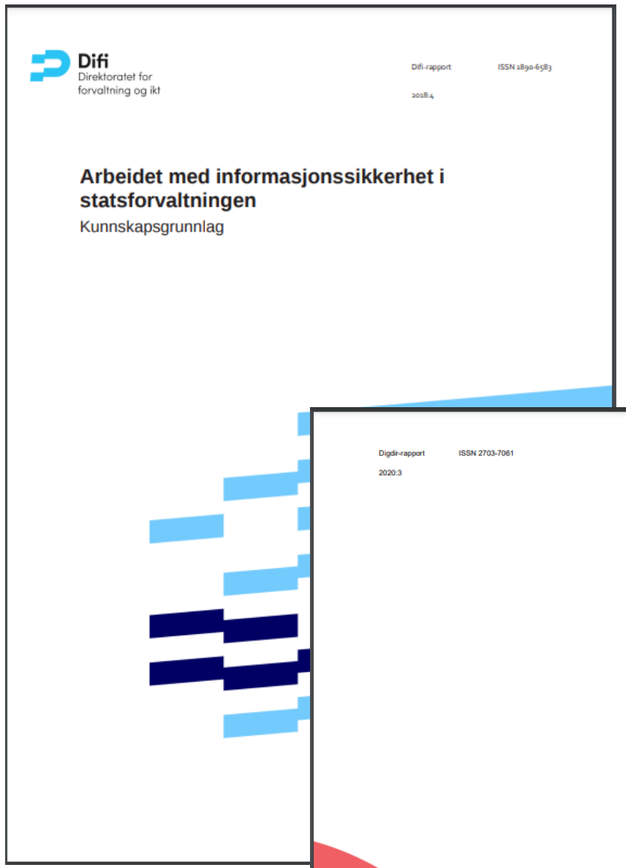
Digdir

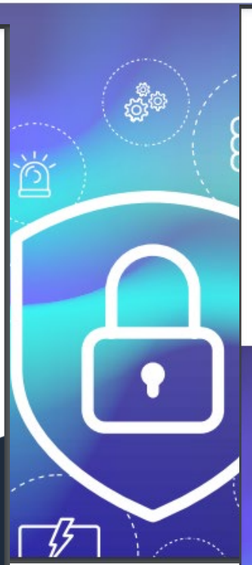
digdir.no

Helhetlig styring og kontroll av informasjonssikkerhet

KiNS-konferansen 2021
21. oktober
Kjetil Korslien

Digdir Utfordringsbildet





Oppfølging av Difi rapport 2018:4

- Fem fokusområder:
  - Informasjonssikkerhet i styringsdialogen
  - Øvelser for bedre informasjonssikkerhet
  - Sikkerhetskultur
  - Kompetanse
  - Styring og kontroll av informasjonssikkerhet

NASJONAL SIKKERHETSMYNDIGHET

Direktoratet for forvaltning og økonomistyring

NorSIS Norsk senter for informasjonssikring

dsb

Digdir

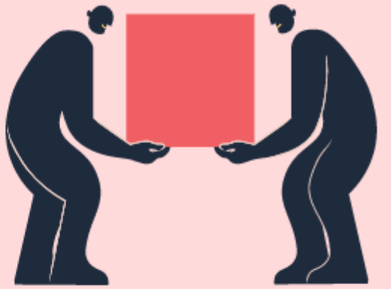
Helhetlig styring og kontroll

- Utviklet av Digdir, NSM og DFØ
  - Dialog med Datatilsynet og KS m/kvalitetssikring underveis

Helhetlig styring og kontroll av informasjonssikkerhet | Digdir

Helhetlig styring og kontroll av informasjonssikkerhet

For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Her kan du lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.



Hva vil det si?

Å jobbe helhetlig betyr at man skal se sammenhengen mellom viktige områder og aktiviteter i virksomheten.

Hva er felles?

De samme grunnreglene gjelder uavhengig av hvilket fagområde man skal drive styring og kontroll på. Les mer om fellestrekkene her.

Hva er ulikt?

Helheten er ikke den samme for alle, og ulike perspektiver gir ulikt fokus. Les mer om noe av det som må tas hensyn til dersom man skal lykkes med å jobbe helhetlig.

Hvor får du hjelp?

Aktører som veileder innen styring og kontroll

DFØ, Digitaliseringsdirektoratet, KS, NSM og Datatilsynet har alle veiledning som er relevant når man jobber med ulike deler av informasjonssikkerhet.

→

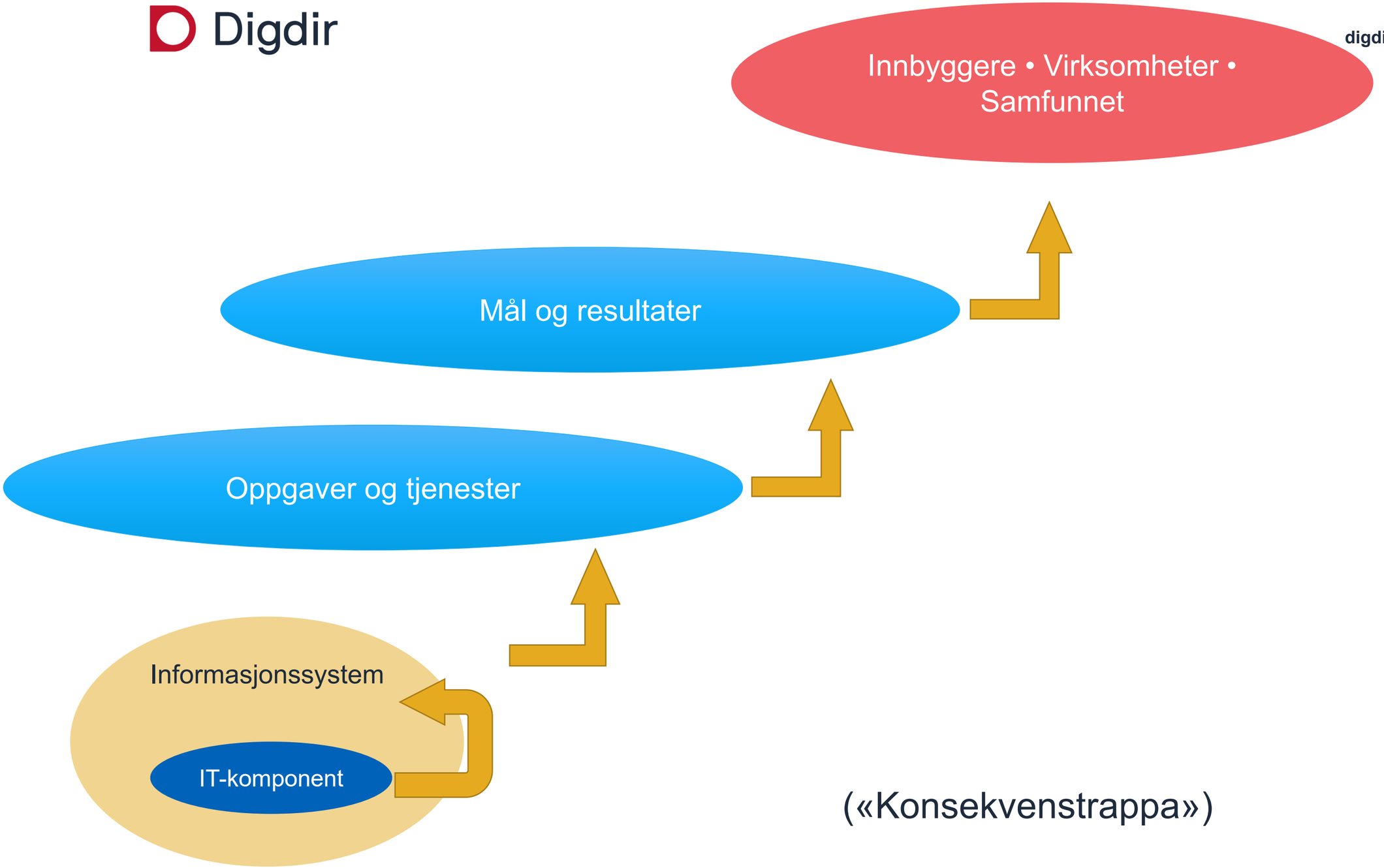
Om denne veiledningen

Denne veiledningen er resultatet av et samarbeid mellom NSM, DFØ og Digitaliseringsdirektoratet. Datatilsynet og KS har også bidratt i arbeidet.

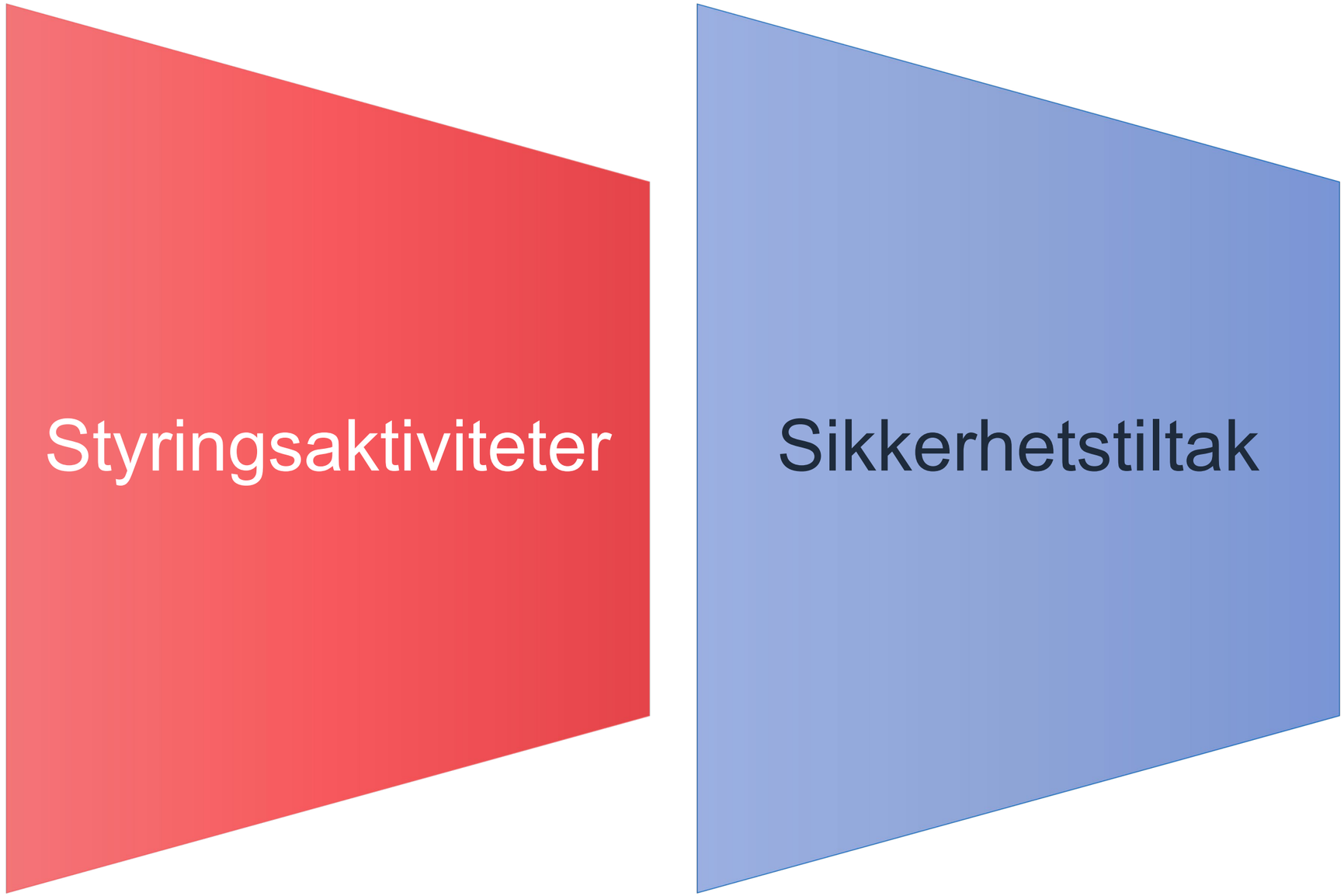
→

Digdir

digdir.no



(«Konsekvenstrappa»)

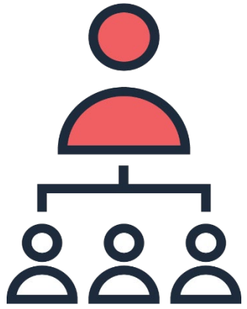

Styringsaktiviteter
Sikkerhetstiltak

Digdir

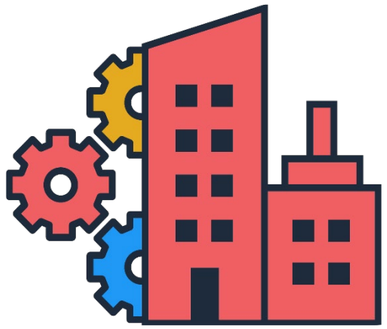
digdir.no

Fellestrekk for styring og kontroll

Ledelsen må lede an



Ha tydelige roller og ansvar

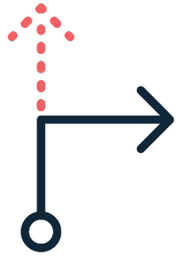


Jobb systematisk

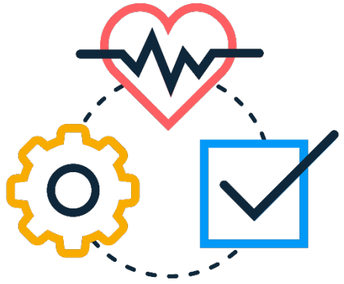
Jobb risikobasert

Bygg riktig kompetanse og en god kultur

Gjennomfør ledelsens gjennomgang

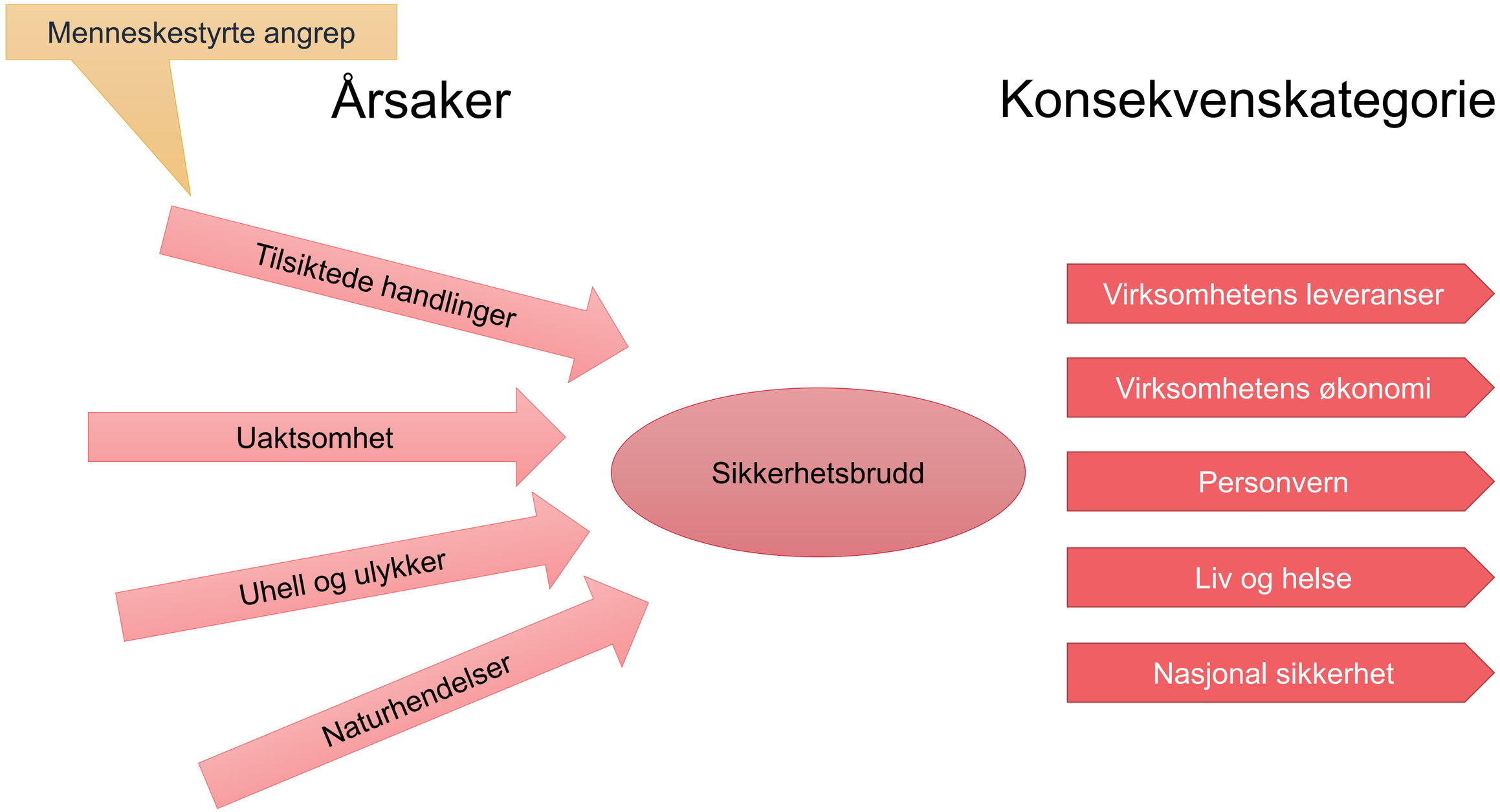


Gjennomfør evalueringer

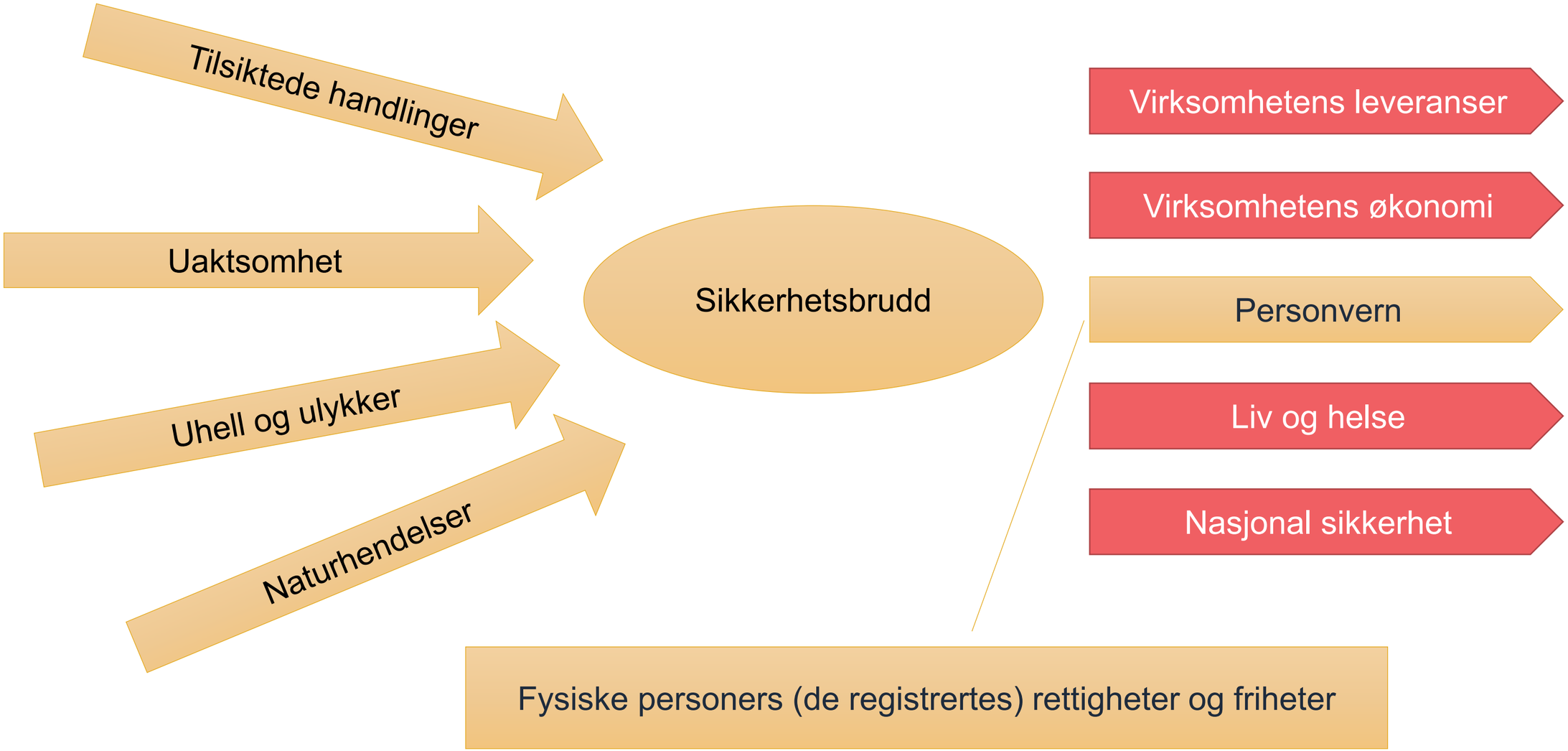


Sørg for kontinuerlig forbedring

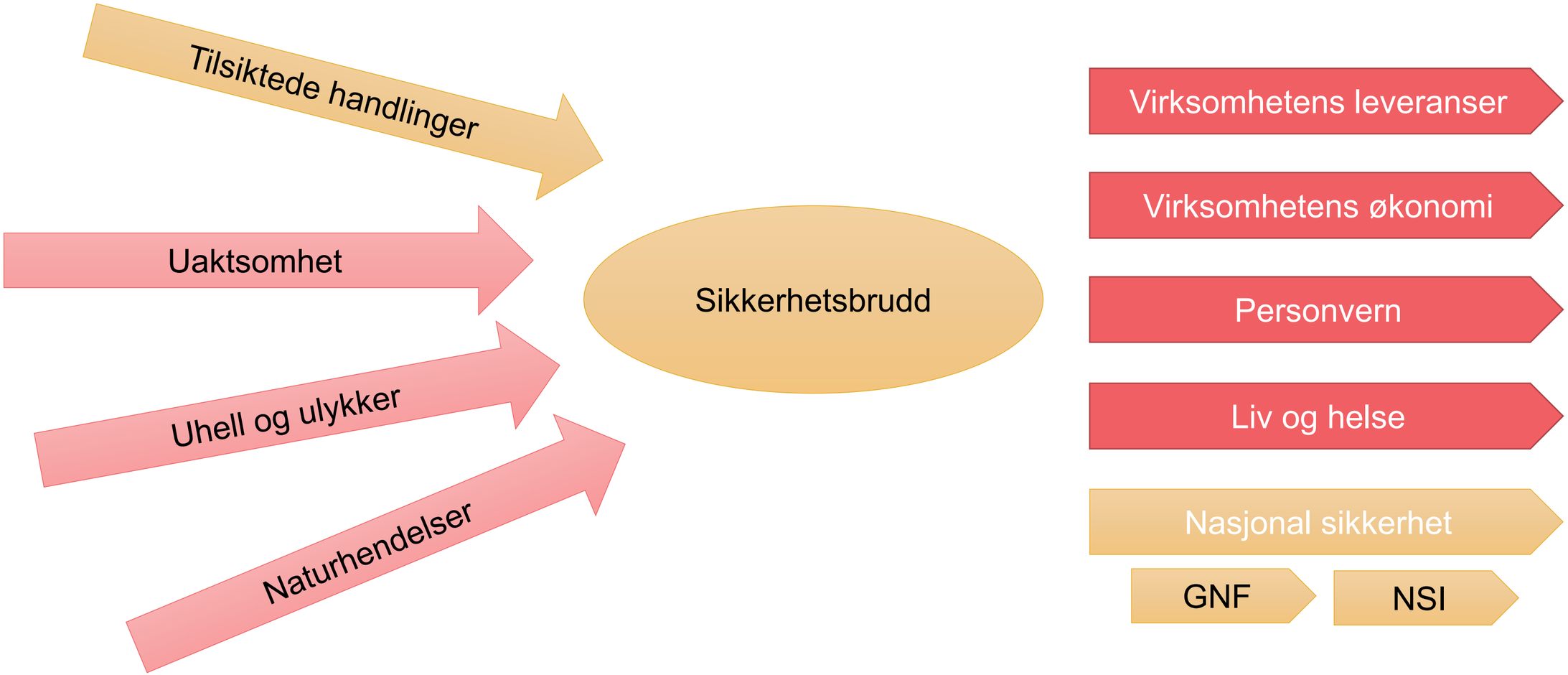
Ulike perspektiver gir ulikt fokus


Menneskestyrte angrep
Årsaker
Konsekvenskategorier
Tilsiktede handlinger
Uaktsomhet
Uhell og ulykker
Naturhendelser
Sikkerhetsbrudd
Virksomhetens leveranser
Virksomhetens økonomi
Personvern
Liv og helse
Nasjonal sikkerhet

Personopplysningsloven m/personvernforordningen

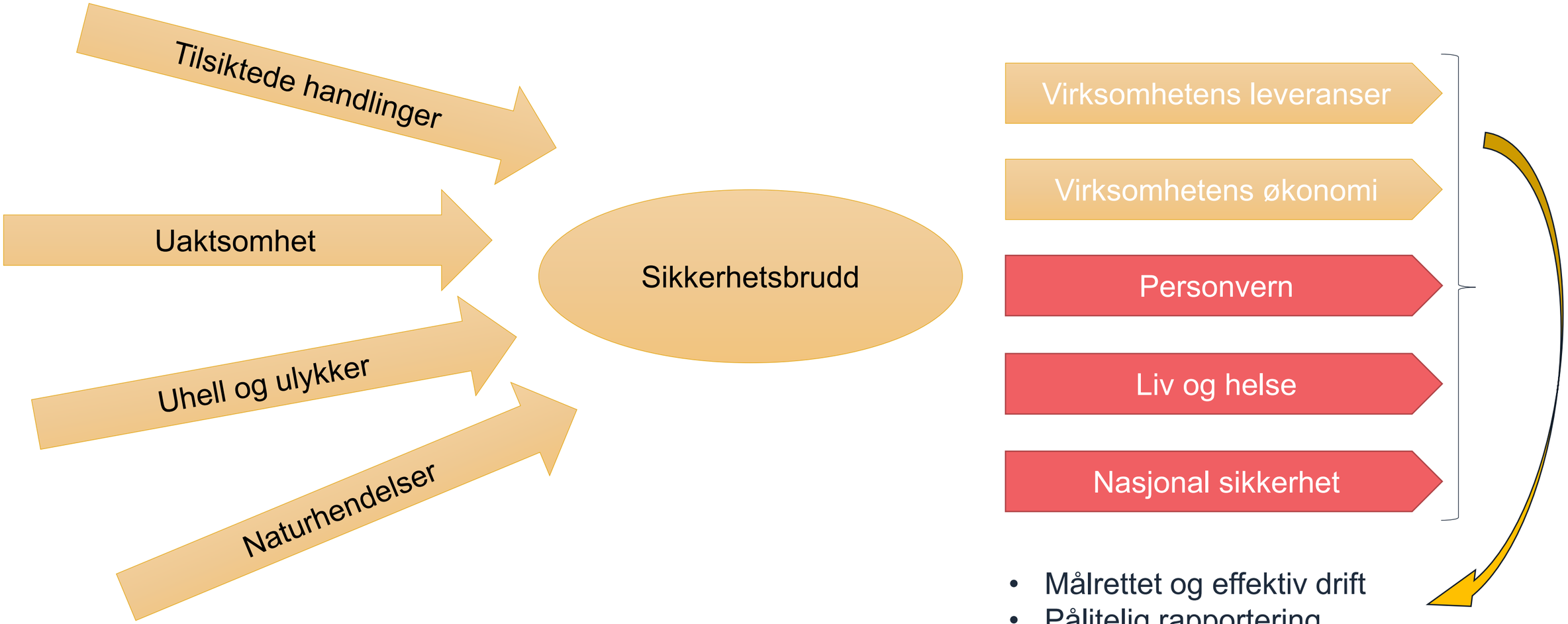


Lov om nasjonal sikkerhet (sikkerhetsloven)



Obs: konseptuell forståelse. Det er f.eks. krav om å sikre at informasjonssystem fungerer slik de skal i sl § 6-2 a.
GNF = Grunnleggende nasjonale funksjoner
NSI = Nasjonale sikkerhetsinteresser

Øk-regelverket i staten / Kommunelovens bestemmelser og egenkontroll og internkontroll



- Målrettet og effektiv drift
- Pålitelig rapportering
- Overholdelse av lover og regler

Tilstand i kommunene

Vi ser forbedring i kommunene

	2020	2021
Evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet	61,2	62,4
Etablert nye sikkerhetstiltak	74,5	80,9
Forbedret eller fjernet sikkerhetstiltak	72,9	80,1
Rapportert erfaringer fra håndtering av uønskede hendelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten	54,8	59,5
Rapportert erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten	25,8	28,5

Kilde: Bruk av IKT i offentlig sektor, tabell 12042: Tiltak som del av internkontroll for informasjonssikkerhet 2020-2021

Hjelp til etablering/ forbedring av internkontroll

Digdir

digdir.no

Stifinneren

https://www.digdir.no/informasjonssikkerhet/stifinneren/2620

Hva er Stifinneren?

- Etablering
- Etapper
- Enkel vei til mål

Kurs i Stifinnerens etappe 1 og 2

- 26. november.
- Hvor er vi? Hvor skal vi?
  - Analyse av status
  - Plan for etablering/forbedring
- Hvordan skal ting fungere hos oss?
  - Utforme føringer
  - Få på plass fagansvarlig informasjonssikkerhet
  - Etablere rammeverk for dokumentasjon

Digdir

Søk Meny

Hjem › Informasjonssikkerhet › Styring av informasjonssikkerhet › Internkontroll i praksis

Internkontroll i praksis - Informasjonssikkerhet

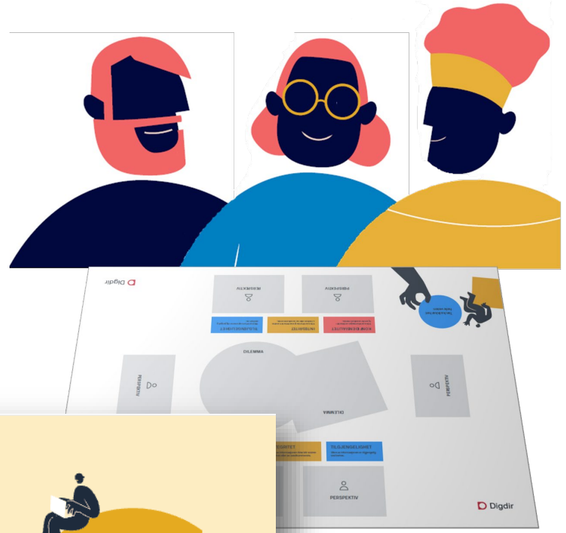
Internkontroll er leders redskap for å styre risiko på informasjonssikkerhetsområdet. Kjernen i internkontrollen er systematiske aktiviteter som gjennomføres av ledere med ansvar for virksomhetens oppgaver og tjenester.

NIFS

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Kompetansebeskrivelser

Ansvar, oppgaver og ønsket kompetanse for roller knyttet til styring og kontroll av informasjonssikkerhet



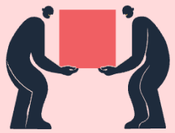
Digdir

Søk Meny

Hjem › Informasjonssikkerhet › Styring av informasjonssikkerhet › Helhetlig styring og kontroll

Helhetlig styring og kontroll av informasjonssikkerhet

For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Her kan du lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.



Hva vil det si?

Å jobbe helhetlig betyr at man skal se sammenhengen mellom viktige områder og aktiviteter i virksomheten.

Hva er felles?

De samme grunnreglene gjelder uavhengig av hvilket fagområde man skal drive styring og kontroll på. Les mer om fellestrekkene her.

Hva er ulikt?

Helheten er ikke den samme for alle, og ulike perspektiver gir ulikt fokus. Les mer om noe av det som må tas hensyn til dersom man skal lykkes med å jobbe helhetlig.

Hvor får du hjelp?

Aktører som veileder innen styring og kontroll

DFØ, Digitaliseringsdirektoratet, KS, NSM og Datatilsynet har alle veiledning som er relevant når man jobber med ulike deler av informasjonssikkerhet.

→

Om denne veiledningen

Denne veiledningen er resultatet av et samarbeid mellom NSM, DFØ og Digitaliseringsdirektoratet. Datatilsynet og KS har også bidratt i arbeidet.

→

Hjem › Informasjonssikkerhet › Kompetanse- og kulturutvikling

Kompetanse- og kulturutvikling innen informasjonssikkerhet

Her finner du veiledning som kan hjelpe deg når du skal arbeide med kompetanse og kultur innen informasjonssikkerhet i din virksomhet.

Kartlegging av digital sikkerhetskultur

Få veiledning om hvordan du kan kartlegge den digitale sikkerhetskulturen i din virksomhet.

Kompetanse- og kulturutvikling innen digital sikkerhet

Få veiledning om hvordan du kan arbeide med utvikling av kompetanse og kultur knyttet til digital sikkerhet.

Virkemidler

Kompetansebeskrivelser

Les om ansvar, arbeidsoppgaver og kompetansebehov for ulike roller innen styring og kontroll av informasjonssikkerhet.

→

Dilemmatrening innen informasjonssikkerhet

Bruk dilemmatrening for å arbeide med kultur og kompetanse.

→

E-læring for ledere

E-læringskurset "Er det sikkert" forteller om leders ansvar for informasjons-sikkerhet, og hvorfor det lønner seg å ta informasjonssikkerhet på alvor.

→

Hjem › Informasjonssikkerhet › Etterlevelse av fire sikkerhetsstandarder › Etablering av sikkerhetsstandardene

Etterlevelse av fire sikkerhetsstandarder

- Etablering av sikkerhetsstandardene
- Testing av etterlevelsen

Veileder for etablering

Her finner du formålet med hver av fire sikkerhetsrelaterte forvaltningsstandarder og hvordan de bør iverksettes på systemene hvor de skal brukes.

På denne siden

- Anbefalte standarder for sikker datakommunikasjon
  - HTTPS med HSTS
- Anbefalt standard for transportsikring av e-post

Digdir

Søk Meny

Hjem › Informasjonssikkerhet › Etterlevelse av fire sikkerhetsstandarder › Testing av etterlevelsen

Etterlevelse av fire sikkerhetsstandarder

- Etablering av sikkerhetsstandardene
- Testing av etterlevelsen

Veileder for testing av etterlevelse

Her beskriver vi hvordan du kan teste etterlevelse av fire sikkerhetsrelaterte forvaltningsstandarder anbefalt i Referansekatalogen for IT-standarder.

Digitaliseringsdirektoratets tilbud

- Internkontroll i praksis – informasjonssikkerhet
  - Stifinneren
  - Fire historier om styring av informasjonssikkerhet
- Helhetlig styring og kontroll av informasjonssikkerhet
- Veiledere og virkemidler til kompetanse- og kulturutvikling innen informasjonssikkerhet
- Kompetansebeskrivelser for roller innen styring og kontroll av informasjonssikkerhet
- Dilemmatrening
- E-læringskurs «Er det sikkert?» på statens læringsplattform

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo