Digdir

digdir.no

Helhetlig styringssystem for sikkerhet i Digdir

NIFS-møte: Helhetlig styring og kontroll onsdag 17. november

Amandeep Kaur Sharma og Yngve Dyrøy

Digdir

Difi
Direktoratet for forvaltning og ikt

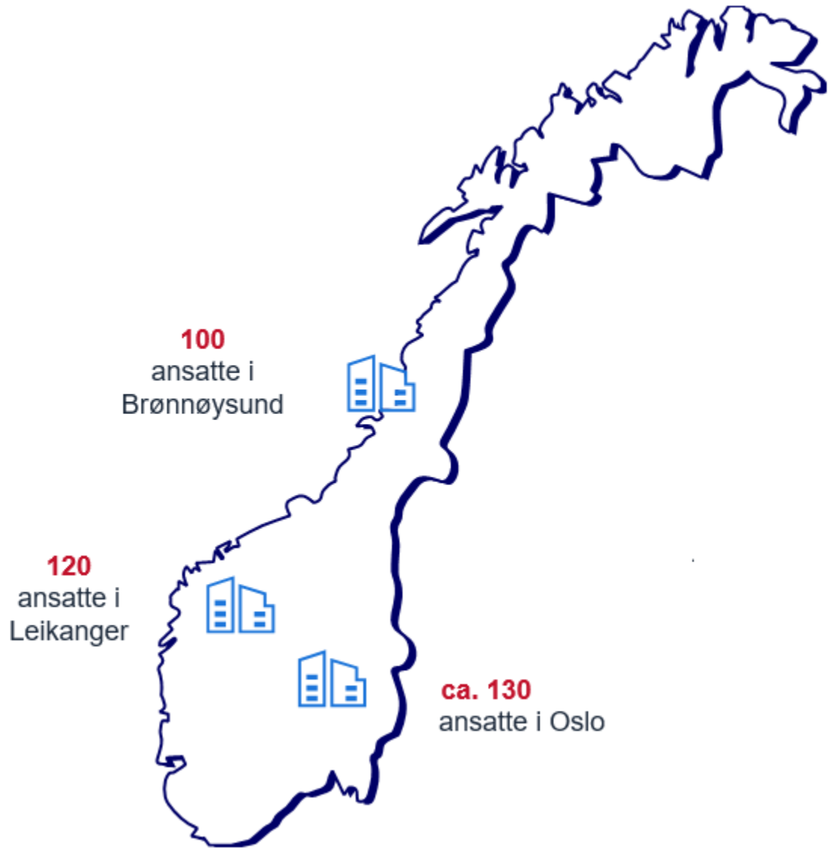
Ledelse
Utredning og analyse
Anskaffelser

altinn

Deler av miljøet for informasjonsforvaltning

Brønnøysundregistrene

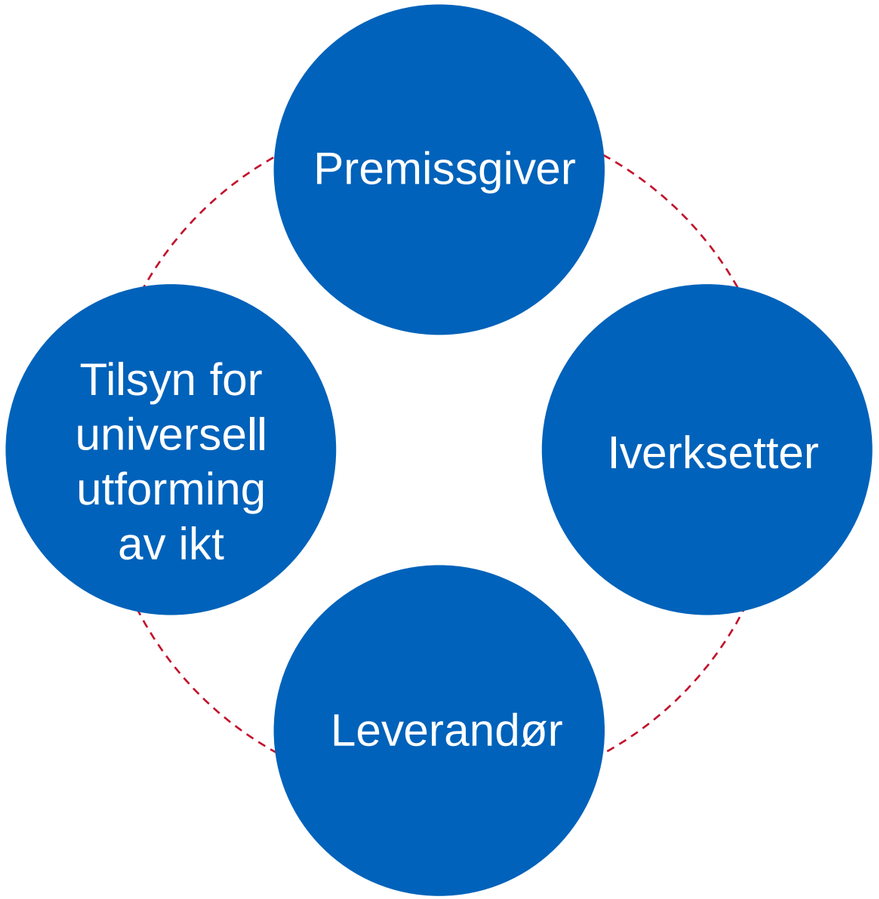
Direktoratet for forvaltning og økonomistyring



Det vi skal innfri | Dette gjør vi | Det vi skaper

Raskere og mer samordnet digitalisering av offentlig sektor

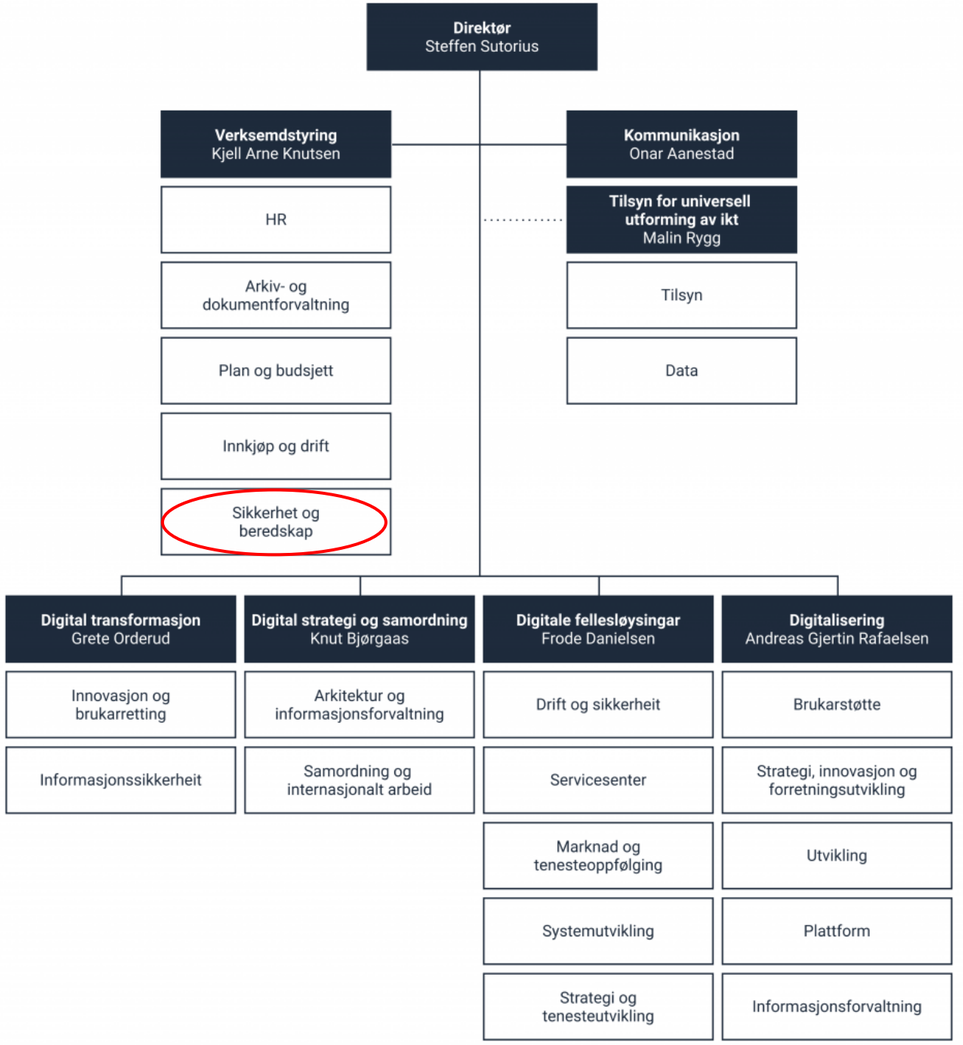
Bidra til en digitalisering av samfunnet som helhet



Regjeringen har to hovedmål for utviklingen av forvaltningen og IKT-politikken:

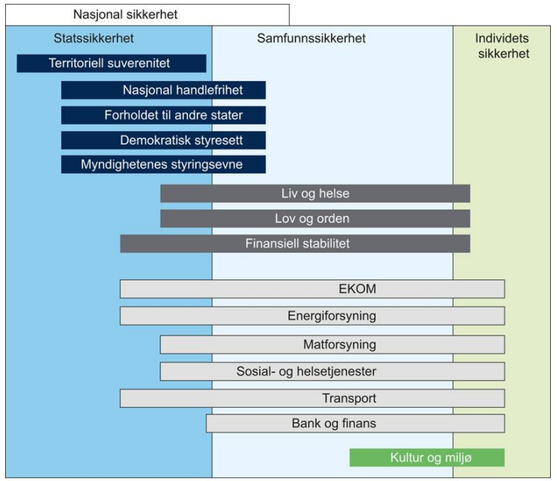
- Digitalisering i samfunnet gir gode vilkår for deltagelse, verdiskaping og innovasjon i offentlig sektor
- Forvaltningen i Norge er effektiv, åpen, samordnet og har høy tillit i befolkningen

Sikkerhet som en del av virksomhetsstyring



Seksjon for sikkerhet og beredskap (VSB)

- Sentralt ansvar for sikkerhetsarbeidet på tvers av de ulike sikkerhetsområdene i Digdir
- Overordnet ansvar i direktoratet
  - Nasjonal forebyggende sikkerhet
  - Samfunnssikkerhet og beredskap
  - Informasjonssikkerhet
- Styrende, koordinerende og kontrollerende oppgaver



VSB – opprettet 2020

- Per Viggo Kristiansen:
  - Seksjonssjef og sikkerhetsleder
  - Fagansvarlig nasjonal sikkerhet
  - Ansatt oktober 2020

- Yngve Dyrøy:
  - Fagansvarlig beredskap og krisehåndtering
  - Beredskapsleder
  - Ansatt april 2021

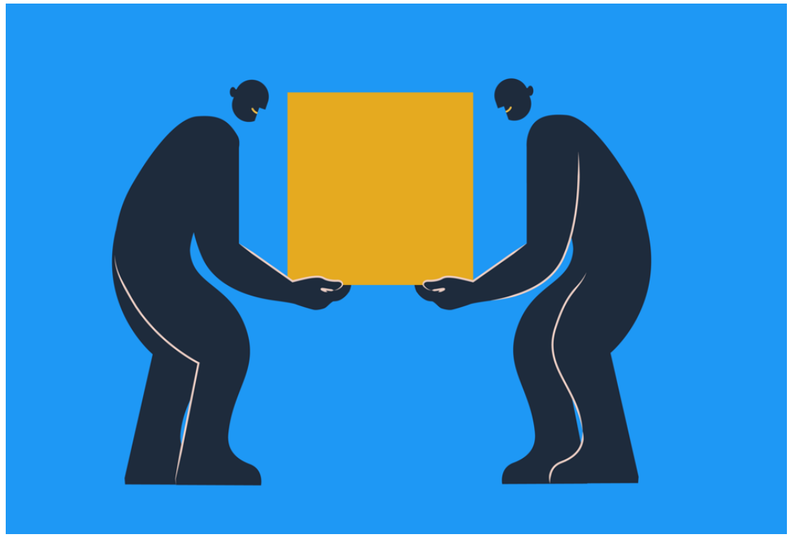
- Amandeep Kaur Sharma:
  - CISO/ Fagansvarlig informasjonssikkerhet
  - Datasikkerhetsleder
  - Ansatt juni 2021

Sikkerhetsorganisasjonen

- Sikkerhetsleder/Fagansv. nasjonal sikkerhet
- Beredskapsleder/Fagansv. beredskap
- CISO/ Fagansv. informasjonssikkerhet
- Sikkerhetsfaglige ressurser i avdelingene
- Andre
  - Lokasjonsansvarlige
  - Personvernombud
  - Systemeiere
  - Faglige nettverk
  - Risikoeiere

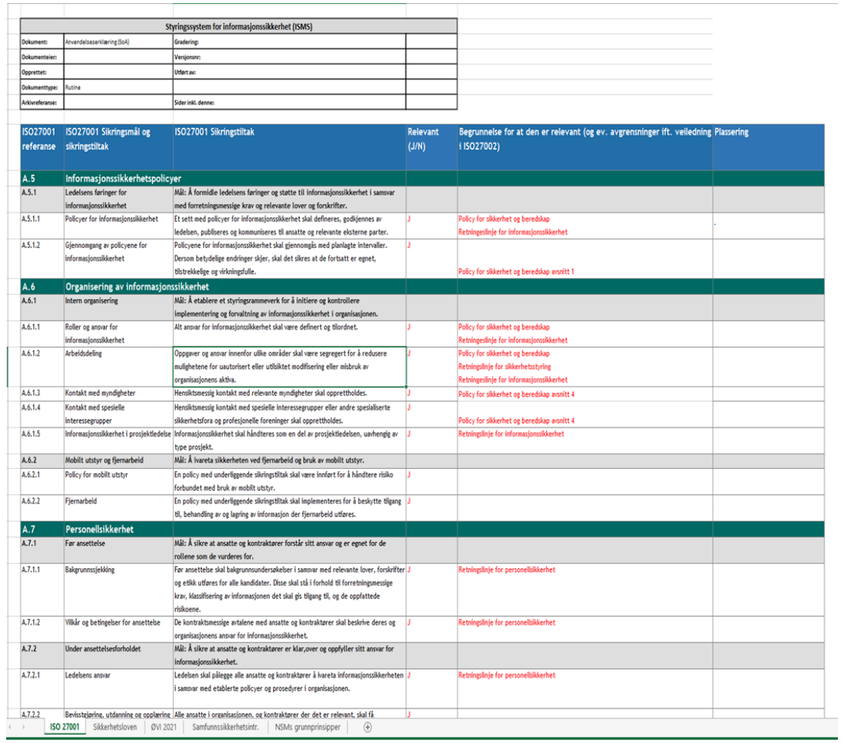
Helhetlig styring og kontroll

- Organisatorisk plassering i VIS
- Virksomhetsplan
- Ett styringssystem på tvers av fagområder
- Ett overordnet policydokument: skal se flere fagområder i sammenheng, herunder nasjonal sikkerhet, beredskap, informasjonssikkerhet og personvern



Revidering og videreutvikling av styringssystemet

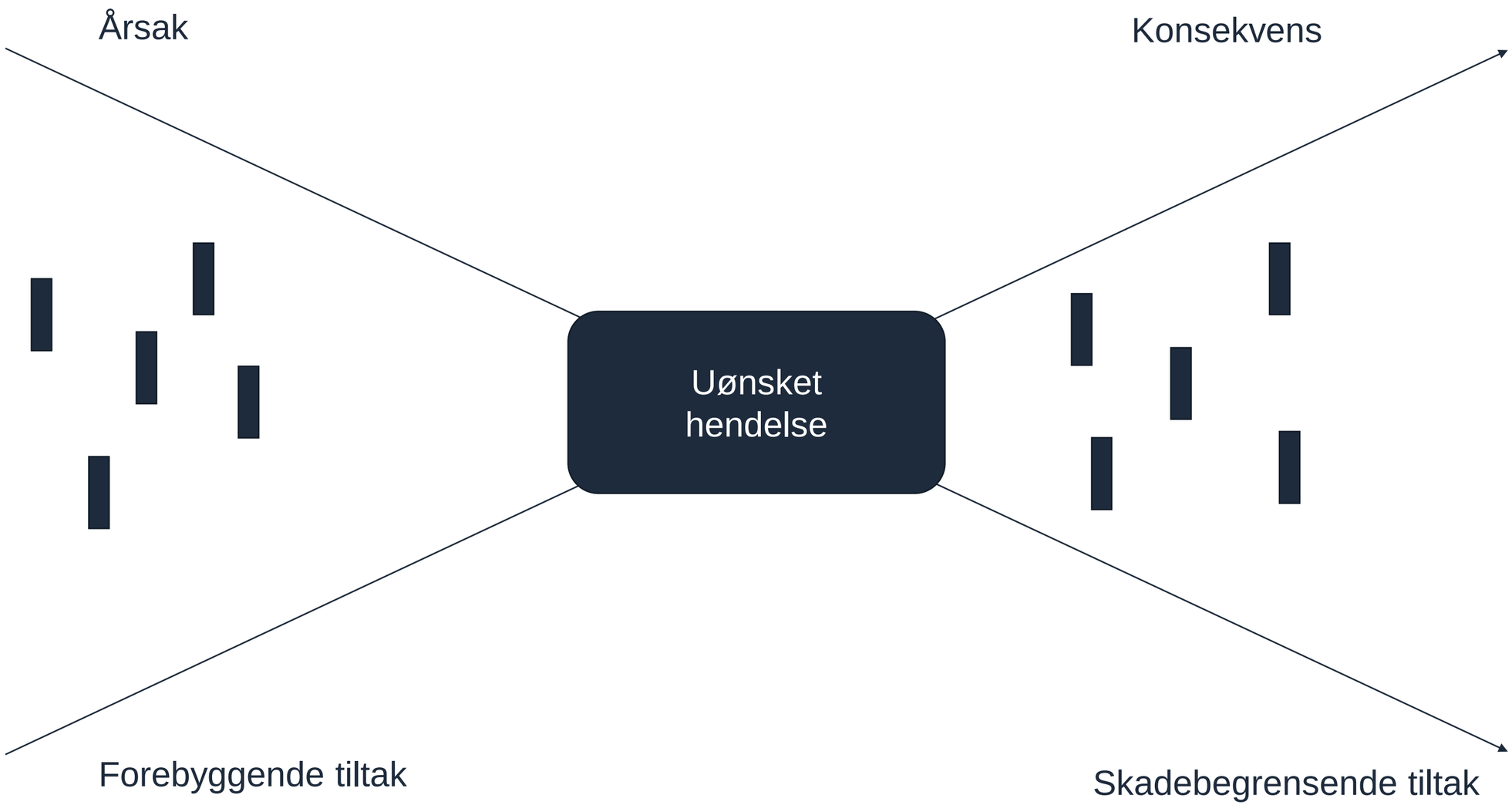
- Dokumentfangst
- Etablere overordnende styrende dokumenter
- Revidering av rutiner
- SoA (Statement of Applicabilty)



Styringssystem for informasjonssikkerhet (ISMS)			
Dokument:	Anvendelseserklæring (SoA)	Gradering:	
Dokumenteier:		Versjonsnr:	
Opprettet:		Utført av:	
Dokumenttype:	Rutine		
Arkivreferanse:		Sider inkl. denne:	

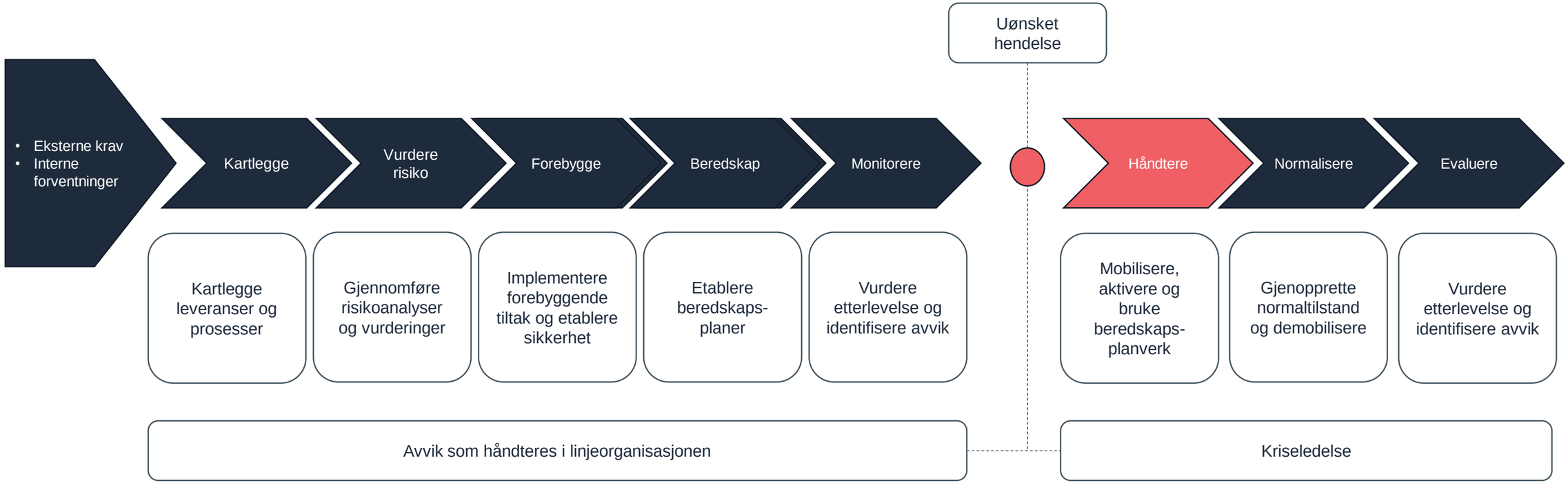
ISO27001 referanse	ISO27001 Sikringsmål og sikringstiltak	ISO27001 Sikringstiltak	Relevant (J/N)	Begrunnelse for at den er relevant (og ev. avgrensninger ift. veiledning i ISO27002)	Plassering
A.5	Informasjonssikkerhetspolicyer				
A.5.1	Ledelsens føringer for informasjonssikkerhet	Mål: Å formidle ledelsens føringer og støtte til informasjonssikkerhet i samsvar med forretningsmessige krav og relevante lover og forskrifter.			
A.5.1.1	Policyer for informasjonssikkerhet	Et sett med policyer for informasjonssikkerhet skal defineres, godkjennes av ledelsen, publiseres og kommuniseres til ansatte og relevante eksterne parter.	J	Policy for sikkerhet og beredskap Retningslinje for informasjonssikkerhet	
A.5.1.2	Gjennomgang av policyene for informasjonssikkerhet	Policyene for informasjonssikkerhet skal gjennomgås med planlagte intervaller. Dersom betydelige endringer skjer, skal det sikres at de fortsatt er egnet, tilstrekkelige og virkningsfulle.	J	Policy for sikkerhet og beredskap avsnitt 1	
A.6	Organisering av informasjonssikkerhet				
A.6.1	Intern organisering	Mål: Å etablere et styringsrammeverk for å initiere og kontrollere implementering og forvaltning av informasjonssikkerhet i organisasjonen.			
A.6.1.1	Roller og ansvar for informasjonssikkerhet	Alt ansvar for informasjonssikkerhet skal være definert og tilordnet.	J	Policy for sikkerhet og beredskap Retningslinje for informasjonssikkerhet	
A.6.1.2	Arbeidsdeling	Oppgaver og ansvar innenfor ulike områder skal være segregert for å redusere mulighetene for uautorisert eller utilsiktet modifisering eller misbruk av organisasjonens aktiva.	J	Policy for sikkerhet og beredskap Retningslinje for sikkerhetsstyring Retningslinje for informasjonssikkerhet	
A.6.1.3	Kontakt med myndigheter	Hensiktsmessig kontakt med relevante myndigheter skal opprettholdes.	J	Policy for sikkerhet og beredskap avsnitt 4	
A.6.1.4	Kontakt med spesielle interessegrupper	Hensiktsmessig kontakt med spesielle interessegrupper eller andre spesialiserte sikkerhetsfora og profesjonelle foreninger skal opprettholdes.	J	Policy for sikkerhet og beredskap avsnitt 4	
A.6.1.5	Informasjonssikkerhet i prosjektledelse	Informasjonssikkerhet skal håndteres som en del av prosjektledelsen, uavhengig av type prosjekt.	J	Retningslinje for informasjonssikkerhet	
A.6.2	Mobilt utstyr og fjernarbeid	Mål: Å ivareta sikkerheten ved fjernarbeid og bruk av mobilt utstyr.			
A.6.2.1	Policy for mobilt utstyr	En policy med underliggende sikringstiltak skal være innført for å håndtere risiko forbundet med bruk av mobilt utstyr.	J		
A.6.2.2	Fjernarbeid	En policy med underliggende sikringstiltak skal implementeres for å beskytte tilgang til, behandling av og lagring av informasjon der fjernarbeid utføres.	J		
A.7	Personellsikkerhet				
A.7.1	Før ansettelse	Mål: Å sikre at ansatte og kontraktører forstår sitt ansvar og er egnet for de rollene som de vurderes for.			
A.7.1.1	Bakgrunnssjekking	Før ansettelse skal bakgrunnsundersøkelser i samsvar med relevante lover, forskrifter og etikk utføres for alle kandidater. Disse skal stå i forhold til forretningsmessige krav, klassifisering av informasjonen det skal gis tilgang til, og de oppfattede risikoene.	J	Retningslinje for personellsikkerhet	
A.7.1.2	Vilkår og betingelser for ansettelse	De kontraktsmessige avtalene med ansatte og kontraktører skal beskrive deres og organisasjonens ansvar for informasjonssikkerhet.	J	Retningslinje for personellsikkerhet	
A.7.2	Under ansettelsesforholdet	Mål: Å sikre at ansatte og kontraktører er klar,over og oppfyller sitt ansvar for informasjonssikkerhet.			
A.7.2.1	Ledelsens ansvar	Ledelsen skal pålegge alle ansatte og kontraktører å ivareta informasjonssikkerheten i samsvar med etablerte policyer og prosedyrer i organisasjonen.	J	Retningslinje for personellsikkerhet	
A.7.2.2	Bevisstgjøring, utdanning og opplæring	Alle ansatte i organisasjonen, og kontraktører der det er relevant, skal få	J		

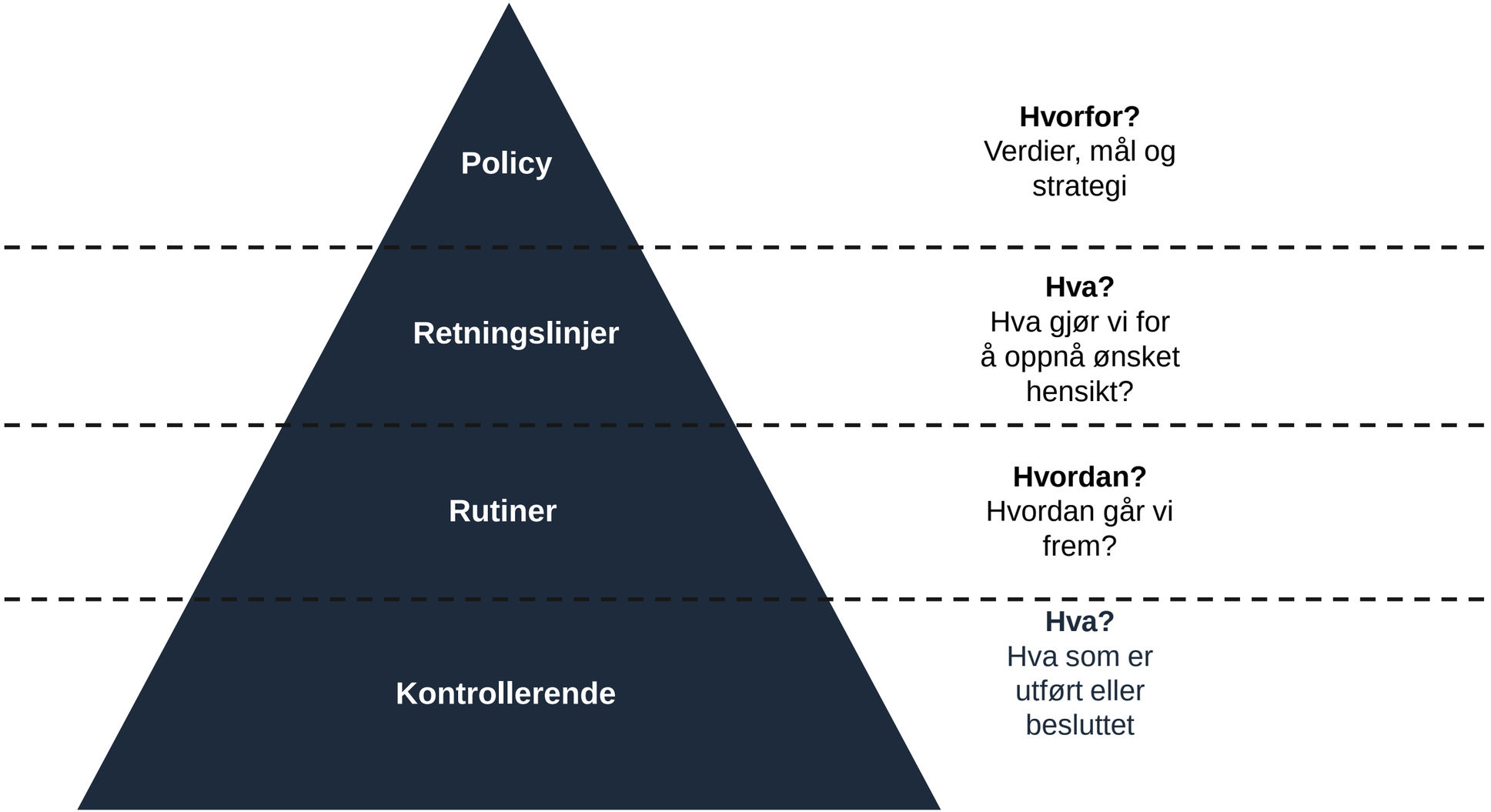
ISO 27001 | Sikkerhetsloven | ØVI 2021 | Samfunnssikkerhetsintr. | NSMs grunnprinsipper


Årsak
Konsekvens
Uønsket hendelse
Forebyggende tiltak
Skadebegrensende tiltak

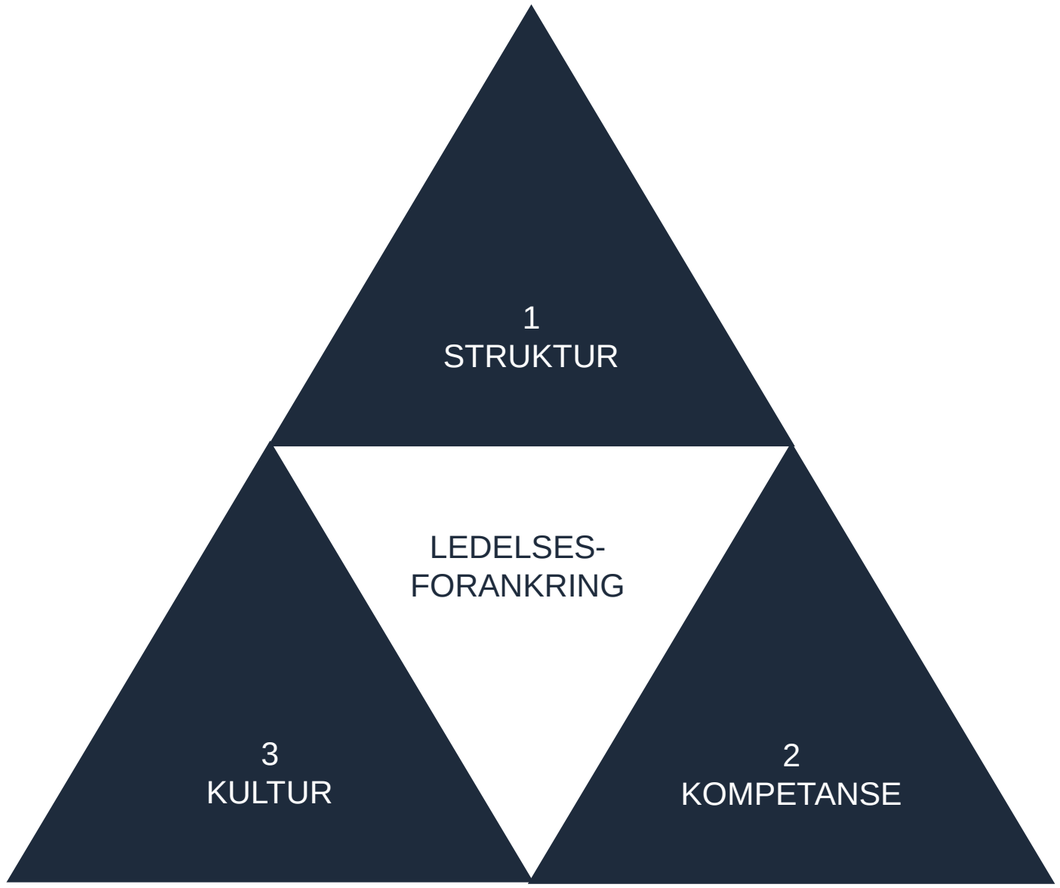
Reason, 2000

Verdikjede for sikkerhet og beredskap

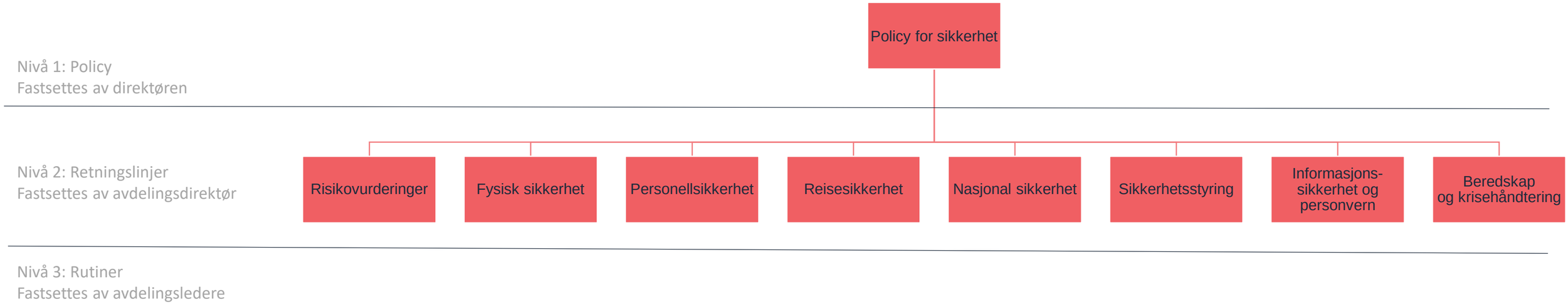



Policy
Retningslinjer
Rutiner
Kontrollerende
Hvorfor?
Verdier, mål og strategi
Hva?
Hva gjør vi for å oppnå ønsket hensikt?
Hvordan?
Hvordan går vi frem?
Hva?
Hva som er utført eller besluttet

Bærende elementer i sikkerhetsarbeidet

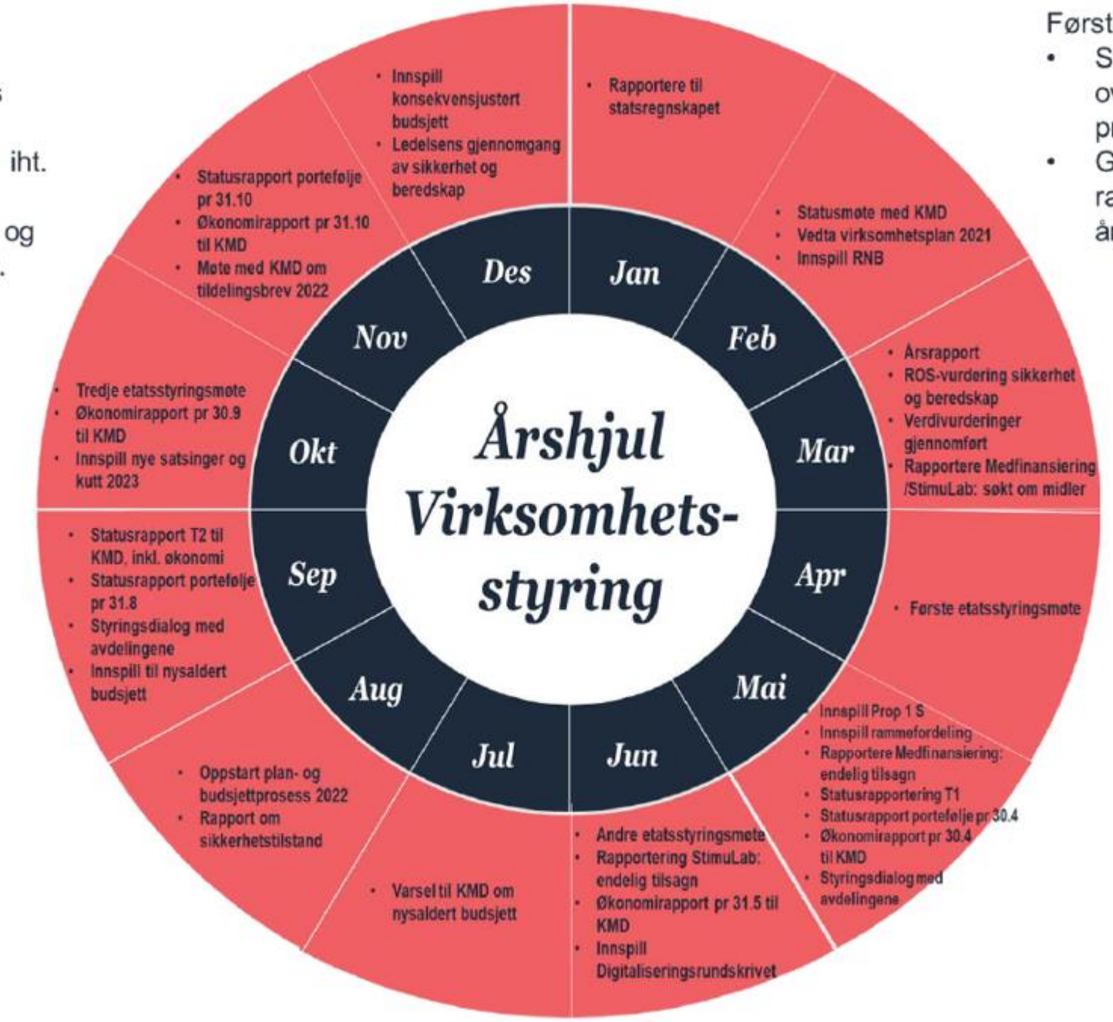


Styrende dokumenter for sikkerhet



Andre halvår:

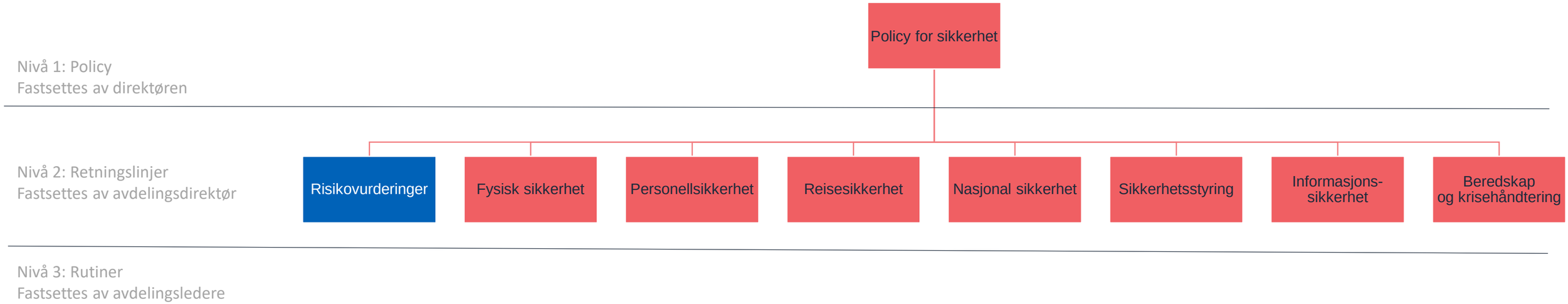
- Plan- og budsjettprosess kommende år
- Satsingsforslag iht. prioriteringer
- Gjennomføring og rapportering iht. årets plan



Første halvår:

- Strategiprosess/ overordnende prioriteringer
- Gjennomføring og rapportering iht. årets plan

Risikovurderinger



Leverandør

Digdir

digdir.no

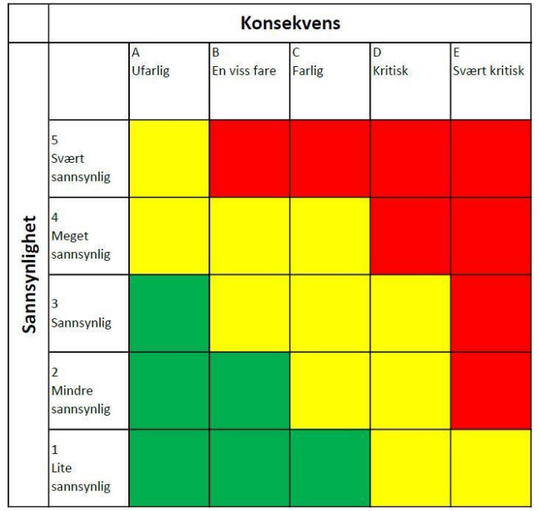
Leverandør av digitale fellesløsninger med ansvar for forvaltning, videreutvikling og utbredelse

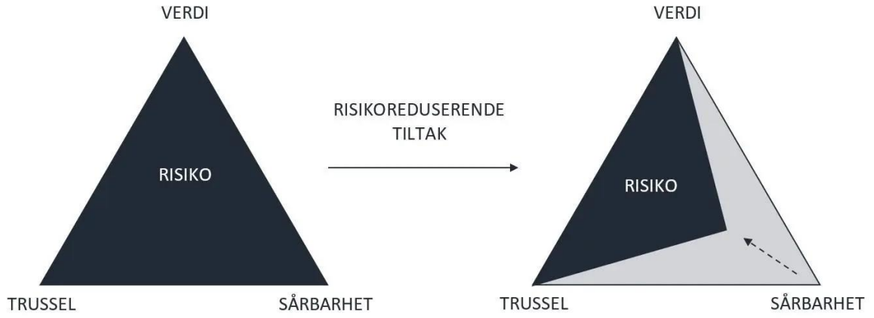
Verdiområder

1. Digdirs samfunnsoppdrag
   a) Samfunnskritiske nasjonale fellesløsninger (Altinn, ID-porten, Digital postkasse og Kontakt- og reservasjonsregisteret)
   b) Andre nasjonale fellesløsninger (eInnsyn, ELMA, eSignering, Maskinporten, eFormidling og Felles datakatalog)
   c) Legger premisser, samordner og er pådriver for digitalisering
   d) Setter i verk tiltak, prosjekter og handlingsplaner i tråd med vedtatt politikk
   e) Føre tilsyn med universell utforming av nett, apper og automater
2. Menneskers liv, helse og personvern
3. Økonomiske og materielle verdier
4. Omdømme

Metodikk for risikovurderinger

- For tilsiktede handlinger og utilsiktede hendelser
- Verdivurderinger
- Konsekvenstabell
- Sannsynlighetsskala
- Sårbarhetsvurderinger
- Trusselvurderinger
- Risikoregister





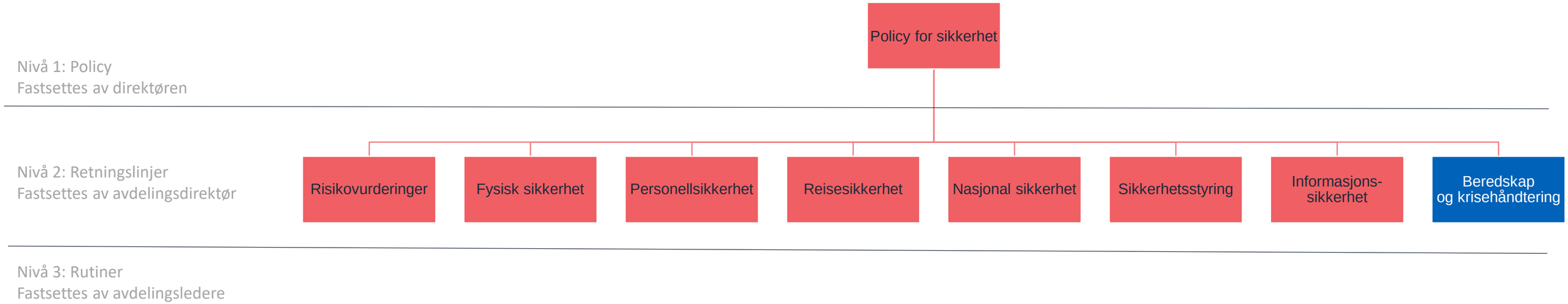
Digdir

Konsekvenstabell

digdir.no

	Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
1. A Samfunnsoppdrag – Samfunnskritiske nasjonale fellesløsninger					
1. B Samfunnsoppdrag – Andre nasjonale fellesløsninger					
1. C Samfunnsoppdrag - Legger premisser, samordner og er pådriver for digitalisering					
1. D Samfunnsoppdrag - Setter i verk tiltak, prosjekter og handlingsplaner i tråd med vedtatt politikk					
1. E Samfunnsoppdrag - Føre tilsyn med universell utforming av nett, apper og automater					
2. A Personvern					
2. B Menneskers liv og helse					
4. Økonomiske og materielle verdier					
5. Omdømme					

Beredskap og krisehåndtering



Beredskapsutvikling i Digdir - 2024

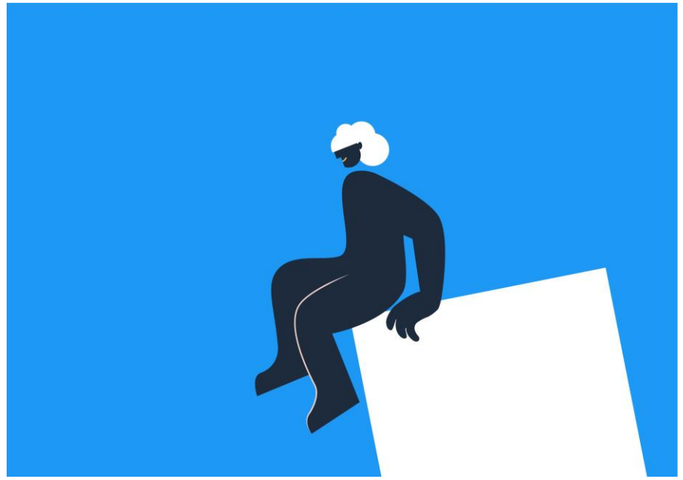
Ambisjon:

Et oppdatert, brukervennlig og relevant beredskapsplanverk og reell håndteringsevne på alle nivåer i kriseorganisasjonen

Beredskapsutvikling i Digdir - 2024

Beredskapsplanverket:

- Roller og ansvar
  - Nivådelt krisehåndtering
  - Krisehåndteringsmetodikk
- Krav til kompetanse
  - opplæring, trening og øvelser
- Erfaringer fra øvelser og hendelser er innarbeidet
- Basert på beredskapsanalyse som gir grunnlag for organisering og dimensjonering av beredskapen
- Samvirkeaktører
- Tilgjengelig i CIM



Alle deltakere i kriseledelsen har da:

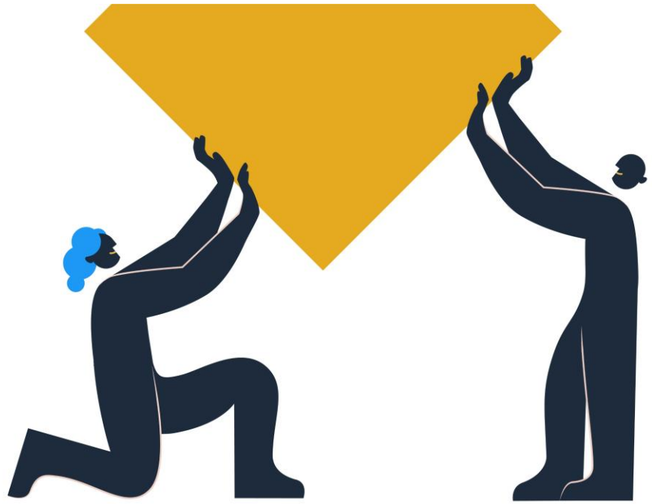
- Gjennomført grunnkurs i beredskap og krisehåndtering
- Deltatt i obligatoriske treninger og øvelser
- Ferdigheter i egen rolle i kriseorganisasjonen
- Ferdigheter i bruk av CIM i kriseorganisasjonen

Plan for beredskapsutvikling i Digdir

1. Innmelding av uønskede hendelser
   - Teknisk løsning (intranett/Teams)
   - Etablere rutiner
2. Policy for sikkerhet og beredskap
3. Retningslinje for beredskap og krisehåndtering
   - Krav til beredskap og kontinuitet
   - Kriseledelse og kriseorganisasjon
   - Opplæring, trening og øvelser
4. Table-top for kriseledelsen
   - Nivådelt kriseorganisasjon
   - Krisehåndteringsmetodikk
   - Fra normal drift til krisehåndtering
5. Rutine for etablering av kriseledelse
6. Avdelingsvise og lokale beredskapsplaner
7. IKT-verktøy for beredskap og krisehåndtering (CIM)

Plan for beredskapsutvikling i Digdir (forts.)

8. Opplæring av kriseledelsen
   - Krisehåndteringsmetodikk
   - CIM i egen rolle
9. Varslingsøvelser
   - Varsling, loggføring og innkalling
10. Krisekommunikasjonsplan
11. Ansatt- og pårørendeberedskap
12. Table-top for kriseledelsen
    - Samspill mellom strategisk og operasjonell kriseledelse
13. Deltakelse i øvelser for sektoren
14. Deltakelse i nasjonale øvelser



Digdir

digdir.no

Spørsmål?