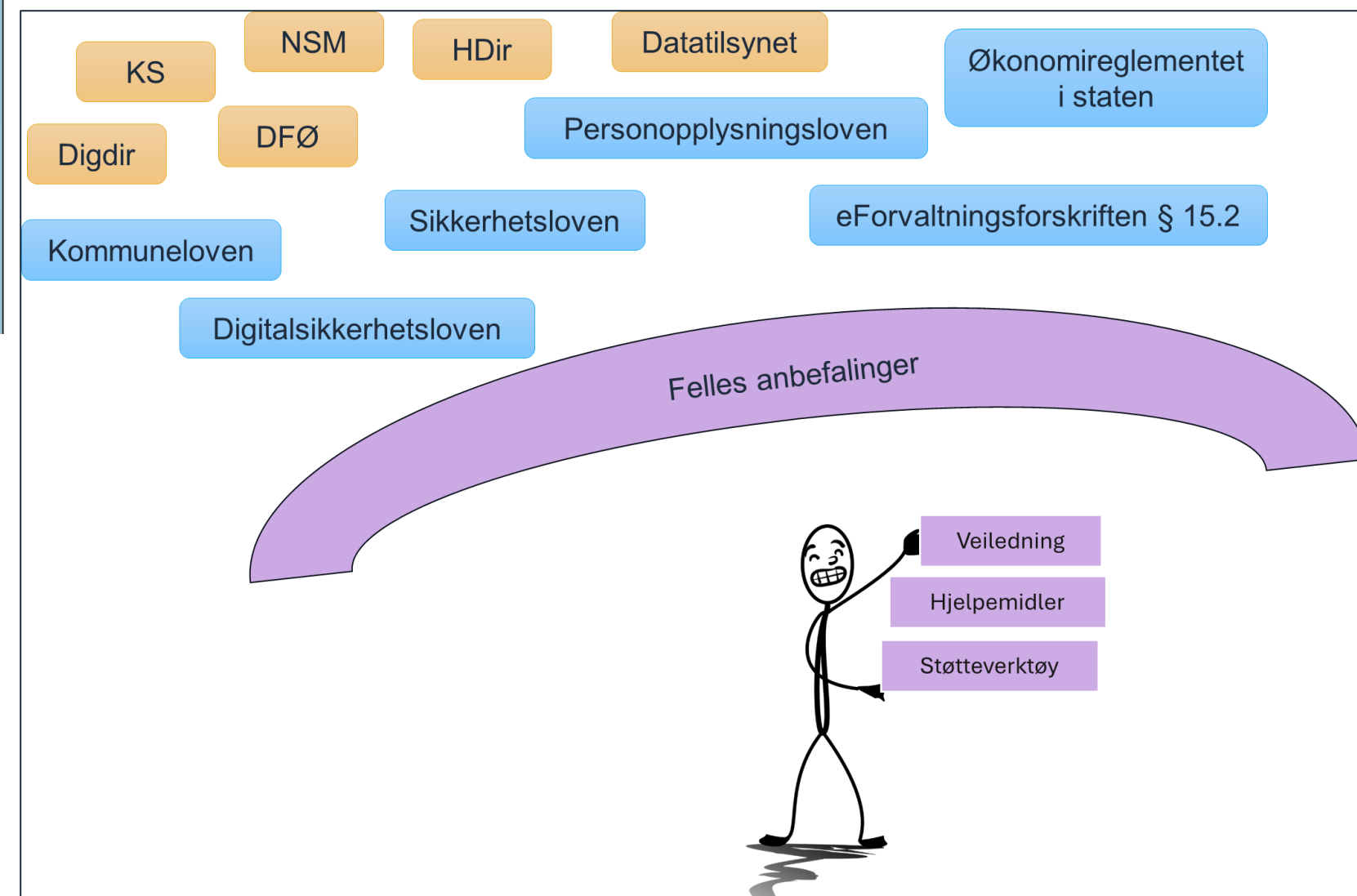
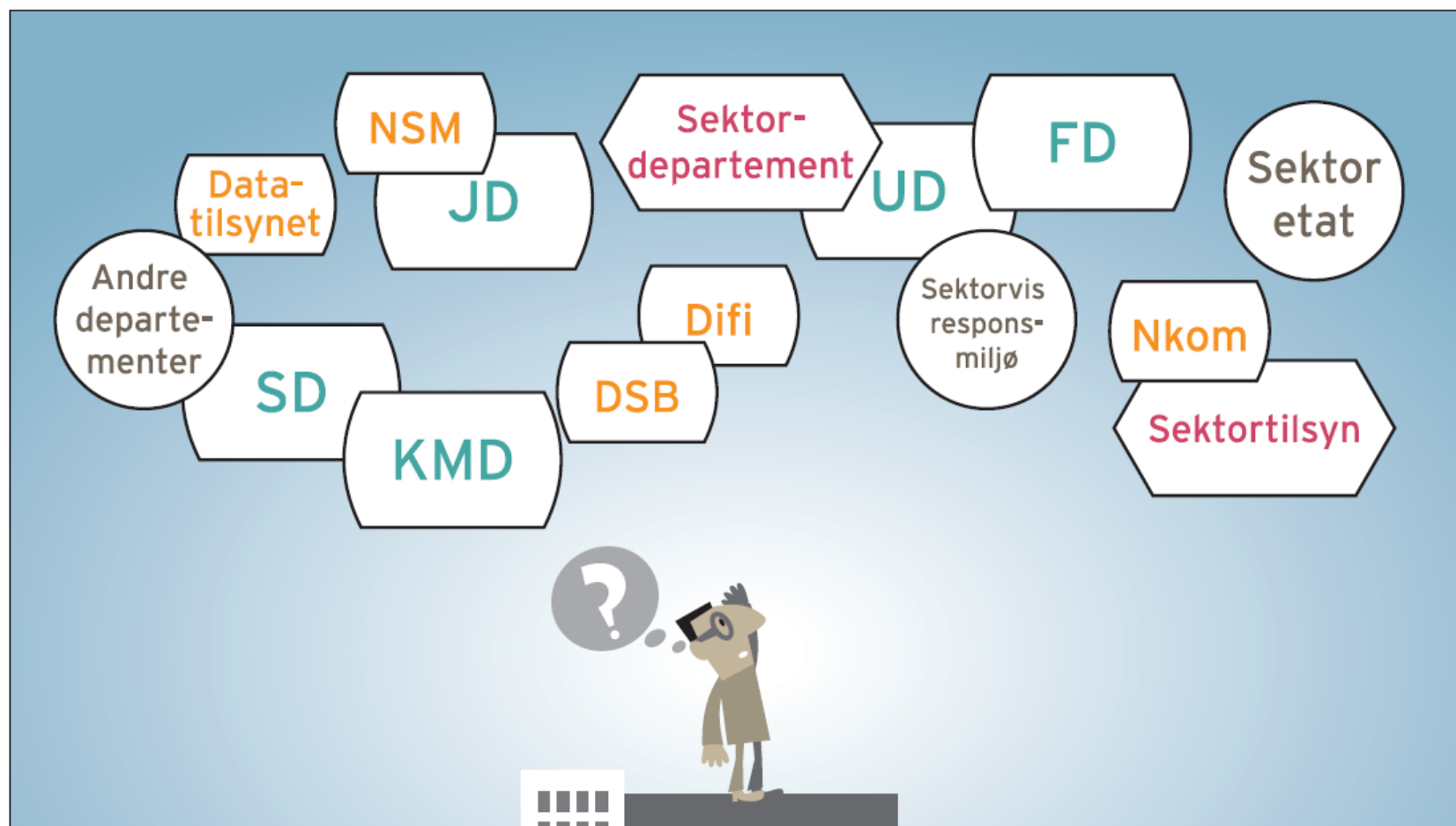


Anbefalinger for styring av informasjonssikkerhet og personopplysningsvern





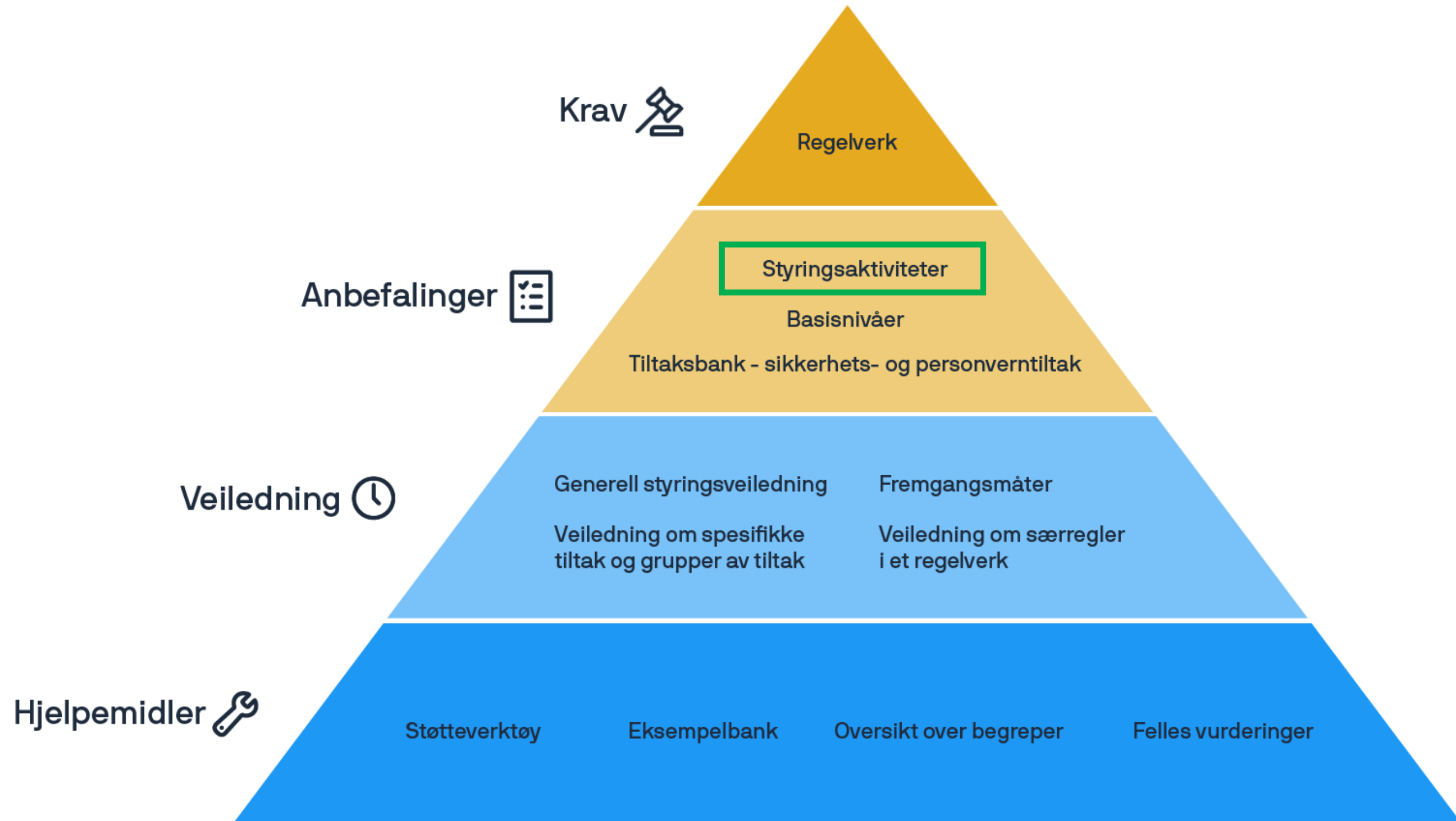


Offentlig

Styring av informasjonssikkerhet og
personopplysningsvern

→

Felles anbefalinger for styringsaktiviteter



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

Gi føringer

Sørge for budsjett til
arbeidet

Kommunisere
viktighet

Løfte og håndtere
problemstillinger
gjennom linjen

Virksomhetsledelsens gjennomgang



Ledelsens styring og oppfølging – Gi føringer

- Struktur og innhold i styringsaktivitetene
- Roller og myndighet
- Delegering av oppgaver til risikoeiere
- Hvordan risikoeiere skal forstå, vurdere og håndtere risiko, inkludert kriterier for å akseptere risiko
- Hvordan risikoeiere skal sørge for innebygd personvern i oppgaver og tjenester som behandler personopplysninger
- Hvordan styringsaktivitetene skal gjennomføres



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Sørg for at sikkerhetsstyringen er integrert i virksomhetens overordnede styringssystem.
- Ha tydelige beskrivelser av ansattes roller, ansvar og myndighet innen sikkerhet, og sørg for at disse er godt kjent i virksomheten.

Ha oversikt og prioritere



Oversikt over ansvarsområde

Kartlegge eksterne krav

Vurdere behov for risikovurderinger

Oppdatert oversikt over risikovurderinger

Ha oversikt og prioritere – oversikt over ansvarsområde



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Hold oppdatert oversikt over verdier og avhengigheter samt sårbarheter og trusler som påvirker disse verdiene.

- Oversikt over
 - oppgaver og tjenester som utføres
 - hvilken informasjon som behandles, inkludert hvilke personopplysninger
 - formål med behandling av personopplysninger, behandlingsgrunnlag og behandlingsansvar
 - overføring av personopplysninger utenfor EØS og overføringsgrunnlag som benyttes
 - digitale systemer og digitale tjenester som benyttes, inkludert avhengigheter til eksterne tjenester
- En vurdering av hvor store konsekvensene ved brudd på informasjonssikkerhet eller personopplysningsvern kan bli, for virksomheten og for eksterne parter
- Vedlikehold av protokoll over behandlingsaktiviteter, med informasjon om behandling av personopplysninger
- En gjennomgang av vesentlige trusler, farer og sårbarheter

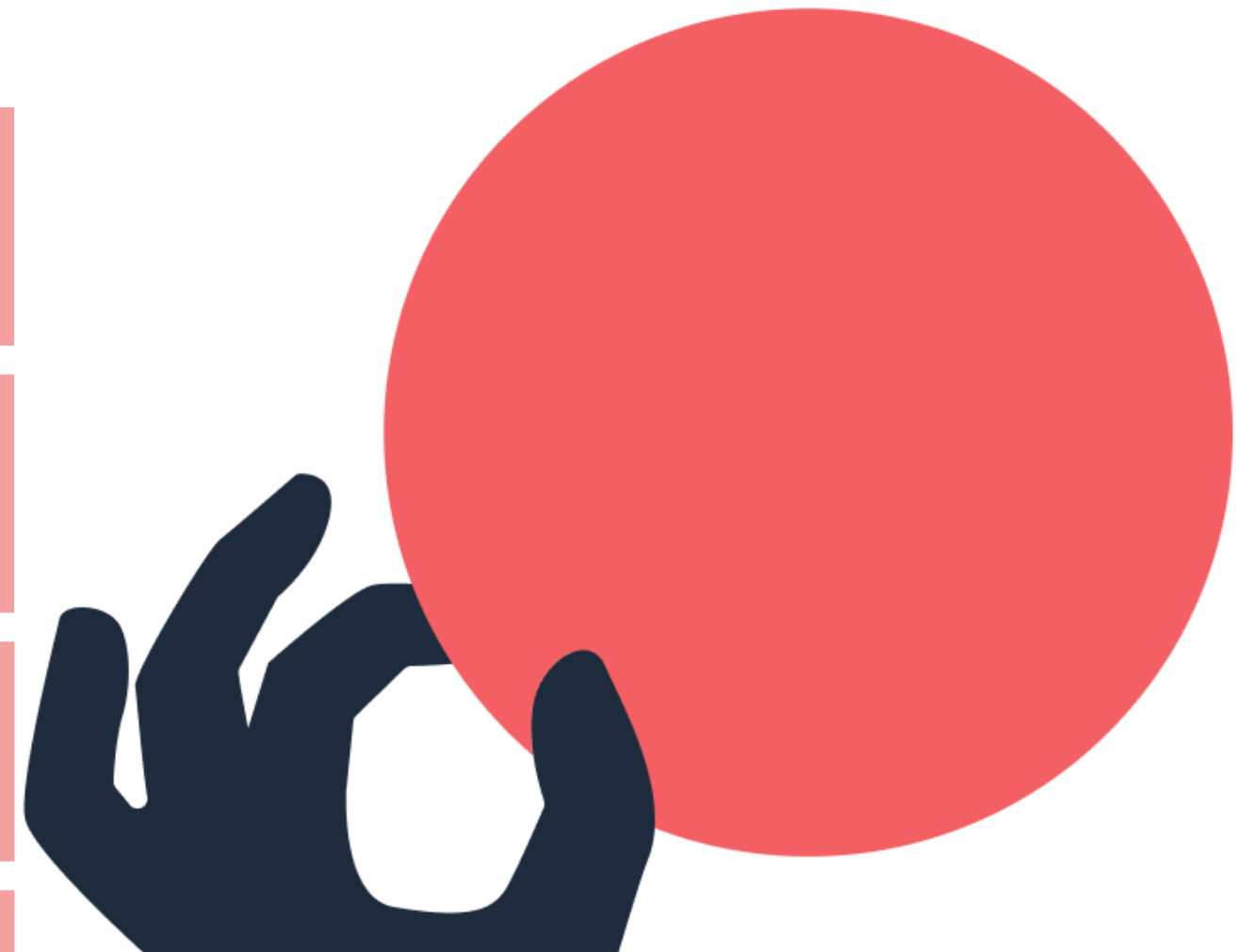
Vurdering av risiko

Planlegge risikovurdering

Vurdere personvernkonsekvensvurdering (DPIA)

Gjennomføre risikovurdering

Vurdere risiko etter hendelser



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Gjennomfør jevnlig risikovurderinger slik at sikkerhetstiltakene er tilpasset trussel- og risikobildet.

Håndtering av risiko

Foreslå håndtering av risikoer

Godkjenne forslag til risikohåndtering

Iverksette godkjent håndtering av risiko

Forvalte fellessikring og tilleggssikring



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Planlegg påbyggingstiltak og tiltak som reduserer skadefølgene ved en uønsket hendelse, og øv også på disse tiltakene.

Måling, evaluering og revisjon

Vurdere status på eget ansvarsområde

Måle tilstanden på områder over tid

Gjennomføre evalueringer/internrevisjon

Vurdere effektiviteten av sikkerhets- og personverntiltak



Måling, evaluering og revisjon – Vurdere effektivitet av sikkerhet- og personverntiltak

ME-4 Vurdere effektivitet av sikkerhets- og personverntiltak

Virksomhetsledelsen har ansvar for at det regelmessig vurderes om sikkerhets- og personverntiltakene er effektive. Hensikten er å undersøke om tiltakene er etablert, at de virker som tiltenkt, og at de har ønsket effekt på virksomhetens informasjonssikkerhet og personopplysningsvern.

Gir evne til

- å kjenne status på sikkerhets- og personverntiltak
- å ha formåls- og kostnadseffektive sikkerhets- og personverntiltak
- å vurdere om styringsaktivitetene for å vurdere og håndtere risiko fungerer godt



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Gå jevnlig gjennom sikkerhetstiltakene og bruk øvelser til å sjekke at de er hensiktsmessige.

Overvåking og hendelseshåndtering



Overvåking etter behov

Følge opp hendelser og avvik

Varsling ved hendelser

Beredskap og krisehåndtering

Anbefalinger til virksomheter for å redusere risikoen for cyberoperasjoner

- Etabler overvåking av egne systemer for å kunne avdekke uvanlig eller mistenkelig aktivitet. Logger må lagres sikkert og tilstrekkelig lenge slik at analyse av hendelsesforløp er mulig.

Kompetanse- og kulturutvikling

Gi grunnopplæring til risikoeiere

Identifisere og følge opp behov

Øvelser



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Gå jevnlig gjennom sikkerhetstiltakene og bruk øvelser til å sjekke at de er hensiktsmessige.
- Planlegg påbyggingstiltak og tiltak som reduserer skadefølgene ved en uønsket hendelse, og øv også på disse tiltakene.

Anskaffelser og leverandørstyring

Identifisere behov

Håndtere risiko og stille krav

Vurdering av leverandører

Oppfølging av tjenesteleveranser

Holde helhetlig oversikt over leverandører



Anbefalinger til virksomheter for å redusere risiko i leverandørkjeder

- Gjennomfør gode og dekkende risikovurderinger for å velge riktige sikkerhetstiltak før anskaffelser.
- Sikre at relevante krav til sikkerhet framgår av konkurransevilkår og kontrakt.

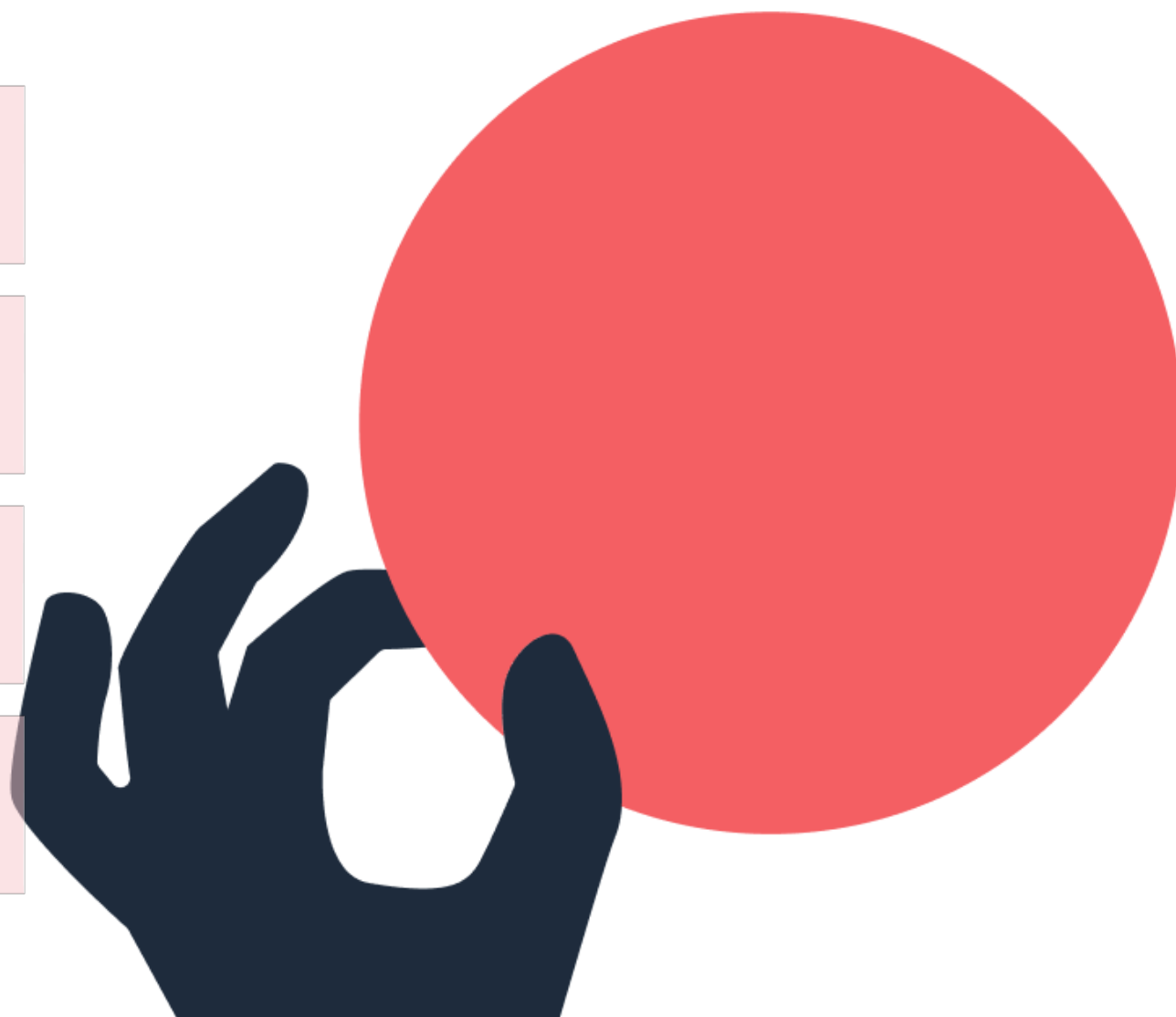
Kommunikasjon

Formidle føringer

Dokumentere gjennomførte styringsaktiviteter

Utarbeide underlagsdokumentasjon

Dialog med styrende organ



Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Ha tydelige beskrivelser av ansattes roller, ansvar og myndighet innen sikkerhet, og sørg for at disse er godt kjent i virksomheten.

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 over
prioriteter

av risiko

Legger til rette for god og effektiv styring av informasjonssikkerhet og personopplysningsvern, og etterlevelse av krav til styring i blant annet:

- eForvaltningsforskriften
- Sikkerhetsloven
- Digitalsikkerhetsloven
- GDPR

Måling, evaluering og
revisjon

Anskaffelser og
leverandørstyring

<https://www.sikkert.no/offentlig/artikler/styring-av-informasjonssikkerhet-og-personopplysningsvern>

Kommunikasjon



NSM



Helsedirektoratet



www.digdir.no/infosikkerhet

E-post: infosikkerhet@digdir.no

digdir.no

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

Besøksadresser:
Havnegata 48, 8900 Brønnøysund
Skrivarvegen 2, 6863 Leikanger
Lørenfarete 1C, 0580 Oslo