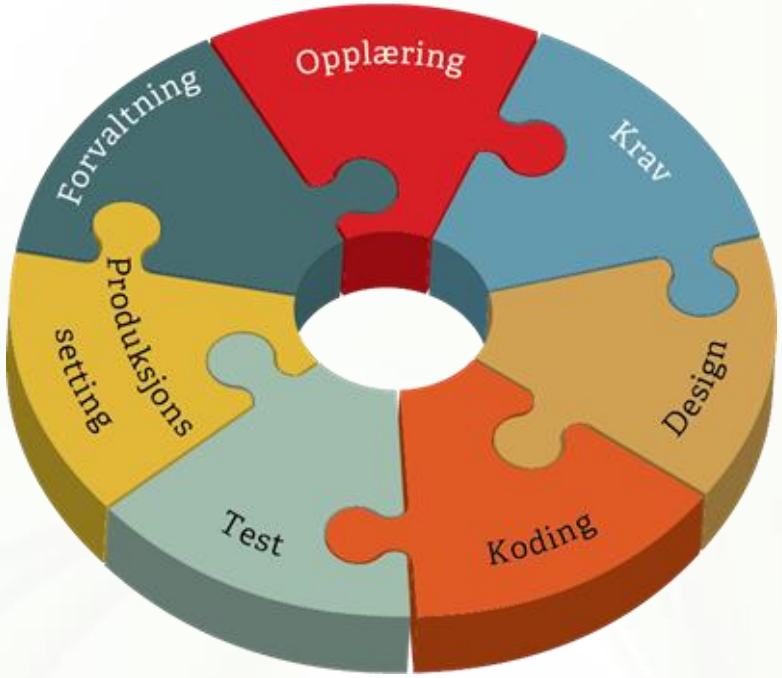
Informasjonssikkerhet i den norske geodatainfrastrukturen

Knut Sælid, Teknologiforum 2018

Innhold

- Hvordan informasjonssikkerhet kan bygges inn i systemer på en systematisk måte
  - Hensynet til ISO 27001
  - Hensynet til GDPR og kravet om innebygget personvern
- Karttjenester og applikasjonssikkerhet
- Skytjenester i et sikkerhetsperspektiv



Informasjonssikkerhet

- Verdivurderinger/generelle sikkerhetsvurderinger
- Informasjonssikring
- Applikasjonssikkerhet
- Ingen quick fix, men noen best practices.

Kartverket

Informasjonssikring

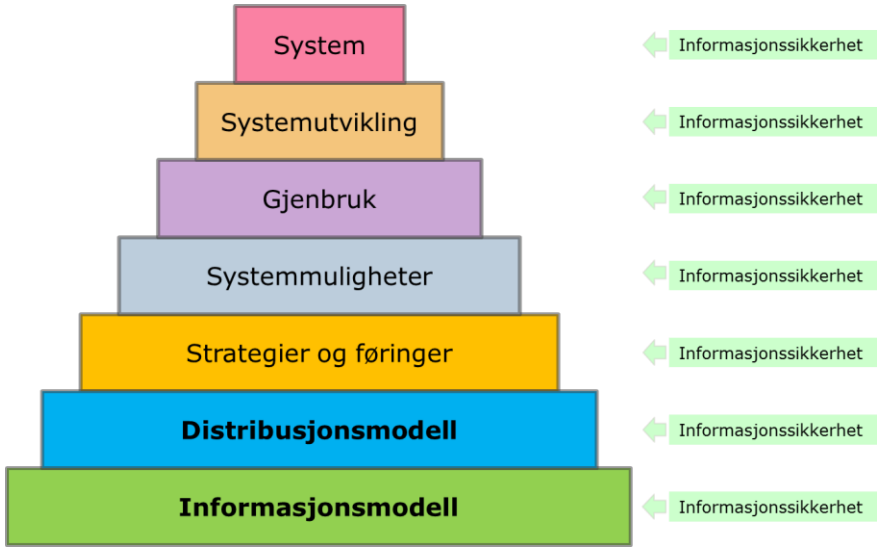
Informasjonssikring handler om **KITA**, dvs å sikre at informasjonen

- **ikke blir kjent for uvedkommende** (konfidensialitet) – *misbruk*
- **ikke blir endret utilsiktet eller av uvedkommende** (integritet) – *misbruk*
- **er tilgjengelig ved behov** (tilgjengelighet) – *bruk*
- **kommer fra en kjent og pålitelig kilde** (autensitet) - *misbruk*

Ofte mest fokus på tredje punkt, og da i form av funksjonelle systemkrav
Hvordan forvalte og distribuere informasjon (data) slik at vi ivaretar alle fire punktene?

Informasjonssikring

- Først informasjonssikring – sikkerhetsanalyse
- Deretter funksjonell analyse



Kartverket

Informasjonssikring

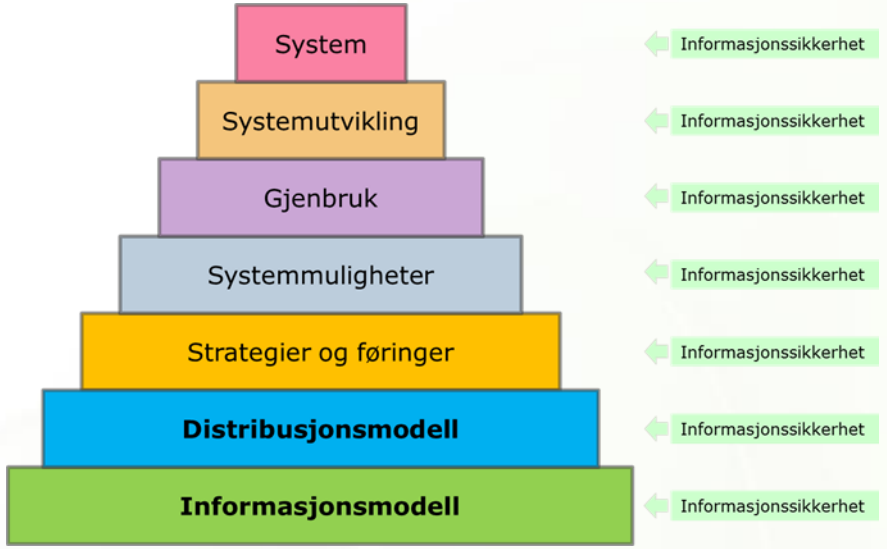
Systematisere praktisk arbeid med informasjonssikring:

Informasjonsmodell

- datamodell
- informasjonssikkerhetsanalyse
- informasjonssikkerhetskrav

Distribusjonsmodell

- dataflytmodell



Ofte en utfordring at informasjonsmodellen og distribusjonsmodellen er knyttet tett sammen med de andre trinnene i pyramiden i et samlet forvaltningssystem (monolittisk).

Informasjonsmodell - informasjonssikkerhetsanalyse

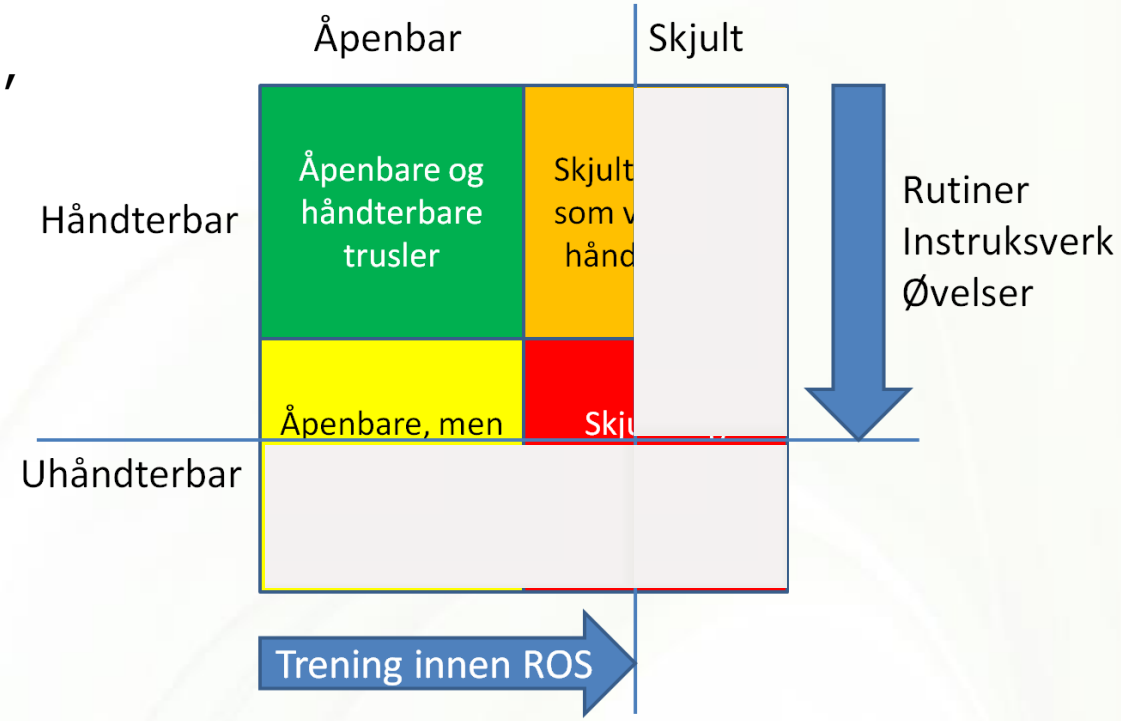
SRT:

- **S**årbarhetsanalyse (våre bevisste eller ubeviste svakheter iht KITA)
- **R**isikoanalyse (skadepotensialet for våre sårbarheter)
- **T**russelanalyse (aktive krefter som jobber mot KITA)

Ofte blir alt håndtert samlet i en ROS-analyse, men det fanger sjelden truslene (aktive)

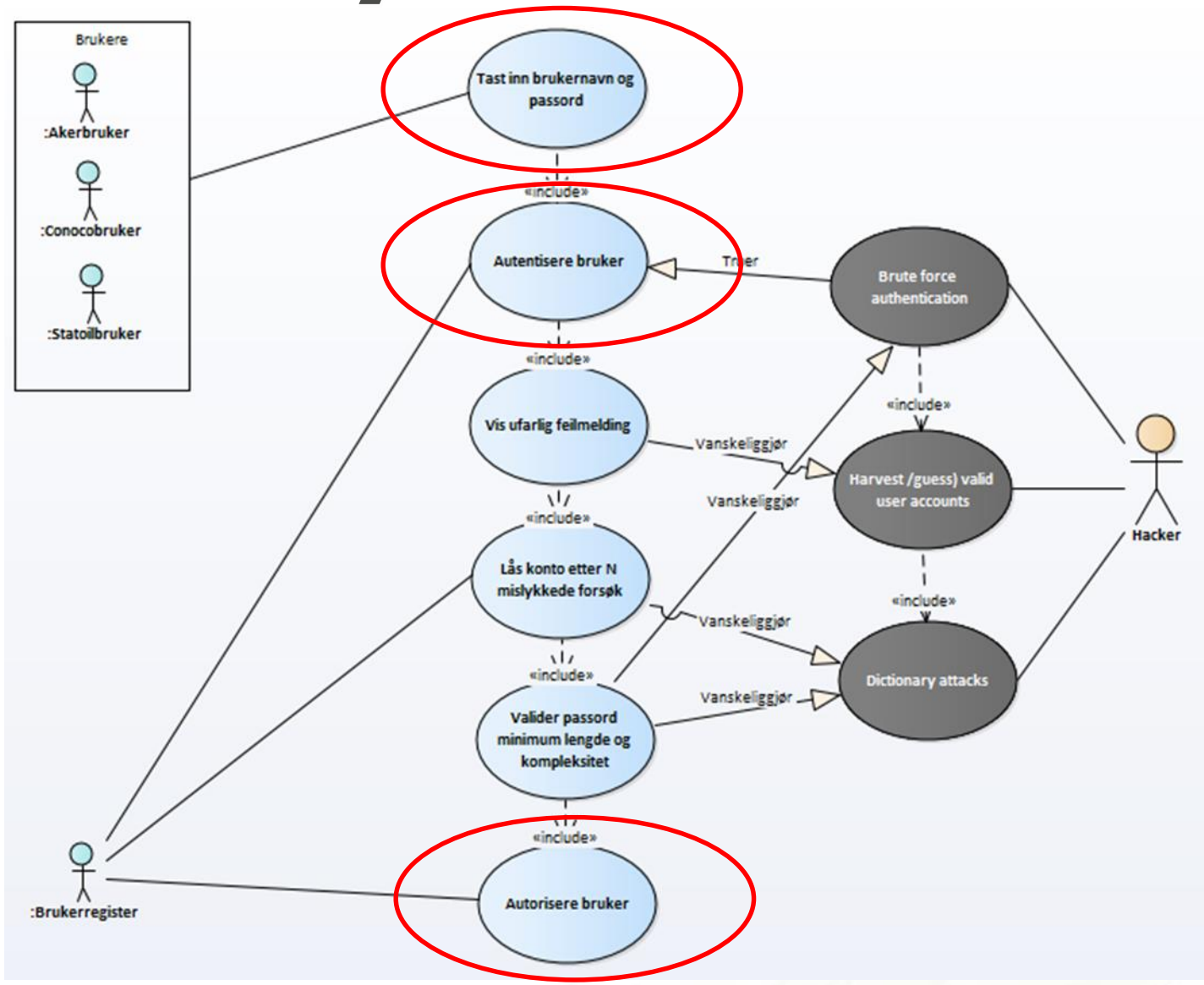
SRT skal redusere faren for brudd på KITA

Resulterer i informasjonssikkerhetskrav



Kartverket

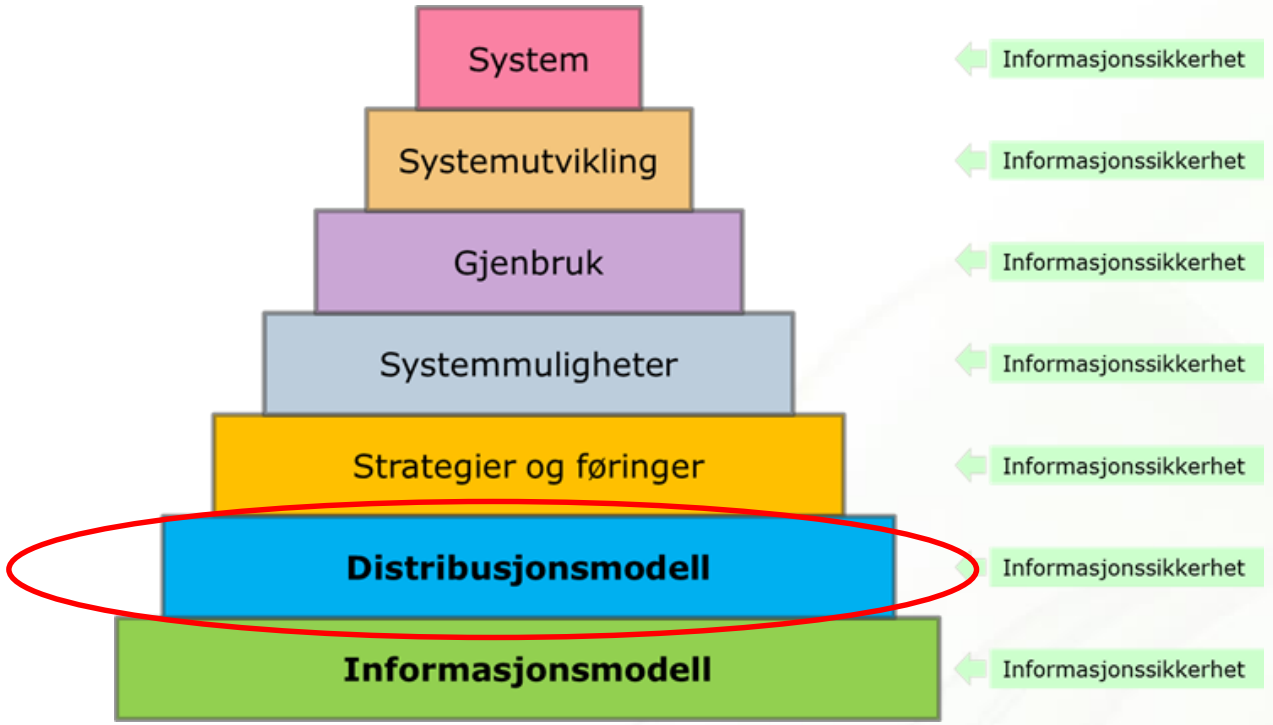
Trusselanalyse - bruk vs. misbruk



Kartverket

Distribusjonsmodell

- Hvordan og hvor kan lagring, forvaltning og distribusjon av dataene skje for å ivareta informasjonssikkerhetskravene?
- Baseres på informasjonsmodellen og sikkerhetskravene



Kartverket

Applikasjonssikkerhet

Modenhetsmålinger

Sikre arbeidsprosessene - SSDLC

Documentation Systems

Source Code Repository

Platforms

Development

Code Review

Architecture Review

Automated Deployment

Test environment

Prod environment

Task Management Systems

IDE Quality Control

Security Requirements & Principles

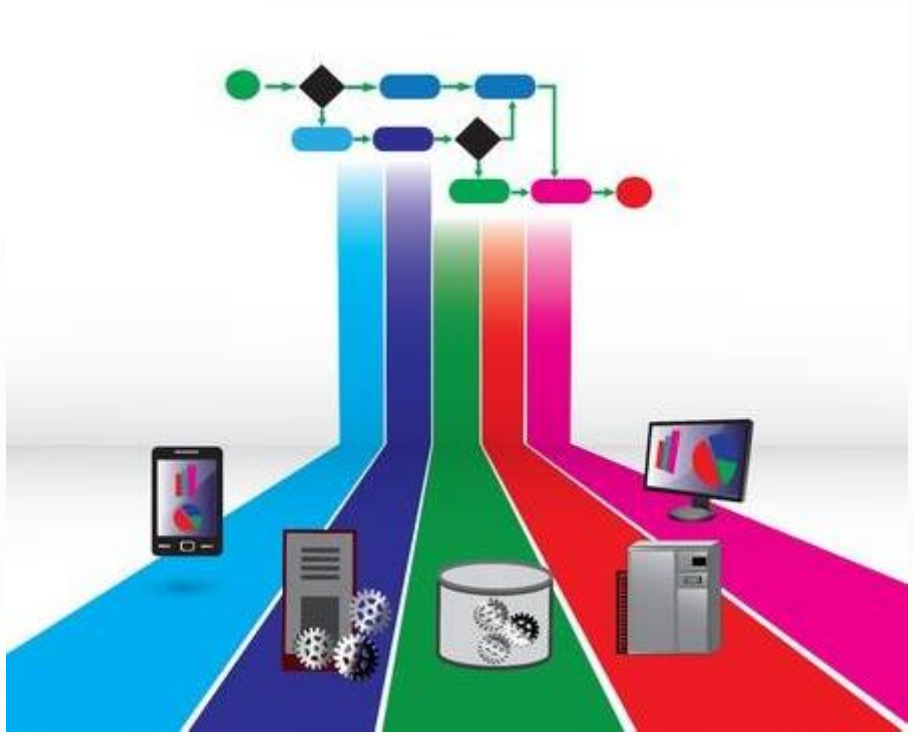
Secure Architecture Patterns & Policies

Automated Security Testing

Kartverket

Felles for tjenester

- Datastrømmen fra en server ut til omverdenen
- Maskingrensesnitt
- Ingen kontroll på manuelle brukerflater (GUI)
- Ingen kontroll på dataene etter de har forlatt vår server
- Må ivareta KITA og dermed informasjonssikkerhetskravene i hele informasjonskjeden og livssyklusen



Skytjenester

- Skytjenester kan være både sikre og usikre
- Hva er en skytjeneste?
  - Egne data hos en fremmed tjenestetilbyder?
  - Egne data i en egen tjeneste?
  - Programvare som kjører i skyen?

- I følge datatilsynet:
  - *«Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.»*
  - *Se https://www.datatilsynet.no/regelverk-og-skjema/veiledere/skytjenester---cloud-computing/hva-er-nettskytjenester/*

Skytjenester

Hva må virksomheten din gjøre før du kan ta i bruk skytjenester?

Gjennomfør en risiko- og sårbarhetsanalyse

- Kartlegg alle systemer i virksomheten som inneholder/behandler informasjon.
- Gradèr deretter informasjonen iht regelverk og forpliktelser.
- Evaluèr hva som kan gå galt for hvert graderingsnivå.
- Vurder hvilke følger det kan få om noe går galt, for eksempel at personopplysninger eller skjermet informasjon kommer på avveie.
- Lag en oversikt over hvilke sikkerhetstiltak som er iverksatt for å håndtere eventuelle hendelser.
- Vurder sikkerhetstiltakene i forhold til de systemene dere benytter til informasjonsbehandling og distribusjon.
- Tilfredsstiller skytjenester kravene som følger av risikovurderingen?

Skytjenester

Se mer på
https://www.datatilsynet.no/regelverk-og-skjema/veiledere/skytjenester---cloud-computing/?id=2196

Spørsmål?

Kartverket