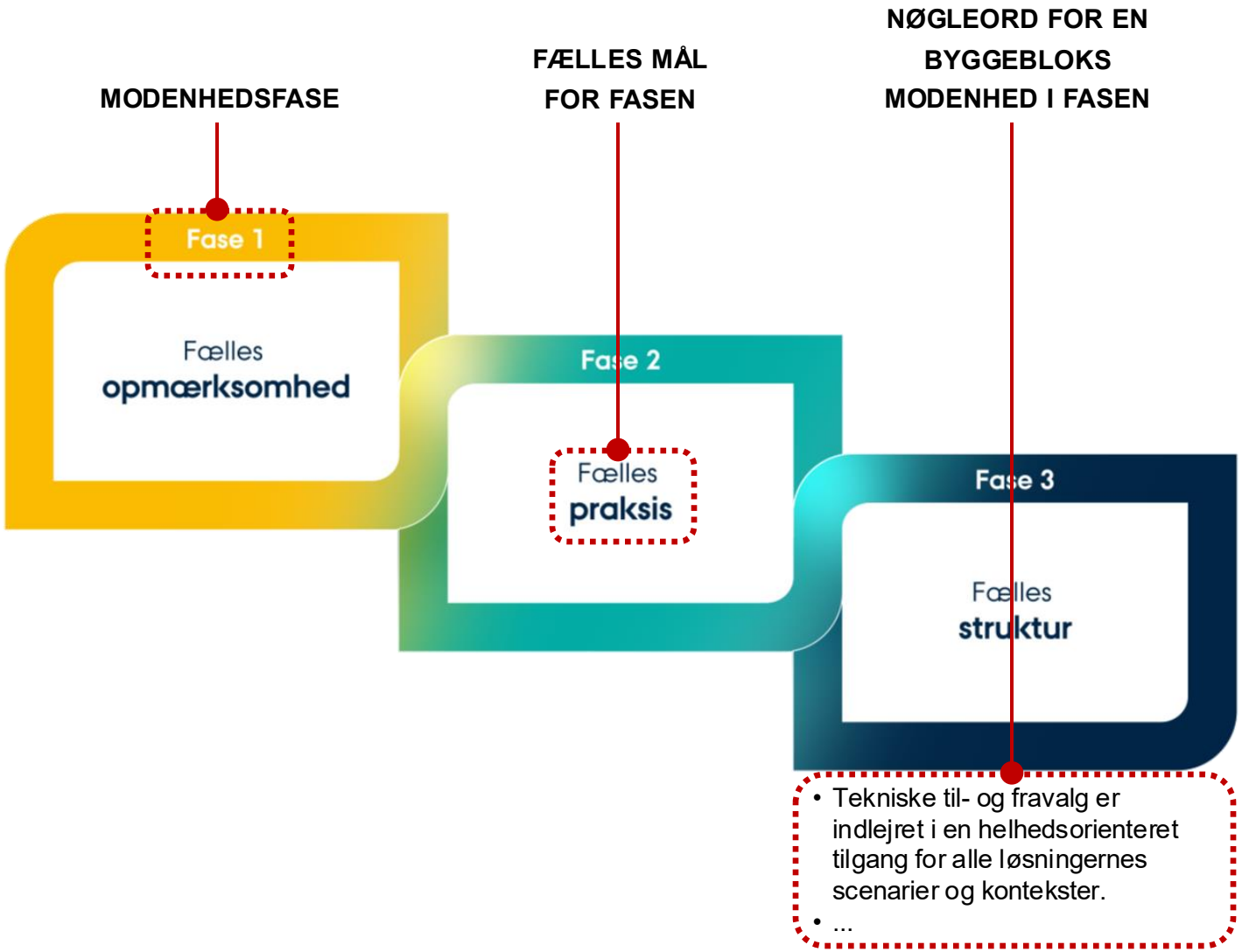
Byggeblokkenes modenhed

På de følgende fire sider præsenteres de tre modenhedsfaser tilpasset hver af de fire byggeblokke.

For at hjælpe med læsningen af byggeblokkenes modenhed, har vi lavet en lille signaturforklaring her til højre.

Det er klart, at byggeblokkene spiller sammen i jeres virksomheds praksis, og modenhed indenfor én byggeblok kan forme indsatsen med en anden byggeblok. Det er, fordi flere arbejdsopgaver sættes sammen og tilpasses hinanden over tid og efter vigtighed for virksomheden.

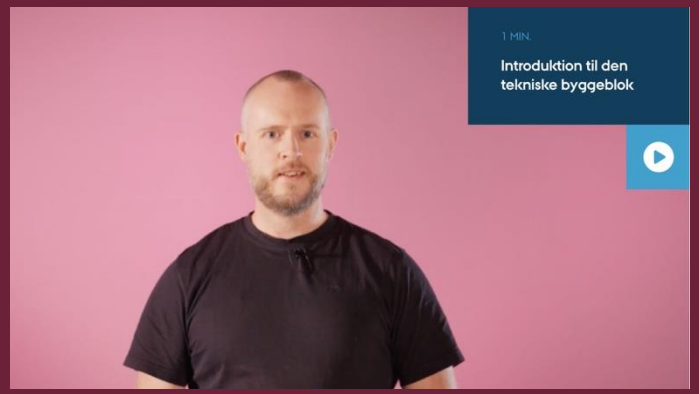
Med afsæt i klarlægning af hver byggebloks modenhed får I et grundlag at forstå og videreudvikle jeres IoT-cybersikkerhed ud fra.



TEKNISK BYGGEBLOK

Nøgleord for modenhedsfaser i den tekniske byggeblok

→ Gå til den tekniske byggebloks online værktøjer



Fælles **opmærksomhed**

- **Tekniske til- og fravalg** afgøres af, at IoT-løsningens funktioner og data ikke opfattes som kritiske for forretningen. Stort fokus på driftssikkerhed.
- **Tekniske aktiviteter** inkluderer ofte ikke IoT-cybersikkerhed. Der er tiltro til, at leverandøren har styr på IoT-sikkerheden. Kan udsende opdateringer. Få har logning. Ikke stort fokus på brugeradgang til enheder.
- **Risikovurdering** er ikke systematisk eller tydelig.

Fælles **praksis**

- **Tekniske til- og fravalg** er, at IoT-cybersikkerhed er bygget ind fra starten eller opdateres løbende.
- De nødvendige IoT-sikkerhedskompetencer til **tekniske aktiviteter** er tilgængelige: patch management, logning og monitorering, og brugeradgang er systematiseret.
- **Risikovurdering**, hvor man bevæger sig væk fra ad hoc-cybersikkerhedstilgang til risikobaseret IoT-sikkerhedsniveau.

Fælles **struktur**

- **Tekniske til- og fravalg** er indlejret i en helhedsorienteret tilgang for alle løsningernes scenarier og kontekster.
- **Tekniske aktiviteter** sker i fælles og strukturerede processer. Der er flere lag af IoT-cybersikkerhed bygget ind i løsningerne. Der er dedikerede ressourcer.
- Til- og fravalg baseres på **kontinuerlig risikovurdering**, hvor både ledere og medarbejdere deltager.

ORGANISATIONS-BYGGEBLOK

Nøgleord for modenhedsfaser i organisationsbyggeblokken

→ Gå til organisationsbyggeblokkens online værktøjer

Fælles **opmærksomhed**

- **Ansvar** er ikke i fokus eller er uafklaret.
- Ingen eller få **kompetencer**, måske ildsjæle. Ledelsen er uinteresseret.
- **Tilgang:** forholder sig til IoT-cybersikkerhed gennem kundernes spørgsmål, ingen beredskabsplaner mv.

Fælles **praksis**

- En eller flere personer har formelt **ansvar**.
- Enkelte interne **kompetencer** samt sparring med eksterne fagfolk. Ledelsen interesseret i økonomiske konsekvenser.
- Er ved at opbygge en **tilgang** med planer og procedurer for IoT-cybersikkerhed og er optaget af fælles forståelse.

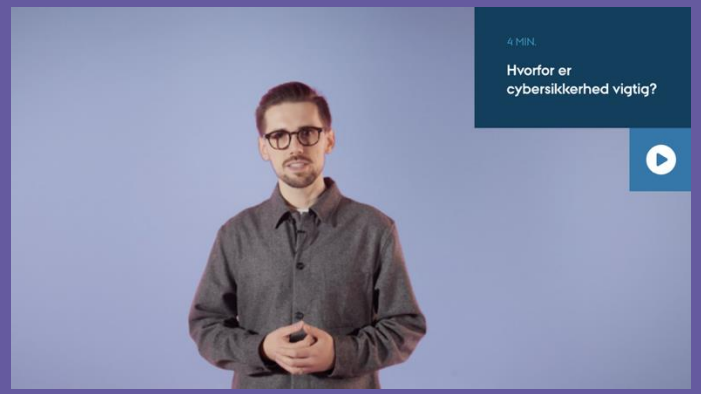
Fælles **struktur**

- Forankret internt **ansvar** og klar organisering af arbejdet.
- Har adgang til alle nødvendige **kompetencer** internt og/eller eksternt. Ledelsen deltager aktivt og informeret i vurderinger.
- **Struktureret tilgang** og proces for beredskab og risikovurdering – alle dele af forretningen.

FORRETNINGS-BYGGEBLOK

Nøgleord for modenhedsfaser i forretningsbyggeblokken

→ Gå til forretningsbyggeblokkens online værktøjer



Fælles **opmærksomhed**

- **Forretningsformål** med IoT-løsninger er typisk at overvåge drift og tage hensyn til fordele og ulemper ved sikkerhedsvalg for kunderne.
- **Kritikalitet** for driftsdata er fortrolighed.
- **Forretningsudvikling** er ikke koblet sammen med IoT-løsningen eller data.

Fælles **praksis**

- **Forretningsformål** med IoT-løsninger er automatisering, optimering og driftssikkerhed.
- **Kritikalitet** for data er typisk tilgængelighed og integritet. Fokus på økonomisk effektivt niveau of IoT-cybersikkerhed.
- **Forretningsudvikling** har fokus på systematisk datahøst, datas integritet og fortrolighed. Stor interesse for potentialer i cloud-løsninger.

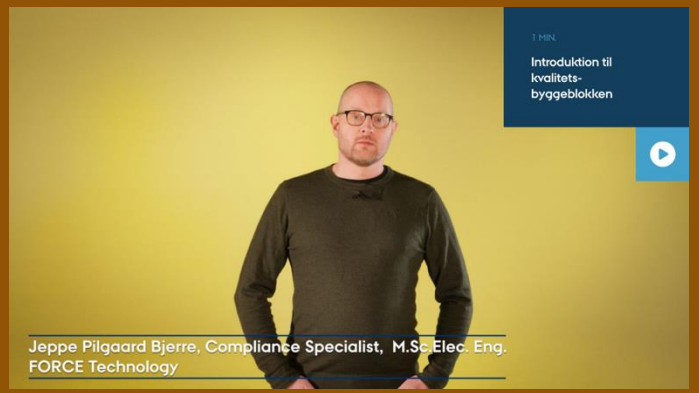
Fælles **struktur**

- **Forretningsformål** med IoT-løsninger er automatisering og forbundne produkter og services.
- **Kritikalitet** og risikoappetit vurderes og tilpasse løsningerne særskilt.
- **Forretningsudvikling** sker i form af nye forretnings-modeller, fordi IoT-cybersikkerhed er et 'selling-point'. Cloud-løsninger og digitale platforme til kunderne.

KVALITETS-BYGGEBLOK

Nøgleord for modenhedsfaser i kvalitetsbyggeblokken

→ Gå til kvalitetsbyggeblokkens online-værktøjer



Fælles **opmærksomhed**

- Virksomhederne forholder sig afventende i forhold til **standarder og lovgivning**.
- **Sikkerhedsrutiner** kan forekomme i forbindelse med sikkerhedsreview, men der er få rutiner og procedurer. Mange ad-hoc cybersikker-hedsløsninger.
- **Brug af standarder** ses som en mulighed, men standar-diseringsprocessen opfattes som overvældende.

Fælles **praksis**

- Virksomheder ønsker eller har domænespecifikke **standarder** og/eller ISO-certificeringer. Bruger evt. dele af standarder som en systematik.
- **Sikkerhedsrutiner** lægger sig op ad generaliserede niveauer og målsætninger. Stigende fokus på IoT-cybersikkerheden i det samlede system/løsning.
- **Brug af standarder** ses som et fælles sprog både internt og eksternt og som valid baggrund for sikkerhedsbeslutninger.

Fælles **struktur**

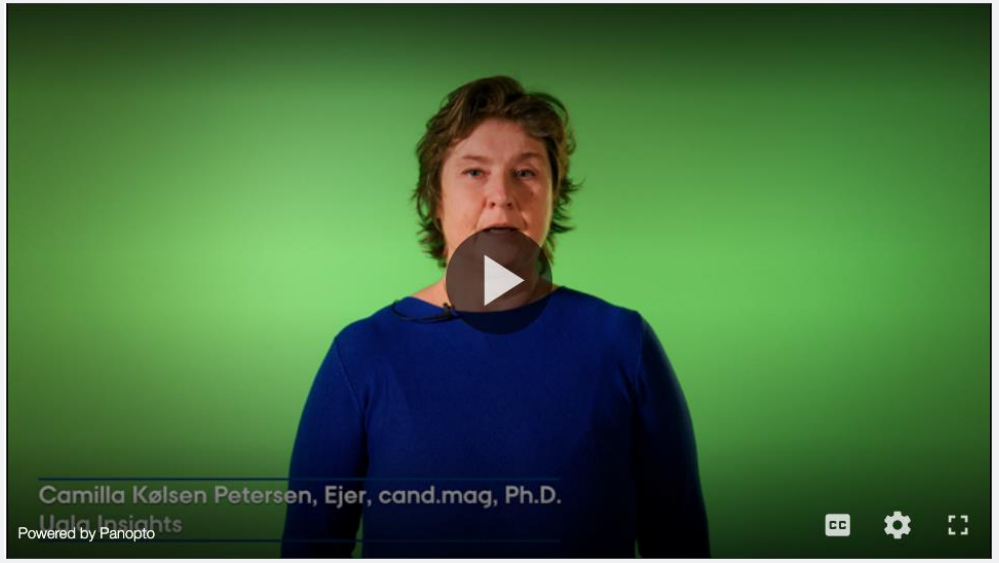
- Virksomhederne har typisk flere **ISO-standarder** og domænespecifikke it- og cybersikkerhedsstandarder. Letter arbejdet med at leve op til lovkrav.
- **Sikkerhedsrutiner** og ramme-værk er tænkt ind fra starten af udviklingsprocesserne.
- **Brug af standarder** er et fælles sprog for alle og en konkurrencefordel

Forstå og form jeres IoT-cybersikkerhed

- Find jeres afsæt og kom videre med byggeblokkene.
- Se på beskrivelserne af de fire byggeblokkes modenhed og tal om, hvilken fase hver af jeres byggeblokke er i.
- Inddrag gerne personer på tværs af funktioner og fagligheder.
- Brug forståelsen af jeres tilgang til IoT-cybersikkerhed til at finde de næste bedste skridt og til at opstille handlingsorienterede mål inden for hver af byggeblokkene.
- Dialogen omkring modenhedsmodellen gør det muligt for jer at koble jeres egen praksis med beskrivelser af adfærd, systemer og struktur i faserne i modenhedsmodellen.

TRIN FOR TRIN VEJLEDNING

Denne video viser, hvordan I afholder modenhedsdialogen om IoT-cybersikkerhed ved hjælp af modellen.

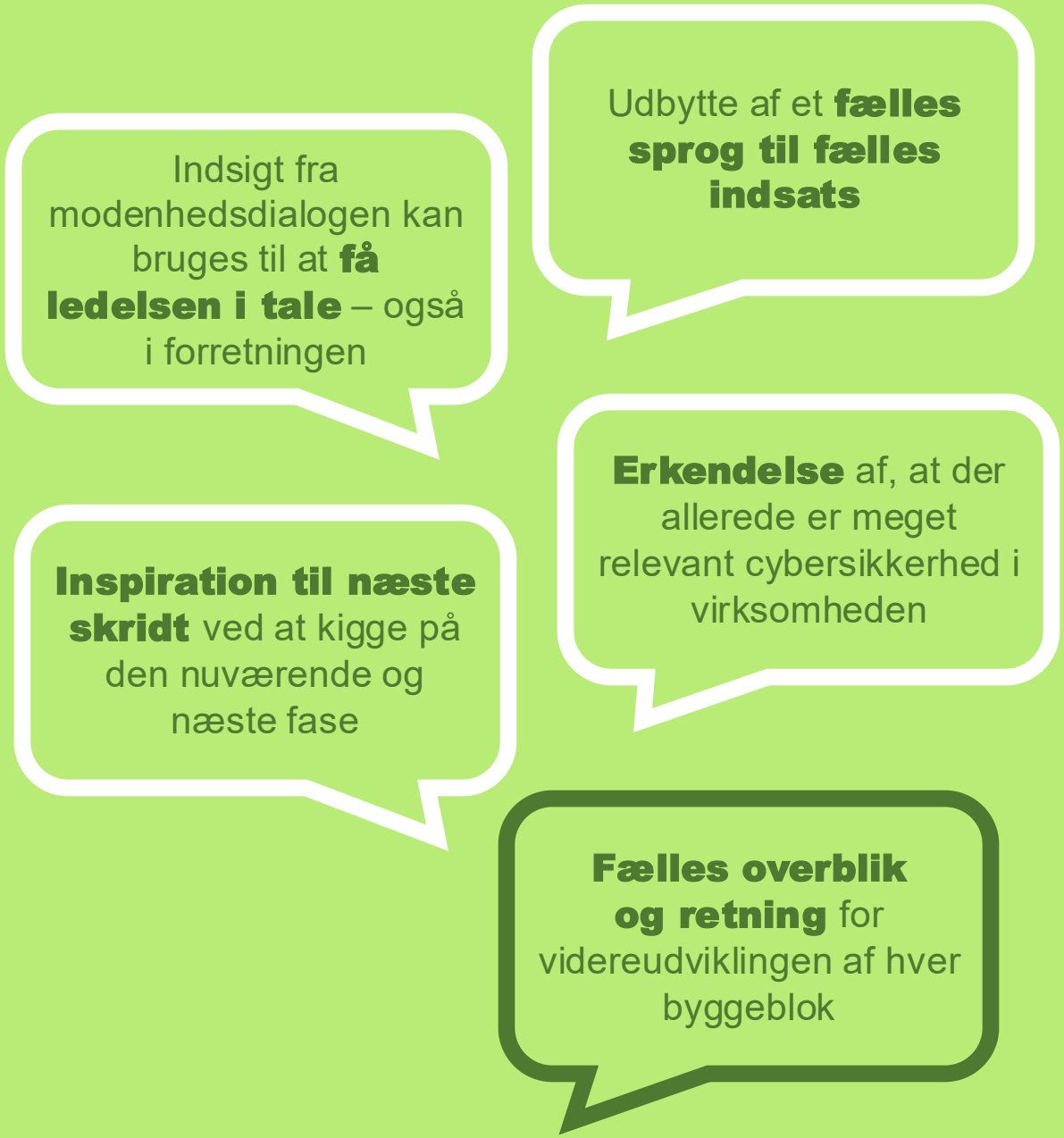


Fælles sprog til fælles indsats

Det er svært at lave en fælles indsats uden et fælles sprog. Jeres forskellige fagsprog udgør forskellige linser, I ser virksomhedens cybersikkerhed igennem.

Hvis I ikke mener det samme, når I taler om handlinger, processer og teknologier, kan I ikke lave en fælles fortolkning af risici, konsekvenser og kriterier, fx på tværs af forretning, teknik og udvikling.

Gennem dialogen om modenhed og risiko i de fire byggeblokke kommer I ud over jeres eget fagsprog og ind i det fælles sprog for virksomhedens IoT-cybersikkerhed.



Risikovurdering i byggeblokkene

Hver byggeblok har et indbygget fokus på risiko: *Hvad er risikoen, og hvad kan vi acceptere?*

De forskellige faglige risikovurderinger medvirker til, at sikkerheden er opdateret og lever op til krav fra kunder, partnere, lovgivning og standarder. Risikovurderingerne spiller dermed en central rolle i virksomhedens tilpasning til marked, partnere og konkurrence-landskab.

De fire byggeblokkes faglige fokus på risikovurdering er:

Teknisk byggeblok: Den konkrete tekniske tilgang til risikovurdering. Gennem mål, test, overvågning og opfølgning m.v. identificeres tekniske risici og deres tekniske mitigering. Risikovurdering og -mitigering kan inkludere samarbejde med en tredjepart.

Organisationsbyggeblok: Fokus på styringsprocesser omkring risikovurderinger, og hvordan der kommunikeres mellem ledere og medarbejdere om risiko. Eksempelvis kan risikovurdering være tilbagevendende i faste intervaller, og forretning og udviklere kan drøfte risici i virksomhedens IoT-cybersikkerhed.

Forretningsbyggeblok: Forretningsmæssig vurdering af IoT-løsningens betydning for forretningen og den medfølgende risikoappetit og/eller investering i IoT-cybersikkerhed. Her inkluderes de risici, der kan opstå i virksomhedssamarbejde eller gennem leverandører, og der er ideelt set både fokus på eksisterende og potentielle IoT-løsninger.

Kvalitetsbyggeblok: Risikovurderingen handler om forretnings-mæssige risici i lovgivningen, fx nye krav til IoT-cybersikkerhed. Kravene medfører et behov for investering i, overblik over og systematisk dokumentation af arbejdet med kvaliteten i tilbudte IoT-løsningers processer og produkter over for ledelse, kunder og samarbejdspartnere, eksempelvis baseret på standarder.

BEMÆRK: *Byggeblokkenes risiko kan kobles sammen i en overordnet risikovurdering, når I arbejder med byggeblokkene i praksis.*

Flere ressourcer fra Cypro-projektet til arbejdet med IoT-cybersikkerhed i praksis

Baggrund: IoT-cybersikkerhed som fælles indsats

Online univers med værktøjer til hver byggeblok

Kurser og andre tilbud om IoT-cybersikkerhed

Kontakt

LAURA LYNGGAARD NIELSEN
Senior Security Anthropologist
Alexandra Instituttet
laura.nielsen@alexandra.dk
+45 4017 6553

CAMILLA KØLSEN
Ejer, cand.mag, PhD
Ugla Insights ApS
camilla@ugla-insights.dk
+45 2217 2840

CyPro

CYBERSIKKER PRODUKTION

17. september 2025

ALEXANDRA INSTITUTTET

AARHUS BSS SCHOOL OF BUSINESS AND SOCIAL SCIENCES AARHUS UNIVERSITET

DAMRC

FORCE TECHNOLOGY

UGLA INSIGHTS

INDUSTRIENS FOND