



Nasjonal sikkerhetsmyndighet

IKT-sikkerhet som suksessfaktor

- med fokus på teknologi og kultur

Jan Tobiassen

Strategi og policy

Nasjonal sikkerhetsmyndighet



Agenda

- Nasjonal sikkerhetsmyndighet
- KIS og Nasjonal strategi for IT-sikkerhet
- Menneske – Teknologi - Organisasjon
- Hvordan jobbe med informasjonssikkerhet?
- Suksesskriterium for å lykkes

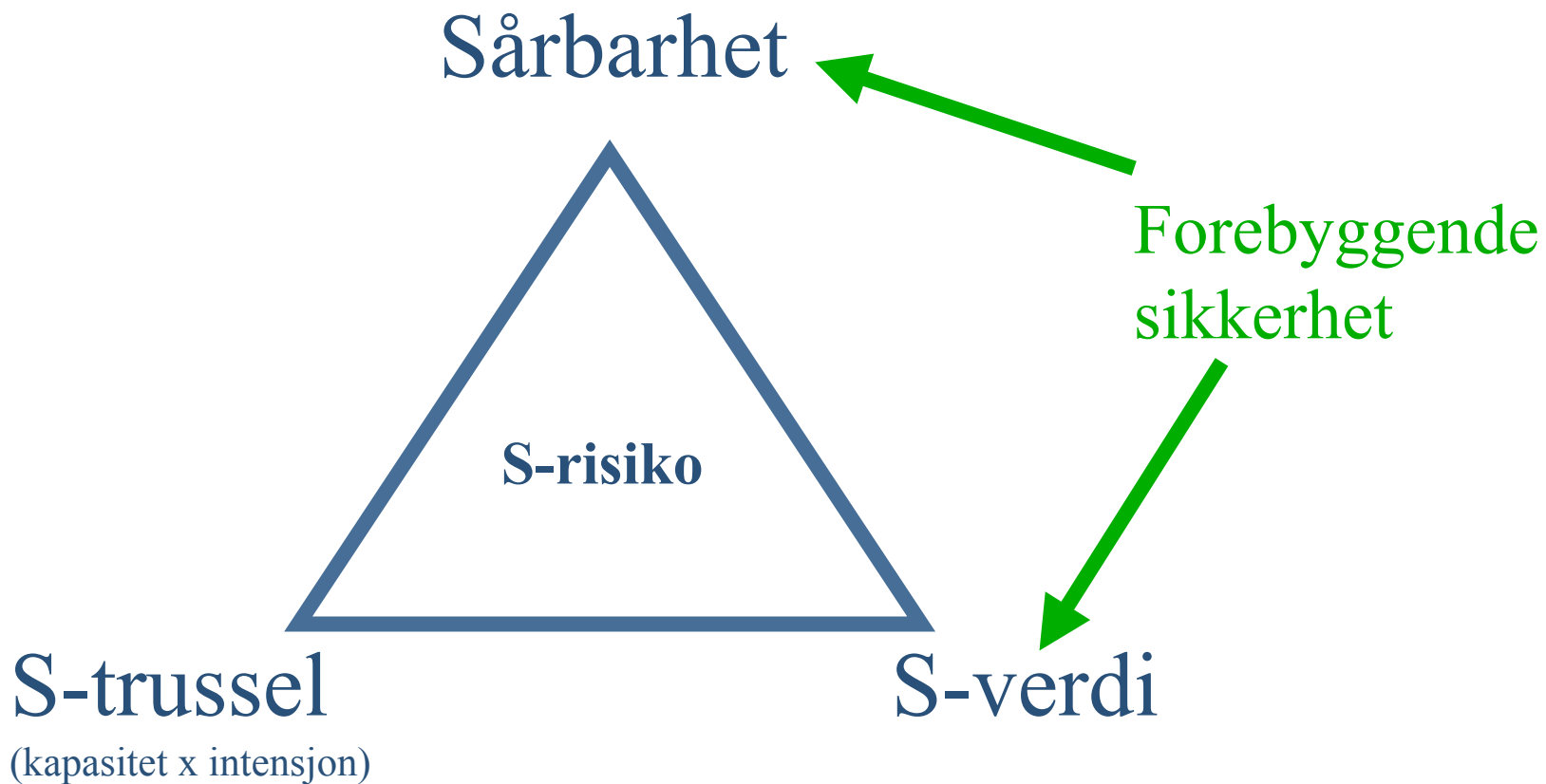


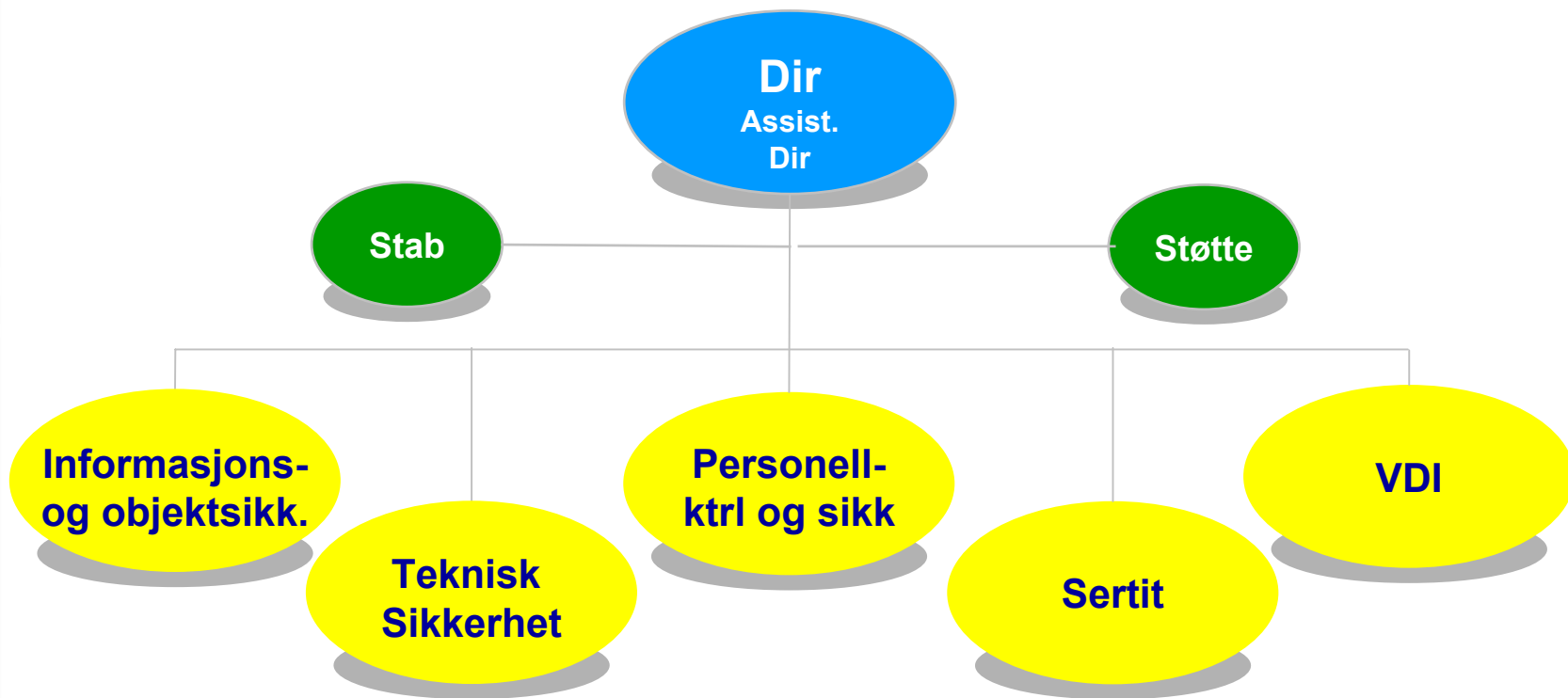
Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet



Sikkerhetsrisiko







Fagområder innen forebyggende sikkerhetstjeneste

	Sikkerhets- administrasjon	
Gradering/ klassifisering	Fysisk sikkerhet	Monitoring
Dokument- sikkerhet	Informasjon eller objekt	Krypto
Informasjons- systemsikkerhet		Industrisikkerhet
Personell- sikkerhet	TSU	Tempest



Oppgaver

- Utøve de oppgaver som påhviler NSM i medhold av sikkerhetsloven
- Utøve andre sikkerhetsoppgaver i sivil og militær sektor etter pålegg fra Justis- eller Forsvarsdepartementet
- Holde Justis- og Forsvarsdepartementet orientert om den sikkerhetsmessige tilstand i henholdsvis sivil og militær sektor



Nasjonal sikkerhetsmyndighet

Koordineringsutvalg for informasjonssikkerhet (KIS)



IKT-sikkerhet: Hvem gjør hva ?

FD



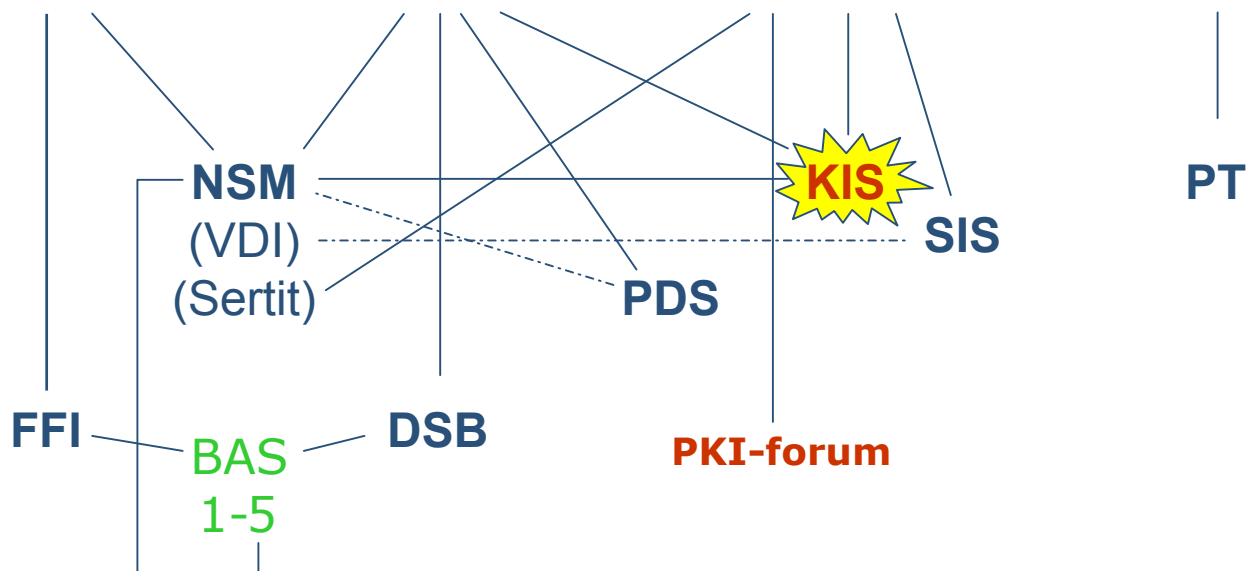
JD



NHD

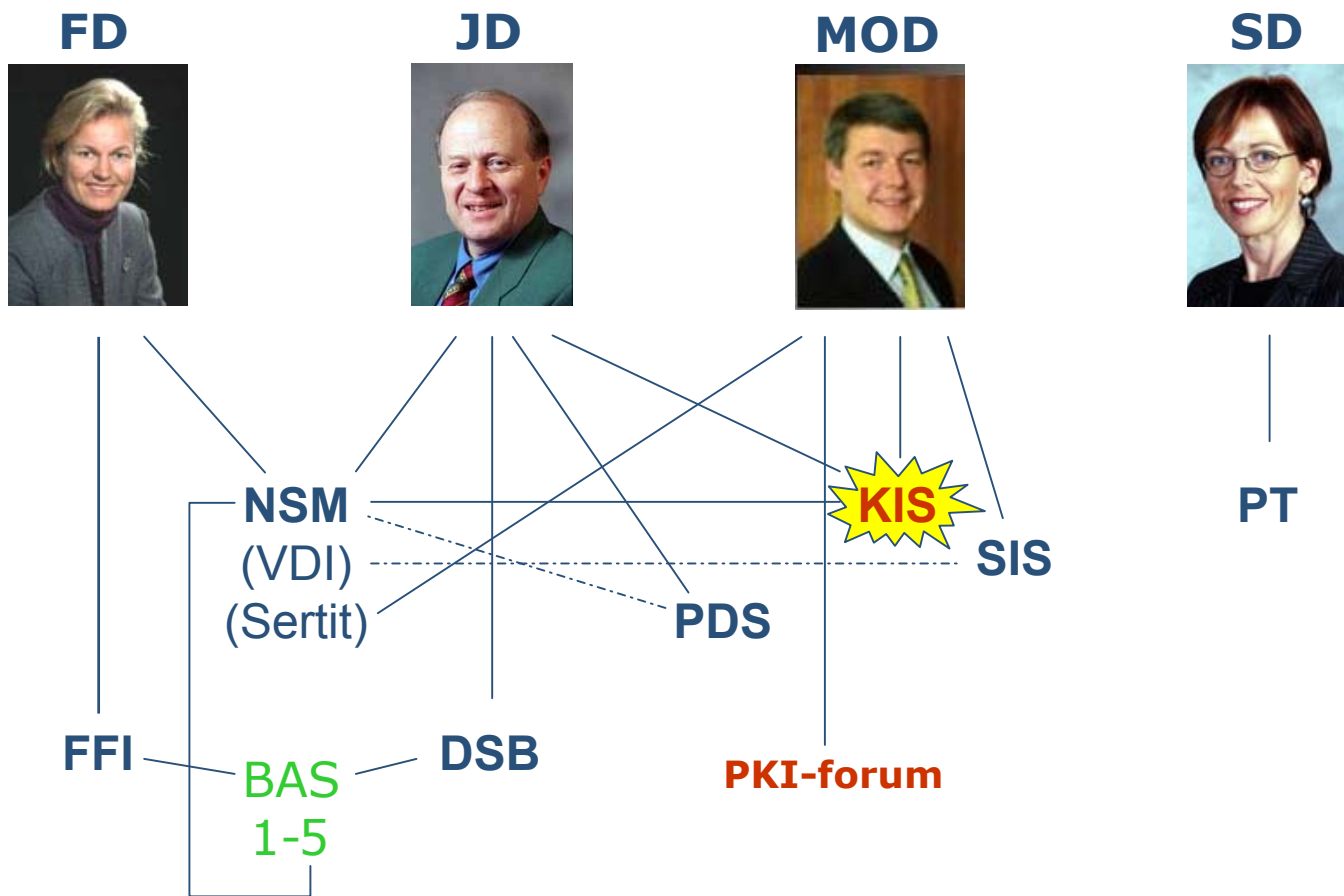


SD





IKT-sikkerhet: Hvem gjør hva ?





KIS

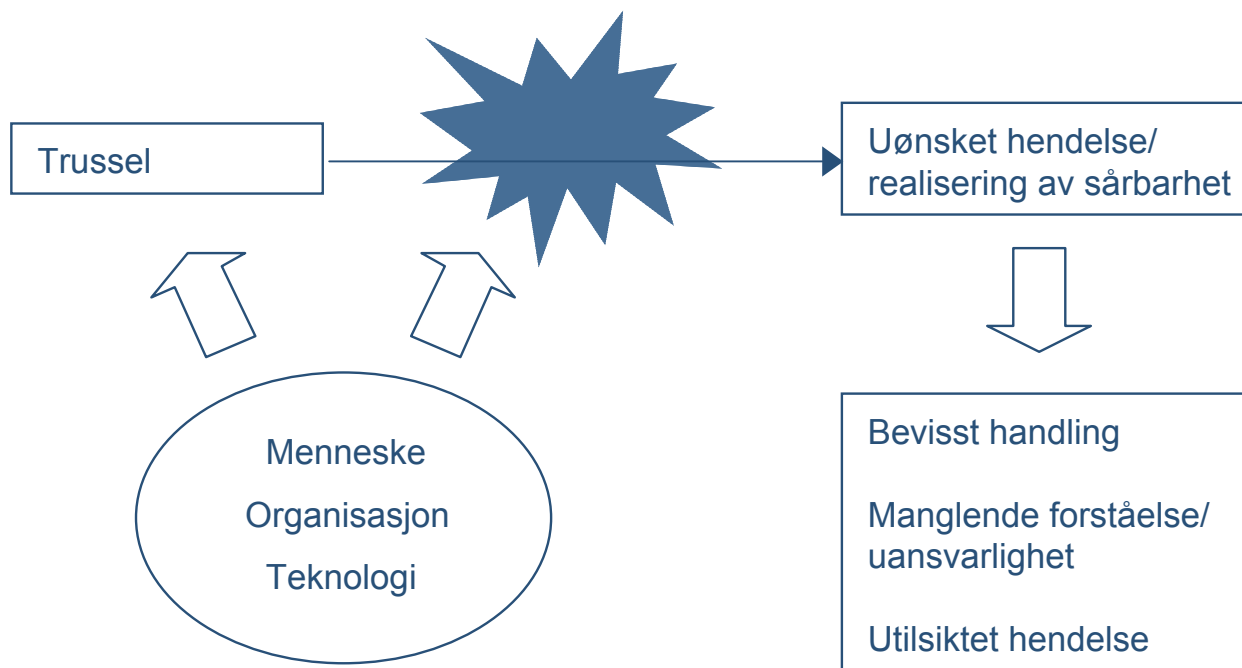
- Koordineringsutvalg for informasjonssikkerhet
- Leder fra MOD, nestleder fra JD, sekretariatet i NSM
- Nasjonal strategi for informasjonssikkerhet:
"Det skal bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling i Norge. IT-sikkerhet skal være en sentral faktor ved forbrukernes og norske virksomheters bruk av IT"



Menneske – Teknologi – Organisasjon



Grunnleggende sammenheng





Trussel og sårbarhet

- Uærlige tilsiktede handlinger
- Manglende forståelse, uansvarlighet
- Utilsiktede, tilfeldige hendelser



Mørketallsundersøkelsen 2003 (I)

60 % av norske virksomheter har vært utsatt for uønskede hendelser i 2003

**Virus-
infeksjoner**

**Tyveri
av
IT-
utstyr**

**Misbruk
av
IT-
ressurse**



Mørketallsundersøkelsen 2003 (II)

- Følger av datakriminalitet
 - **5 milliarder** kroner i samlede tap
 - 70 % av virksomhetene fikk ekstra arbeid
 - 38 % foretok en gjennomgang av sikkerheten etter hendelsen
 - 5 % opplevde tap av forretning
 - 2 % opplevde tap av omdømme

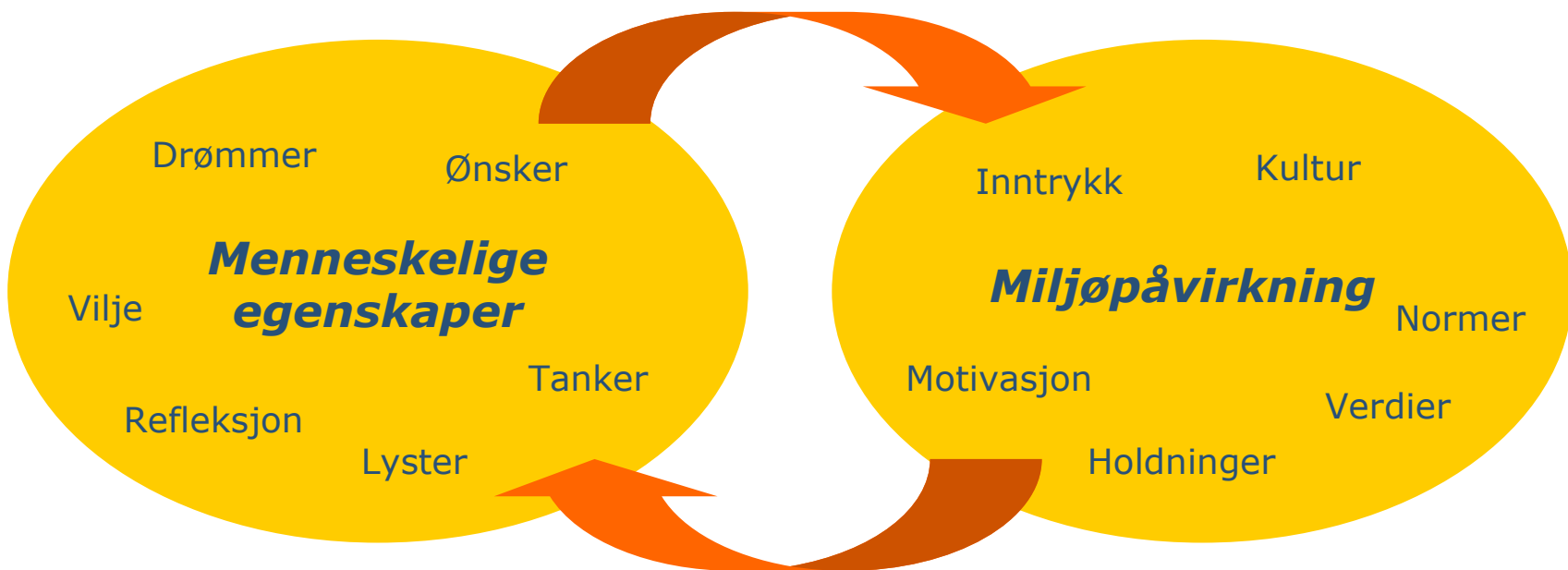


Insider sikkerhetsbrudd

Insider Security Breaches	%
Installation/use of unauthorized software	78 %
Use of company computing resources for illegal or illicit communications or activities (porn surfing, email harassment)	60 %
Use of company computing resources for personal profit (gambling, spam, managing personal e-commerce site, online investing)	60 %
Abuse of computer access controls	56 %
Physical theft, sabotage or intentional destruction of computing equipment	49 %
Installation/use of unauthorized hardware/peripherals	47 %
Electronic theft, sabotage or intentional destruction/disclosure of proprietary data or information	22 %
Fraud	9 %



Menneske - Miljø





Hvordan jobbe med IKT-sikkerhet?



Verktøykasse





Verktøykassen dekker...



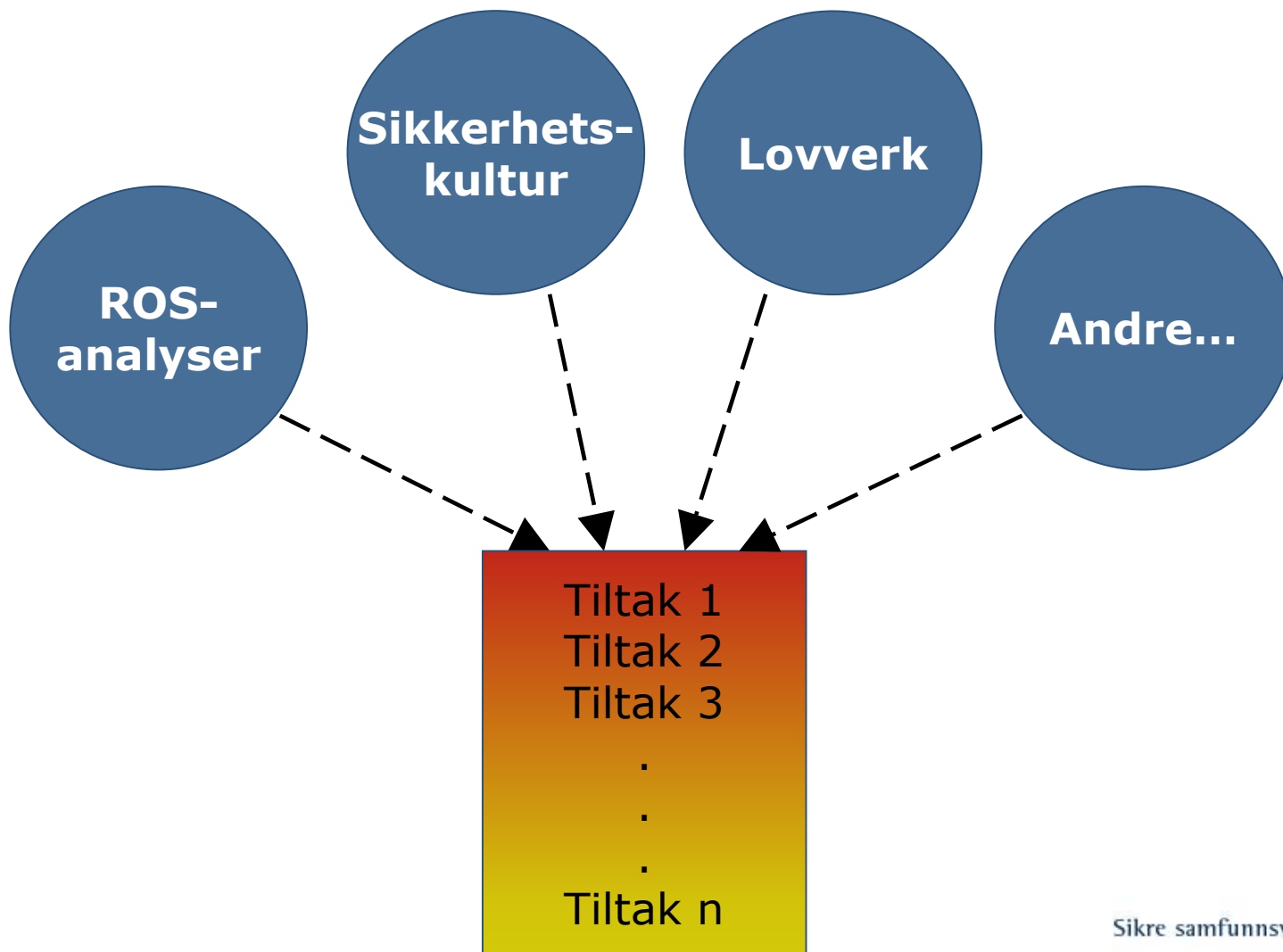


Kulturverktøy

- "Et undersøkelsesverktøy for kartlegging av holdninger og sikkerhetskultur"
- Presentert i rapporten "Informasjonssikkerhet og innsideproblematikk"
- Samarbeidsprosjekt mellom NTNU og NSM



Suksesskriterium for tiltak





Suksesskriterium for å lykkes



Bruk av verktøyet



*...benytter
verktøyene
til å...*



Identifiserer svakheter,
sårbarheter, utfordringer,
problemområder

*...for å
prioritere...*

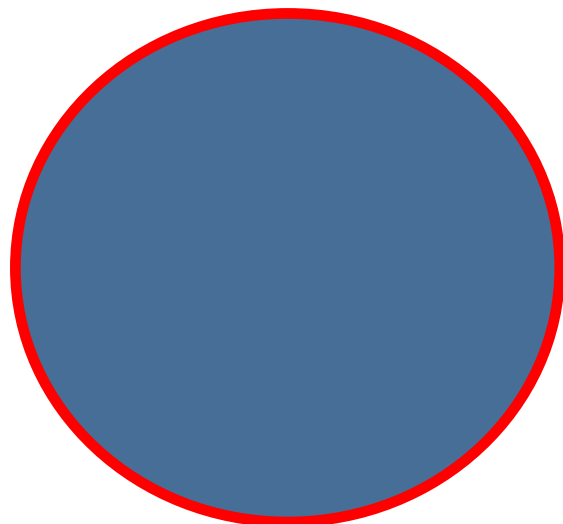


Tiltak 1

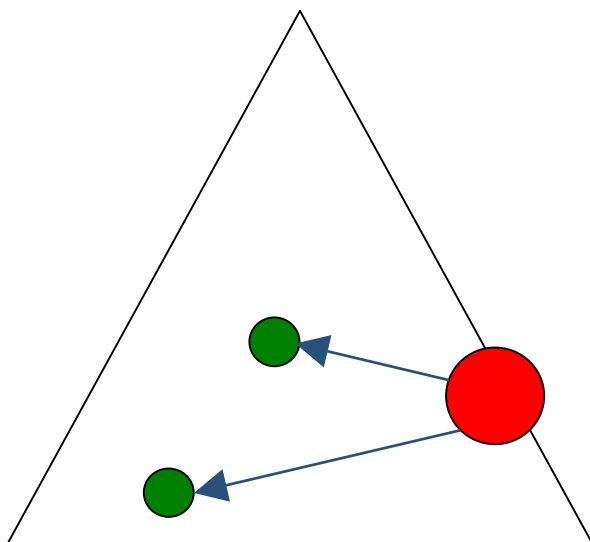
Tiltak 2

Tiltak 3

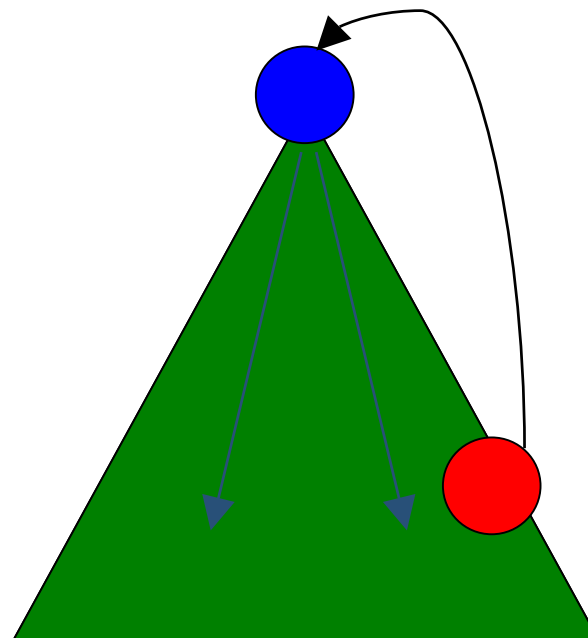
*...som
presenteres for...*



Virksomhetslederens ansvar



Sikkerhetsleder kan påvirke celler i virksomheten



Virksomhetsleder sitt fokus på sikkerhet vil forplante seg nedover i organisasjonen



Sikkerhet som et kvalitetsstempel

**Sikkerhet i
utvikling og
drift**

**Sikkerhet som
en del av
modernisering**



**Sikkerhet
som en
suksessfaktor**

**Sikkerhet som et
salgsargument**