Felles anbefalinger gir samordnet hjelp

Katrine Aam Svendsen, Digdir
Pål Alexander Gaure, KS og Asker Kommune

Hva er Felles sikkerhet i forvaltningen, og felles anbefalinger for styringsaktiviteter?


NSM
Data-
tilsynet
JD
Sektor-
departement
UD
FD
Sektor
etat
Andre
departe-
menter
SD
KMD
Difi
DSB
Sektorvis
respons-
miljø
Nkom
Sektortilsyn
2018

NSM

KS

HDir

Datatilsynet

Økonomireglementet i staten

Digdir

DFØ

Personopplysningsloven

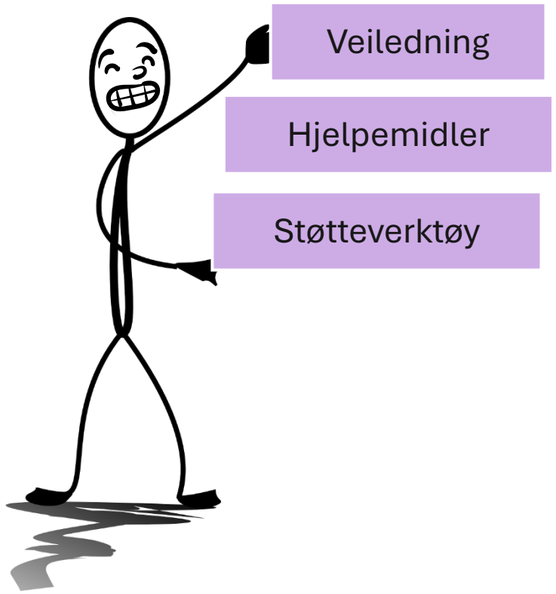
Sikkerhetsloven

eForvaltningsforskriften § 15.2

Kommuneloven

Digitalsikkerhetsloven

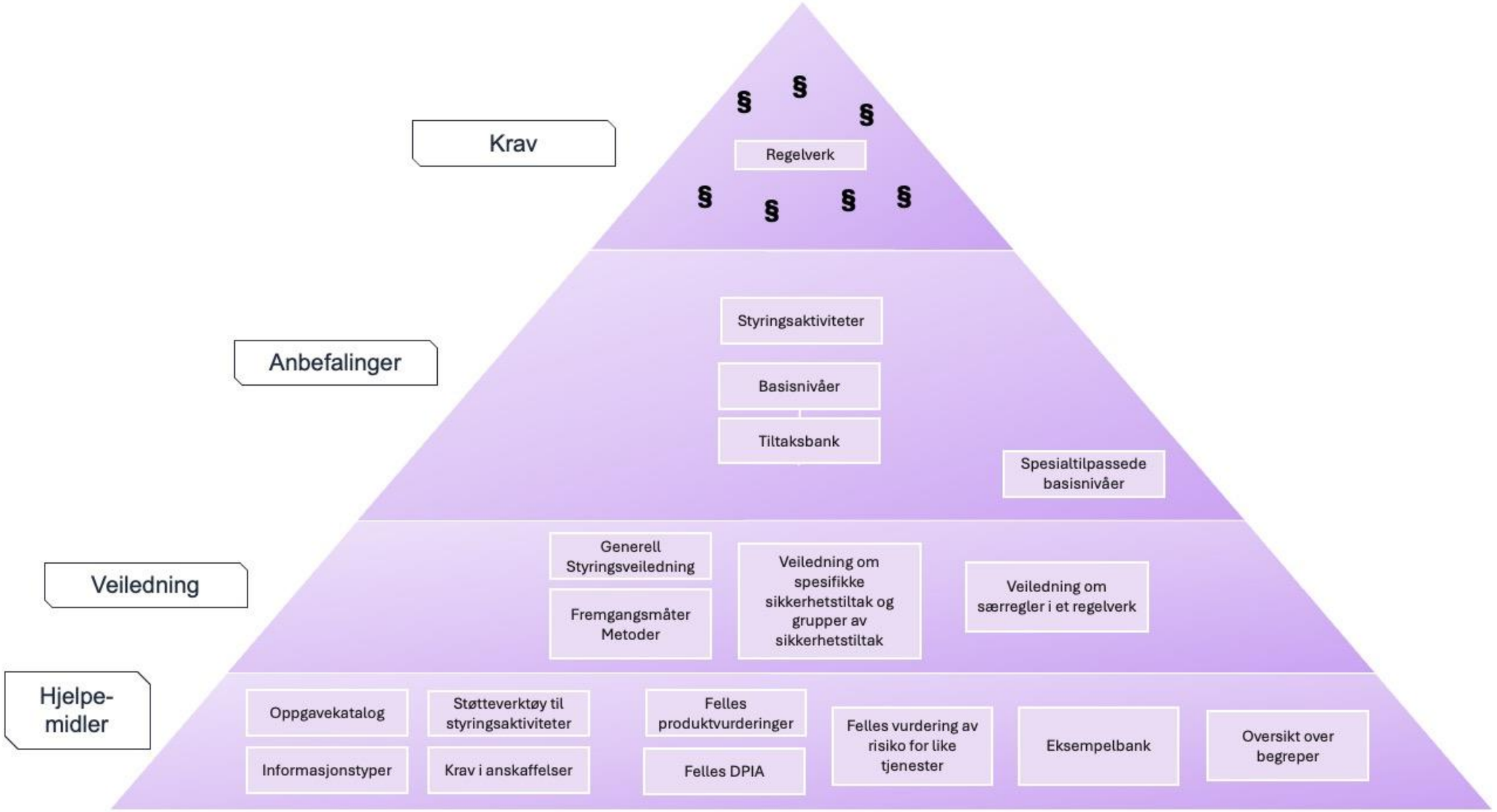
Felles anbefalinger



Veiledning

Hjelpemidler

Støtteverktøy


Krav
§
§
§
Regelverk
§
§
§
§
Anbefalinger
Styringsaktiviteter
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer
Veiledning
Generell Styringsveiledning
Fremgangsmåter Metoder
Veiledning om spesifikke sikkerhetstiltak og grupper av sikkerhetstiltak
Veiledning om særregler i et regelverk
Hjelpe-midler
Oppgavekatalog
Informasjonstyper
Støtteverktøy til styringsaktiviteter
Krav i anskaffelser
Felles produktvurderinger
Felles DPIA
Felles vurdering av risiko for like tjenester
Eksempelbank
Oversikt over begreper

Anbefalinger

NSM

KS

HDir

Datatilsynet

Økonomireglementet i staten

Digdir

DFØ

Personopplysningsloven

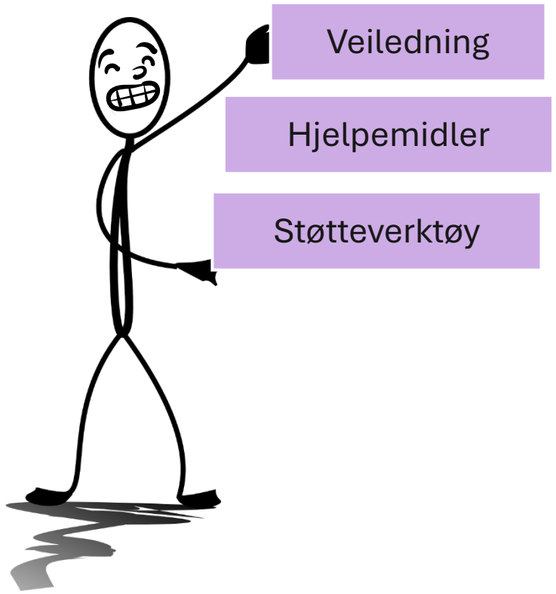
Sikkerhetsloven

eForvaltningsforskriften § 15.2

Kommuneloven

Digitalsikkerhetsloven

Felles anbefalinger



Veiledning

Hjelpemidler

Støtteverktøy

Ledelsens styring og oppfølging

Ha oversikt og prioritere

Vurdering av risiko

Håndtering av risiko

Måling, evaluering og revisjon

Overvåking og hendelseshåndtering

Kompetanse- og kulturutvikling

Anskaffelser og leverandørstyring

Kommunikasjon


Ledelsens styring og oppfølging
Ha oversikt og prioritere
Vurdering av risiko
Håndtering av risiko
Måling, evaluering og revisjon
Overvåking og hendelseshåndtering
Kompetanse- og kulturutvikling
Anskaffelser og leverandørstyring
Kommunikasjon

§ 4-2. *Vurdering av risiko*

Sikkerhetsloven

Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

§ 7. *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

Digitalsikkerhetsloven

En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

§ 10. *Krav om sikkerhet for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Artikkel 32. *Sikkerhet ved behandlingen*

GDPR

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisat
sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

Artikkel 24. *Den behandlingsansvarliges ansvar*

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

RV - Vurdering av risiko

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko på sitt ansv
hvilke risikoer som må håndteres.

Risikoeiere planlegger og gjer
gjøres på oppgaver, tjenester

Vurdering av risiko gjennomfø
risikovurderinger), men også
forbindelse med endringer i o
systemer.

RV-1 Planlegge risikovurdering

Risikoeier skal sørge for at det legges en pl

Planleggingen bør som minimum innehold

- Beskrivelse av omfang og avgrensn
- Valg av deltakere
- Valg av framgangsmåte, inkludert h
- Estimat av ressursbruk
- Hvordan arbeidet skal dokument

Gir evne til

- Effektiv gje omfør g av risi vur
- Å sørg or at rson med rikti
- Å sør for et go beslut sgrun
  sult er

esultat

- Plan or gjennomføring av risikovur

RV-2 Gjennomføre risikovurdering

Risikoeiere skal sørge for nødvendige risikovurderinger blir gj nnomfø . Omfa og innretning på arbeid og metodebruk tilpasses det som skal vurderes.

Når risikoeiere vurderer risiko, skal de benytte resulta foran lyser *Ha over* og *prioritere*, og blant annet ta hensyn til

- hvilke trusler og farer info nasj and i opp ver og tjenester kan bli utsatt for, og hvilke informasjonssikk ets- og p son nbrud det kan føre til

---

- hvilke konsekvense nformas ssikke ets- og personvernbrudd kan få for virksom sten oppga er og tjen virksomhetens økonomi, individer, andre virks heter nfun funksjoner eller nasjonale sikkerhetsinteresser
- allerede tablert kkerhets- og personverntiltak for å forebygge, oppdage og reagere på hendels som an føre til informasjonssikkerhets- eller personvernbrudd

når vurderinger oppdateres kan det være tilstrekkelig å vurdere om det har skjedd endringer som p virker eksisterende vurderinger. For eksempel ny kunnskap om sårbarheter, hvilke hendelser so kan inntreffe, eller hvilke konsekvenser som kan oppstå.

Gir evne til

- Å få oversikt over risiko på et område (oppgave, tjeneste, digitalt system eller annen avgrensing)
- Å ta beslutninger om risiko, inkludert bruk av virksomhetens ressurser på håndtering av risiko

Resultat

- Dokumentert risikovurdering med beslutningsgrunnlag for håndtering av risiko

§ 4-3. *Plikt til å gjennomføre sikkerhetstiltak og øvelser*

Sikkerhetsloven

Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. Slike tiltak kan gjennomføres i sammenheng med andre forebyggende sikkerhetstiltak i virksomheten, så lenge kravene i denne loven oppfylles.

Kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket.

Digitalsikkerhetsloven

§ 7. *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en risikovu
benyttes for å levere tjenesten.

Tilbyderen skal iverksette hensiktsmessige og proporsjonale teknisk
for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva so
til den teknologiske utviklingen.

Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdek
tjenesteleveransen kan opprettholdes.

§ 10. *Krav om sikkerhet for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen og tas hensyn til

a. sikkerheten i systemer, utstyr og anlegg
b. hendelseshåndtering
c. styring av opprettholdelse av tjenesteleveransen
d. overvåking, revisjon og testing
e. anerkjente internasjonale standarder.

Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.

GDPR

Artikkel 32. *Sikkerhet ved behandlingen*

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettighe
friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å
sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

a. pseudonymisering og kryptering av personopplysninger,
b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjene
c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk e
hendelse,
d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisa
sikkerhetstiltak er.

Artikkel 24. *Den behandlingsansvarliges ansvar*

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

RH – Håndtering av risiko

I forlengelse av risikovurderinger, skal virksomheten fatte en beslutning om hvordan de identifiserte risikoene håndteres. Om en risiko må håndteres, skal virksomheten identifisere og velge tiltak, for deretter å iverksette dem.

Virksomheten skal sørge for:

- at det blir avklart hvilke risikoer som
  håndtering. Det siste innebærer at ul
  foreslå håndtering av risikoer
- sørge for at forslag til risikohåndterin
- å iverksette de godkjente tiltakene, o

RH-1 Foreslå håndtering av risikoer

Risikoeiere skal sørge for at det utarbeides forslag til hvordan risikoer som trenger håndtering, skal håndteres.

Arbeidet bør inkludere forslag til
avtaler. Dette skal være identifis
oversikt og prioritere er gjenno

For hver risiko, skal risikoeiere v
redusere risikoen. Kost/nytte av

- risikoreduserende effekt
- direkte økonomisk kostn
- negative sideeffekter

Virksomhetens kriterier for å aks
omfang av tiltak. Der det er behc
plass.

Gir evne til

- å finne sikkerhetstiltak o
  med minst
  g negativ

Resultat

- En liste
  ed sik
  etsti

RH-2 Godkjenne forslag til risikohåndtering

Risikoeier skal vurdere og godkjenne forslagene til håndtering av risiko.

Risikoeier skal:

- Ta stilling til kvaliteten på grunnarbeidet
- Vurdere om restrisiko på forslagene er akseptal
- Vurdere kost/nytte på foreslåtte tiltak
- Sikre finansi
- vurdere beh
- sørge at tilt

Gir evne til

rkset
vur inger

Res t

- Beskr se
  behov:
  området risi
- Ved behov: vurdering om at andre beslutningsta

RH-3 Iverks te godk te til k

Det skal utformes en for g nomfø eller etablering av de godkjente tiltakene, og
ableres en dialog ed de sor gjennomføre arbeidet.

Risikoeier må godk en,

Gir evne til

- å ha oversikt over gjennon
  ansvar for at tiltakene gjer

Resultat

- En plan for gjennomføring

RH-4 Utforme og etablere sikkerhetstiltak

Basert på vurdering av risiko, og beslutninger om hvordan identifisert risiko skal håndteres, sikkerhetstiltak utformes, etableres og forvaltes.

Tiltakene må testes for å sikre at de fungerer etter hensikten. Det bør ut fra behov skje ved utforming, etablering, og forvaltning av sikkerhetstiltak.

Dersom testing under etablering eller forvaltning viser at tiltakene ikke fungerer som tiltenkt, må de justeres. Dette bør inngå forvaltningen av sikkerhetstiltak.

Gir evne til

- redusere identifiserte risikoer ved å utforme og etablere tiltak
- vurdere om etablerte tiltak fungerer slik de skal, og finne ut om eventuelle justeringer behøves.

Resultat

- Etablerte sikkerhetstiltak, og en samlet oversikt over alle tiltak
- Hensiktsmessig dokumentasjon av det enkelte tiltak

Vurdering av risiko

Sikkerhetsloven

§ 4-2, § 4-4 første ledd

Virksomhetssikkerhetsforskriften

§ 12 første ledd

Digitalsikkerhetsloven

[tilbyder av en samfunnsviktig tjeneste] § 7 første ledd, § 6 andre ledd

[tilbyder av en digital tjeneste] § 10 første ledd

GDPR

Artikkel 24.1, 32.1, 35.1-3, 35.7-10

…

Håndtering av risiko

Sikkerhetsloven

§ 4-3 første og annet ledd, §§ 5-2, 5-4, 6-2, 7-3

Virksomhetssikkerhetsforskriften

§§ 13, 14, 22, 49, 58

Digitalsikkerhetsloven

[tilbyder av en samfunnsviktig tjeneste] § 7 andre og tredje ledd

[tilbyder av en digital tjeneste] § 10 første ledd

GDPR

Artikkel 24.1-2, 25.1-2, 32.1-2, 32.4

…

Ledelsens styring og oppfølging

Ha oversikt og prioritere

Vurdering av risiko

Håndtering av risiko

Måling, evaluering og revisjon

Overvåking og hendelseshåndtering

Kompetanse- og kulturutvikling

Anskaffelser og leverandørstyring

Kommunikasjon

NSM

KS

HDir

Datatilsynet

Økonomireglementet i staten

Digdir

DFØ

Personopplysningsloven

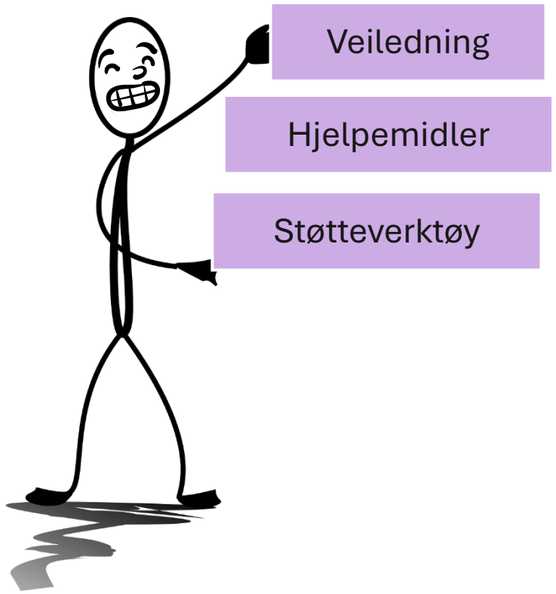
Sikkerhetsloven

eForvaltningsforskriften § 15.2

Kommuneloven

Digitalsikkerhetsloven

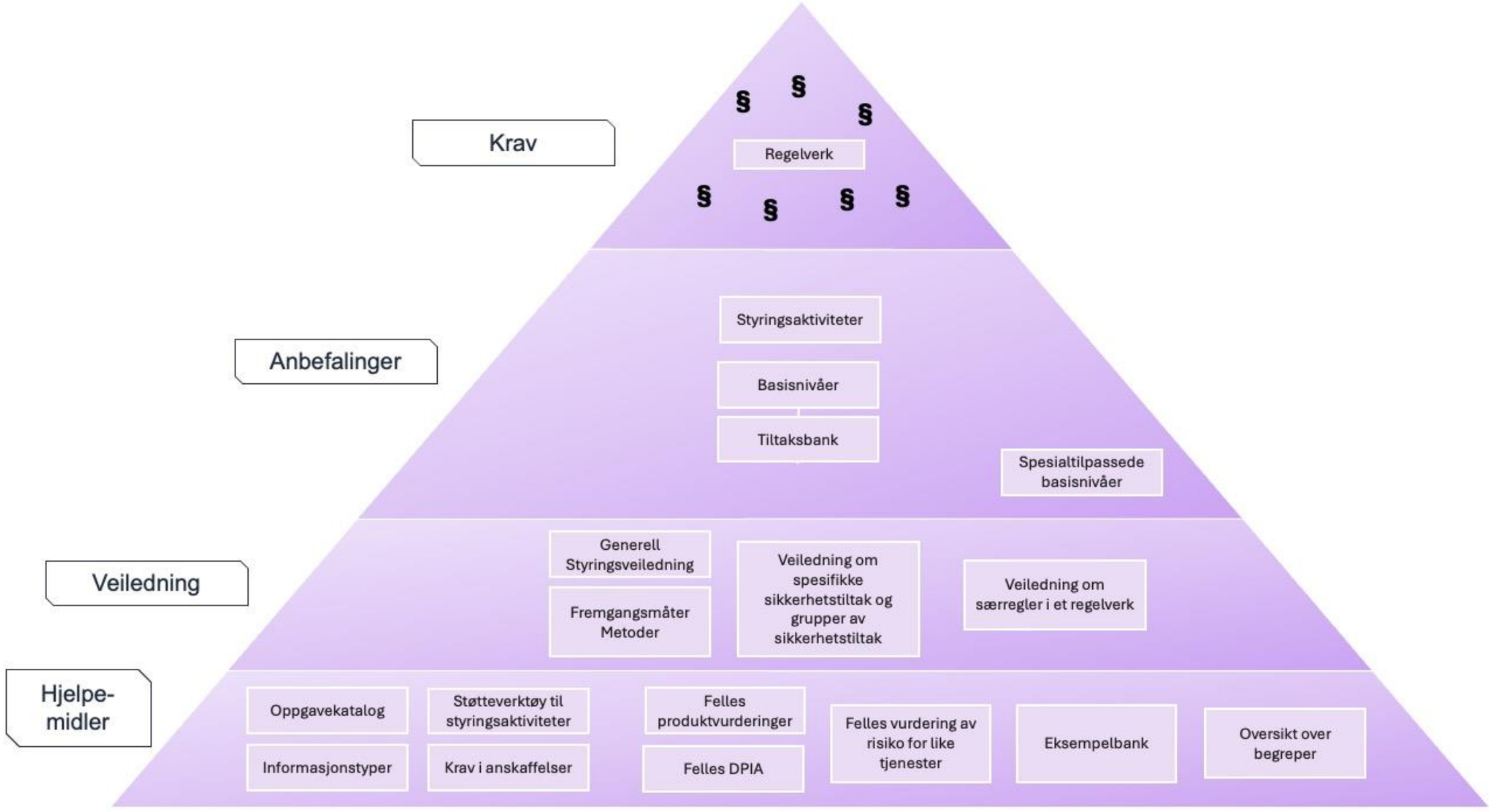
Felles anbefalinger

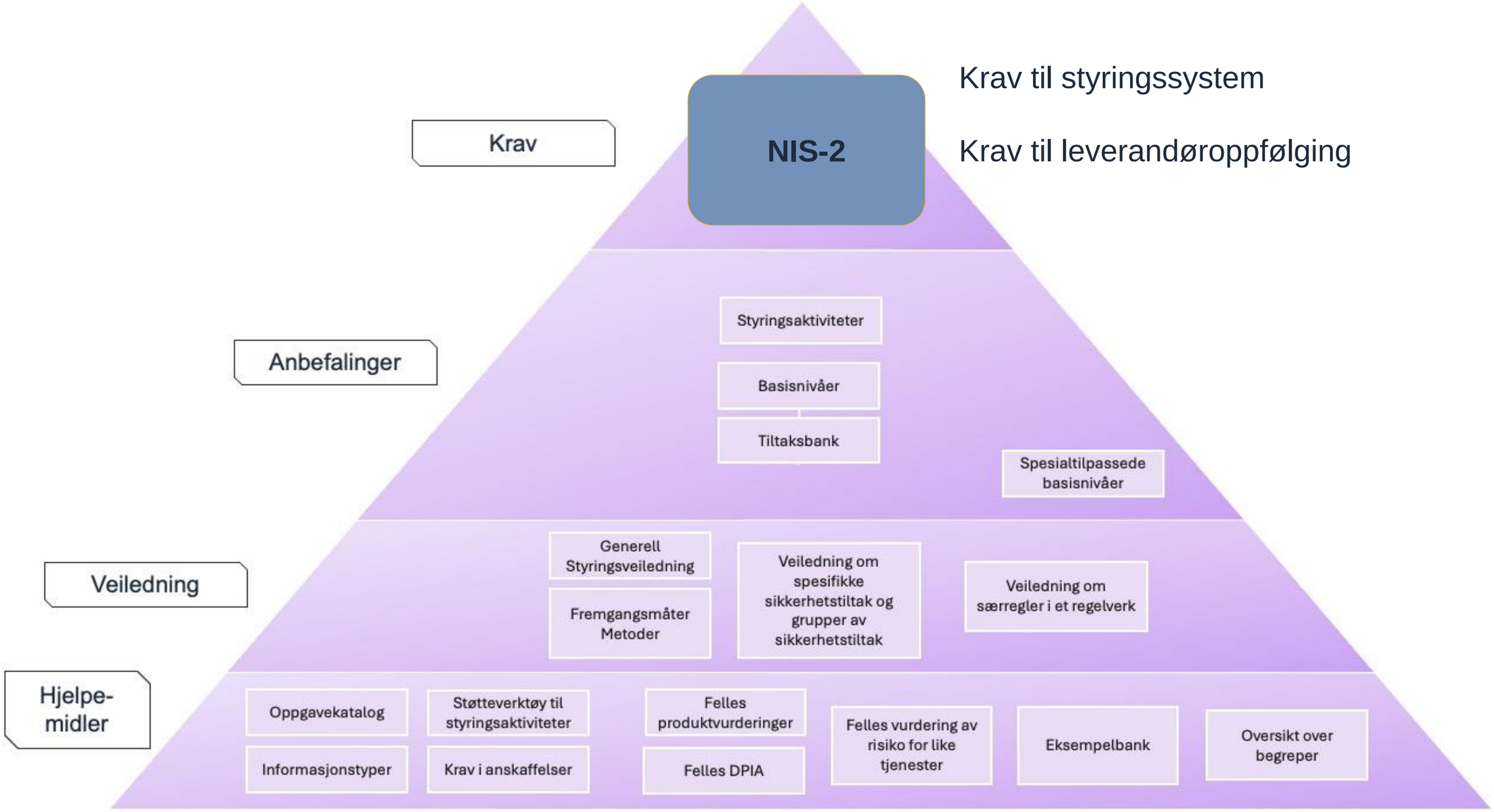


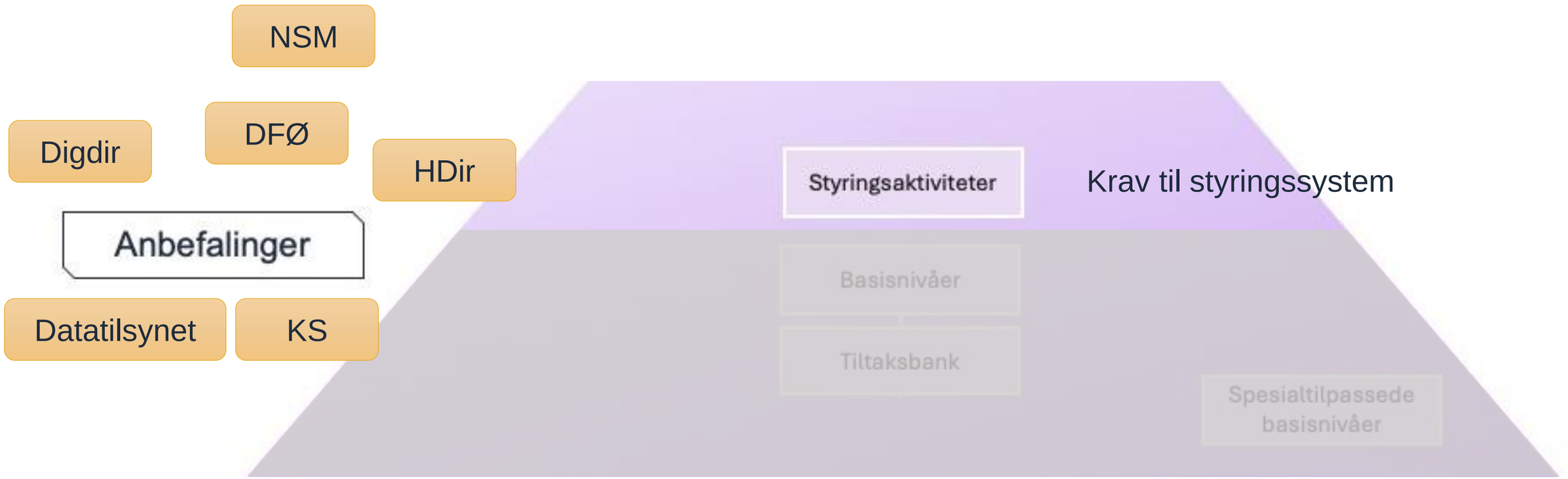
Veiledning

Hjelpemidler

Støtteverktøy

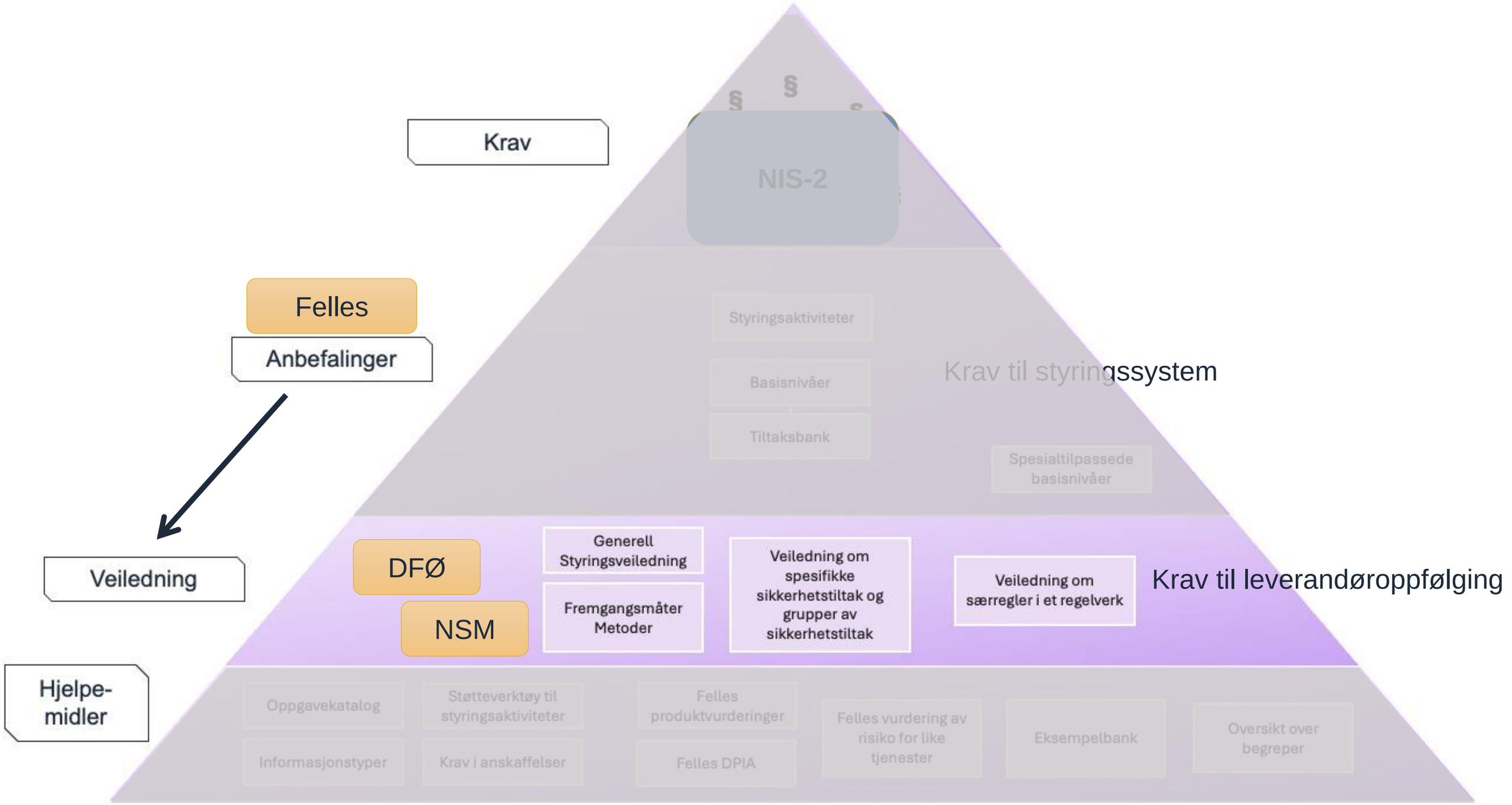

Krav
§ § § § § § §
Regelverk
Anbefalinger
Styringsaktiviteter
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer
Veiledning
Generell Styringsveiledning
Fremgangsmåter Metoder
Veiledning om spesifikke sikkerhetstiltak og grupper av sikkerhetstiltak
Veiledning om særregler i et regelverk
Hjelpe-midler
Oppgavekatalog
Støtteverktøy til styringsaktiviteter
Felles produktvurderinger
Felles vurdering av risiko for like tjenester
Eksempelbank
Oversikt over begreper
Informasjonstyper
Krav i anskaffelser
Felles DPIA


Krav
NIS-2
Krav til styringssystem
Krav til leverandøroppfølging
Anbefalinger
Styringsaktiviteter
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer
Veiledning
Generell Styringsveiledning
Fremgangsmåter Metoder
Veiledning om spesifikke sikkerhetstiltak og grupper av sikkerhetstiltak
Veiledning om særregler i et regelverk
Hjelpe-midler
Oppgavekatalog
Støtteverktøy til styringsaktiviteter
Felles produktvurderinger
Felles vurdering av risiko for like tjenester
Eksempelbank
Oversikt over begreper
Informasjonstyper
Krav i anskaffelser
Felles DPIA


NSM
DFØ
Digdir
HDir
Anbefalinger
Datatilsynet
KS
Styringsaktiviteter
Krav til styringssystem
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer

Felles

Anbefalinger


Krav
NIS-2
Felles
Anbefalinger
Styringsaktiviteter
Basisnivåer
Tiltaksbank
Spesialtilpassede basisnivåer
Krav til styringssystem
Veiledning
DFØ
NSM
Generell Styringsveiledning
Fremgangsmåter Metoder
Veiledning om spesifikke sikkerhetstiltak og grupper av sikkerhetstiltak
Veiledning om særregler i et regelverk
Krav til leverandøroppfølging
Hjelpe-midler
Oppgavekatalog
Støtteverktøy til styringsaktiviteter
Felles produktvurderinger
Felles vurdering av risiko for like tjenester
Eksempelbank
Oversikt over begreper
Informasjonstyper
Krav i anskaffelser
Felles DPIA

Hjelpemidler fra KS

-

Hjelpemidler fra KS

- 357 kommuner må operasjonalisere «pyramiden»
  - Inn i (dagens) applikasjoner fra et dusin leverandører
  - Inn i digitaliserte informasjonsmodeller
    - som kan utnytte KI-metoder på tvers av siloer og på tvers av kommuner
  - slik at 357 kommuner slutter å
    - vurdere M365 357 ganger
    - 357 kommuner ber om 357 erklæringer fra samme leverandør

Med FSIF får 357 kommuner redusert antall overordnede føringer om personopplysningsvern og informasjonssikkerhet. Da får vi tid til å jobbe med konkrete tiltak. En **kommune vil heller beskytte et vannverk enn å diskutere** hvilken veiledningsaktør som har den beste veiledningen.

Jeg ser også frem til at KS raskere kan oppdatere veilederen for kommunedirektørene når det kommer nye lovkrav. FSIF tar det som er felles og KS kan konsentrere seg om det som er spesifikt for sektoren.

Takk for oss!

Spørsmål, innspill eller kommentarer?
infosikkerhet@digdir.no

digdir.no/fsif

NSM Datatilsynet Digdir KS dfø Helsedirektoratet