NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0

Inside Telecom konferansen 2020

NASJONAL SIKKERHETSMYNDIGHET

Are Søndenaa
Oktober 2020

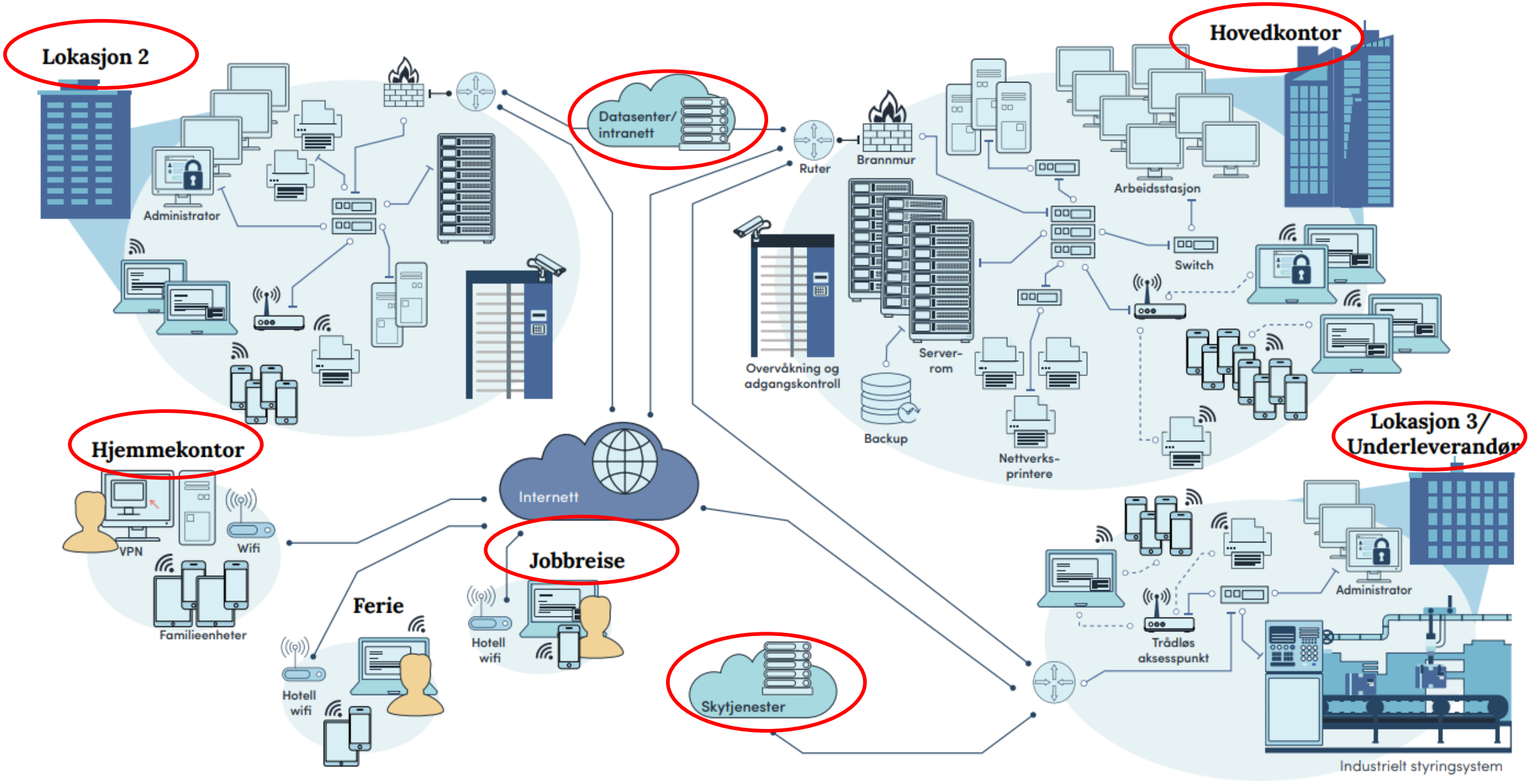
Agenda

1. Utfordringer og risikoer
   - Grunnprinsippenes rolle
2. Grunnprinsippene
   - Kategori 1 – Identifisere og kartlegge
   - Kategori 2 – Beskytte og opprettholde
   - Kategori 3 – Oppdage
   - Kategori 4 – Håndtere og gjenopprett
3. Avslutning og spørsmål

Utfordringer og risikoer

- og grunnprinsippenes rolle

NASJONAL
SIKKERHETSMYNDIGHET
Helhetlig digitalt
risikobilde 2020


Lokasjon 2
Administrator
Datasenter/
intranett
Ruter
Brannmur
Hovedkontor
Arbeidsstasjon
Switch
Overvåkning og
adgangskontroll
Server-
rom
Backup
Nettverks-
printere
Hjemmekontor
VPN
Wifi
Familieenheter
Internett
Jobbreise
Hotell
wifi
Ferie
Hotell
wifi
Skytjenester
Lokasjon 3/
Underleverandør
Administrator
Trådløs
aksesspunkt
Industrielt styringsystem

Målgrupper for Grunnprinsippene

- Generelt: virksomheter i Norge
  - Offentlig og privat virksomhet
  - Herunder kritisk infrastruktur
- Roller i virksomheten
  - IT-ledere, Sikkerhetsledere, IT-arkitekter, Driftsledelse
- Antagelse: virksomhet med en IT-avdeling

Kritisk infrastruktur

Kraftforsyning	Telekom
Vann og avløp	Forsvar
Helse	Forsynings-sikkerhet
Finansielle tjenester	Transport
Satellittbaserte tjenester	Viktig offentlig administrasjon

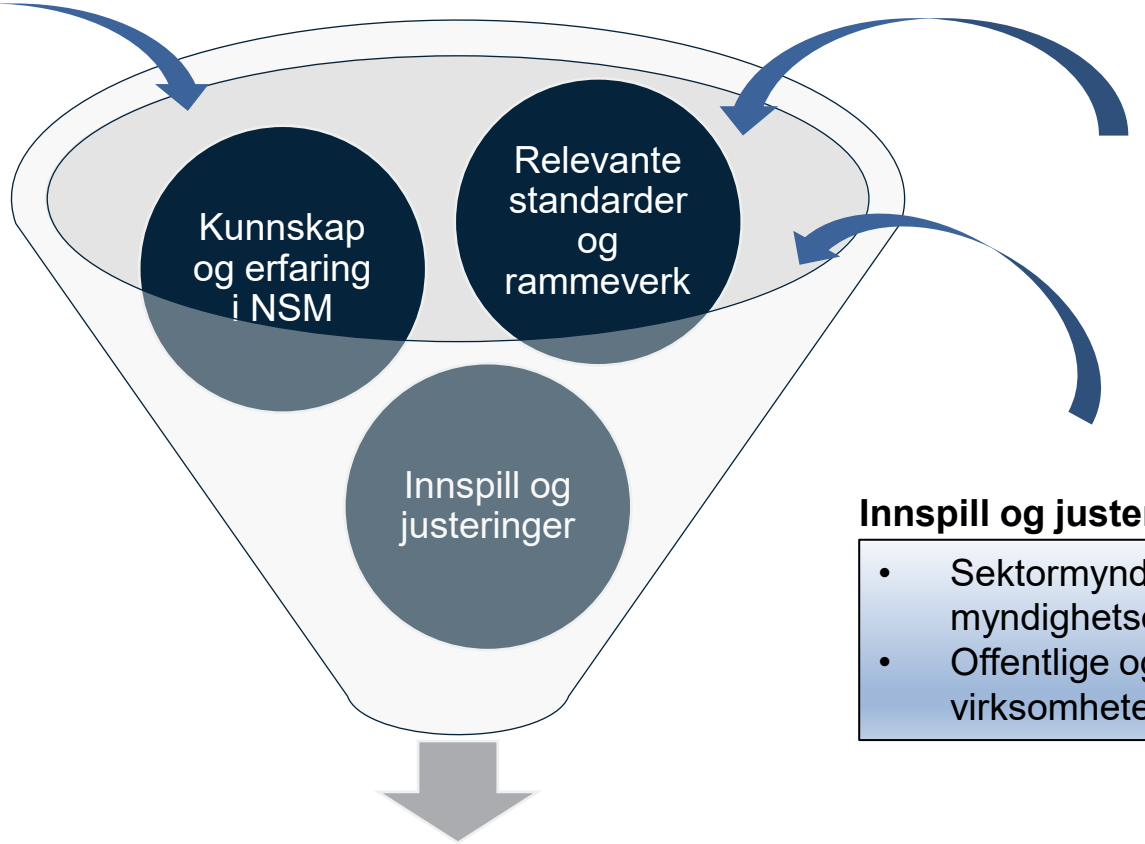
Hvorfor lage Grunnprinsipper?

- Masse gode anbefalinger og rammeverk «out there» …
  - Hvorfor finne opp hjulet på nytt?
- Utfordringer med internasjonale rammeverk:
  - Ukjent for mange, noen krever pålogging/betaling, mye å sette seg inn i
  - Ikke alltid optimalt for Norske virksomheter
- Norge:
  - Lite land, små IT-avdelinger
  - Mindre hierarkisk, færre nivåer, mer delegert myndighet
  - Litt raskere til å kjøpe nyere teknologi

Hvordan har grunnprinsippene blitt til?

Kunnskap og erfaringer NSM

- Rådgivning
- Hendelser (NCSC)
- Inntrengingstester
- Tilsyn
- Kravutvikling
- Samarbeidspartnere



Relevante standarder og rammeverk

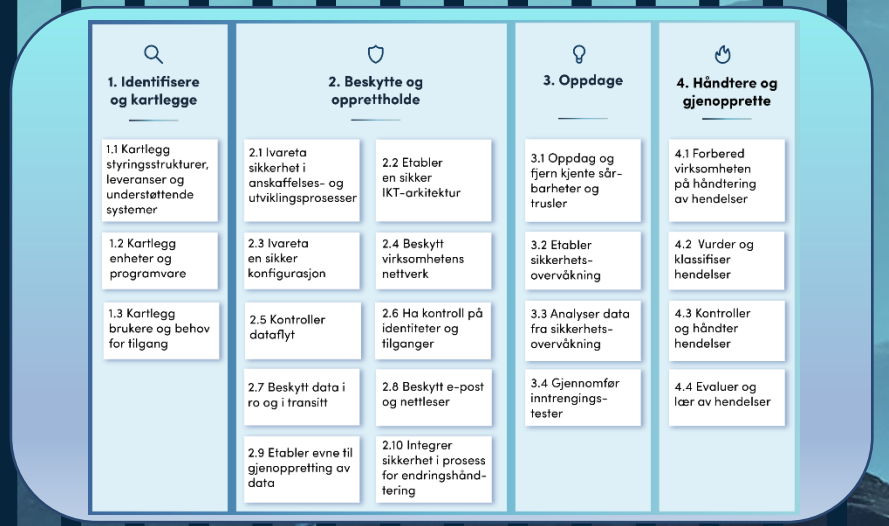
- ISO 27002
- NIST CSF
- CIS CSC 20
- UK Cyber Essentials
- BSI Grundschutz
- ++

Innspill og justeringer

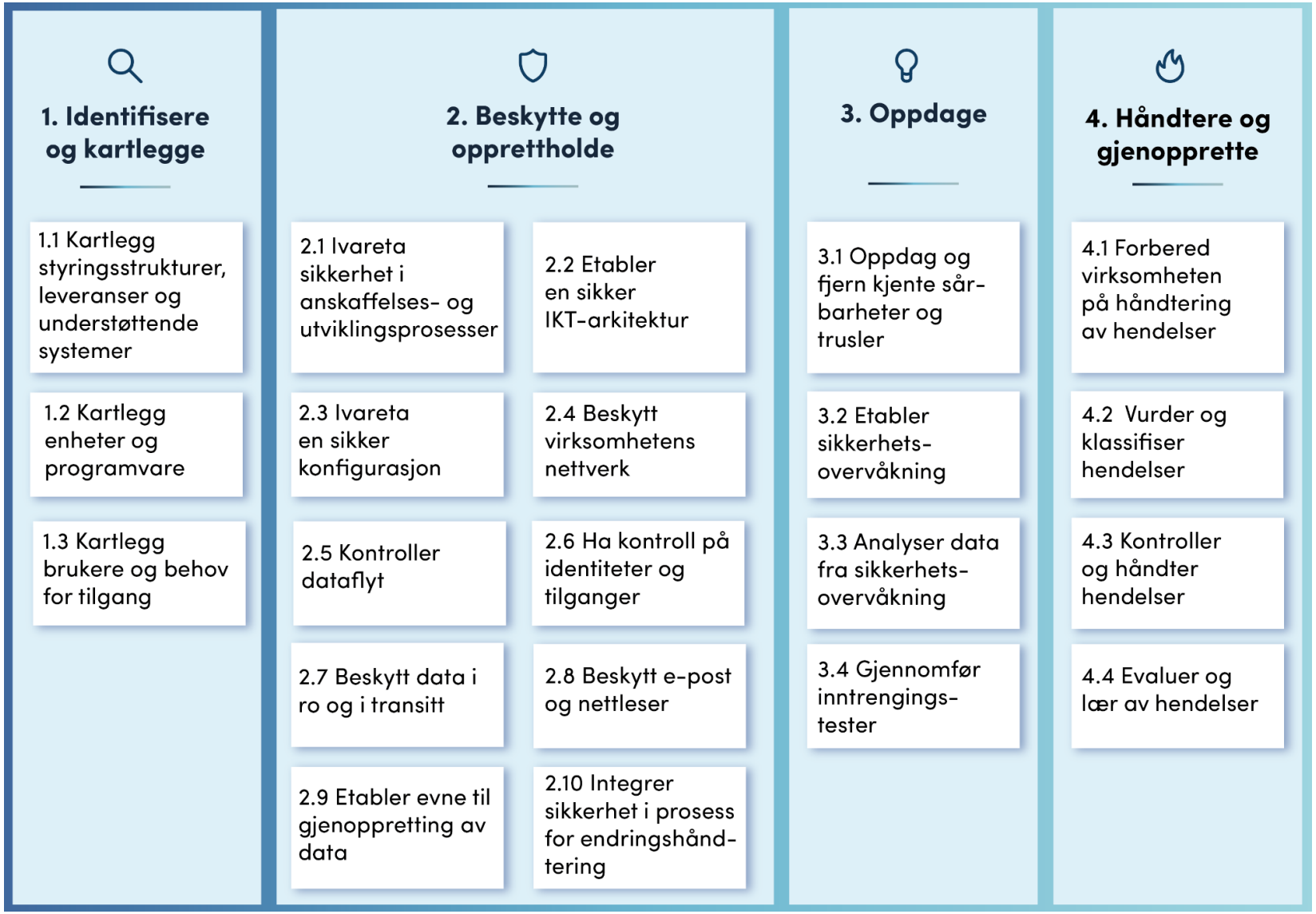
- Sektormyndigheter og myndighetsorganer
- Offentlige og private virksomheter

De fire kategoriene

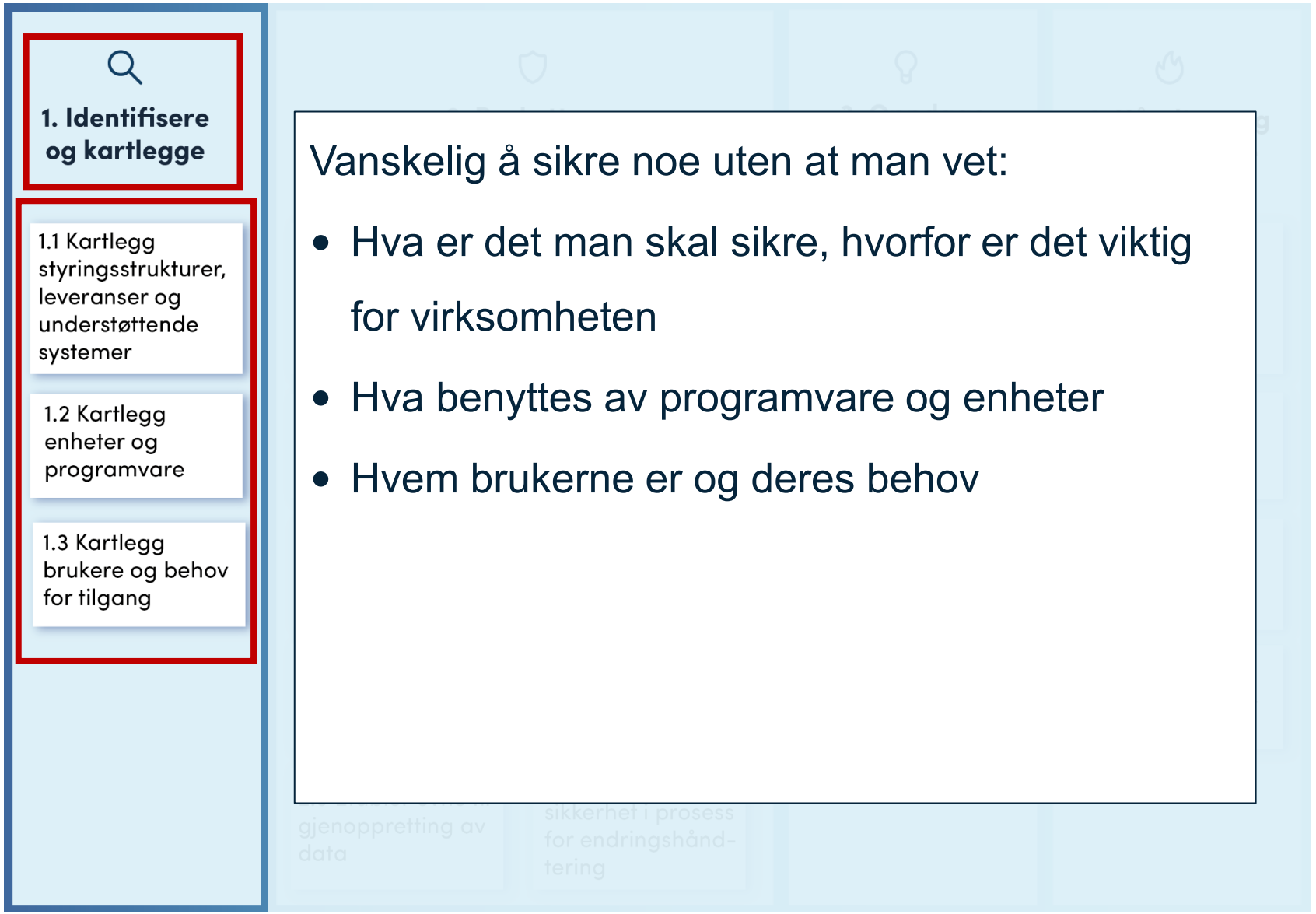
NASJONAL
SIKKERHETSMYNDIGHET



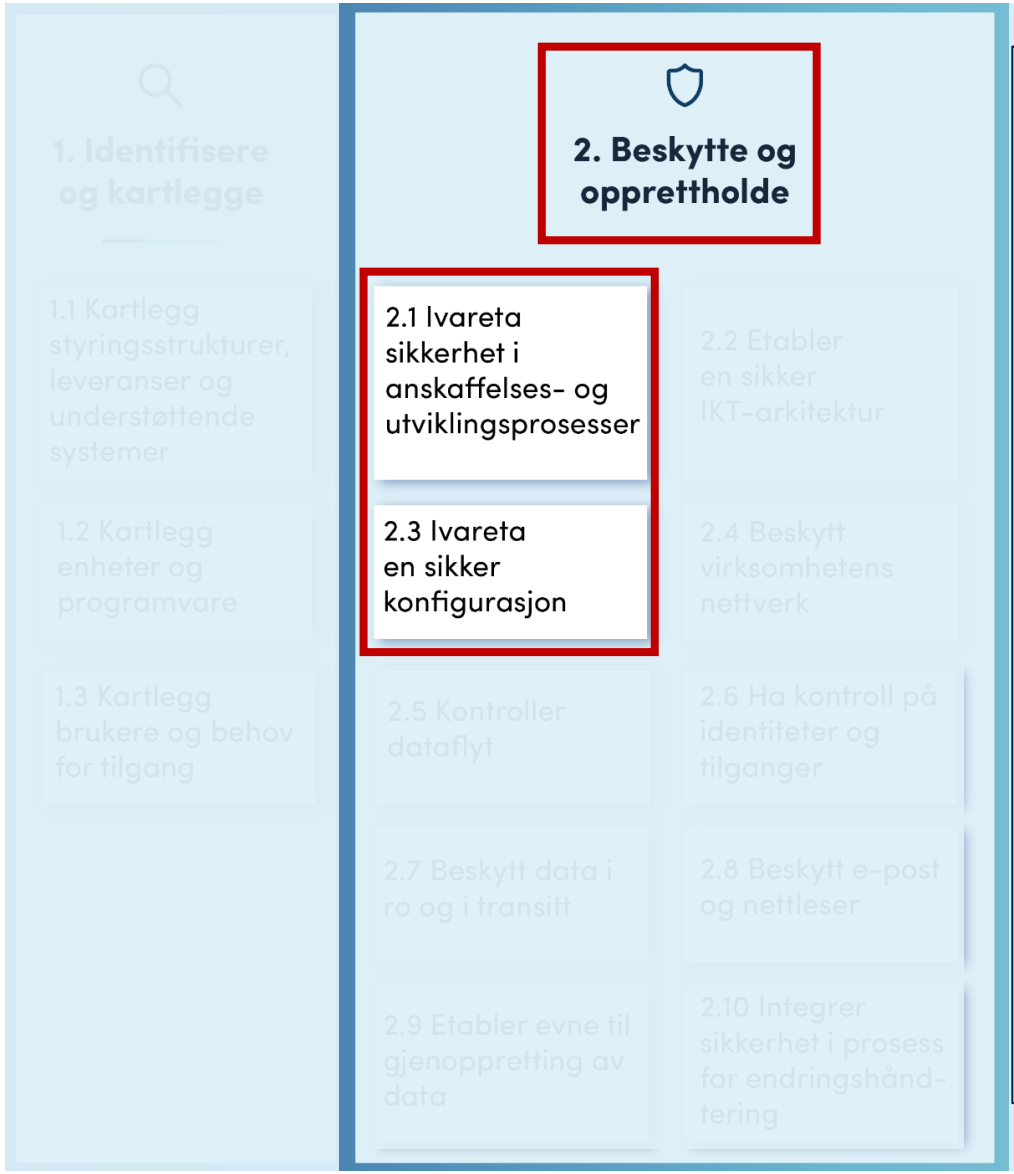
NSMs grunnprinsipper for IKT-sikkerhet (v 2.0)



Kategori 1 – Identifisere og kartlegge

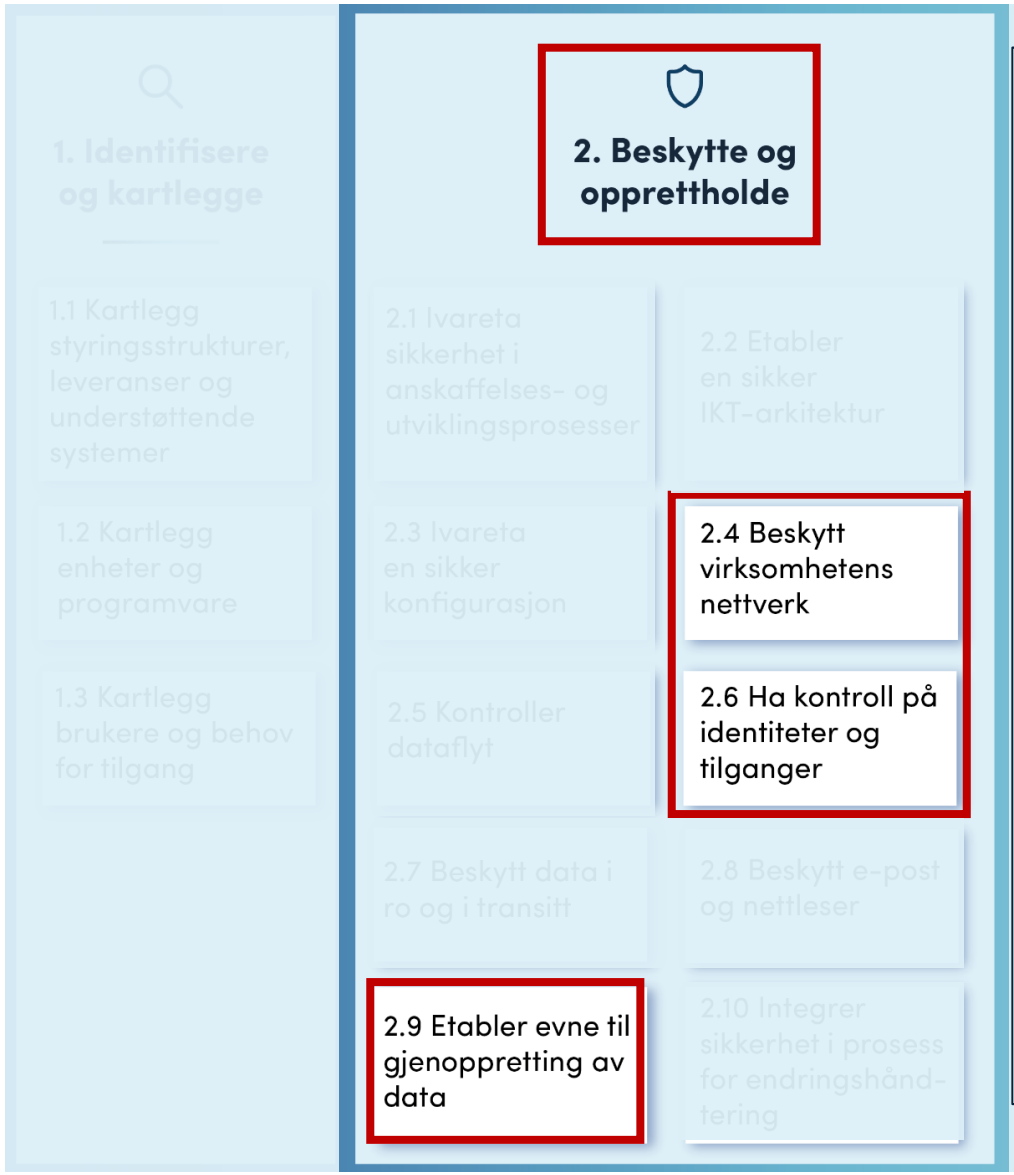


Kategori 2 – Beskytte og opprettholde



- Sikkert kjøp
  - Sikkerhet angår ikke bare sikkerhetsprodukter!
  - Fas ut eldre IKT-produkter
  - Virtualisering og “sky”
- Sikkerhetskonfigurasjon
  - sentralt styrt regime for sikkerhetsoppdatering
  - klienter slik at kun kjent programvare kjører på dem

Kategori 2 – Beskytte og opprettholde (forts.)



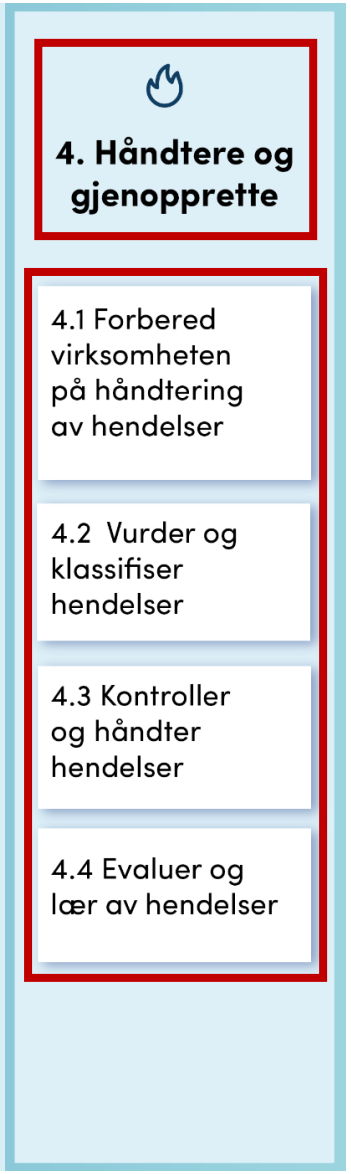
- Nettverk
  - Etabler tilgangskontroll på flest mulige nettverksporter
  - Krypter alle trådløse og kablede forbindelse
- Identiteter og tilganger
  - Gi ansatte kun de rettighetene de trenger
  - Driftskontoer: ikke alle egg i en kurv …
- Backup
  - Lag en plan
  - Test plan og sikkerhetskopi

Kategori 3 – Oppdage

- Oppdage trusler og sårbarheter
  - Jevnlig sårbarhetskartlegging, helst automatiserte verktøy
- Etabler sikkerhetsovervåkning
  - Beslutt hvilke data som er sikkerhetsrelevant
  - Verifiser at innsamling fungerer
  - Analyser data fra sikkerhetsovervåkning
- Inntrengningstester

Kategori 4 - Håndtere og gjenopprette

- Forbered virksomheten på håndtering av hendelser
  - Plan!
  - Øve!
- Håndter hendelser når de inntreffer
- Lær av hendelsen



Avsluttende tips

- Få *oversikt* over maskiner og programvare *i bruk*
- Fjern de vanligste *sårbarhetene*:
  - Klientkonfigurasjon (+ serverkonfigurasjon)
  - Nettverkskonfigurasjon
  - Sikkerhetsoppdatering
- Sørg for god *tilgangsstyring*
  - Bedre og mer finmasket styring av rettigheter
    - sluttbrukere og drift
  - Avslutt bruk av enkle passord
  - Avslutt bruk av enkle påloggingsmekanismer (→MFA)
- Ha tilstrekkelig *beredskap*
  - Backup, systemovervåkning og logging
  - Plan ved hendelser (og øve)

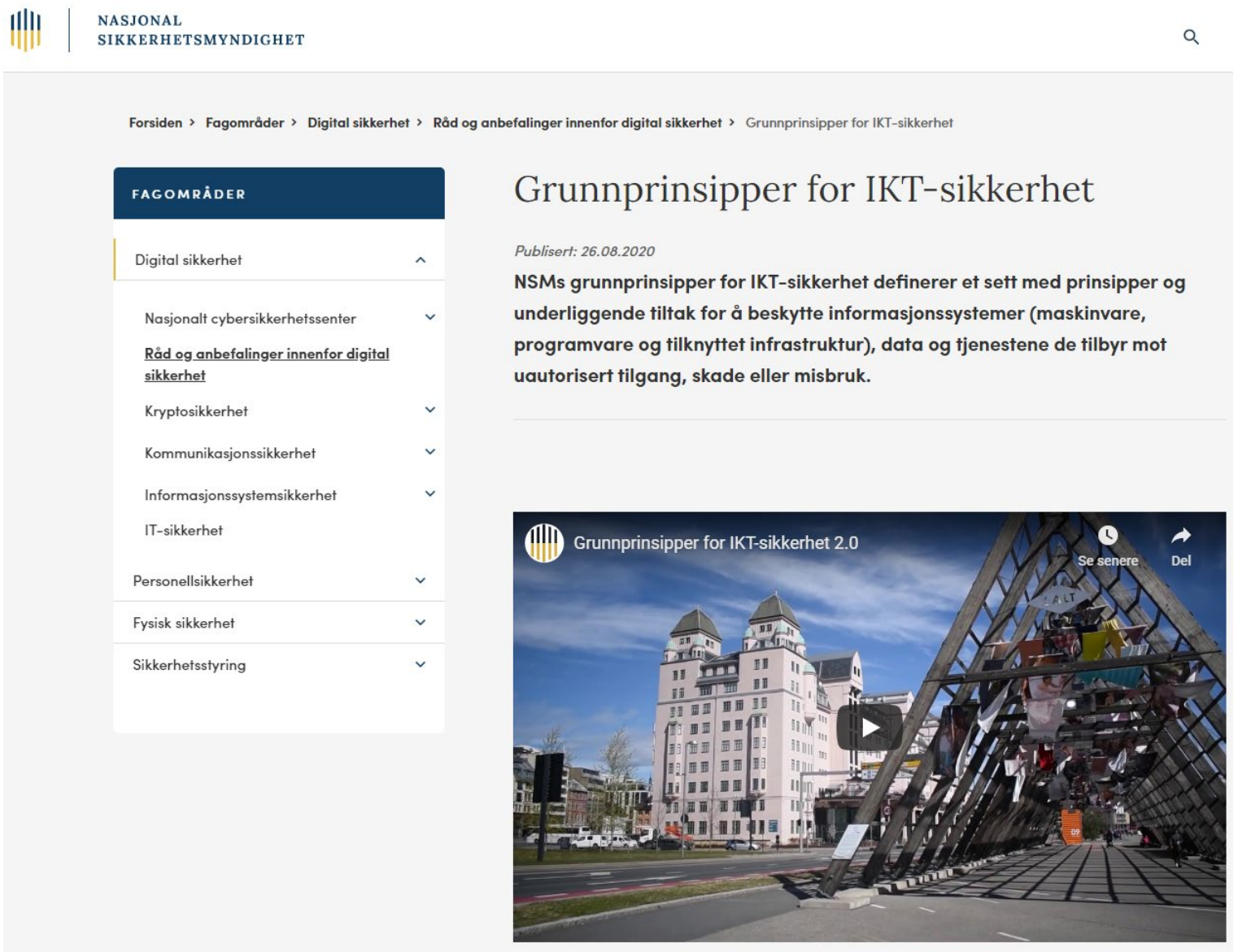
Merknader:

- **Gjennomgående:** mest mulig *sentralisert, automatisert og standardisert drift* av klienter, servere og nettverk.
- **Sky:** Tiltakene er like relevant for både virtualisert og fysisk infrastruktur, og både for «on-prem» og ved kjøp av f.eks. IaaS-tjenester.
- **I sum:** *Forebygg, forebygg, forebygg*, men vær også forberedt på at noe kan gå galt.

Støtteprodukter

- 5 Viktigste tiltak (kommer)
- Prioriteringsliste
  - 15 tiltak – Prioritetsgruppe 1
  - 20 tiltak – prioriteringsgruppe 2
  - 83 tiltak – prioriteringsgruppe 3
- Kobling mot ISO 27002
- Ofte stilte spørsmål (OSS)

- nsm.no/grunnprinsipper-ikt



Avslutning

Takk for oppmerksomheten!

www.nsm.no/grunnprinsipper-ikt