

Helhetlig risikotilnærming – safety og security i en sammenheng

Jens Thomas Sagør
Proactima

PREPARED.

Hva skal jeg snakke om?

- Erfaring med security arbeid i praksis
- Helhetlig risikostyring
- "Verktøykassen" og metoder
- Kilder/Standarder innenfor security

Proactima



- Konsulentselskap etablert i september 2003
- I dag et fagmiljø med over 170 medarbeidere
- 100 prosent eid av de ansatte



Stavanger



Oslo



Bergen



Trondheim

Tjenesteområder



- Risikostyring
- Beredskap
- Samfunnssikkerhet
- Arbeidsmiljø
- Ytre Miljø
- Styringssystem
- Kultur og organisasjon
- Media og kommunikasjon
- Prosjektledelse

Rådgiving – Kurs – Verktøy



Kundegrupper - segmenter



Olje og gass



Kraft



Maritim



Samferdsel



Offentlig



Forskning og utvikling



Helse



Bank og forsikring



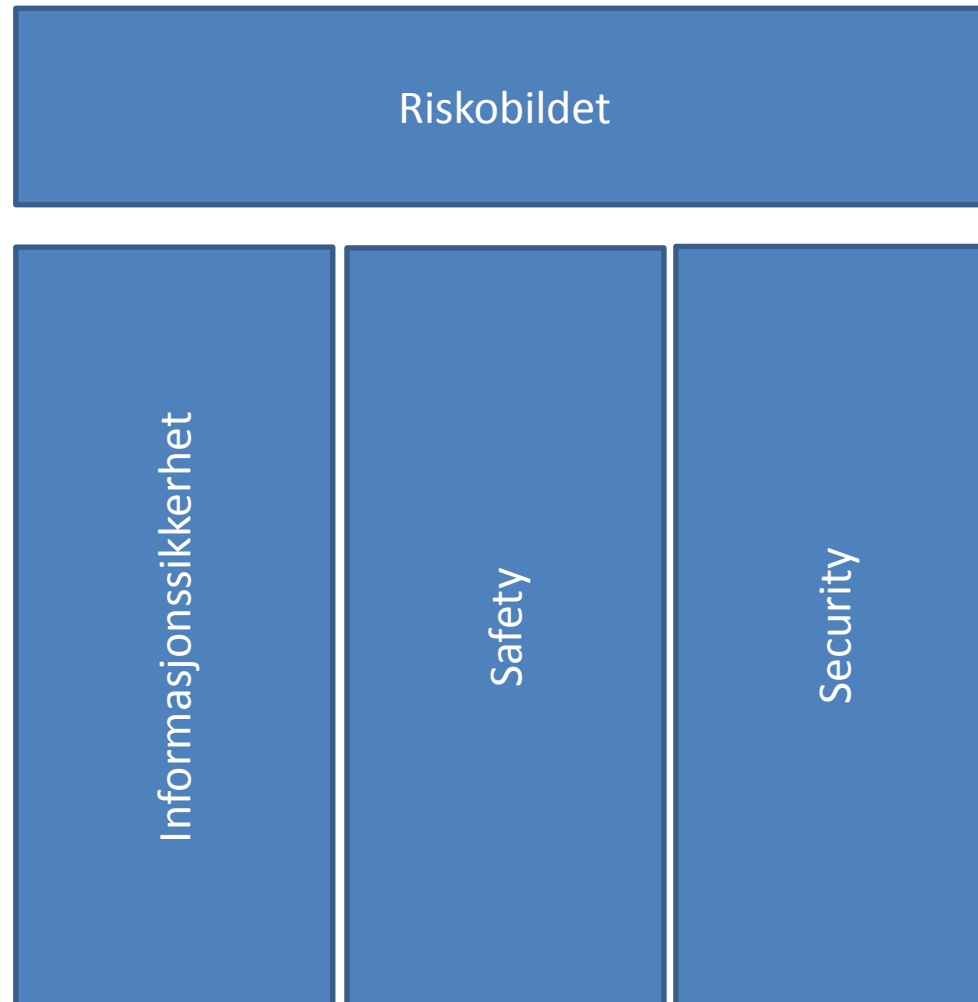
Andre bransjer

Definisjoner



- Security
Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging
(ref NOU 2000:24 "Et sårbart samfunn")
- Safety
Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter
(ref NOU 2000:24 "Et sårbart samfunn")

Tradisjonell tilnærming til sikkerhet



Betraktninger rundt Security

- Sikkerhetsarbeidet er fragmentert
 - Ulike fagmiljøer jobber parallelt med sikkerhet
- Security har ofte vært ivaretatt av 3. part
 - Lite forankret i organisasjoner og en regulatorisk tilnærming
 - Ikke forankret i et felles og erkjent risikobilde – fører til sårbarhet og manglende evne til tilpasning
 - Uten en helhetlig tilnærming vil godheten av barrierer bli redusert

Profil på tiltak = nye konsekvenser

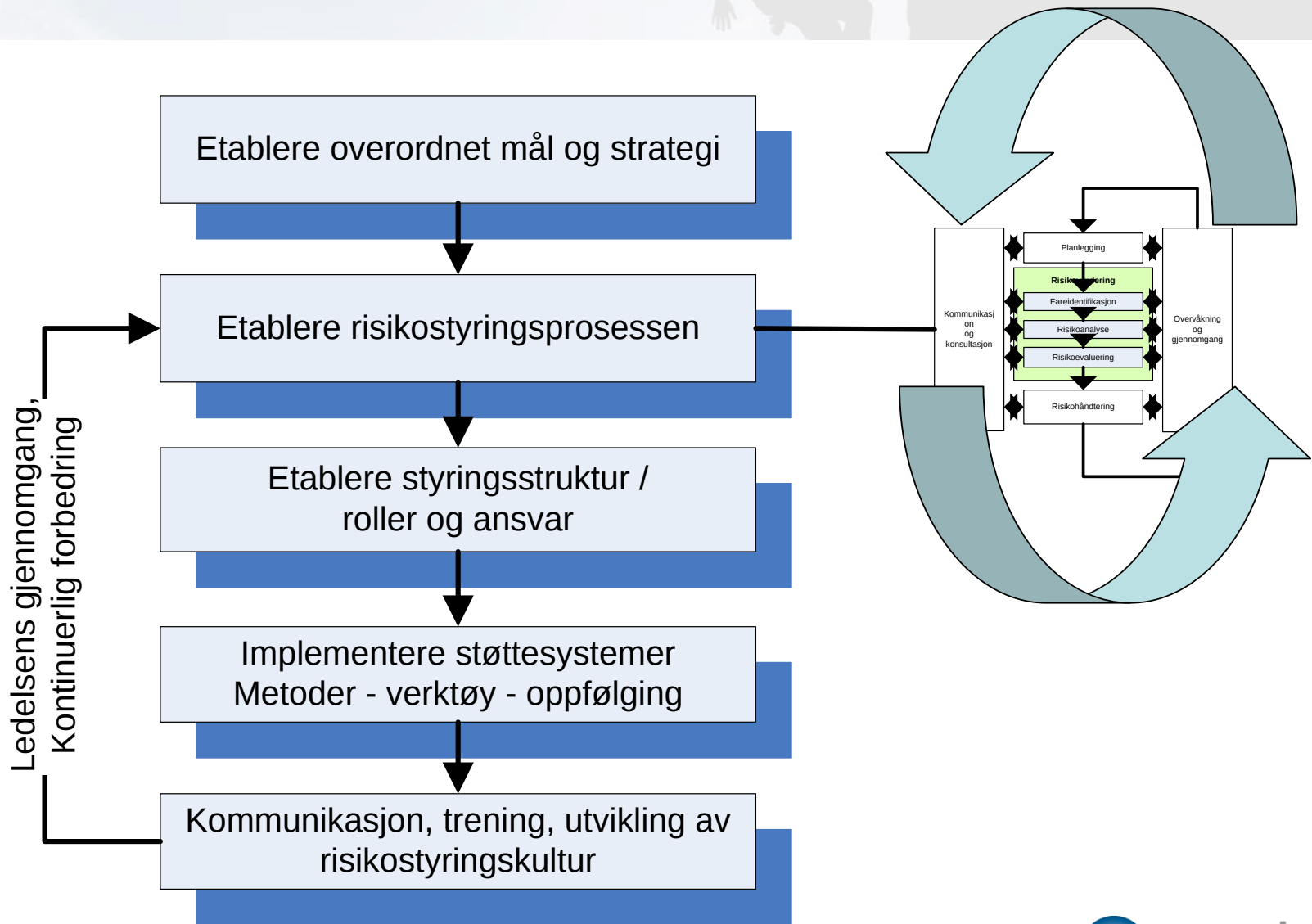


**Helhetlig
risikostyring.**

Hva er det?

PREPARED.

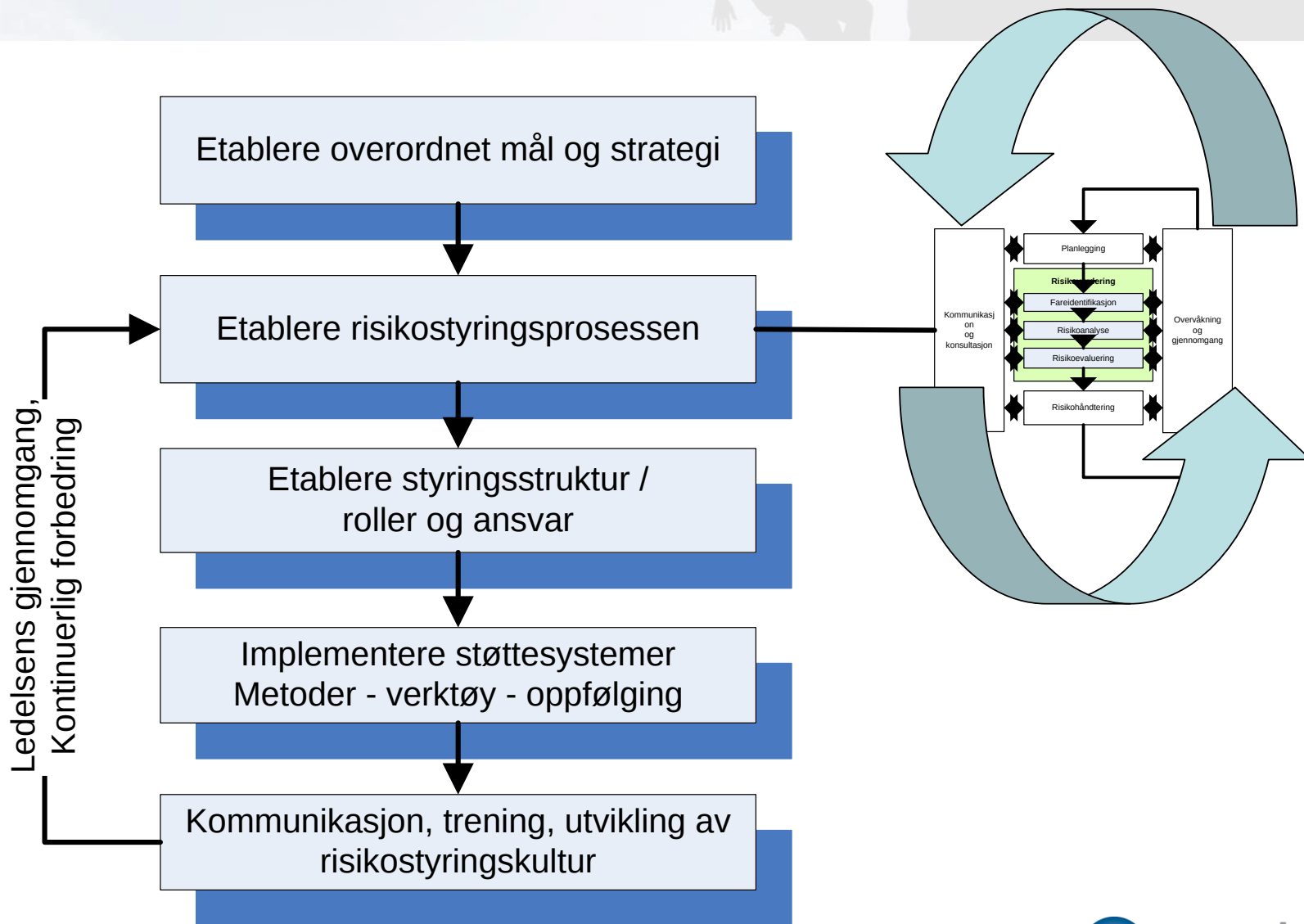
Rammeverk for risikostyring



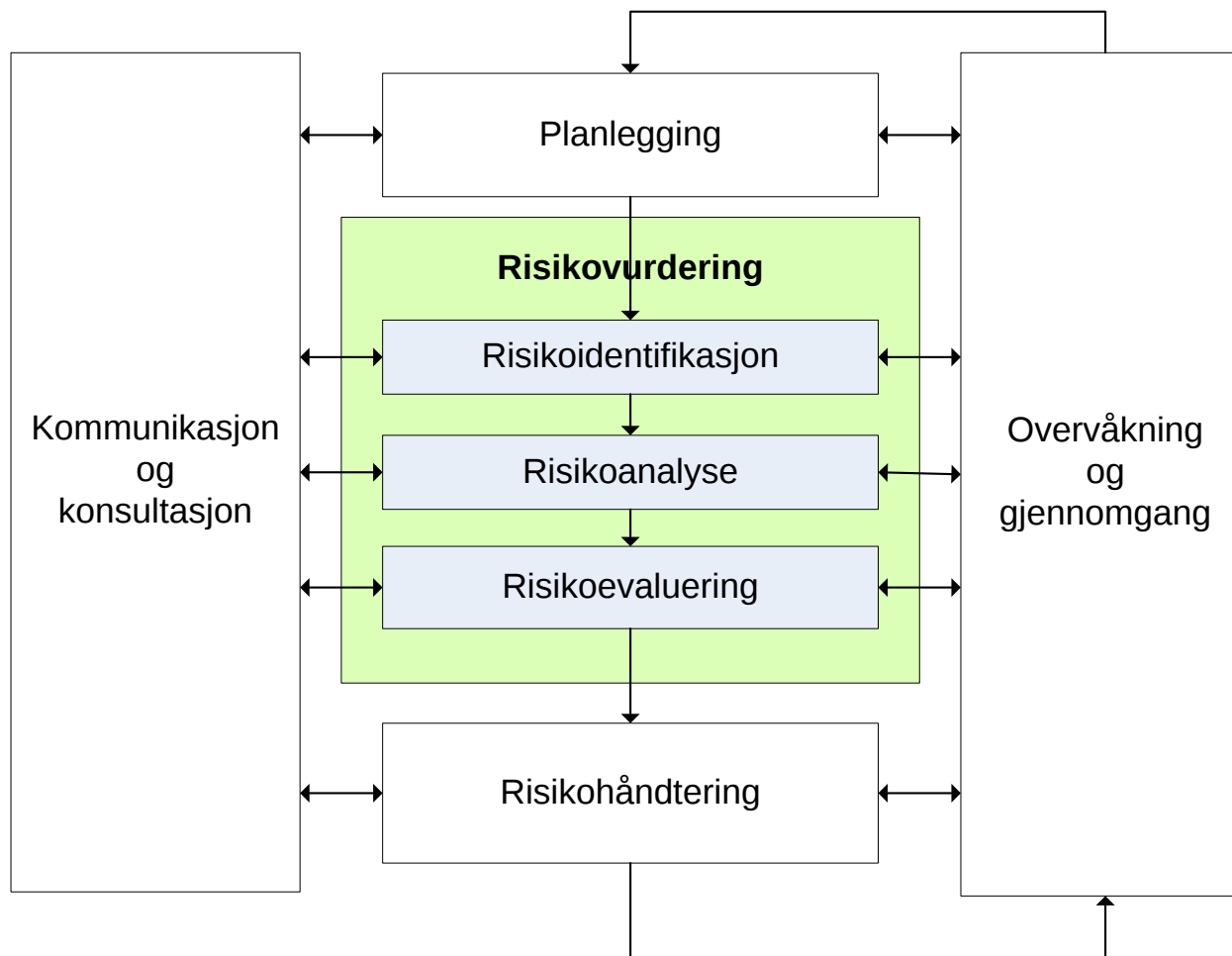
Helhetlig risikostyring – relevant for security som tema?

- **”risikostyring** er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko” (ISO 31000).
 - Generelt sett referer ”risikostyring” til arkitekturen (prinsipper, rammeverk og prosess) for å styre risiko på en effektiv måte
- **”å styre risiko”** refererer til anvendelsen av denne arkitekturen på bestemte risikoer (ISO 31000). I risikostyring inngår alle tiltak og aktiviteter som gjøres for å styre risiko.

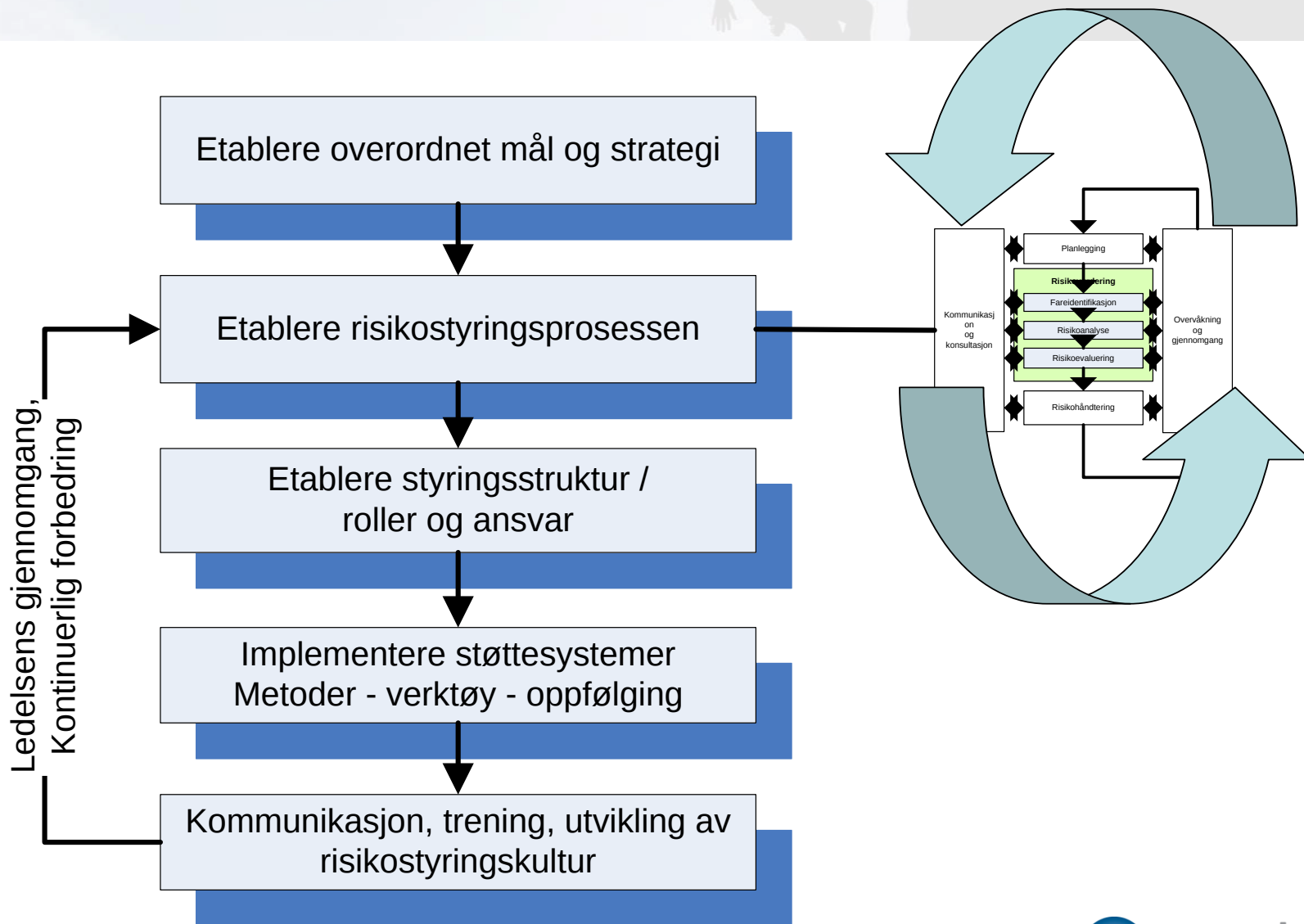
Rammeverk for risikostyring



Risikostyringsprosessen



Rammeverk for risikostyring



Helhetlig risikostyring



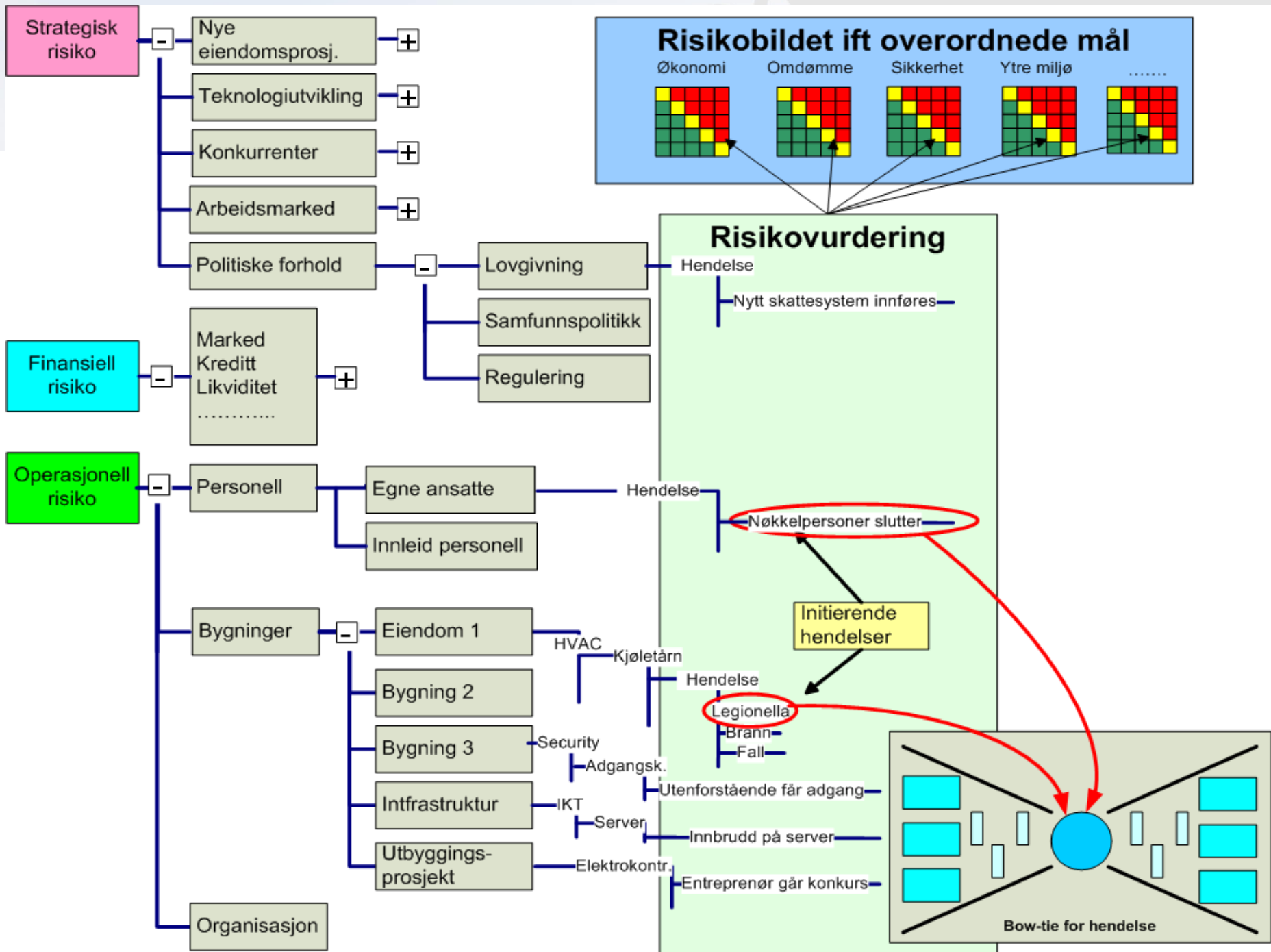
"We've considered every potential risk except the risks of avoiding all risks."

Ulike typer risiko

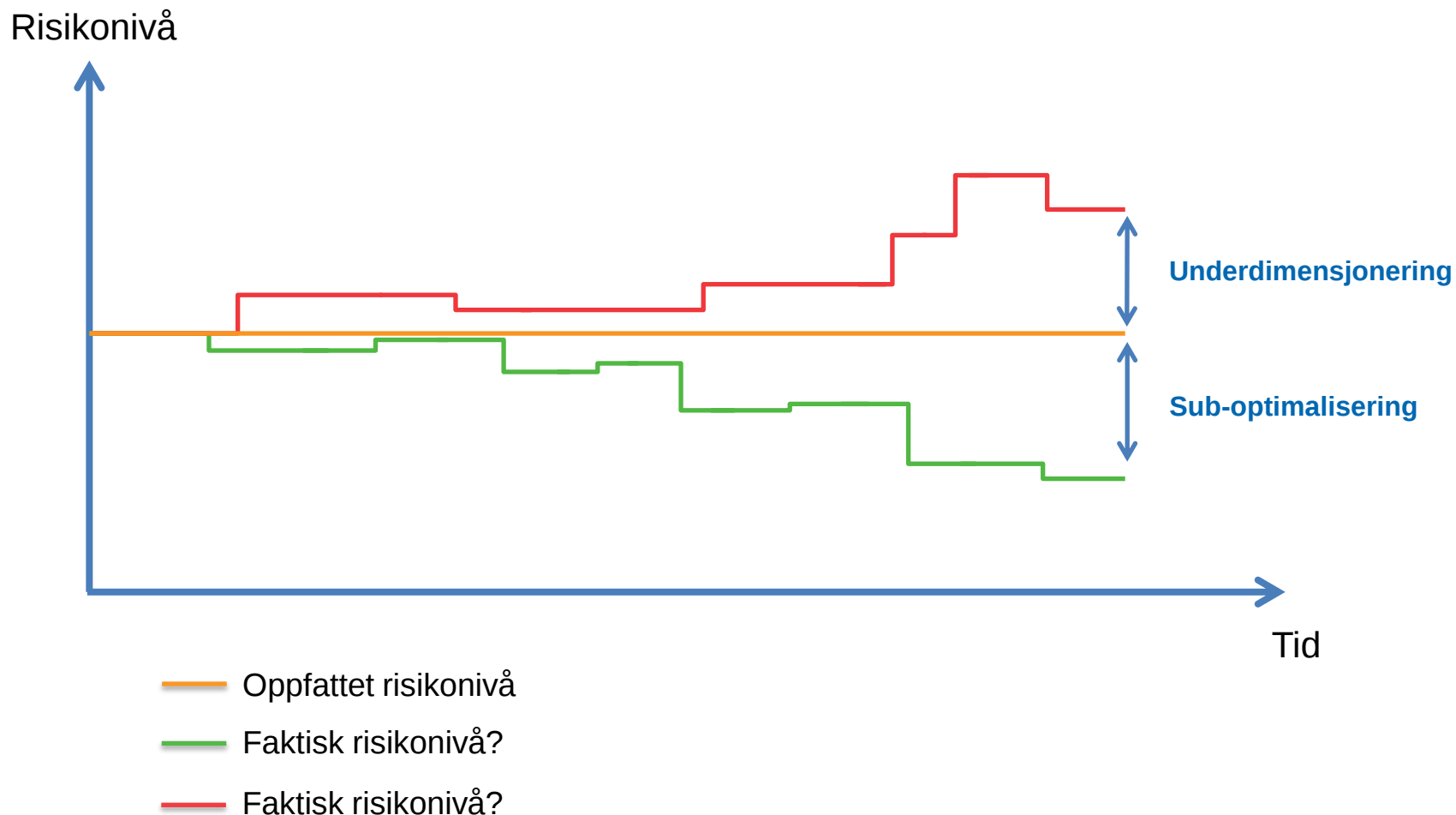


- **Strategisk risiko** er risiko relatert til de strategiske valgene bedriften gjør
- **Operasjonell risiko** er risiko forbundet med de aktiviteter bedriften utfører, herunder omdømmerisiko, prosjektrisiko, personellrisiko (inkl 1, 2. og 3. part), miljørisiko og skade på utstyr/system
- **Finansiell** herunder er relatert til bevegelse i finansielle instrumenter

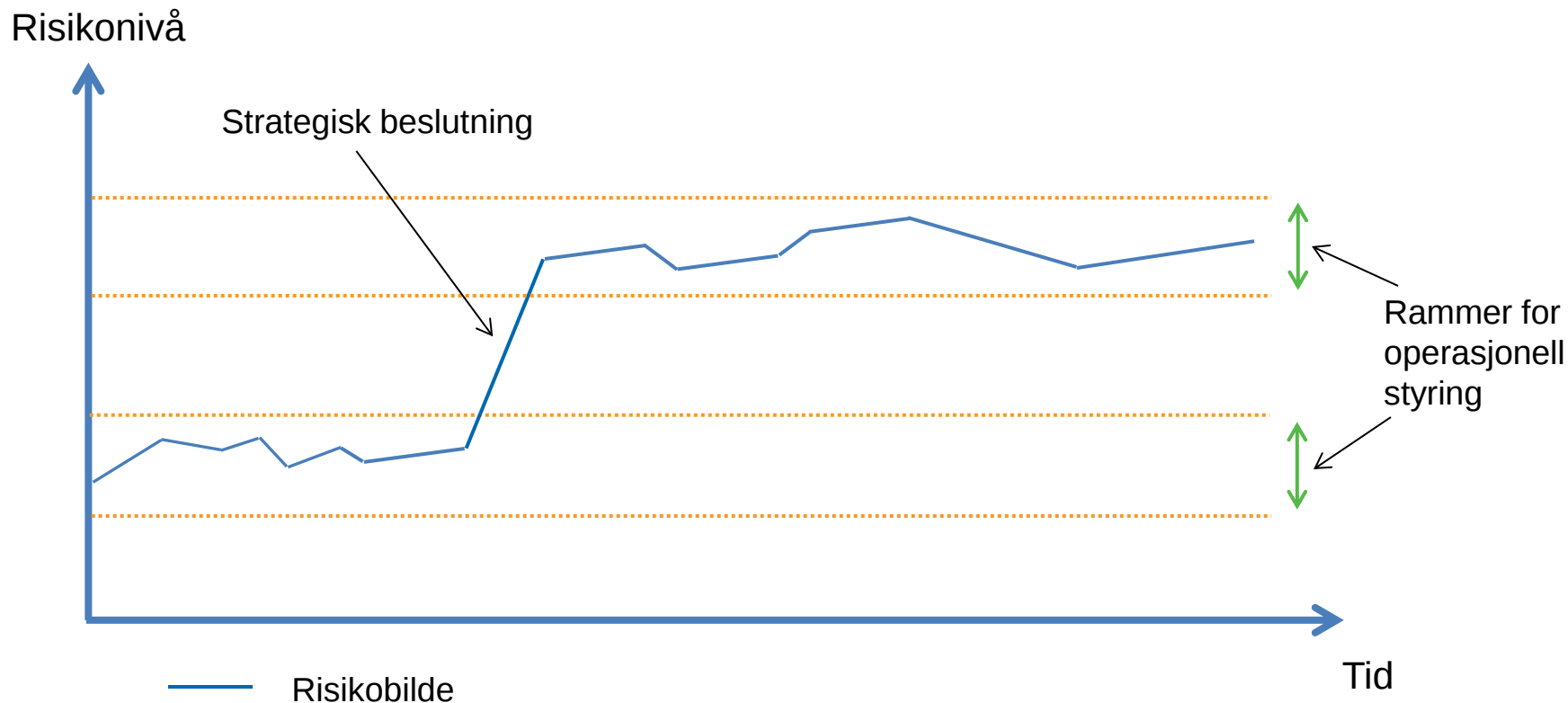




Risikonivået varierer over tid



Strategiske valg legger rammer for operasjonell risiko



Ti på topp risiko

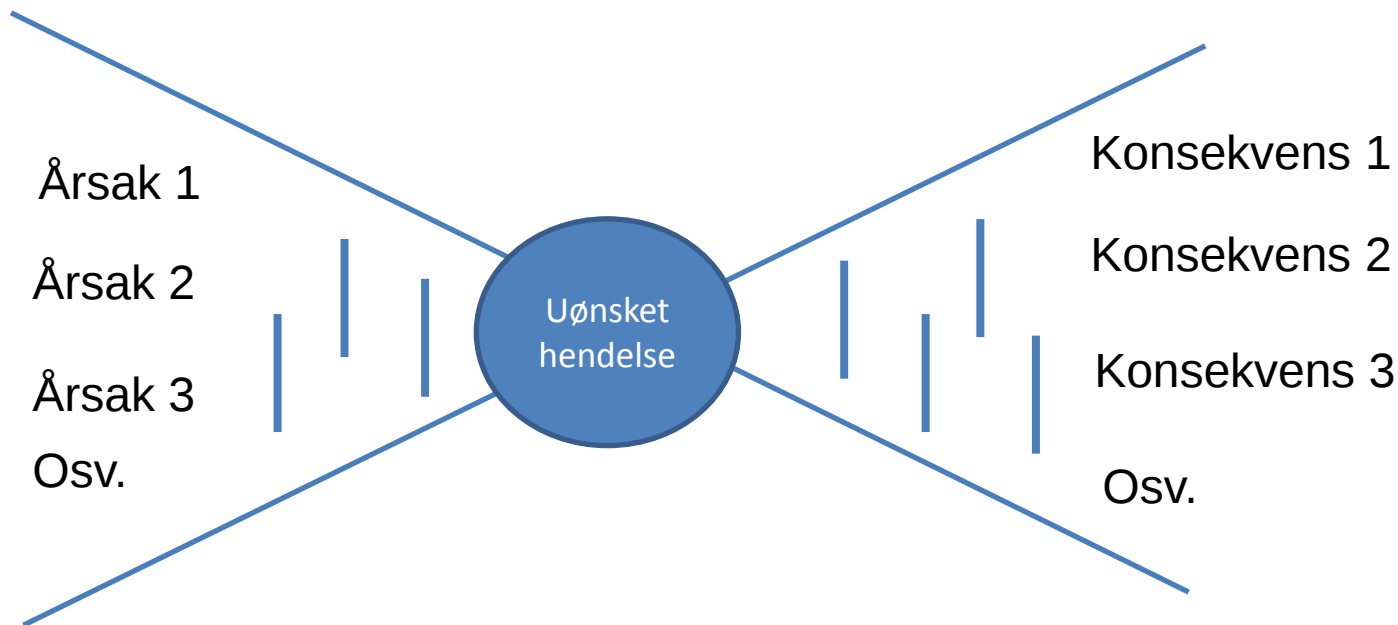


Probability

Consequence

	$p < 10^{-4}$ Highly unlikely (P1)	$10^{-4} < p < 10^{-3}$ Unlikely (P2)	$10^{-3} < p < 10^{-2}$ Could happen (P3)	$10^{-2} < p < 10^{-1}$ Likely (P4)	$p > 0.1$ Very likely (P5)
Catastrophic	Storulykke				
Very serious	Ramme- betingelser	Integritet		Budsjett	
Serious/ Considerable			Aktivitet		Kapasitet Leverandør
Small/Limited					Etterlevelse Styringssyst
Minimal	Sikring		Leveranse		Arbeids marked

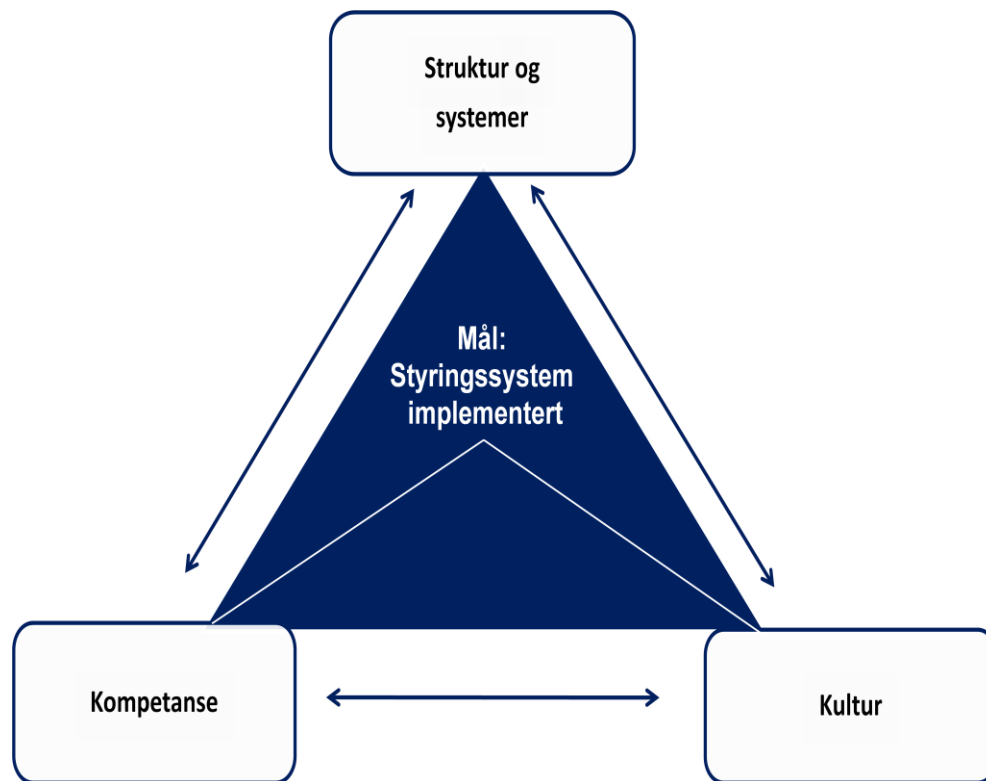
Risikoanalyse - Barrierestyring



Helhetlig risikostyring er relevant for security!

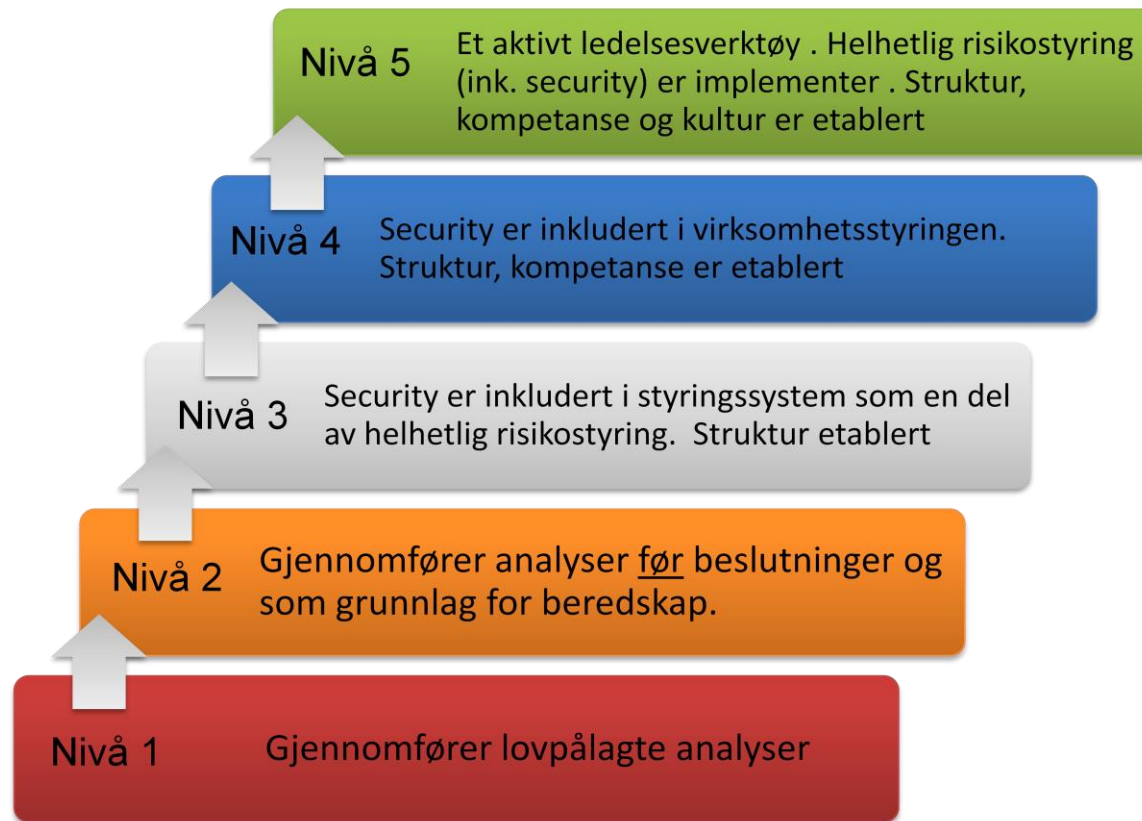
- En kontinuerlig prosess som gjennomsyrrer virksomheten og som utføres av mennesker på alle nivåer i organisasjonen, som tar hensyn til menneskelige og kulturelle faktorer
- Stimulerer til proaktiv adferd og kontinuerlig forbedring
- Risikostyringen har fokus på å vurdere usikkerhet, styrbarhet og sårbarhet – som grunnlag for beslutningstaking
- Anvendes på tvers av virksomheten, på alle nivåer og i alle enheter
- Forankret hos toppledelsen og anvendes i fastsettelse av strategi
- Har fokus på både målstyring og barrierestyring

Sikkerhet og beredskap som en del av helhetlig risikostyring



Figur 1 Hovedmomenter i et robust sikkerhets- og beredskapsarbeid

Kulturstige risikostyring (inkl. security)



Figur 1 Nivå for sikkerhetsstyring

Styring av risiko – verktøykassen og metoder



PREPARED.

Helhetlig risikostyring – relevant for security som tema?

- ”**å styre risiko**” refererer til anvendelsen av denne arkitekturen på bestemte risikoer (ISO 31000). I risikostyring inngår alle tiltak og aktiviteter som gjøres for å styre risiko.

Samme analyse?



Risiko for...



Styring av risiko på ulike nivå

	Strategisk risiko		Finansiell risiko	Operasjonell risiko			
	Overordnet	Prosjektrisiko (beslutning)	Finansiell risiko	Eksisterende anlegg	Vedlikehold	Oppgave	Prosjektrisiko (gjennomføring)
Eksempel	<i>Selskap</i>	<i>Nytt anlegg</i>	<i>Trading</i>	<i>Trafostasjon</i>	<i>Nedstengning</i>	<i>Bytte effektbryter</i>	<i>Nytt anlegg</i>
Planlegging	Årsplan	Prosjektplan	Trading strategi	Design, dokumentasjon	Vedlikeholdsplan	Dokumentasjon	Prosjektplan
Risikovurdering	Risiko Workshop Konsern-analyse security	Prosjekt-risikoanalyse Strategisk region/landanalyse	Portefølje-styring Monitorering av VaR tall.	ROS-analyse (grovanalyse, kvantitativ analyse) Objektanalyse IKT-sikkerhets-analyse	HAZID, FMECA	Sikker jobbanalyse (SJA)	Prosjekt-risikoanalyse Etablere lokalt trusselbilde Objektanalyse
Risikohåndtering	Matrise/diskusjon Etablere barrierer og beredskap	Portefølje-styring	Stop-loss limits, VaR limits	Akseptkriterier/handlingsregler ALARP Tiltaks-håndtering Etablere barrierer og beredskap	Diskusjon ALARP Tiltaks-håndtering	Diskusjon ALARP Tiltakshåndtering	Prosjekt-styring ALARP Tiltakshåndtering Etablere barrierer og beredskap
Kommunikasjon/konsultasjon	Intranett Ledelses-møter	Portefølje-styring	Rapportering av VaR-tall, Stop-loss limits	Rapport	Risikomatrise Tiltaksplan / tabell /	Rapport/ skjema	Risikomatrise Prosjekt-møte
Felles prosess	Prosjektledelse KPI	Helhetlig vurdering, Beslutningspunkt	Mandat, fullmakter	Prosjektledelse KPI HMS	Gjennomgang av plan	Internkontroll	Prosjekt-ledelse KPI

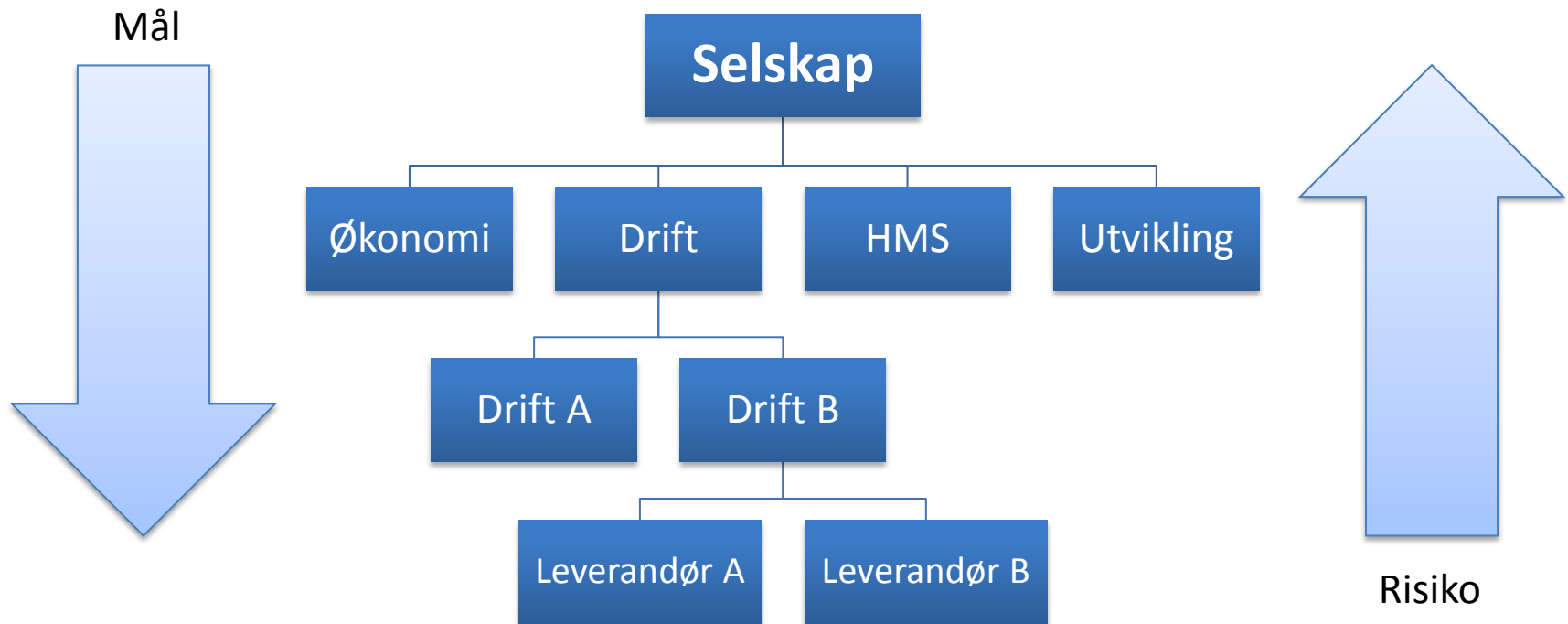
Ulike metoder

Styring av risiko på ulike nivå

	Strategisk risiko		Finansiell risiko	Operasjonell risiko			
	Overordnet	Prosjektrisiko (beslutning)	Finansiell risiko	Eksisterende anlegg	Vedlikehold	Oppgave	Prosjektrisiko (gjennomføring)
Eksempel	<i>Selskap</i>	<i>Nytt anlegg</i>	<i>Trading</i>	<i>Trafostasjon</i>	<i>Nedstengning</i>	<i>Bytte effektbryter</i>	<i>Nytt anlegg</i>
Planlegging	Årsplan	Prosjektplan	Trading strategi	Design, dokumentasjon	Vedlikeholdsplan	Dokumentasjon	Prosjektplan
Risikovurdering	Risiko Workshop Konsern-analyse security	Prosjekt-risikoanalyse Strategisk region/ landanalyse	Portefølje-styring Monitorering av VaR tall.	ROS-analyse (grovanalyse, kvantitativ analyse) Objektanalyse IKT-sikkerhets-analyse	HAZID, FMECA	Sikker jobbanalyse (SJA)	Prosjekt-risikoanalyse Etablere lokalt trusselbilde Objektanalyse
Risikohåndtering	Matrise/ diskusjon Etablere barrierer og beredskap	Portefølje-styring	Stop-loss limits, VaR limits	Akseptkriterier/ handlingsregler ALARP Tiltaks-håndtering Etablere barrierer og beredskap	Diskusjon ALARP Tiltaks-håndtering	Diskusjon ALARP Tiltakshåndtering	Prosjekt-styring ALARP Tiltakshåndtering Etablere barrierer og beredskap
Kommunikasjon/ konsultasjon	Intranett Ledelses-møter	Portefølje-styring	Rapportering av VaR-tall, Stop-loss limits	Rapport	Risikomatrise	Rapport/ skjema	Risikomatrise Prosjekt-møte
Felles prosess	Prosjektledelse KPI	Helhetlig vurdering, Beslutnings-punkt	Mandat, fullmakter	Prosjektledelse KPI HMS	Gjennomgang av plan	Internkontroll	Prosjekt-ledelse KPI

Ulike metoder

Målstyring vs. risikostyring



Målstyring og bruk av måleindikatorer (KPIer)

- **Helse:** Fristbrudd, infeksjonsgrad
- **Politi:** Oppklaringsprosent
- **Industri:** Skadefravær
- **Olje og gass:** Storulykkesrisiko

Verdibasert målstyring - Måloppnåelse

Manuell kvalitativ vurdering

Skal være med i beregningen Ja Nei

Spesifisert strategi og overordnede mål	Kalkulert
Bevisst jobbe for at vi skal ha det gøy	91 %
Vi har det gøy på jobb	91 %
Sikre økonomisk robusthet	81 %
Bedre økonomistyring og oppfølging	79 %
Fagutvikling skjer i prosjektene	63 %
God ressursplanlegging og oversikt over k	90 %
Løs turnover	92 %
Selskapet konsoliderer	100 %
Sikre robusthet i tjenester	76 %
Øke egenkapital-dekningsgraden	73 %
Styrke all ledelse	77 %
Arbidsrelatert sykefravær så lavt som m	99 %
Faggruppeledelsen styrket	98 %
Konsulentrollen styrket (prosjektledelse	71 %
Medarbeiderne ivarettatt og gitt mulighet	88 %
Proactima kultur hos ressurser	71 %
Risikobaserte beslutningsprosesser	69 %
Robusthet rundt lokale lederteam	96 %
Styrke markedsføring, særlig relatert til m	70 %
Styrke intern kommunikasjon	83 %
Avdelingsmålene styrket som arena for k	82 %
God oppfølging av utleide	96 %
Implementert bruk av intranett	90 %
Kompetansematrise implementert	80 %
Videreføre og styrke strategisk kompetan	75 %
Videreutvikle fag og tjenester gjennom eng	60 %
Erfaringer brukt til å forbedre fag og pros	67 %
Felles forståelse for verdier, visjoner og m	65 %
Sikre "Proactima-forankring" av leveranse	50 %
Sikre robusthet i tjenester	53 %
Styrke markedsføring, særlig relatert til m	78 %
Tydlig og profesjonell ekstern kommuni	70 %
Totalt gjennomsnitt	79 %

Hvordan forholde seg
til standarder
innenfor security?



PREPARED.

Kilder (standarder mm.) relevant for security

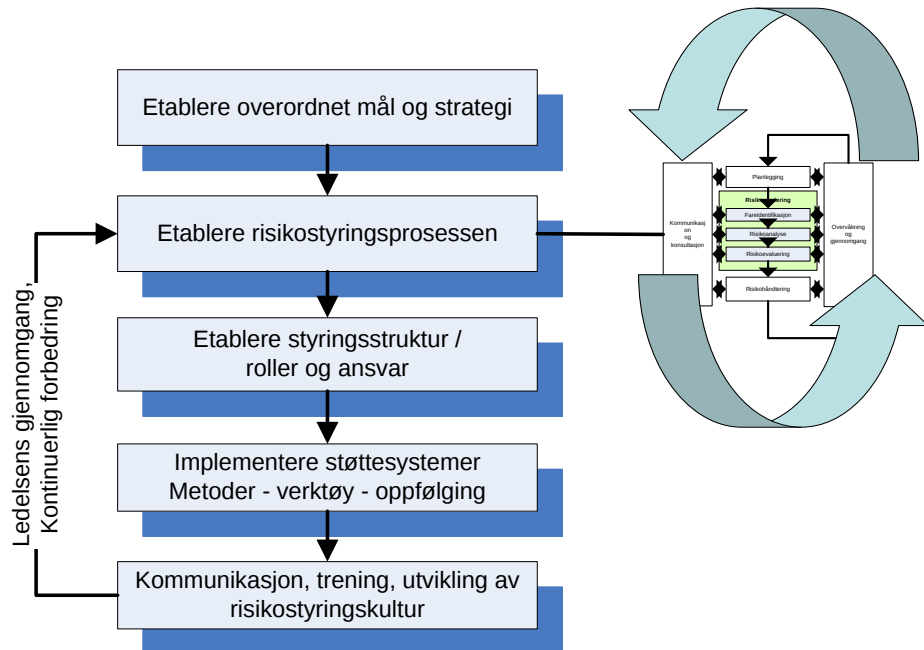
Navn	Hensikt	Målgruppe	Innspill til:
Voluntary principles on security and human rights	Et sett med frivillige prinsipper som søker å rettlegde bedrifter i ivaretagelsen av sikkerhet i sine operasjoner, innenfor et operasjonelt rammeverk som sikrer respekt for menneskerettigheter og grunnleggende friheter.	Alle bedrifter	Innspill til overordnet policy/styrende dokumenter
International Code of Conduct for Private Security Service Providers (ICoC)	ICoC søker å klargjøre internasjonale standarder for privat sikkerhetsindustri som opererer i komplekse miljø, samt å forbedre kontroll av selskapene og ansvarliggjøre disse.	Privat sikkerhetsindustri	Innspill til overordnet policy/styrende dokumenter
Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Definere retningslinjer som støtter implementering av IKT-sikkerhetsstyring i telekommunikasjonsforetak.	Primært telekommunikasjonsforetak	Rammeverk for IKT-sikkerhetsstyring, metodikk
ISO 28000:2007 Specification for security management systems for the supply chain	Spesifisere krav til et sikkerhetsstyringssystem, inkludert kritiske aspekter med hensyn til sikring av verdikjeden. Disse aspektene inkluderer alle aktiviteter kontrollert eller påvirket av virksomheter som har innvirkning på verdikjeden.	Alle virksomhetsstørrelser, fra mindre til multinasjonale selskaper, innenfor produksjon, tjenesteytelser, lagring eller transport, i alle ledd av produksjonen eller verdikjeden.	Rammeverk for risikostyring, metodikk
Veiledning i verdivurdering (utgitt av NSM)	Gi virksomhetene et hjelpemiddel til å identifisere hva som er skjermingsverdig informasjon og skjermingsverdig objekt, og i hvilken grad de er skjermingsverdige, for å finne frem til riktig grad av beskyttelsestiltak.	Primært virksomheter, det være seg offentlige eller private, som er underlagt sikkerhetsloven. Men også andre virksomheter som behandler sensitiv informasjon eller råder over kritiske objekter vil ha nytte av veiledningen.	Metodikk
Fysisk sikring mot ulovlig inntrengning – Veiledning til forskrift om informasjonssikkerhet (utgitt av NSM)	Forskrift om informasjonssikkerhet stiller krav til forebyggende sikkerhetstiltak mot ulovlig inntrengning. Veilederen utdyper forskriftens bestemmelser, orienterer om NSMs gjeldende godkjenninger, samt gir råd om alternative kompenserende sikringstiltak.	Bestemmelsene gjelder generelt for alle virksomheter som faller inn under sikkerhetslovens virkeområde og er å anse som minimumskrav til sikringstiltak i en normalsituasjon.	Metodikk
Sikkerhetsadministrasjon – Veiledning til bestemmelser om sikkerhetsstyring i sikkerhetsloven med forskrifter (utgitt av NSM)	Veilede virksomheter som håndterer skjermingsverdig informasjon eller skjermingsverdige objekter og som derfor plikter å utøve forebyggende sikkerhetstjeneste for å håndtere risiko for spionasje, sabotasje eller terrorvirksomhet.	Virksomheter som behandler skjermingsverdig informasjon eller som råder over skjermingsverdig objekt.	Rammeverk for risikostyring, metodikk

ISO vs COSO

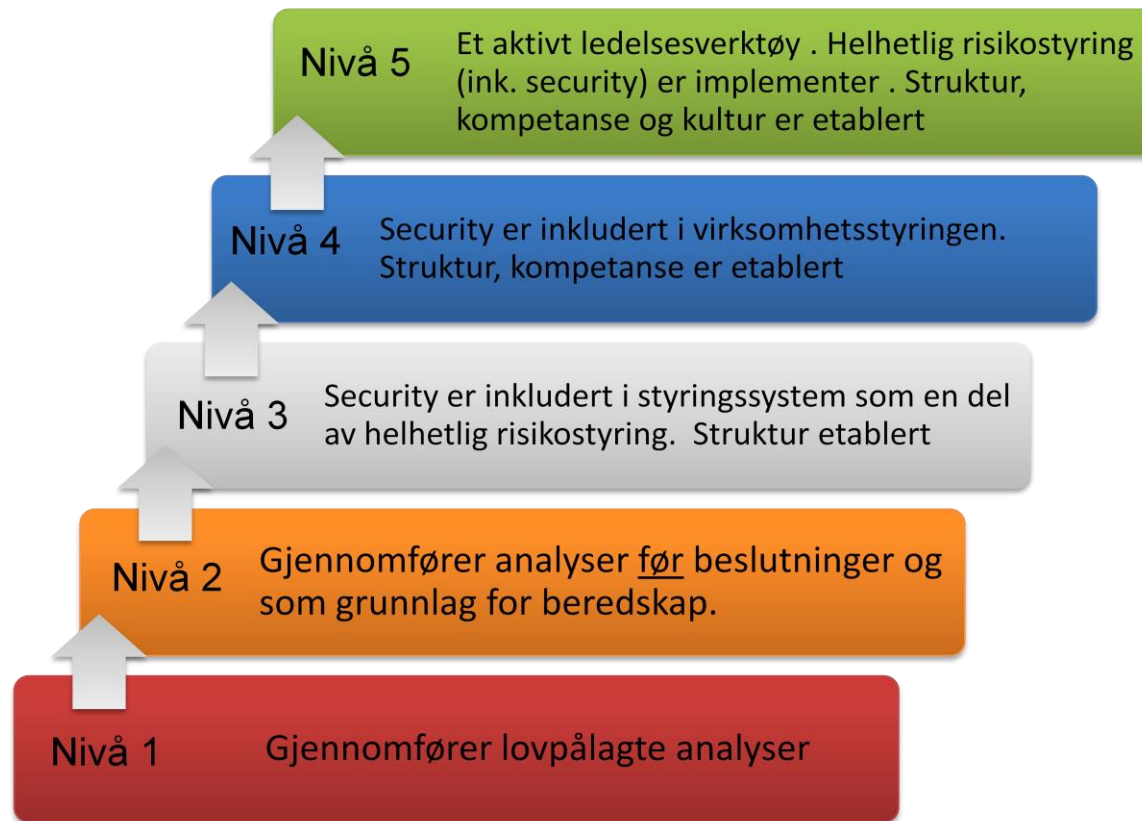


“Enterprise risk is... designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

“Risk management: Coordinated activities to direct and control an organization with regard to risk”. “Risk: Effect of uncertainty on objectives”



Kulturstige risikostyring (inkl. security)

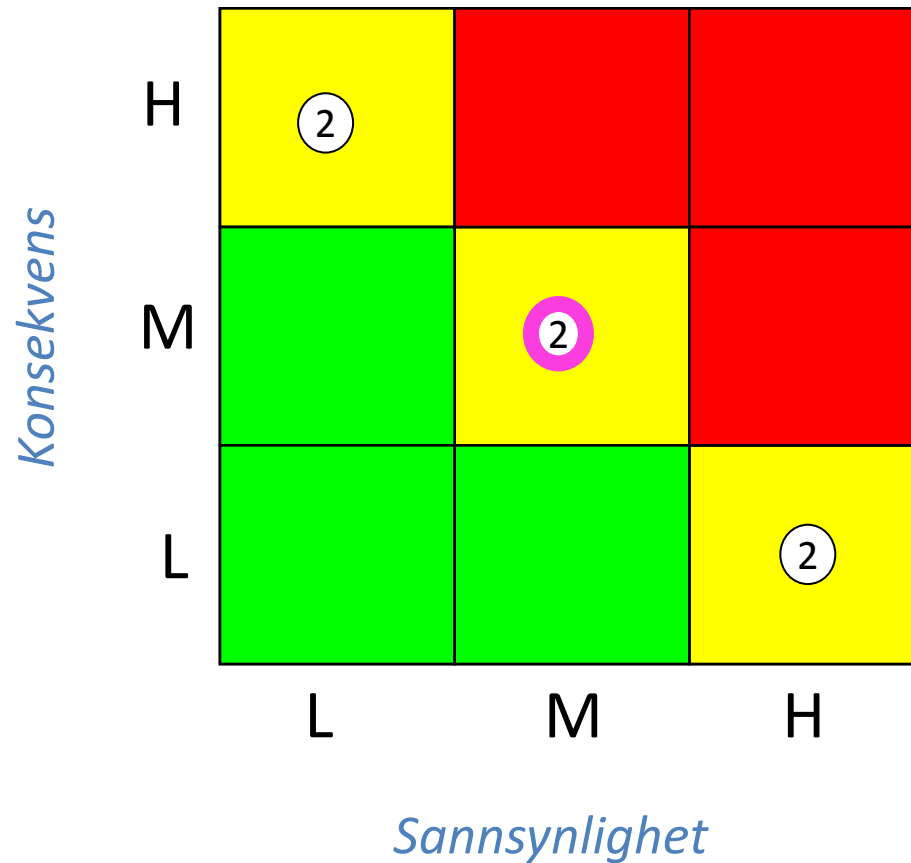


Figur 1 Nivå for sikkerhetsstyring

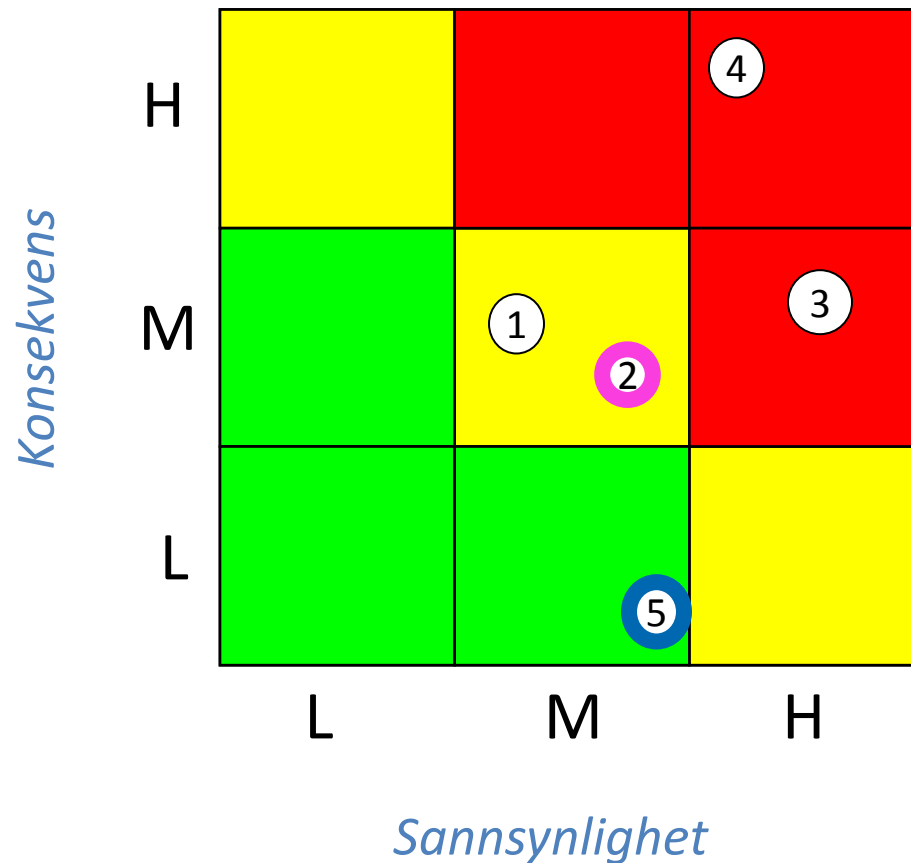


Presentasjon av risiko og beslutning

Presentasjon av risiko – stort utfallsrom



Presentasjon av risiko – usikkerhet

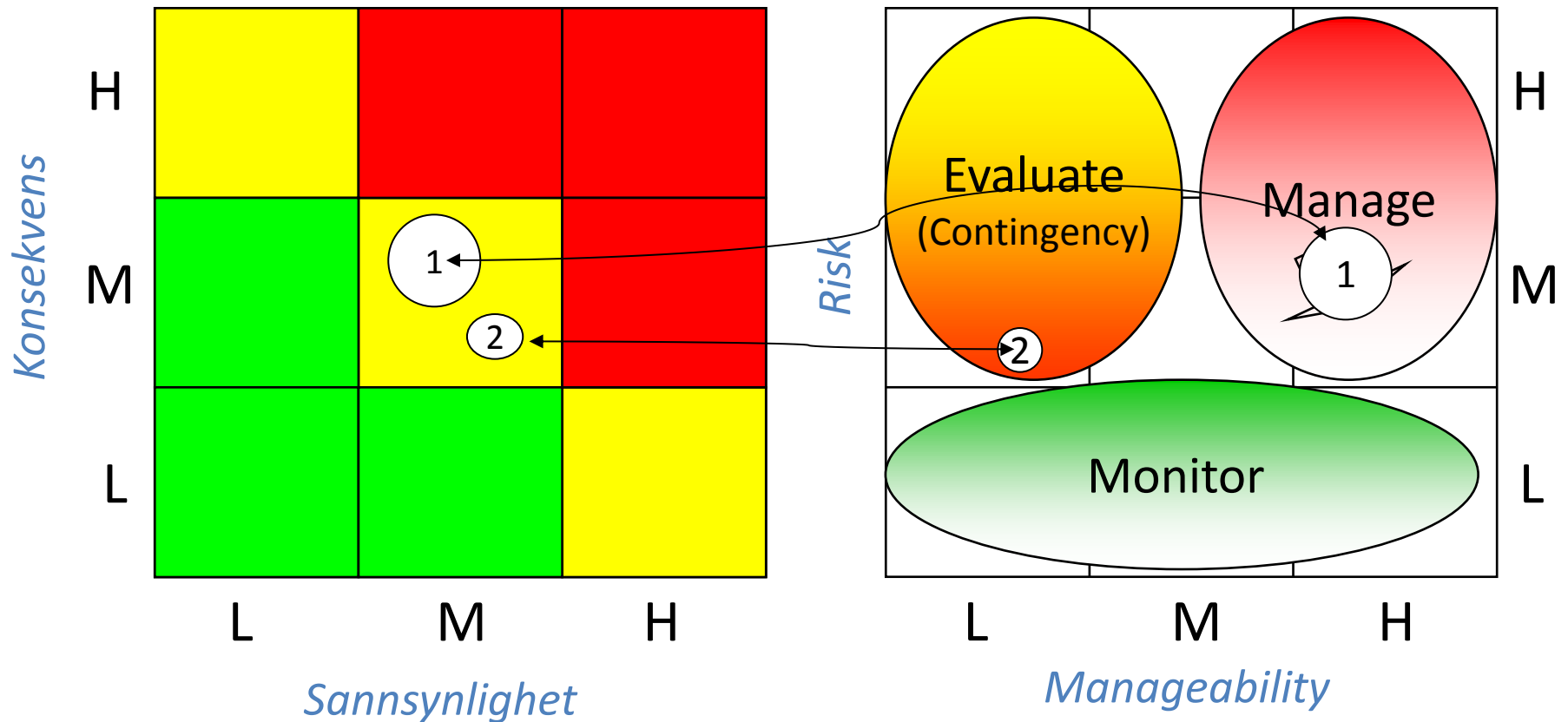


Stort utfallsrom

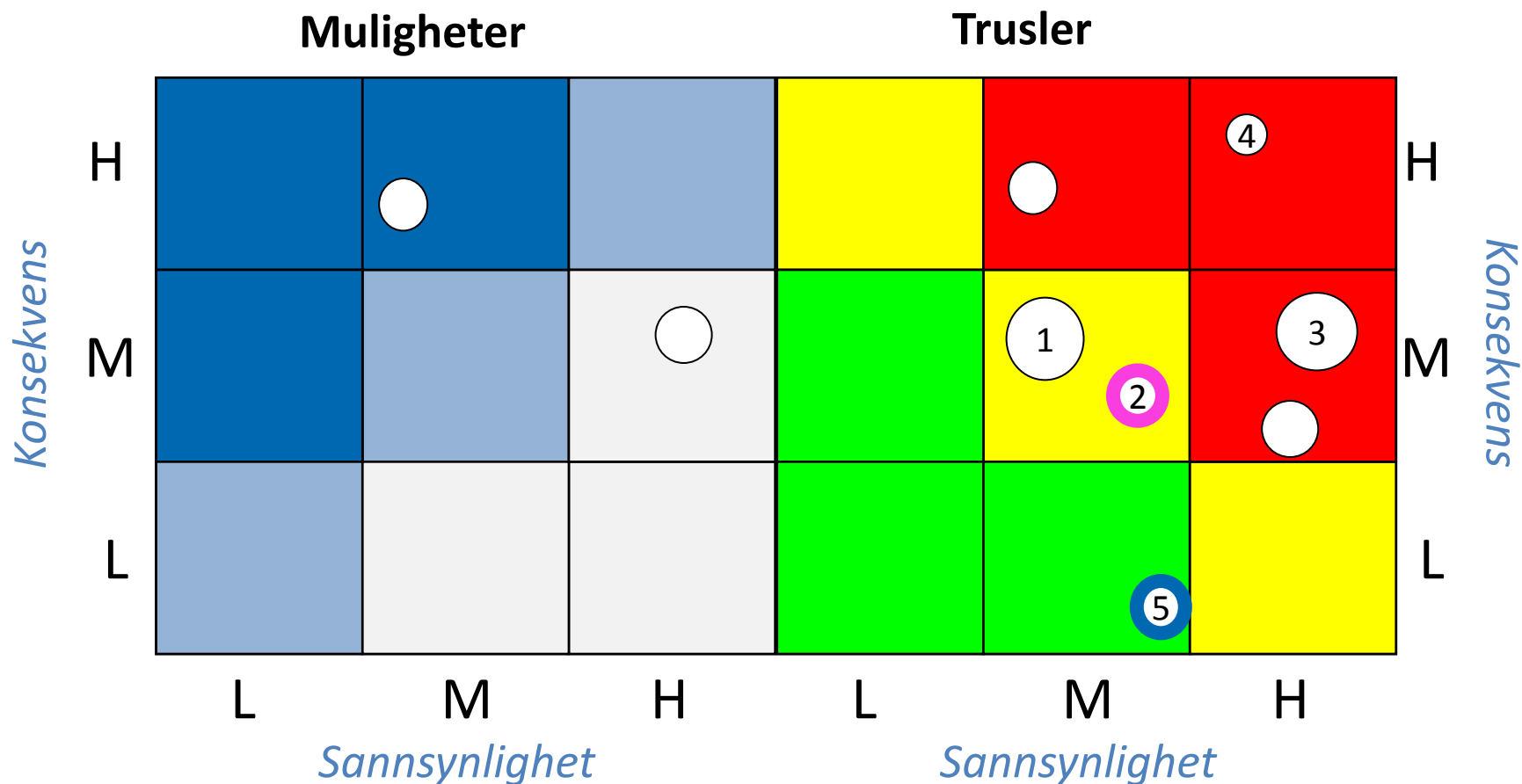


Høy usikkerhet

Beslutning: Risiko vs styrbarhet



Presentasjon av risiko skal understøtte beslutning



Stort utfallsrom



Høy usikkerhet

Risiko over tid

