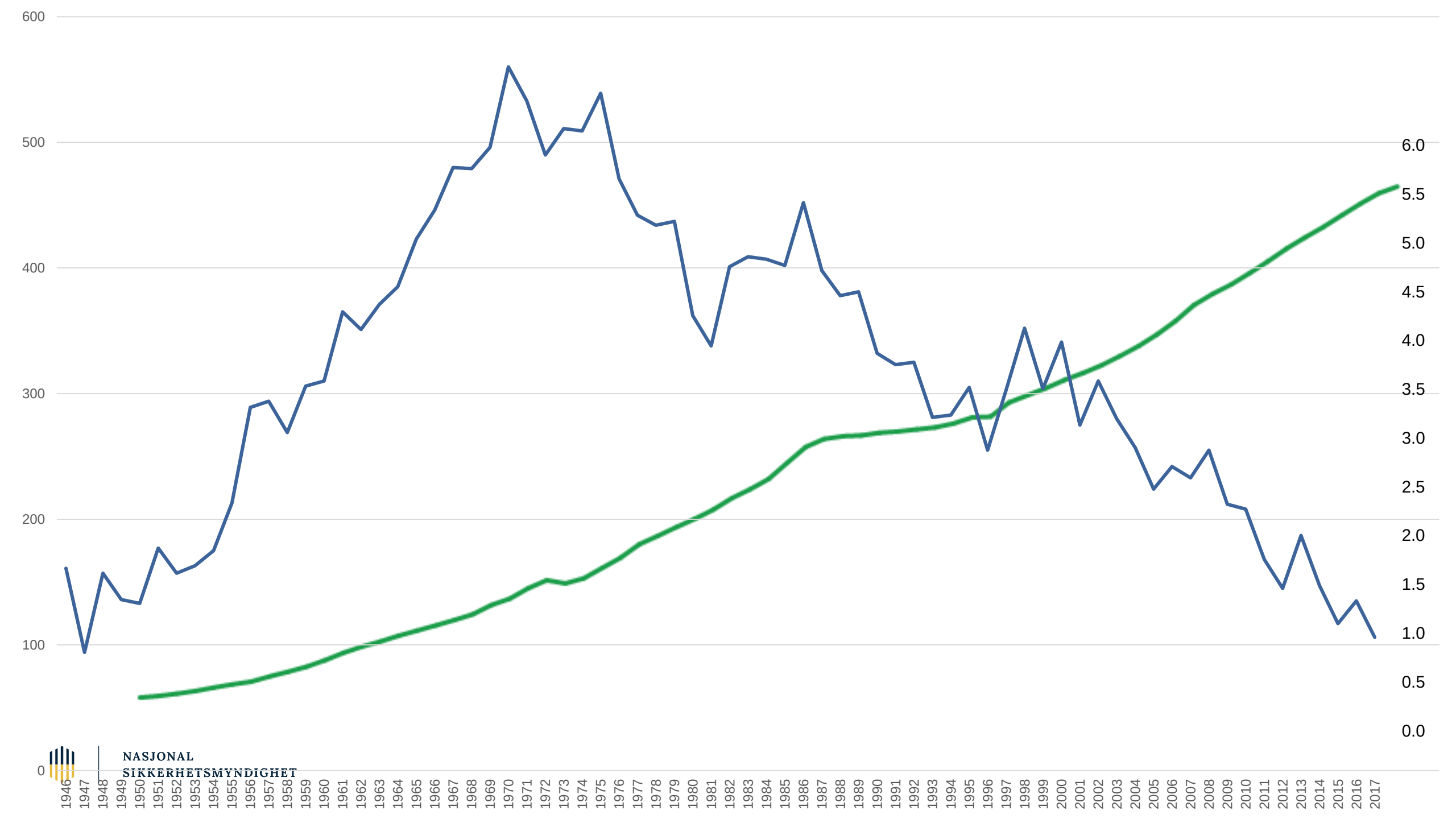
# NSMs Grunnprinsipper for IKT-sikkerhet

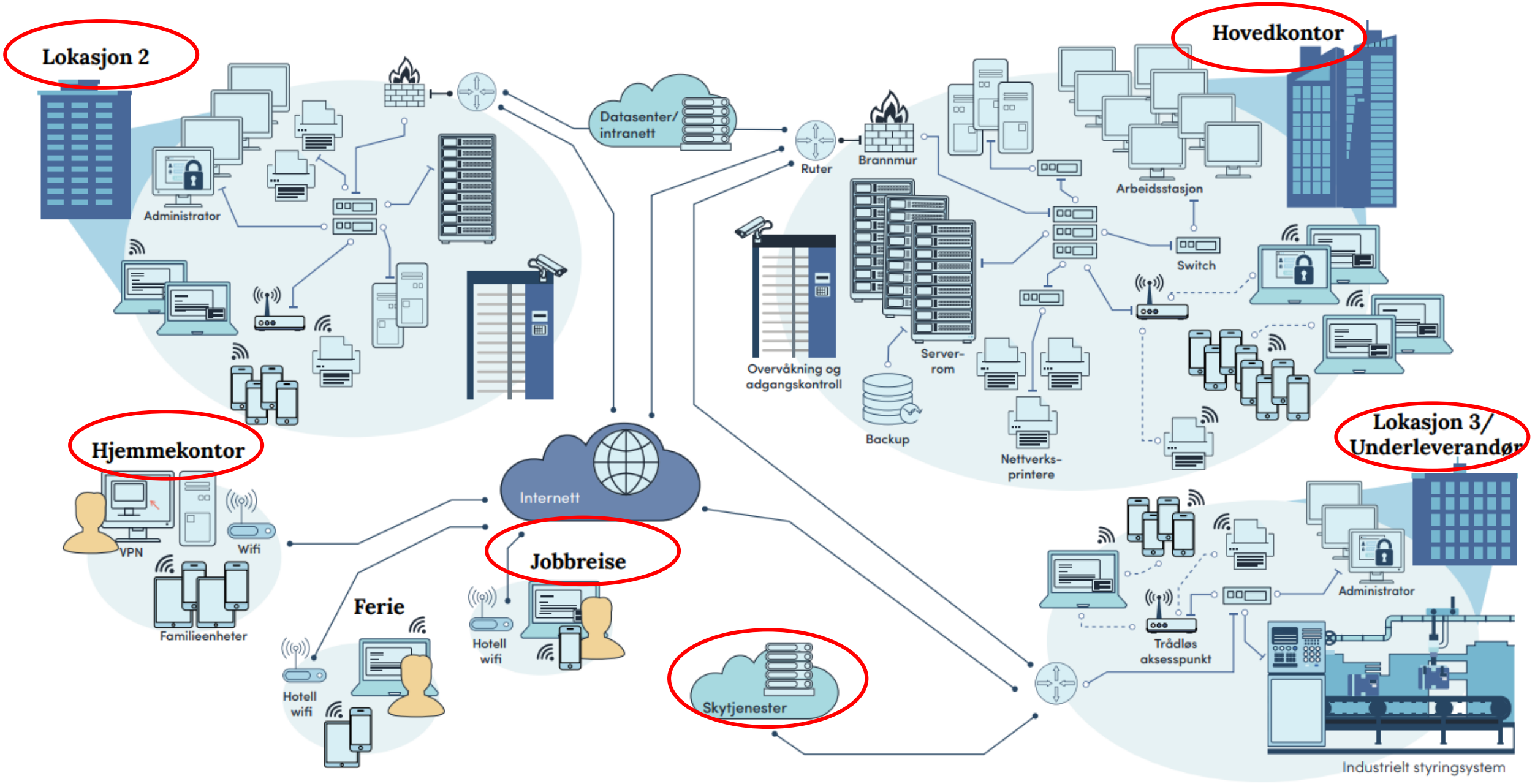
Normkonferansen 2019

NASJONAL SIKKERHETSMYNDIGHET

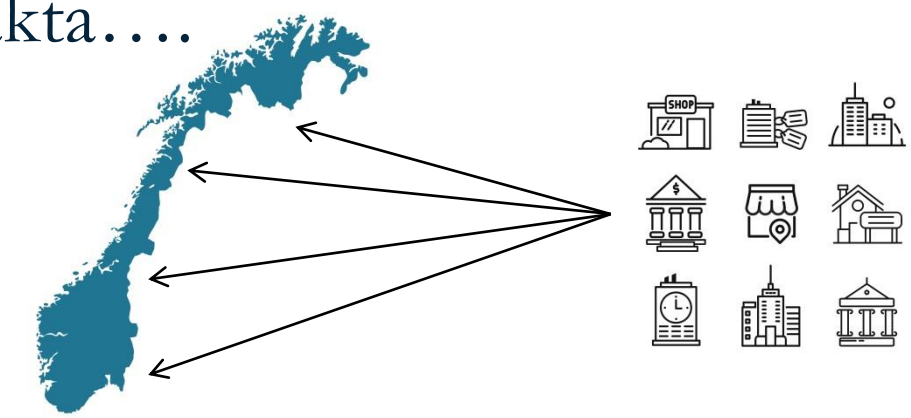
Are Søndenaa
27.11.19


600
500
400
300
200
100
0
6.0
5.5
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
NASJONAL
SIKKERHETSMYNDIGHET

# *«Man skjønner ikke at man ikke skjønner IKT!»*


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

# Litt fakta….



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


**202.101**

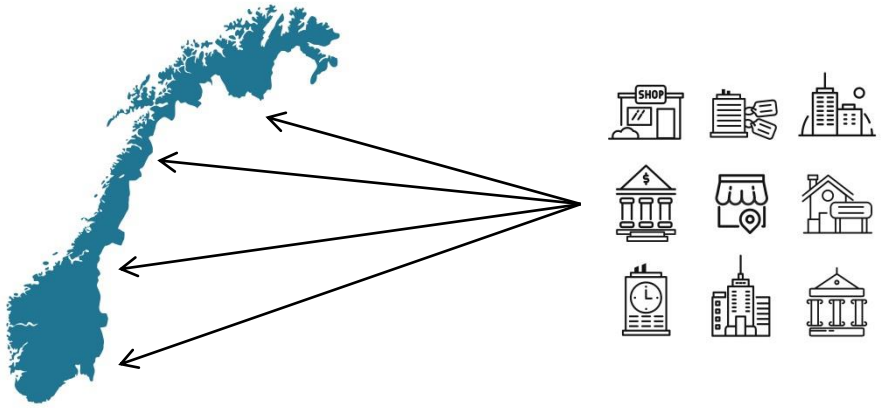
**?**

**10-12.000?**

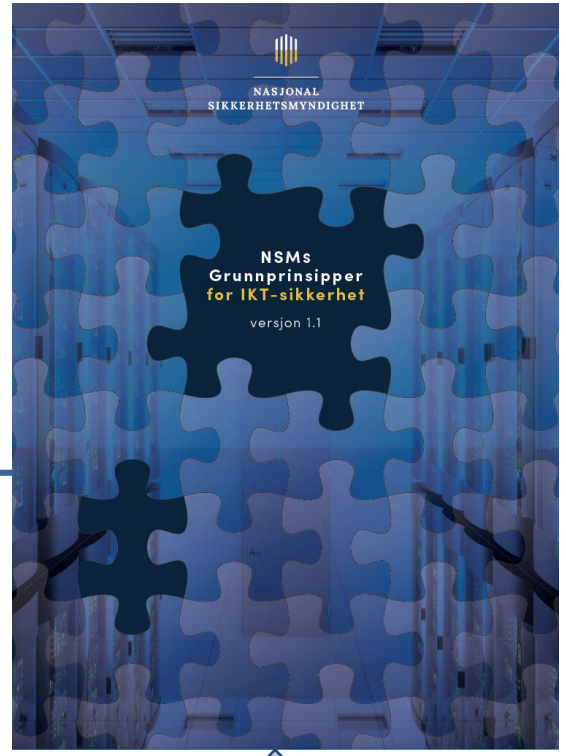
**¿**

**??????**

NASJONAL SIKKERHETSMYNDIGHET



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

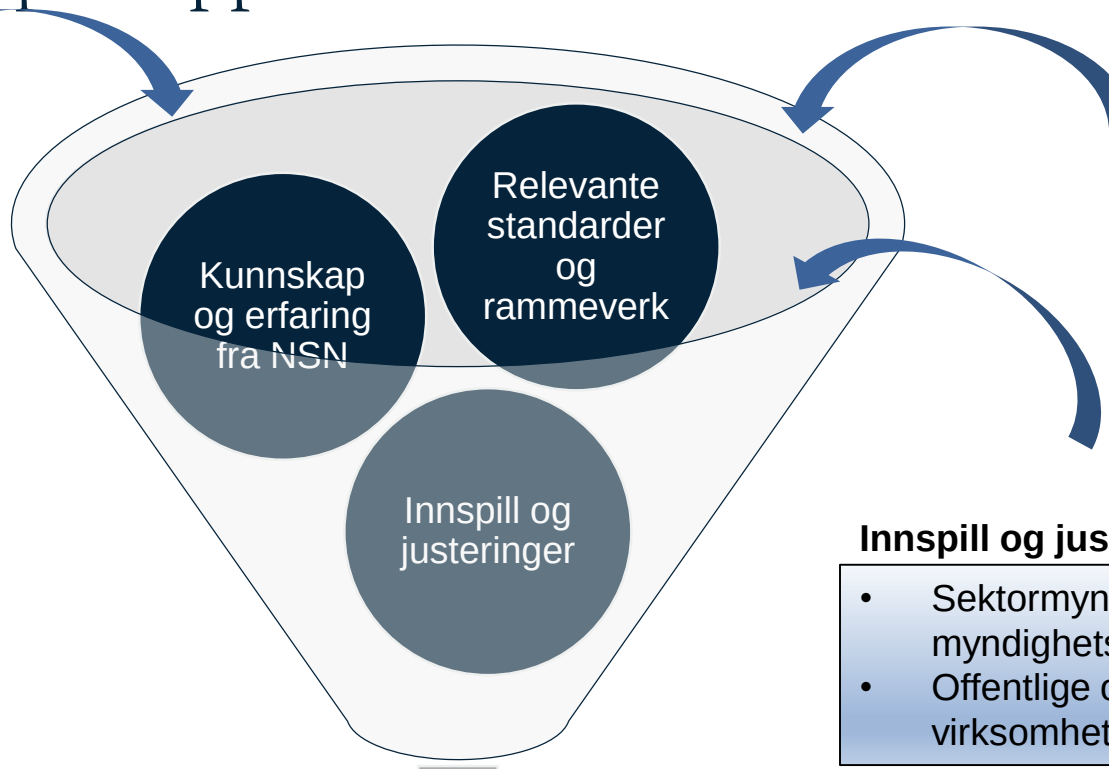

ISO 27002

NASJONAL SIKKERHETSMYNDIGHET

# Hvordan har grunnprinsippene blitt til?

**Kunnskap og erfaringer NSM**

- Rådgivning
- Penetrasjonstest
- Tilsyn
- Hendelser (NorCERT)
- Kravutvikling
- Samarbeids-partnere



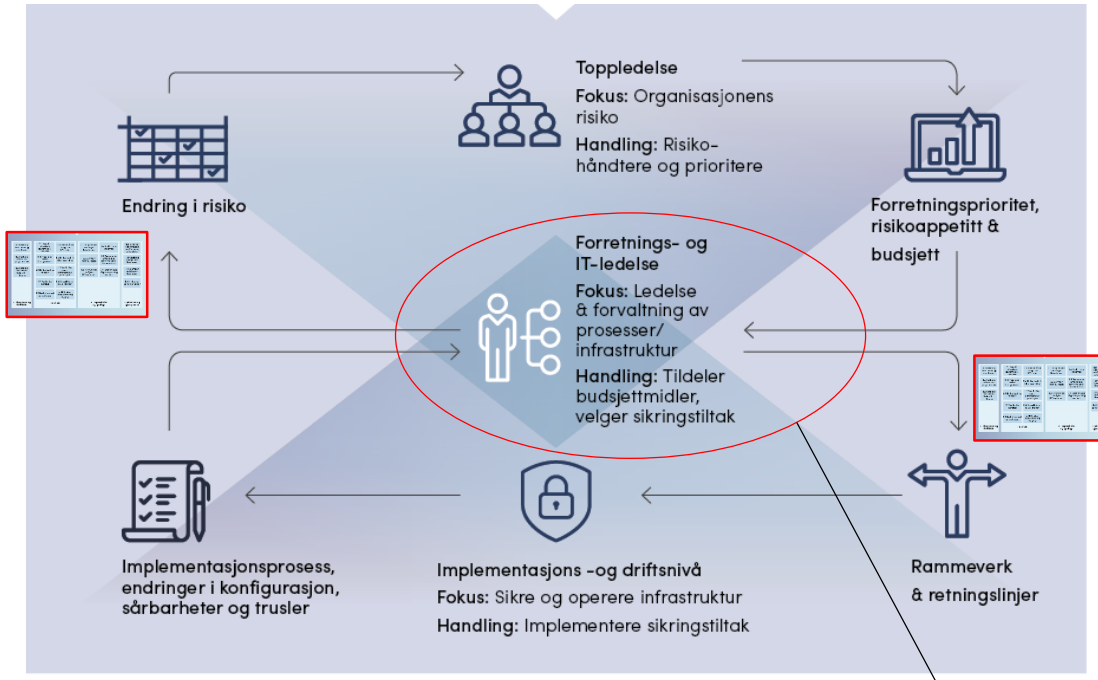

**Relevante standarder og rammeverk**

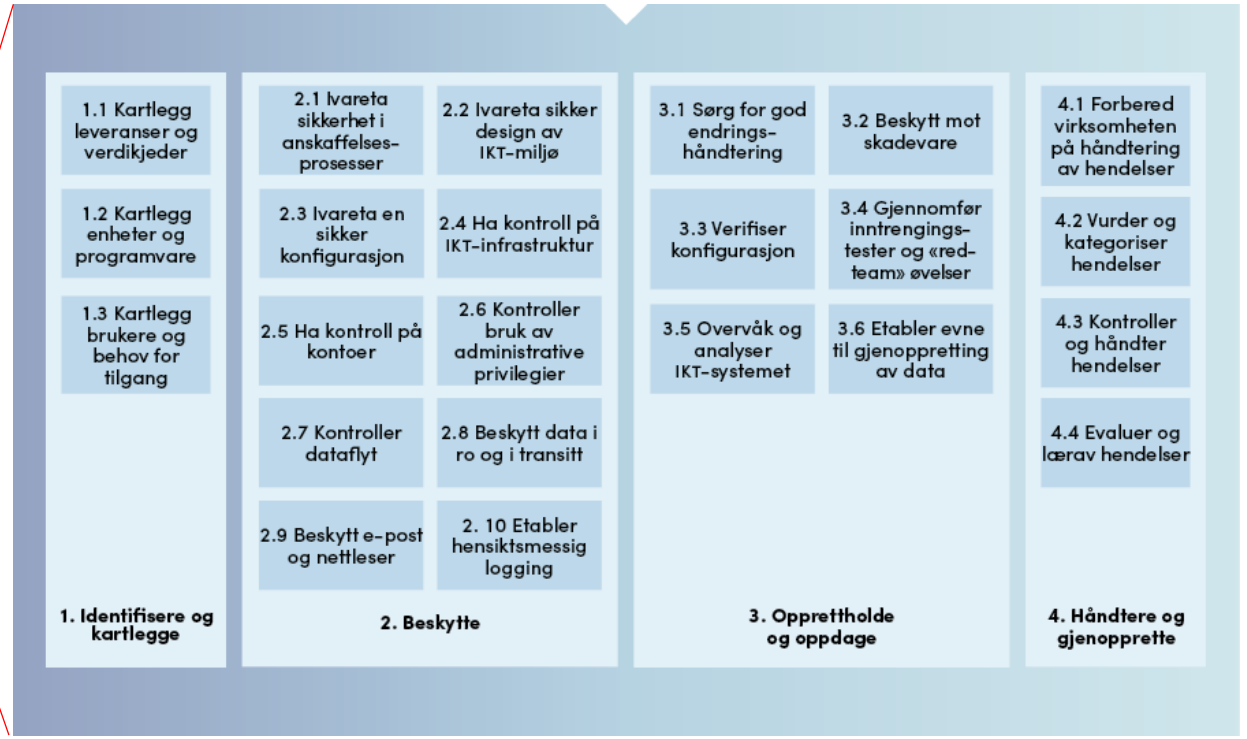
- ISO 27002
- NIST CSF
- CIS CSC 20
- BSI Grundschutz
- Cyber Essentials
- Sikkerhetsloven
- ++

**Innspill og justeringer**

- Sektormyndigheter og myndighetsorganer
- Offentlige og private virksomheter

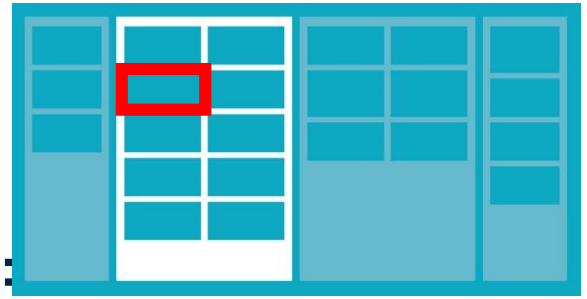
# Litt oppfriskning – hva er Grunnprinsippene?




Hovedmålgruppe

# Oppbygning av hvert Grunnprinsipp

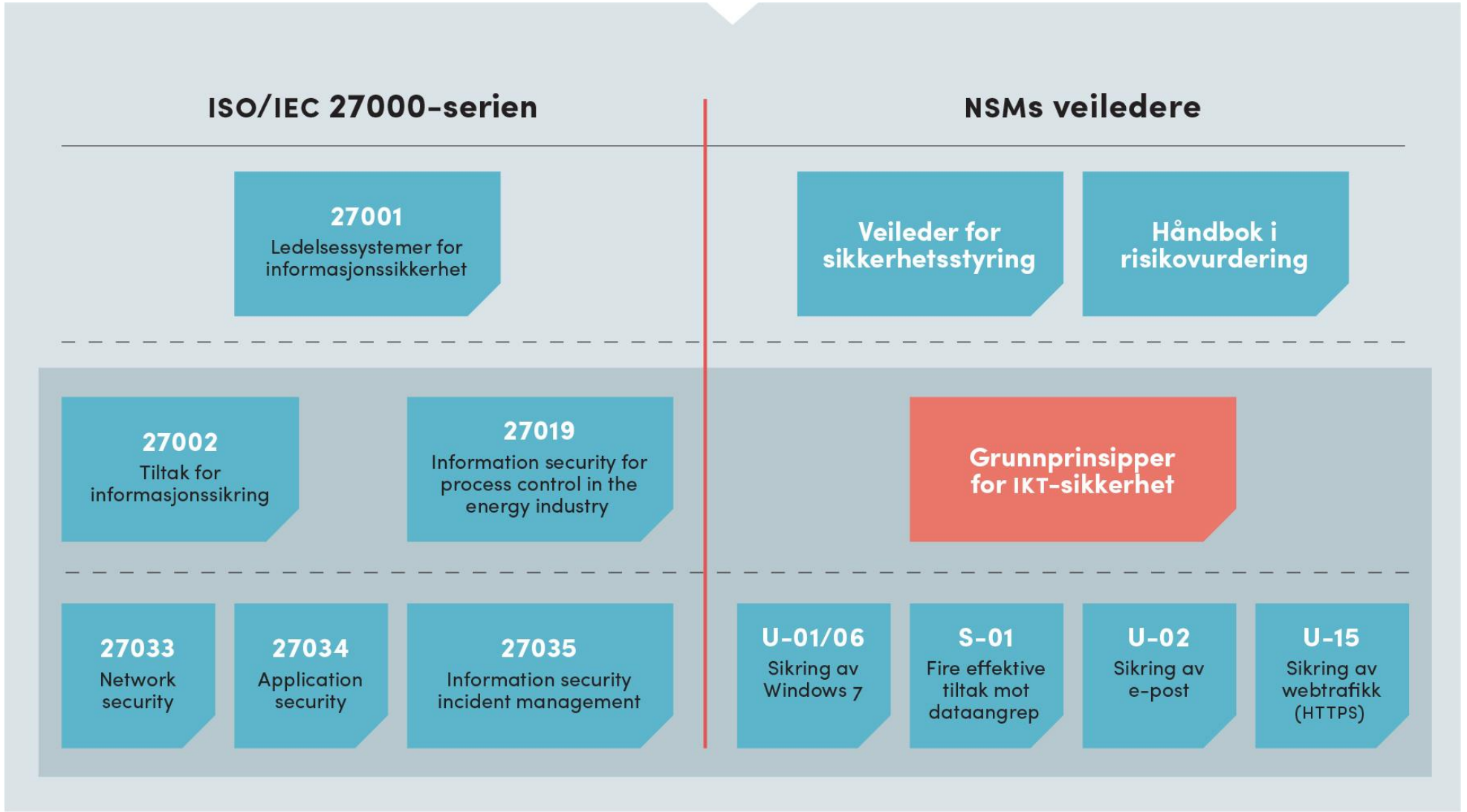


## 2.3 IVARETA EN SIKKER KONFIGURASJON

- **Hensikt:** Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet.
- **Begrunnelse(Hvorfor?)**
  - De fleste systemkomponenter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler…….

**Anbefalte tiltak:**

| ID | BESKRIVELSE |
|---|---|
| 2.3.1 | Installer og konfigurer systemet med kun nødvendi forretningsprosesser. Kun autorisert programvare b AppLocker for å kontrollere at sluttbrukere kun får l utenfor godkjente mapper og på flyttbare media, f |
| 2.3.2 | Etabler standard sikkerhetskonfigurasjoner for ope virksomhetens enheter. Konfigurasjonen bør gjenn være oppdatert i forhold til de nyeste sårbarheter autoriserte brukere. Planlagte endringer bør følge |
| 2.3.3 | Den sikre konfigurasjonen bør anses som en verdi sjekkes jevnlig og automatisk. Endringer i kompone og som ikke har rot i en logget eller sentralstyrt enc analyse. |
| 2.3.4 | Utfør all installasjon og fjernadministrasjon av utst |
| 2.3.5 | Endre alle standardpassord på systemer før produl rutere, brannmurer og aksesspunkter. |


ISO/IEC 27000-serien
NSMs veiledere
27001
Ledelsessystemer for informasjonssikkerhet
Veileder for sikkerhetsstyring
Håndbok i risikovurdering
27002
Tiltak for informasjonssikring
27019
Information security for process control in the energy industry
Grunnprinsipper for IKT-sikkerhet
27033
Network security
27034
Application security
27035
Information security incident management
U-01/06
Sikring av Windows 7
S-01
Fire effektive tiltak mot dataangrep
U-02
Sikring av e-post
U-15
Sikring av webtrafikk (HTTPS)


Råd for systemteknisk sikkerhet
nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/
NASJONAL SIKKERHETSMYNDIGHET
AKTUELT
BLOGG
PUBLIKASJONER
SKJEMAER
KURS
SIKKERHETSKON
NASJONAL SIKKERHETSMYNDIGHET → PUBLIKASJONER → SIKKERHETSLOVEN, FORSKRIFTER OG VEILEDNINGER → VEILEDERE, HÅNDBØKER OG RÅD → RÅD FOR SYSTEMTEKNISK SIKKERHET
Råd for systemteknisk sikkerhet
Publisert: 18.06.2014 | Sist endret: 20.11.2019
NSMs tekniske råd og anbefalinger tar for seg forskjellige typer sikringav IT-systemer: servere, klienter, nettverk, krypto, mm.

# Nasjonalt cybersikkerhetssenter (NCSC)

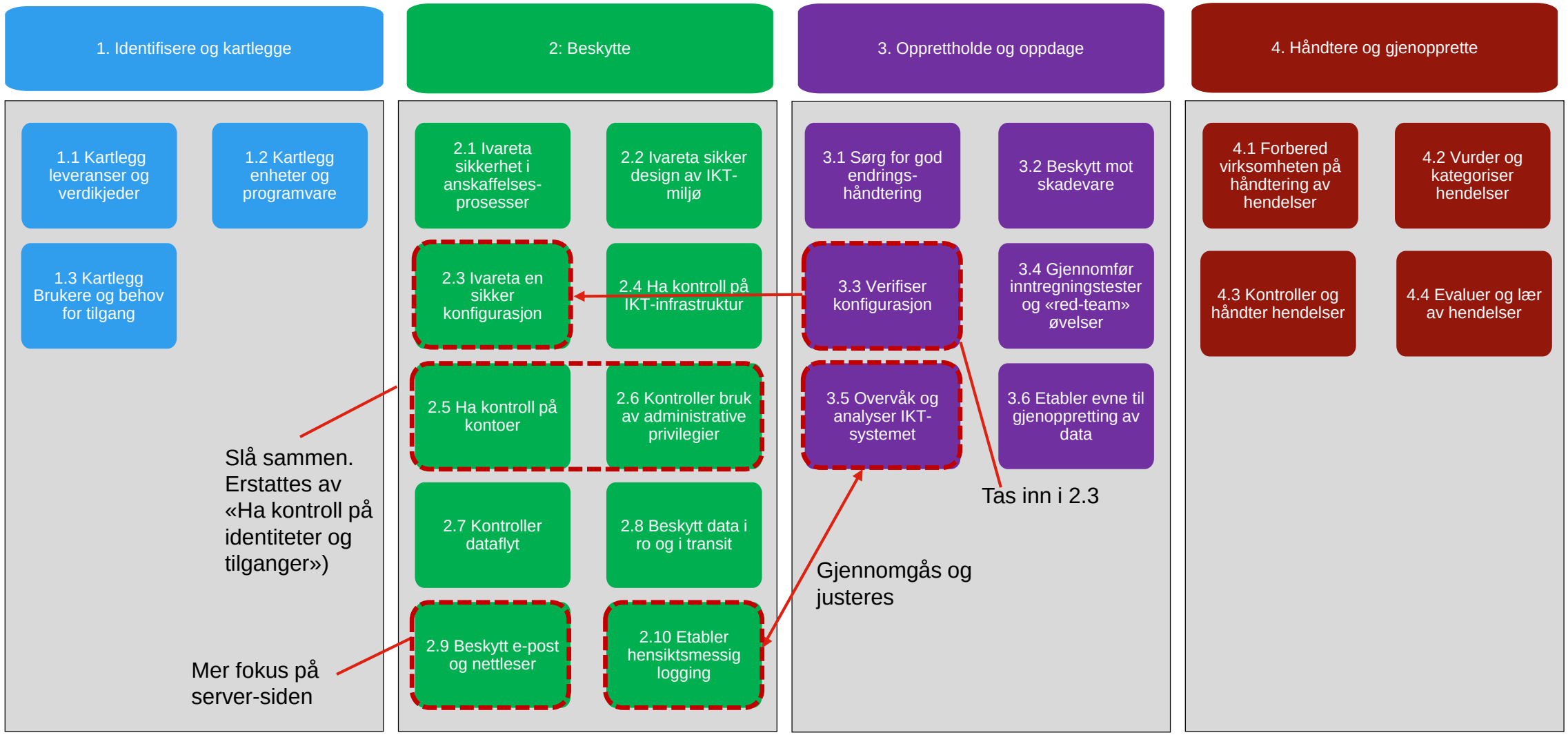
# Tiltak – anbefalinger - rådgiving





https://www.nsm.stat.no/NCSC/NCSS-Radgivning/

# Endringer 1.1->2.0



# Forslag versjon 2.0 - revidert

# Utsnitt fra versjon 2.0 (utkast)

## 2.4 Beskytt virksomhetens nettverk

*Hensikten med prinsippet:* Virksomheten kontrollerer og beskytter nettverkene sine mot interne og eksterne trusler.

### Hvorfor er dette viktig?

Virksomhetens eget nettverk strekker seg ofte ut over kontorlokalet og gjør det utfordrende å definere den fysiske utbredelsen. En virksomhet kan ha flere geografiske lokasjoner, og tjenester kan være satt ut til leverandører.

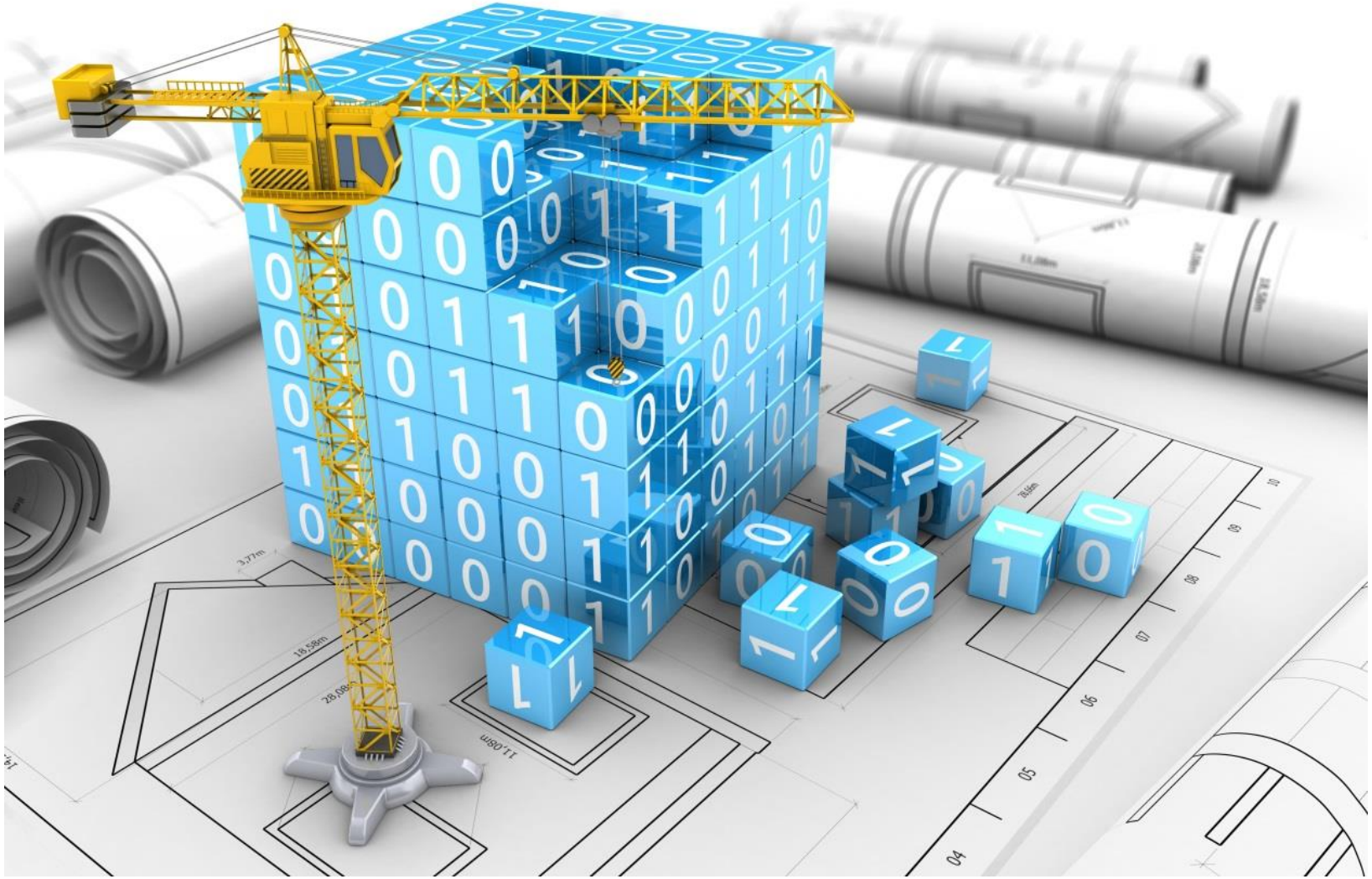
Tilkobling av virksomhetens nettverk til Internett eller andre nettverk utenfor virksomhetens kontroll eksponerer systemene for nye angrepsflater.

*Enheter og datatrafikk kan også angripes fra innsiden*: en kompromittert server eller klient (både virksomhetsstyrt, innleid eller privat), en utro tjener, en (kompromittert) leverandører med tilgang til nettverket, svakt sikret trådløse nett eller manglende fysisk sikring av porter/kabler.

### Anbefalte tiltak: beskytt virksomhetens nettverk

| ID | Beskrivelse |
|---|---|
| 2.4.1 | **Etabler tilgangskontroll på flest mulige nettverksforbindelser.** Ha kontroll på tilgangen til alle nettverksporter. Dette gjelder porter på svitsjer, på servere og for (grupper av) klienter. Nettverkstrafikk bør kun tillates på virksomhetsgodkjente porter (hviteliste-prinsipp). |
| 2.4.2 | **Krypter alle trådløse og kablede forbindelser. a)** Krypter alle trådløse forbindelser. Bruk tidsriktige protokoller som WPA2/WPA3 i «enterprise-modus». **b)** Krypter alle kablede forbindelser i egne nettverk, som minimum de som ikke er fysisk kontrollert av virksomheten. |
| 2.4.3 | **Kartlegg fysisk tilgjengelighet for svitsjer og kabler.** Virksomheter har ofte manglende oversikt over hvor egne kabler går og om uvedkommende har adgang. Hvis man ikke autentiserer og krypterer alle linker, bør man kartlegge beliggenhet til kablede nettverk med tanke på om uvedkommende har fysisk adgang (mellom egne bygninger, mellom etasjer i bygning delt med andre virksomheter, mellom forskjellige geografiske lokasjoner, resepsjoner, mm.). *TBD. Muligens bedre å ha i Kapittel 1. I så fall en referanse herfra.* |
| 2.4.4 | **Aktiver brannmur på alle klienter og servere.** Brannmurer er som regel innbygget i operativsystemer og kan brukes til trafikkstyring eller logging. Benytt brannmurer til å **a)** regulere innkommende/utgående trafikk. **b)** Logge sikkerhetsrelevante hendelser. Inspiser loggfilene regelmessig. **c)** Integrer klient/server-logging med sentralisert virksomhets-logging. *TBD. Flyttes kanskje til Kapittel 2.3 (konfigurasjon) eller 2.9 (logging).* |

# Vil du være med å bygge NSMs grunnprinsipper?



***«Seier venter den, som har alt i orden – hell kaller man det.***

***Nederlag er en absolutt følge for den, som har forsømt at ta de nødvendige forholdsregler i tide – uhell kalles det.»***

*Roald Amundsen*

*«Den norske sydpolsfærd med Fram 1910 – 1912»*

*Takk for oppmerksomheten!*

*www.nsm.stat.no/grunnprinsipper-ikt*

*grunnprinsipper@nsm.no*