Ledelsesforankring for cybersikkerhet

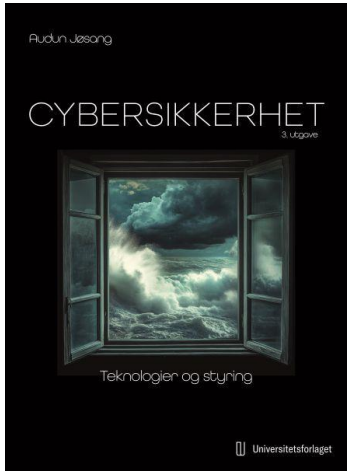
Audun Jøsang

NIFS, Digdir 10.09.2025

Om meg

- Prof. Audun Jøsang, UiO
  - UiO, 2008 →
  - QUT, Australia, 2000 – 2007
  - Telenor FoU, 1998 –1999
  - Alcatel, Belgia 1988 –1994

- Lærebok om cybersikkerhet
  - 3. utgave 2025



- Engelsk versjon
  - 1. utgave 2024

Sikkerhet og usikkerhet

Betydning og oversettelse av begrepet “sikkerhet”

Engelsk		Norsk
• Security	→	• Sikkerhet
• Safety	→	• Trygghet
• Certainty	→	• Visshet

Presis oversettelse

- Security
- Safety
- Certainty

→ • Sikkerhet

Upresis oversettelse

ISO/IEC 27005:2024 Styring av informasjonssikkerhetsrisiko

Risiko er virkningen av uvisshet på måloppnåelse.

Hva er sikkerhet ?

Sikkerhet er beskyttelse av verdier mot skade

eiendom, infrastruktur, demokrati, lov og orden, liv og helse, miljø, digitale verdier, persondata

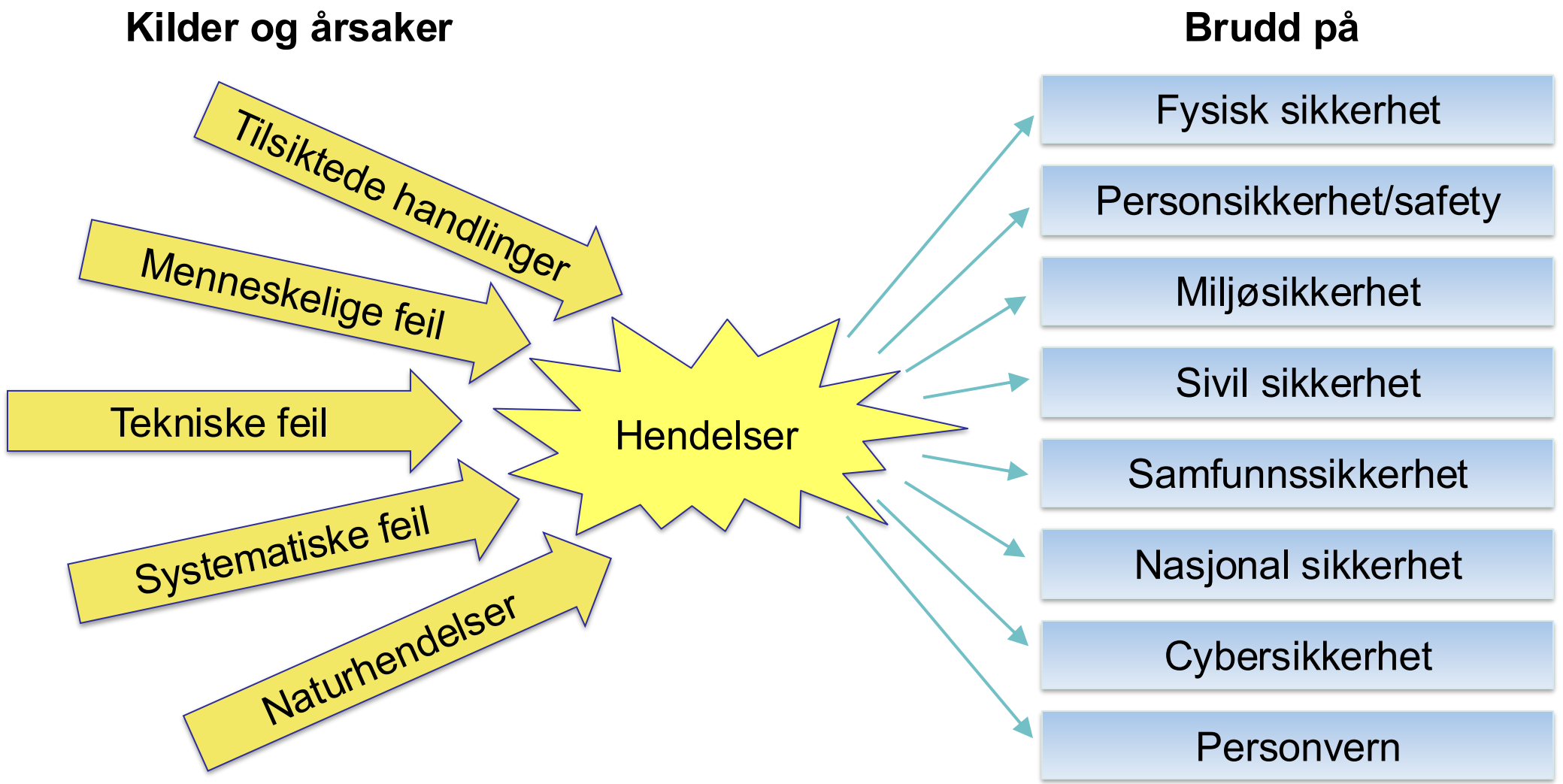







- **Fysisk sikkerhet:** hindre innbrudd, tyveri og tukling med utstyr
- **Samfunnssikkerhet:** opprettholde funksjonalitet i kritiske infrastrukturer
- **Nasjonal sikkerhet:** demokrati, politisk stabilitet, territorial integritet
- **Sivil sikkerhet og rettssikkerhet:** opprettholdelse av lov og orden
- **Personsikkerhet / trygghet / safety:** beskyttelse av liv og helse
- **Miljøsikkerhet:** hindre forurensing og fremmede arter
- **Cybersikkerhet:** beskyttelse av digitale verdier
- **Personvern:** følge prinsipper for innhenting, lagring, behandling og deling av personopplysninger

Ulike kilder til brudd på sikkerhet

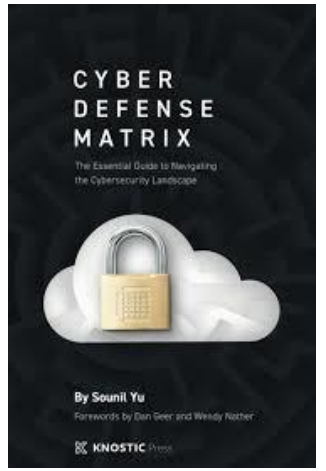


Cybersikkerhet og informasjonssikkerhet

- Cybersikkerhet er beskyttelse av digitale verdier mot skade.

- Informasjonssikkerhet er beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet.

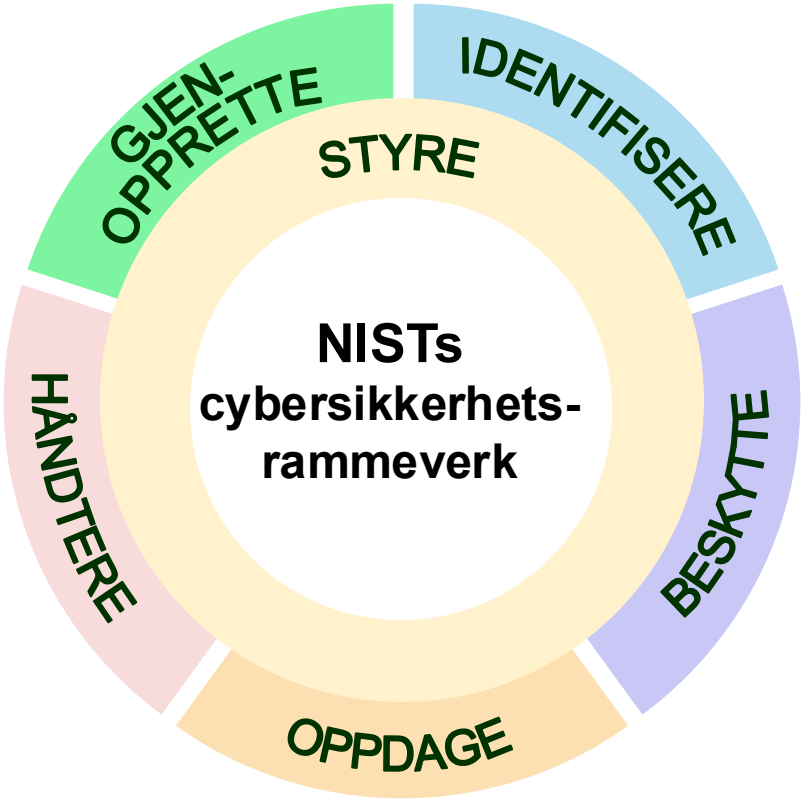
Digitale verdier



- ENHETER er maskinvare og standard installert programvaren som OS.
- APPER er applikasjoner og prosesser spesielt utviklet av eller for virksomheten.
- NETTVERK er kommunikasjonskanaler, rutere, protokoller og brannmurfiltreringer.
- DATA er forretningsdata, som er lagret, overføres eller brukes av verdiene over.
- BRUKERE er personer og KI-agenter, med deres ID-er og autentikatorer.

Cybersikkerhetsrammeverket og Grunnprinsippene for IKT-sikkerhet

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



≈

NSMs grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge
2. Beskytte og opprettholde
3. Oppdage
4. Håndtere og gjenopprette

Grunnprinsipper for sikkerhetsstyring

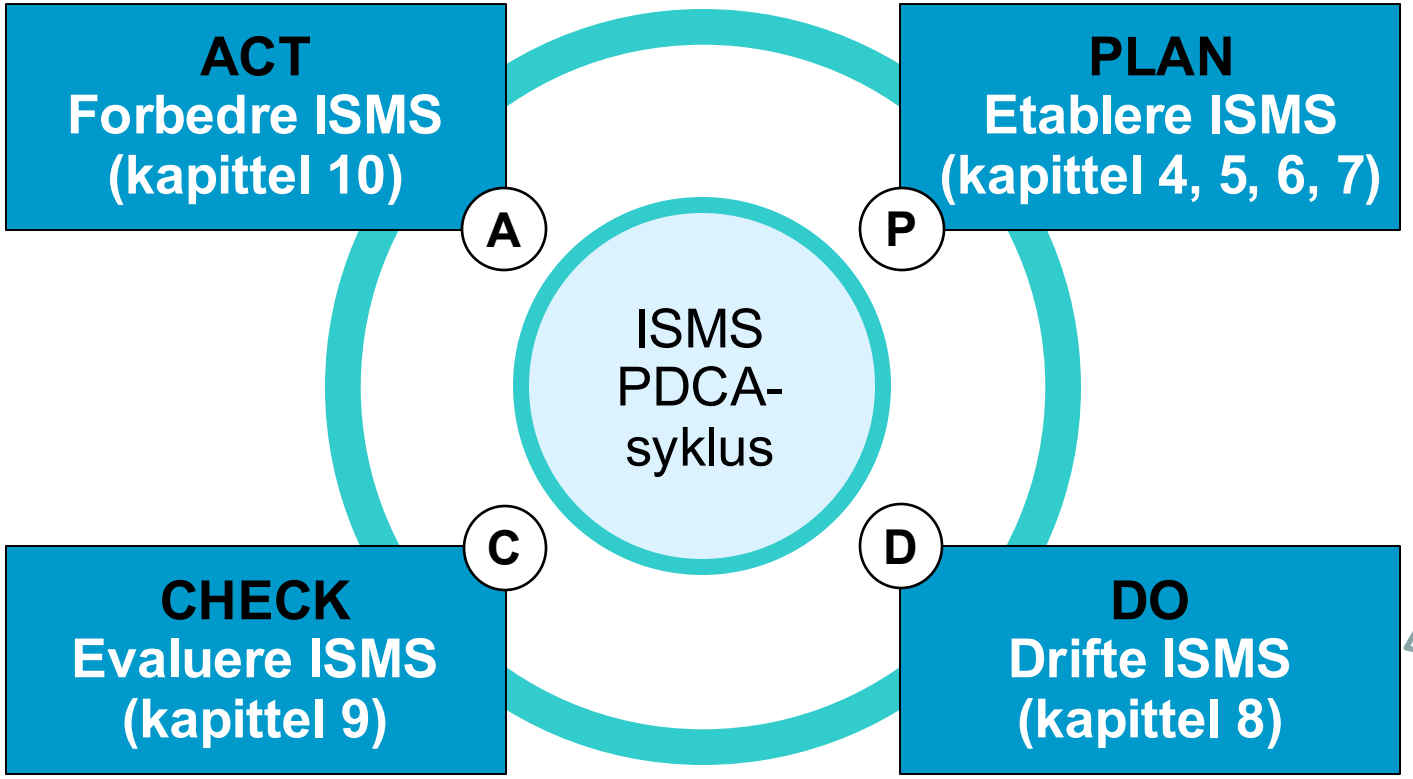
NSM

- Ny funksjon STYRE (GOVERN) lagt til i CSF 2.0 (2024)
- STYRE tilsvarer ISO/IEC 27001

ISO/IEC 27001 ISMS - krav

Krav til styrings-/ledelsessystem for informasjonssikkerhet

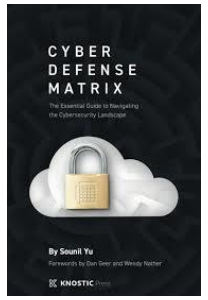
- Standarden beskriver krav til ISMS, som kan struktureres etter PDCA-syklusen.
- God styring av DO-fasen krever oppfyllelse av kravene i de andre fasene.



Implementere og drifte sikkerhetsfunksjonene i NSMs grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge
2. Beskytte og opprettholde
3. Oppdage
4. Håndtere og gjenopprette

Cyberforsvarsmatrisen (Cyber Defense Matrix)

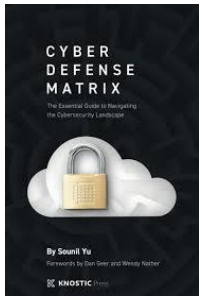


Sikkerhetsfunksjoner

Digitale verdier	IDENTIFISERE	BESKYTTE	OPPDAGE	HÅNDTERE	GJEN-OPPRETTE
ENHETER	■ ● ●	■ ■ ● ● ●	■ ● ●	■ ● ● ●	■ ● ●
APPER	●	■ ■ ■ ● ● ● ●	■ ● ●	●	●
NETTVERK	■ ● ● ● ●	■ ■ ■ ■ ● ● ● ●	■ ■ ● ● ●	■ ● ●	■ ■ ● ●
DATA	■ ● ●	■ ■ ■ ● ●	●	■ ●	■ ● ●
BRUKERE	■ ● ● ●	■ ● ●	● ●	●	●

Forklaring: ■ Nåværende profil ● Ønsket profil

Cyberforsvarsmatrisen brukt til ansvarsfordeling

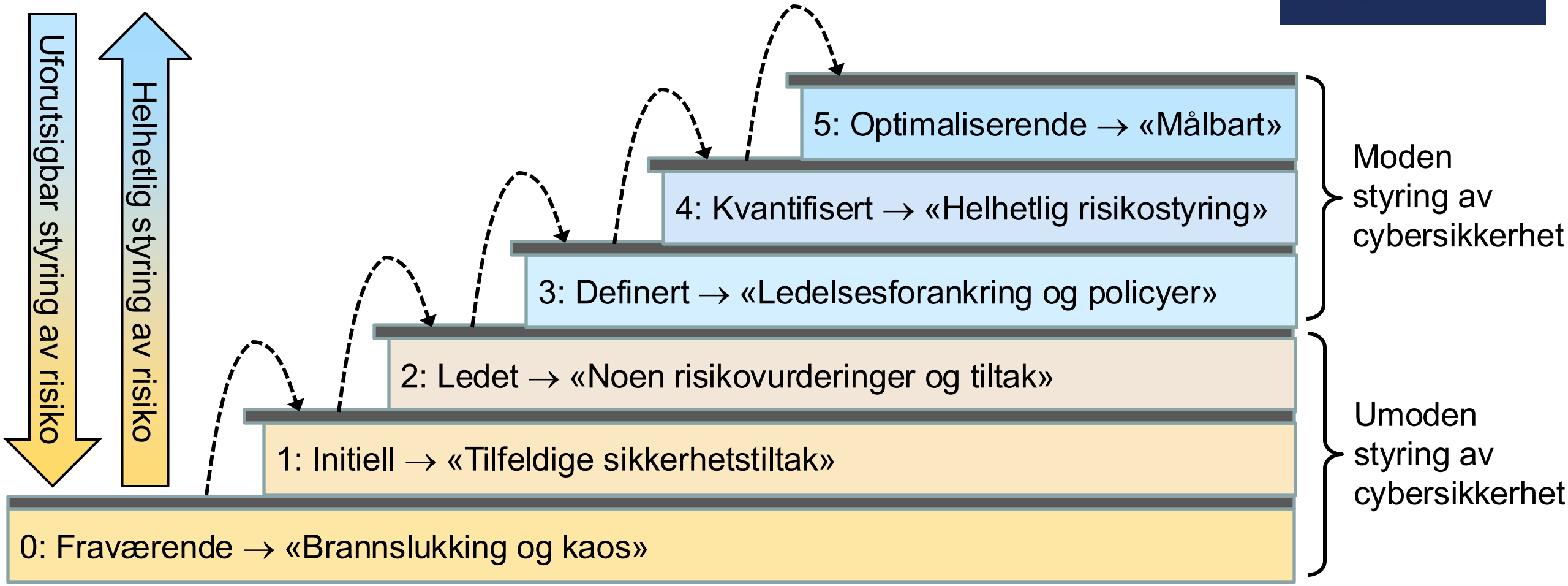


- Cyberforsvarsmatrisen kan vise fordelingen av sikkerhetsansvar i organisasjonen.

Sikkerhetsfunksjoner

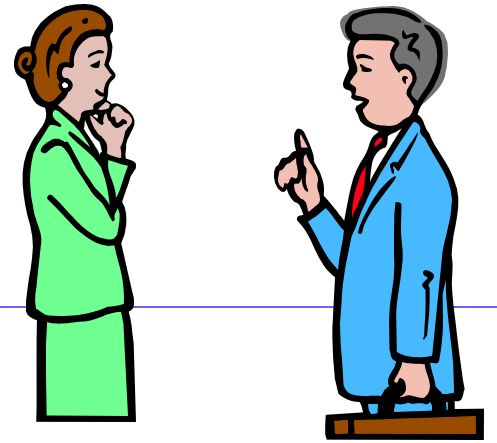
Digitale verdier	IDENTIFISERE	BESKYTTE	OPPDAGE	HÅNDTERE	GJEN-OPPRETTE
ENHETER	IT-tjenester, eiere		SOC/CERT/CSIRT Overvåking av enheter		IT-tjenester, eiere
APPER	DevOps-team, eiere		SOC/CERT/CSIRT Overvåking av apper		DevOps-team, eiere
NETTVERK	Nettverksadministrator		SOC/CERT/CSIRT Overvåking av nettverk		Nettverks-administrator
DATA	Dataeiere (CDO), personvernombud (PVO)		SOC/CERT/CSIRT IT-drift		CDO, PVO, eiere
BRUKERE	HR-avdelingen		Overvåking av innsidetrusler	HR-avdelinge, fysisk sikkerhet	

Modenhet i styring og ledelse av cybersikkerhet
CMMI – Capability Maturity Model Integration



Spørsmål som ledelsen bør stille seg

1. Hvordan holder virksomheten seg oppdatert om cybertrusler generelt, og for egen sektor og virksomhet spesielt?
2. Har virksomheten god oversikt og forståelse av risiko relatert til informasjonssikkerhet?
3. Har ledelsen tilstrekkelig kompetanse om informasjonssikkerhet?
4. Hvor godt er risikostyring for informasjonssikkerhet integrert i helhetlig risikostyring?
5. Bør cyberforsikring inkluderes i virksomhetens forsikringspoliser?
6. Hvor modent er virksomhetens ISMS?
7. Hvor godt er ISMS forankret hos ledelsen? ⚓
8. Jobbes det med god sikkerhetskultur som del av virksomhetskulturen generelt?
9. Dekker beredskapsplanen også cybersikkerhetshendelser, og er planen testet?
10. Hvor god er etterlevelsen av lover og forskrifter om informasjonssikkerhet og personvern?
11. Hvor god er beskyttelsen av informasjon som overføres til tredjeparter?
12. I hvilken grad bør virksomheten outsource sikkerhetsfunksjoner, som f.eks. gjennom å kjøpe MDR (Managed Detection and Response)?



Takk for oppmerksomheten