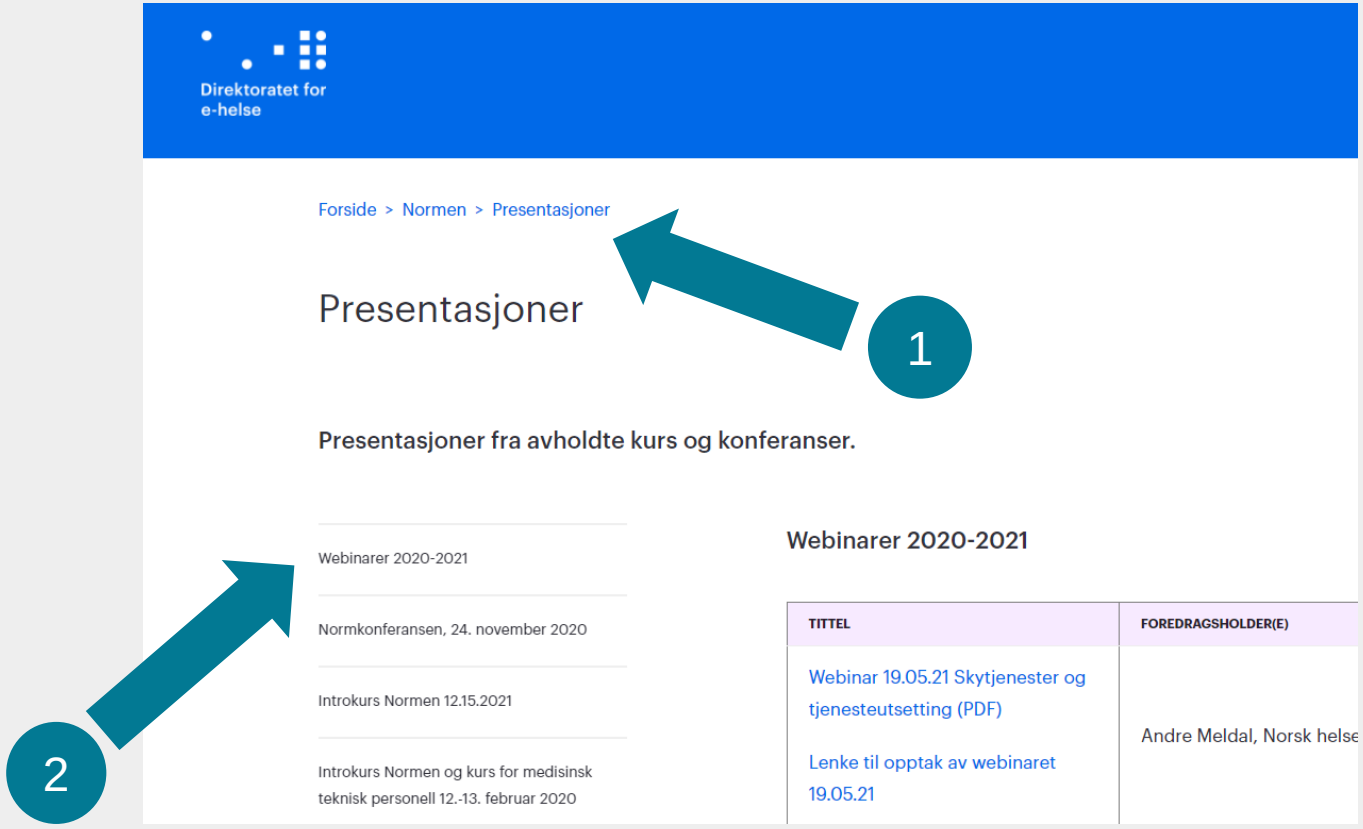
# INNSPILLSWEBINAR:
# Veiledningsmateriell – internkontroll og risikostyring

Siw Tynes Johnsen
Sekretariatet for Normen
25.06.21

# Kjøreregler

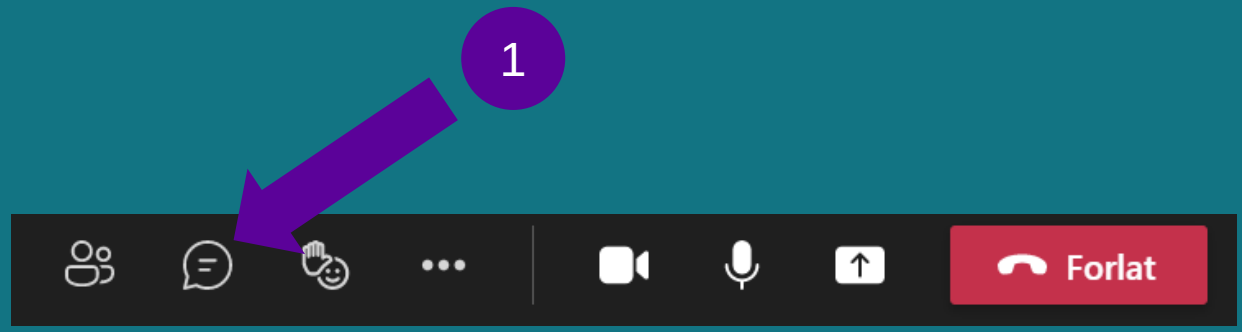
- Møteleder styrer ordet
- Vi setter mikrofonene deres på «mute» fra start
- Det foretas ikke opptak av dette webinaret
- Presentasjonen legges ut på normen.no

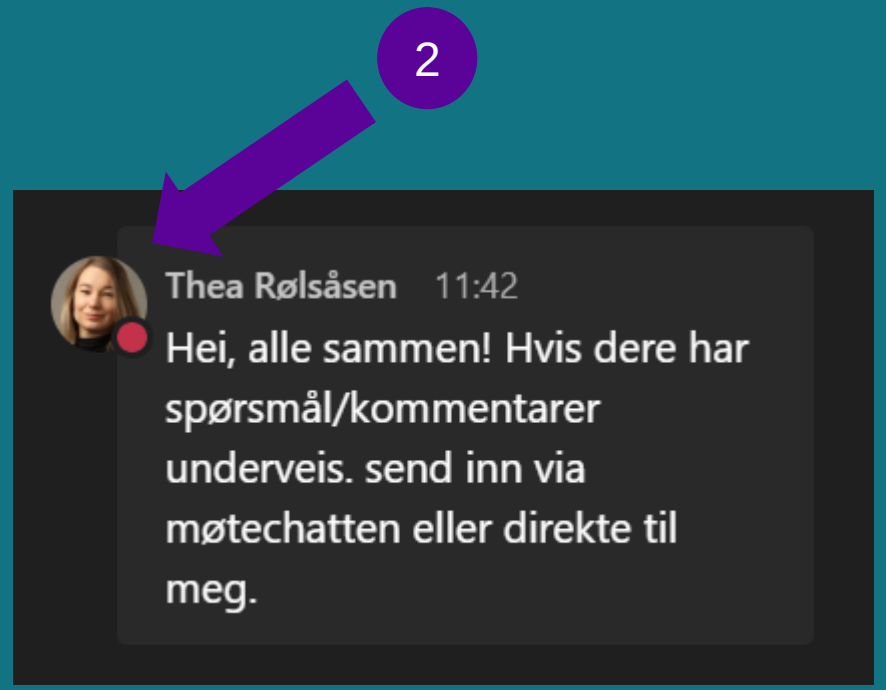



NORMEN

# Spørsmål og kommentarer underveis

- Bruk chatfunksjonen når som helst under webinaret til spørsmål eller kommentarer
- Send spørsmål eller kommentarer direkte til Thea om du ikke ønsker å skrive i møtechatten
- Vi svarer på spørsmål enten i plenum og/eller i chat
- Hvis du har spørsmål som ikke blir besvart under webinaret eller innspill du ønsker å komme med i etterkant, send oss en epost til sikkerhetsnormen@ehelse.no




NORMEN

# Agenda

- Introduksjon til veiledningspakken internkontroll og risikostyring
  - Innhold og relevante problemstillinger
- Diskusjon og innspill
  - Vi ønsker å høre fra dere!
- Veien videre for veiledningspakken

# En liten forsmak på diskusjonstemaene …

- Hvordan fungerer strukturen i veilederne?
- Er det temaer som mangler i innholdsfortegnelsene som bør med?
- Er det temaer som bør strykes eller løftes ut i andre veiledningsprodukter (egne faktaark eller lignende)?
- Hvordan jobber dere med risikoaksept i deres virksomheter?
  - Nivåer for risikoaksept, akseptkriterier, en hybrid mellom de to – eller på en helt annen måte?
  - Fordeler, ulemper, behov? Hvordan veileder vi best?

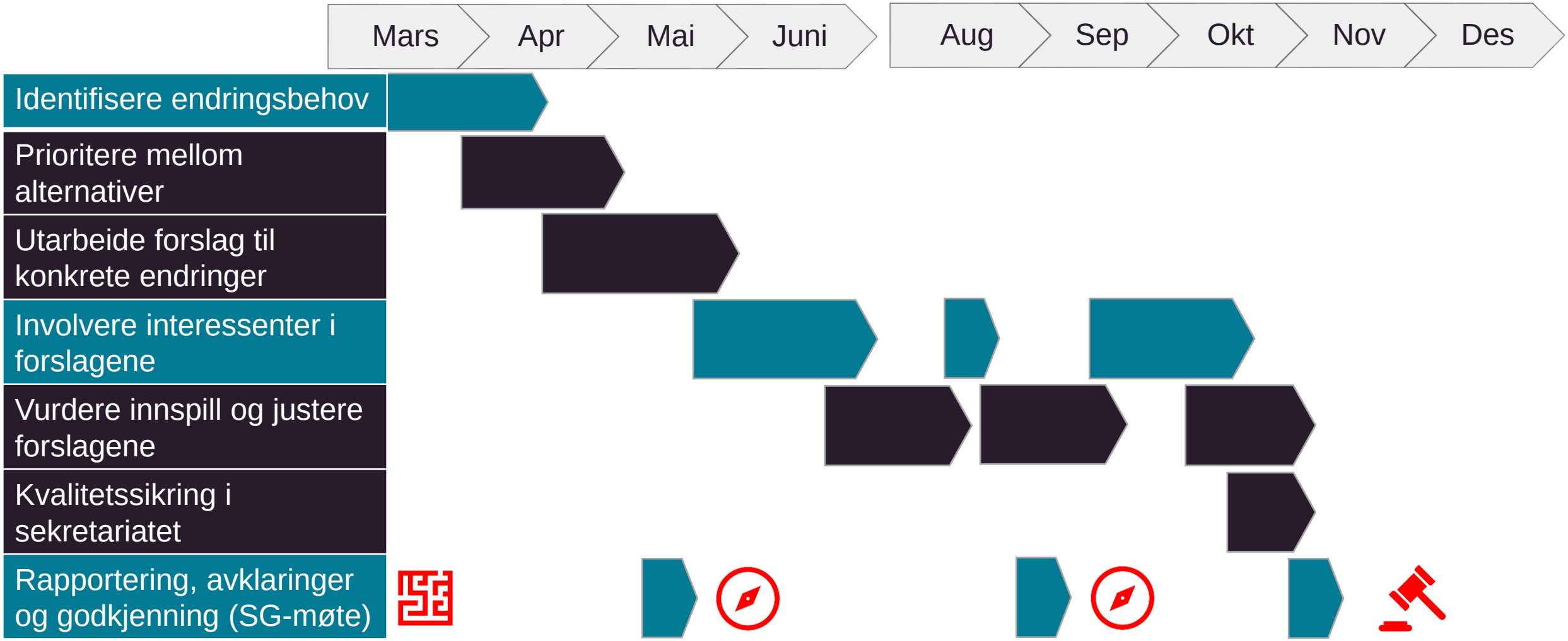
# Introduksjon til veiledningspakken internkontroll og risikostyring

# Oppdatering av veiledningsmateriell: Internkontroll og risikostyring

Temaer som inngår i arbeidspakken

- Faktaark 01 Ansvar og organisering
- Faktaark 02 Styringssystem for informasjonssikkerhet og personvern
- Faktaark 04 Kartlegge og klassifisere systemer
- Faktaark 05 Fastsette nivå for akseptabel risiko
- Faktaark 07 Risikovurdering
- Faktaark 08 Avviksbehandling
- Faktaark 09 Opplæring av ledere og medarbeidere
- Faktaark 27 Retningslinjer for daglig informasjonssikkerhet
- Planlagt veiledning om personvernkonsekvensvurdering (DPIA)
- Veileder for små helsevirksomheter
- Mal for internkontroll legekontor
- Mal for internkontroll psyk, fysio, manuell, og kiropraktor
- Mal for internkontroll tannhelsetjeneste
- Mal for internkontroll apotek

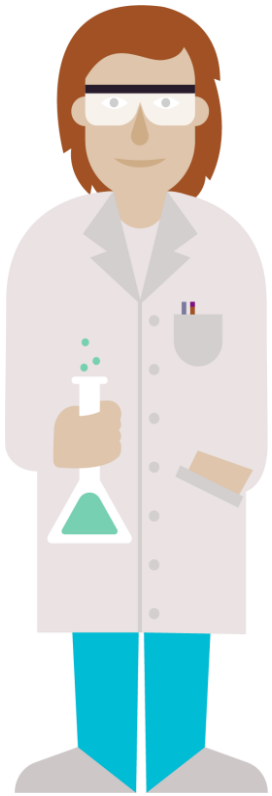
# Plan for arbeidet med veiledningsmateriellet



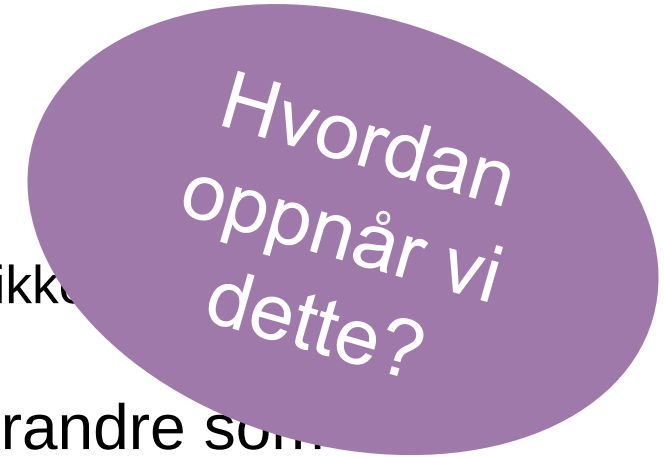

NORMEN

# Kort om gjennomførte aktiviteter

- Innspill fra Normens styringsgruppe og andre aktører i sektoren
- Innspillswebinar for veiledning om DPIA ble gjennomført 5. mai
  - Innspill om utfordringer, behov og eksempler/maler fra sektoren
- Referansegruppe med deltagere fra bredden av sektoren hadde møte 22. juni
  - Konstruktiv faglig diskusjon om internkontroll og risikostyring, fokus på struktur og innhold i veiledningsmateriellet
- Innspillswebinar 1 for veiledningspakken ble gjennomført 23. juni
  - Innspill om struktur og overordnet innhold
  - Ikke alle som ønsket fikk deltatt på grunn av tekniske problemer
- Løpende koordinering med direktoratets arbeid med oppdatering av mal for personvernkonsekvensvurderinger (DPIA) og utarbeidelse av tilhørende veileder



# Målsetninger/prinsipper for veiledningsmateriell i pakken




- Vise sammenhengene mellom ulike delprosesser
  - For eksempel mellom ulike typer risikovurderinger (informasjonssikk
    pasientsikkerhet, DPIA)
- Synliggjøre behovet for å veie ulike hensyn opp mot hverandre som
  del av risikostyringen
- Synliggjøre ledelsens ansvar og behov for beslutningsgrunnlag
- Ikke skrive mye om det samme mange steder
  - Unngå dobbeltarbeid både i arbeidet med veiledningsmateriellet og for virksomhetene som skal benytte materiellet i sine prosesser
- Sektorspesifikt og praktisk rettet
  - Ikke for teoretikerne, men for de som skal gjøre dette i praksis i sektoren

# … ved å organisere de faglige temaene på denne måten

| Internkontroll |
| --- |
| Faktaark 01 - Ansvar og organisering |
| Faktaark 02 - Styringssystem for info.sikkerhet og personvern |
| Faktaark 08 - Avviksbehandling |
| Faktaark 09 - Opplæring av ledere og medarbeidere |
| Faktaark 27 - Retningslinjer for daglig informasjonssikkerhet |
| Nytt tema: Sikkerhetskultur i helse- og omsorgssektoren |
| Maler og eksempler (bl.a. fra maler for internkontroll for små virksomheter) |
| Sette de ulike prosessene som er en del av internkontrollen mer i sammenheng |
| Beskrive at risikostyring er en del av den totale internkontrollen, henvise til risikoveileder |

| Risikostyring |
| --- |
| Faktaark 04 - Kartlegge og klassifisere systemer |
| Faktaark 05 - Fastsette nivå for akseptabel risiko |
| Faktaark 07 - Risikovurdering |
| Nytt tema: Vurdering av personvernkonsekvenser (DPIA) |
| Maler og eksempler |
| Sette de ulike prosessene som er en del av risikostyringen mer i sammenheng |
| Beskrive at risikostyring er en del av den totale internkontrollen, henvise til internkontrollveileder |

Oppdatere og tilpasse veileder for små virksomheter ved behov, i tråd med ny veiledning og med riktige henvisninger

NORMEN

# Veileder i internkontroll – innhold i utkastet som foreligger

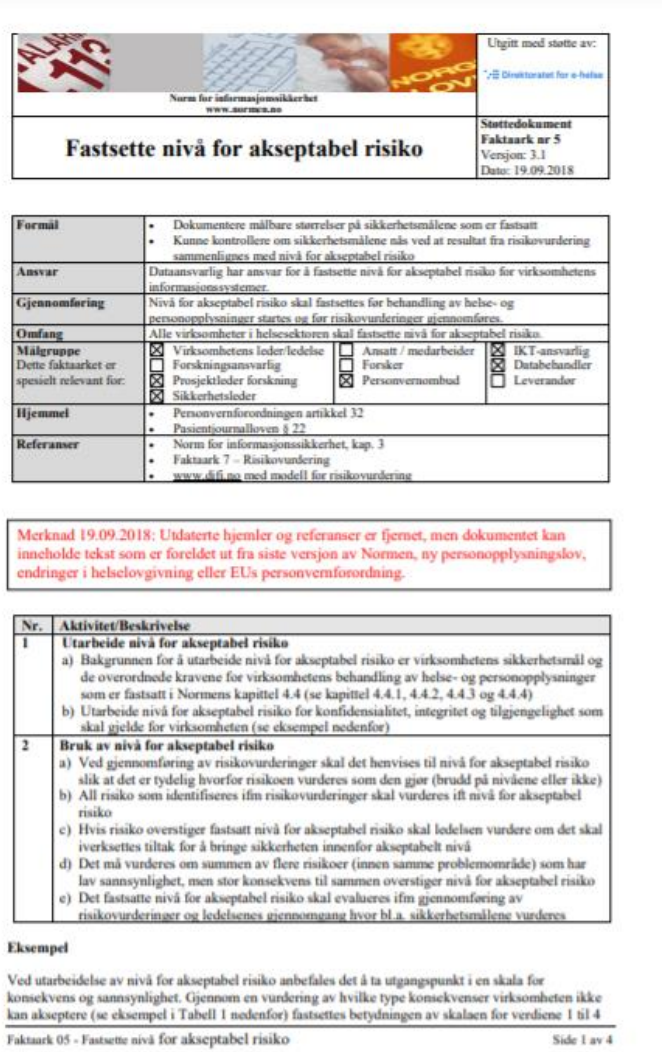
# Veileder i internkontroll forts.

# Veileder i risikostyring – innhold i utkastet som foreligger

# Veileder i risikostyring forts.

# Risikoaksept – nivåer og kriterier

- Ta utgangspunkt i en skala for konsekvens og sannsynlighet
- Vurdere hvilken konsekvens og sannsynlighet virksomheten ikke kan akseptere – kombinere disse for å finne nivå for akseptabel risiko
- For all risiko som er høyere enn nivå for akseptabel risiko skal det iverksettes tiltak for å bringe sikkerheten innenfor et akseptabelt nivå
- Arbeidet med å fastsette akseptabel risiko skal ta utgangspunkt i de enkelte behandlingene av helse- og personopplysninger virksomheten gjør



Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

**Fastsette nivå for akseptabel risiko**

**Støttedokument**
**Faktaark nr 5**
Versjon: 3.1
Dato: 19.09.2018

| | |
|---|---|
| **Formål** | • Dokumentere målbare størrelser på sikkerhetsmålene som er fastsatt<br>• Kunne kontrollere om sikkerhetsmålene nås ved at resultat fra risikovurdering sammenlignes med nivå for akseptabel risiko |
| **Ansvar** | Dataansvarlig har ansvar for å fastsette nivå for akseptabel risiko for virksomhetens informasjonssystemer. |
| **Gjennomføring** | Nivå for akseptabel risiko skal fastsettes før behandling av helse- og personopplysninger startes og før risikovurderinger gjennomføres. |
| **Omfang** | Alle virksomheter i helsesektoren skal fastsette nivå for akseptabel risiko. |
| **Målgruppe**<br>Dette faktaarket er spesielt relevant for: | ☒ Virksomhetens leder/ledelse<br>☐ Forskningsansvarlig<br>☒ Prosjektleder forskning<br>☒ Sikkerhetsleder<br>☐ Ansatt / medarbeider<br>☐ Forsker<br>☒ Personvernombud<br>☒ IKT-ansvarlig<br>☒ Databehandler<br>☐ Leverandør |
| **Hjemmel** | • Personvernforordningen artikkel 32<br>• Pasientjournalloven § 22 |
| **Referanser** | • Norm for informasjonssikkerhet, kap. 3<br>• Faktaark 7 – Risikovurdering<br>• www.dfi.no med modell for risikovurdering |

Merknad 19.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

| Nr. | Aktivitet/Beskrivelse |
|---|---|
| 1 | **Utarbeide nivå for akseptabel risiko**<br>a) Bakgrunnen for å utarbeide nivå for akseptabel risiko er virksomhetens sikkerhetsmål og de overordnede kravene for virksomhetens behandling av helse- og personopplysninger som er fastsatt i Normens kapittel 4.4 (se kapittel 4.4.1, 4.4.2, 4.4.3 og 4.4.4)<br>b) Utarbeide nivå for akseptabel risiko for konfidensialitet, integritet og tilgjengelighet som skal gjelde for virksomheten (se eksempel nedenfor) |
| 2 | **Bruk av nivå for akseptabel risiko**<br>a) Ved gjennomføring av risikovurderinger skal det henvises til nivå for akseptabel risiko slik at det er tydelig hvorfor risikoen vurderes som den gjør (brudd på nivåene eller ikke)<br>b) All risiko som identifiseres ifm risikovurderinger skal vurderes ift nivå for akseptabel risiko<br>c) Hvis risiko overstiger fastsatt nivå for akseptabel risiko skal ledelsen vurdere om det skal iverksettes tiltak for å bringe sikkerheten innenfor akseptabelt nivå<br>d) Det må vurderes om summen av flere risikoer (innen samme problemområde) som har lav sannsynlighet, men stor konsekvens til sammen overstiger nivå for akseptabel risiko<br>e) Det fastsatte nivå for akseptabel risiko skal evalueres ifm gjennomføring av risikovurderinger og ledelsenes gjennomgang hvor bl.a. sikkerhetsmålene vurderes |

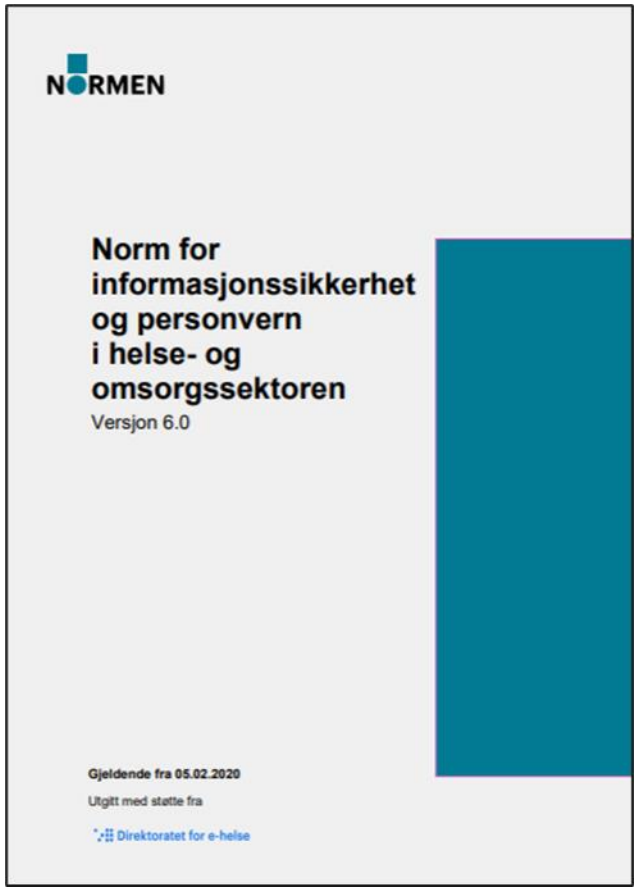
**Eksempel**

Ved utarbeidelse av nivå for akseptabel risiko anbefales det å ta utgangspunkt i en skala for konsekvens og sannsynlighet. Gjennom en vurdering av hvilke type konsekvenser virksomheten ikke kan akseptere (se eksempel i Tabell 1 nedenfor) fastsettes betydningen av skalaen for verdiene 1 til 4

Faktaark 05 - Fastsette nivå for akseptabel risiko Side 1 av 4

# Risikoaksept – nivåer og kriterier

- Normen 6.0 har en risikobasert tilnærming
- Krav til informasjonssikkerhet gjennomgående i hele bransjenormen
- Det er likevel utledet noen såkalte minimumskrav til konfidensialitet, integritet, tilgjengelighet og robusthet
- «Virksomheten skal fastsette nivå for akseptabel risiko basert på Normens minimumskrav til informasjonssikkerhet og eventuelt egne informasjonssikkerhetsmål»
  - En slags hybridløsning mellom tidligere versjoners fokus på nivå for akseptabel risiko og bruk av akseptkriterier



Diskusjon – ordet er fritt!

# Hva tenker dere?

- Hvordan fungerer strukturen i veilederne?
- Er det temaer som mangler i innholdsfortegnelsene som bør med?
- Er det temaer som bør strykes eller løftes ut i andre veiledningsprodukter (egne faktaark eller lignende)?

# Hva tenker dere?

- Hvordan jobber dere med risikoaksept i deres virksomheter?
- Nivåer for risikoaksept, akseptkriterier, en hybrid mellom de to – eller på en helt annen måte?
- Fordeler, ulemper, behov? Hvordan veileder vi best?

# Andre innspill til arbeidet med veilederne i internkontroll og risikostyring?

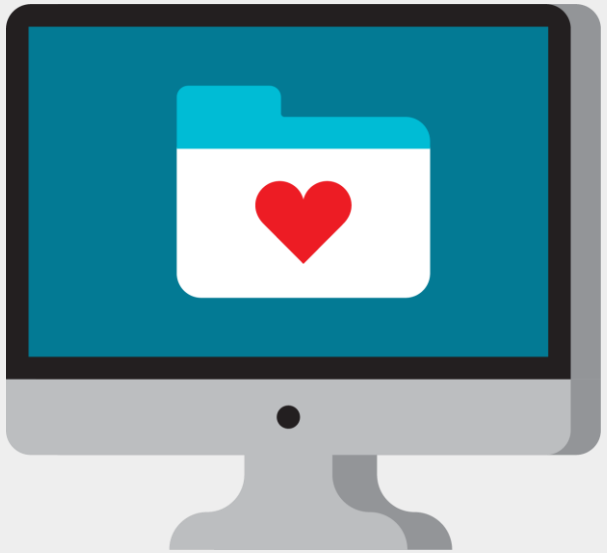
# Veien videre for veiledningspakken og referansegruppen

# Veien videre …

- Skriveperiode i et par uker til – etterarbeid fra dagens innspillswebinar og arbeid med andre mottatte bidrag
- Innspill og beslutninger i styringsgruppemøte 20. september
- Referansegruppemøter i oktober, for henholdsvis internkontroll og risikostyring
- Legges frem for godkjenning av Normens styringsgruppe 1-2. desember
- Planlagt publisering desember 2021

# Ta gjerne kontakt om du har innspill til Normens veiledningsmateriell!

- Hva trenger du?
- Hva mangler?
- Hva kan oppdatert veiledningsmateriell bidra med?



**sikkerhetsnormen@ehelse.no**

# Vi fortsetter med webinarer – onsdager klokken 0900!

Temaer «på blokka» for høstens webinarer er blant annet nytt faktaark om personvernprinsippene, faktaark om hjemmekontor, veileder om medisinsk utstyr, innspillswebinar for forskning …

Vi jobber med timeplanen nå –

Ta gjerne kontakt om du ønsker deg et tema!

**Følg med på normen.no, sosiale medier og Normens nyhetsbrev!**

NORMEN

Takk for gode innspill!