Risiko: risikostyring og risikovurdering

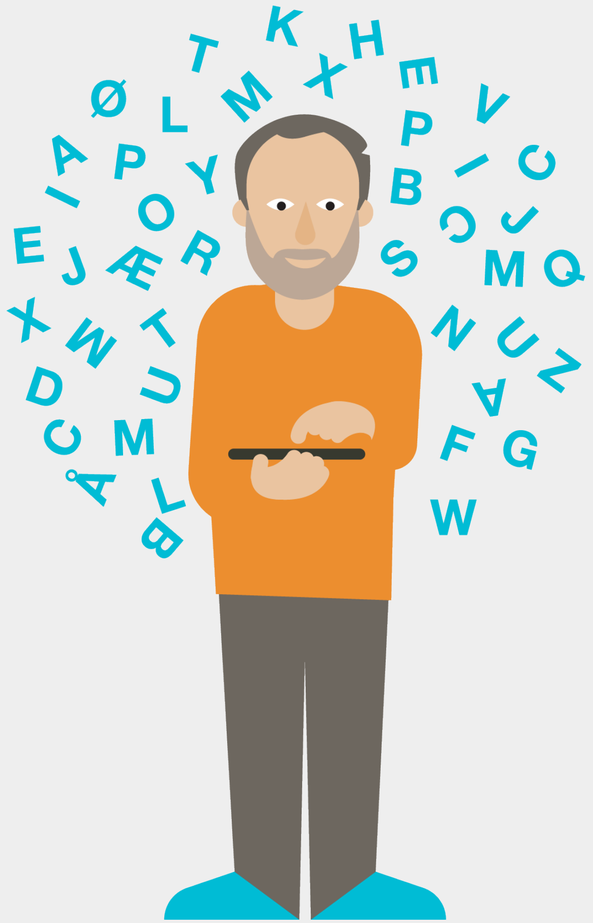
17.02.22

Kurset «Intro om Normen»

Hva er risikostyring?

Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko

- Få oversikt over informasjon og teknologi i virksomheten
- Identifisere trusler og mulige uønskede hendelser for virksomheten og de registrerte
- Analysere risikoen
- Etablere tiltak for å opprettholde nivå for akseptabel risiko



Hva er risikovurdering?

Risikovurdering er et verktøy for å identifisere uønskede hendelser

- Virksomheten skal vurdere **sannsynligheten** for og mulige **konsekvenser** av at en hendelse inntreffer

- Dersom risikoen er uakseptabel, skal virksomheten gjennomføre **tiltak** for å redusere risikoen

Når skal vi risikovurdere?

Risikovurderinger skal som minimum gjennomføres før:

- etablering av eller endring i behandling av helse- og personopplysninger
- etablering av nye systemer eller registre som inneholder eller benytter helse- og personopplysninger
- det etableres organisatoriske, tekniske eller andre endringer med betydning for informasjonssikkerheten
- det etableres eller endres tilgang til helseopplysninger mellom virksomheter

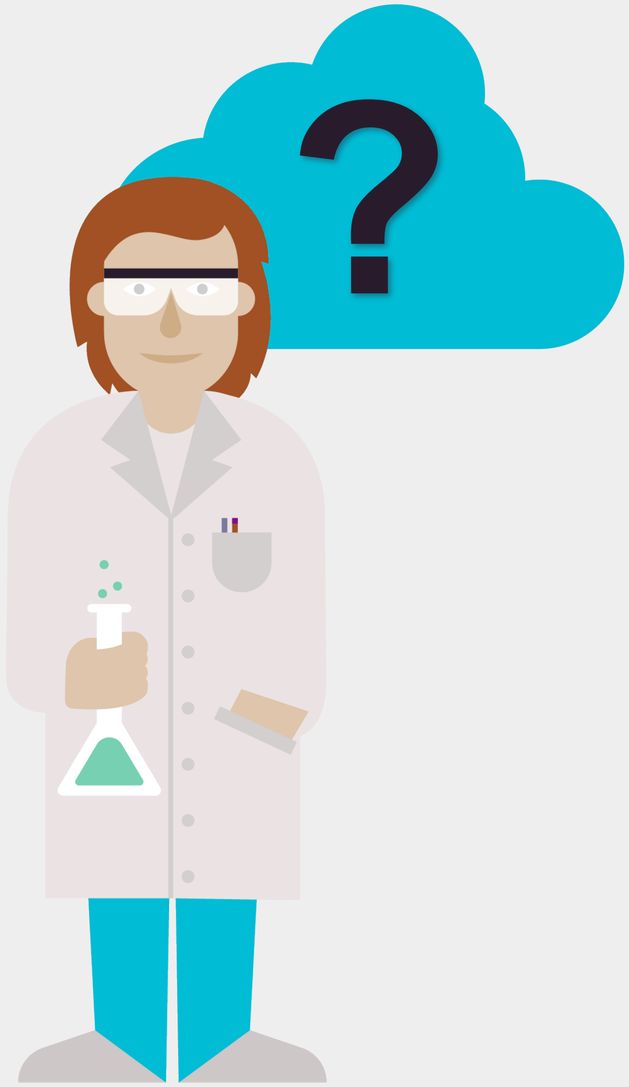
Risikovurdering bør oppdateres ved endring i trusselbildet

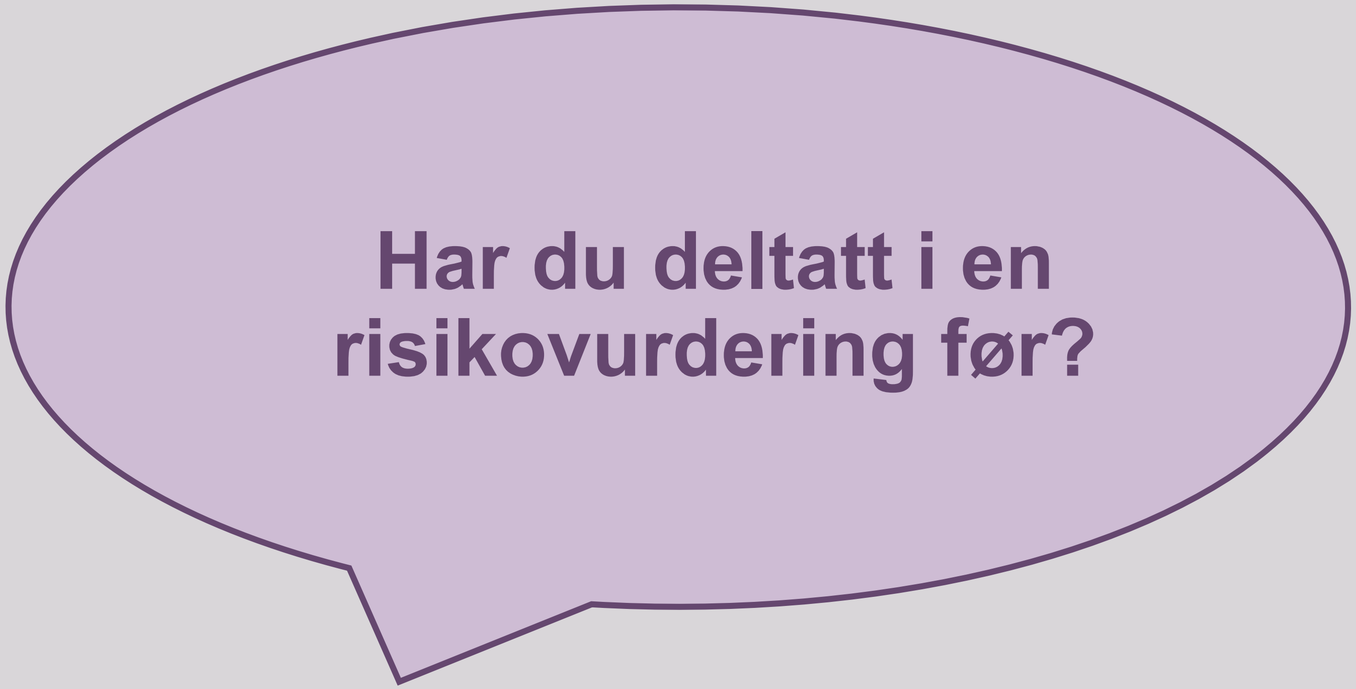
Hvordan risikovurderer vi?

Risikovurderingen bør være en strukturert prosess

- Planlegging
- Forberede risikovurderingen
- Gjennomføre risikovurderingen
- Vurdering og anbefaling av nye tiltak

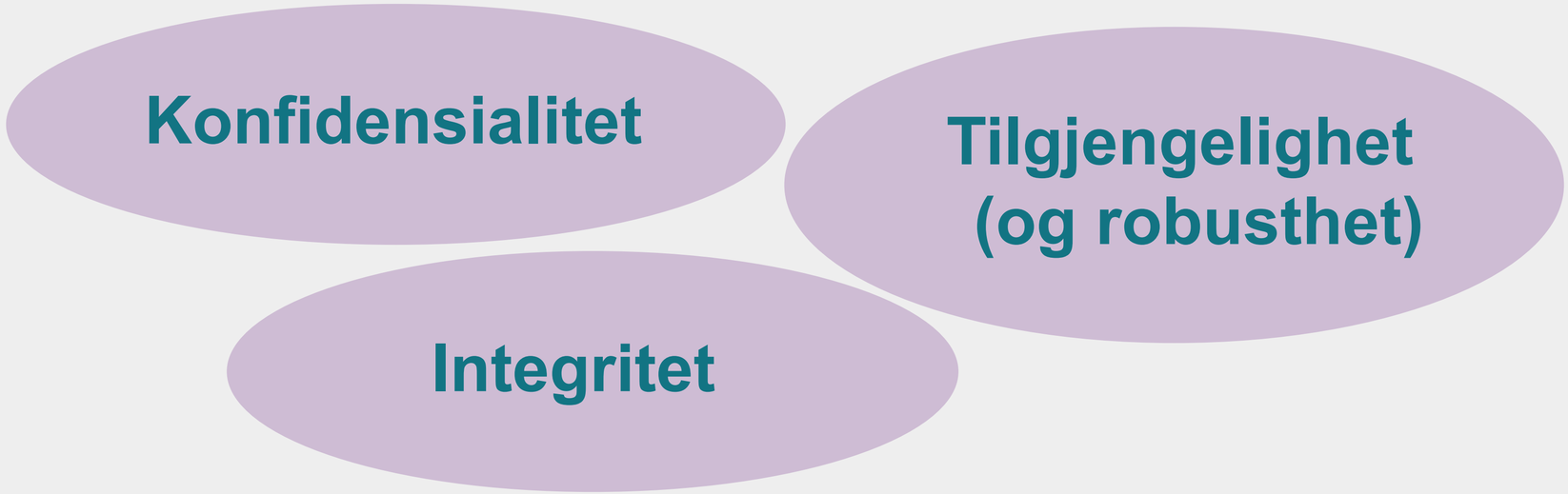
De riktige nøkkelpersonene må være involvert!




Har du deltatt i en risikovurdering før?

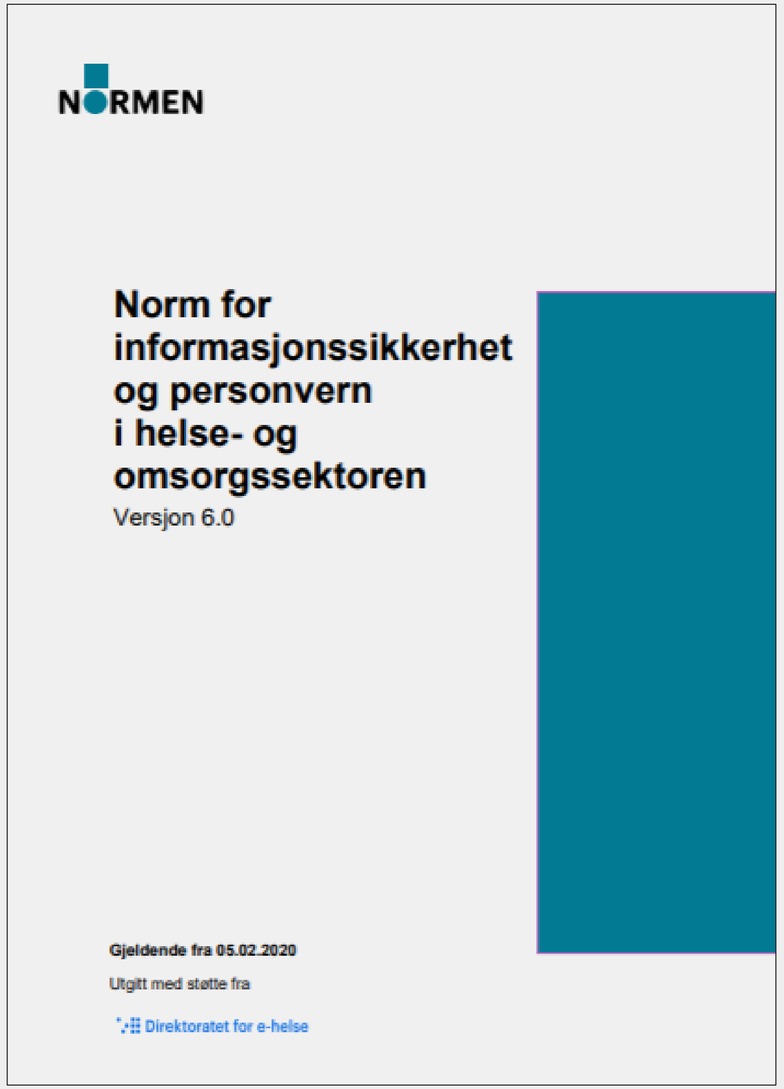
Hva skal vi beskytte?

Risikovurderingen bør ta utgangspunkt i en kartlegging av **informasjonsverdier** og konsekvensen av hendelser som rammer tilgjengeligheten, integriteten og konfidensialiteten til informasjonsverdiene.



Normens krav – minimumskrav

- Normen har en risikobasert tilnærming
- Det finnes krav til konfidensialitet, integritet, tilgjengelighet og robusthet gjennomgående i hele bransjenormen
- Vi har likevel utledet noen såkalte minimumskrav på disse områdene, der alle er formulert som skal-krav

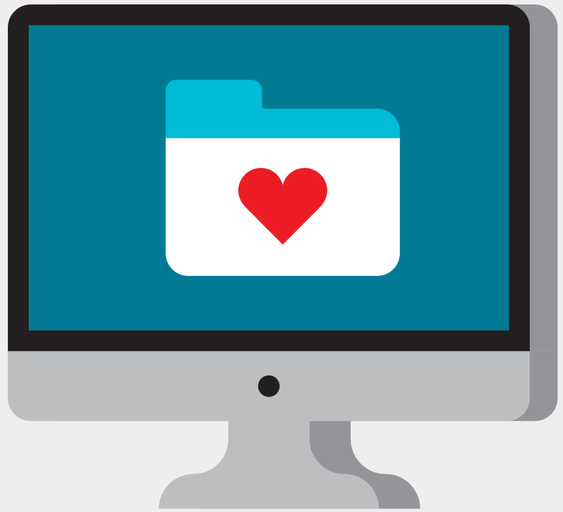


Normens krav for å sikre konfidensialitet

Minimums-krav

Virksomheten skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger

- hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
- avgrense tilgang for autorisert personell iht. tjenstlig behov
- ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten

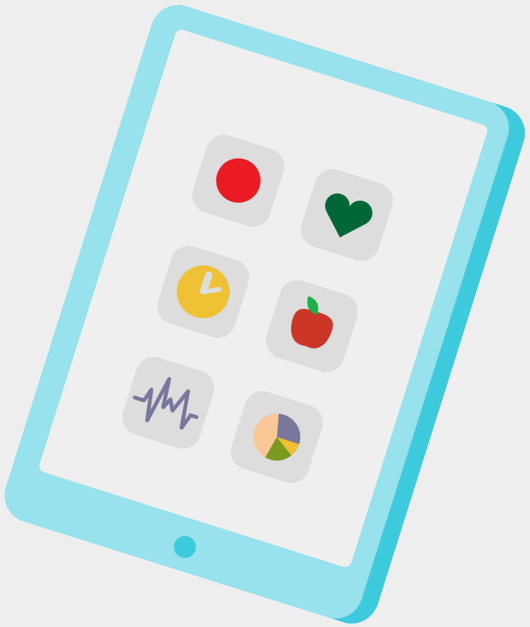


NORMEN

Normens krav for å sikre integritet

Minimums-krav

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er sikret mot utilsiktet eller uautorisert endring eller sletting. Integritet er en forutsetning for god og forsvarlig helsehjelp



- logge hvem som har rettet, registrert, endret og slettet
- hindre utilsiktet eller uautorisert endring eller sletting
- sikre at helse- og personopplysninger registreres på rett person
- sikre at helse- og personopplysninger føres i henhold til relevant kodeverk og terminologi
- sikre at helse- og personopplysninger er korrekte og om nødvendig oppdaterte
- hindre at kopier av data blir en kilde til utdatert informasjon

Normens krav til tilgjengelighet og robusthet

Minimums-krav

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er tilgjengelig til rett tid

- sikre at helse- og personopplysninger er tilgjengelig iht. tjenstlig behov
- sikre forsvarlig og stabil drift av informasjonssystemene
- sikre at det finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting
- sikre at informasjonssystemene er tilgjengelig iht. virksomhetens tilgjengelighetskrav

Eksempel – vi i Normen har risikovurdert webinarverktøy

	Risikoscenario		Eksisterende/planlagte tiltak	Årsak/Sårbarhet	Sannsynlighet		Konsekvens		R
#	Beskrivelse av sikkerhetshendelse	Brudd (K-I-T)	Tiltaksbeskrivelse	Sårbarhetsbeskrivelse	Sannsynlighets-beskrivelse	S	Konsekvens-beskrivelse	K	S*K
	Risikovurdering								
Scenarioer									
A1	Presentatør deler mer informasjon enn ønsket gjennom skjermdelingsfunksjonen		Opplæring av presentatører i forkant Opplærning av webinarverter	Kan være vanskelig å forstå, særlig ved første gangs bruk	Opplæringstiltak gjør mindre sannsynlig	2	Tap av anseelse/personlig integritet, kan oppleves krenkende	2	4
A2	Presentatør misforstår funksjonalitet og ender opp med å gjøre noe annet enn planlagt		Opplæring av presentatører i forkant Opplæring av webinarverter	Kan være vanskelig å forstå, særlig ved første gangs bruk	Opplæringstiltak gjør mindre sannsynlig	2	Tap av anseelse/personlig integritet, kan oppleves krenkende	2	4
A3	Personer som ikke skal ha tilgang til webinaret oppnår tilgang gjennom annens lenke		Informasjon til de påmeldte Kun bruke webinarform til "åpen informasjon"	Ikke sperret tilgang for andre enn de som får tildelt lenke	Mulig ettersom det bare er å videresende lenken på tross av informasjon om at lenken er personlig	3	Webinar skal kun benyttes for åpen informasjon, ubetydelig konsekvens	1	3
A4	Personer deler helseopplysninger gjennom spørsmålsfunksjonen		Gjennomgang av kjøreregler i begynnelsen av webinar Rutine for at webinarvert "skriver om" informasjon før det deles i plenum	Ingen sperrer på hva personer kan skrive i spørsmålsfunksjonen	Gjennomgang av kjøreregler gjør mindre sannsynlig, samt at fokus for webinar er tilbydere av helsetjenester og/eller profesjonelle organisasjoner heller enn enkelt-pasienter/-brukere	2	Tap av anseelse/personlig integritet, kan oppleves krenkende	2	4
A5	Spørsmål/dialog lagres lengre enn nødvendig/slettes ikke (raskt nok)		Etablere rutiner for å slette evt anonymisere	Slettes trolig ikke hos leverandør, men kan trolig anonymiseres	Kjent med at det lagres lengre enn nødvendig, men kan trolig anonymiseres	4	Regelverksbrudd som kan medføre advarsel eller vedtak	2	8
A6	Vi samler inn mer informasjon om deltagernes oppførsel		Etablere rutiner for at man ikke skal nyttiggjøre seg	Mulighet for analyse av data på personnivå	Kjent med at det samles inn mer enn	4	Regelverksbrudd som kan medføre	2	8

Leserveiledning | Metodebeskrivelse | Planlegging og forberedelse | Omfang | System og kritikalitet | Skala | Skjema | Oppsummering og handling ...

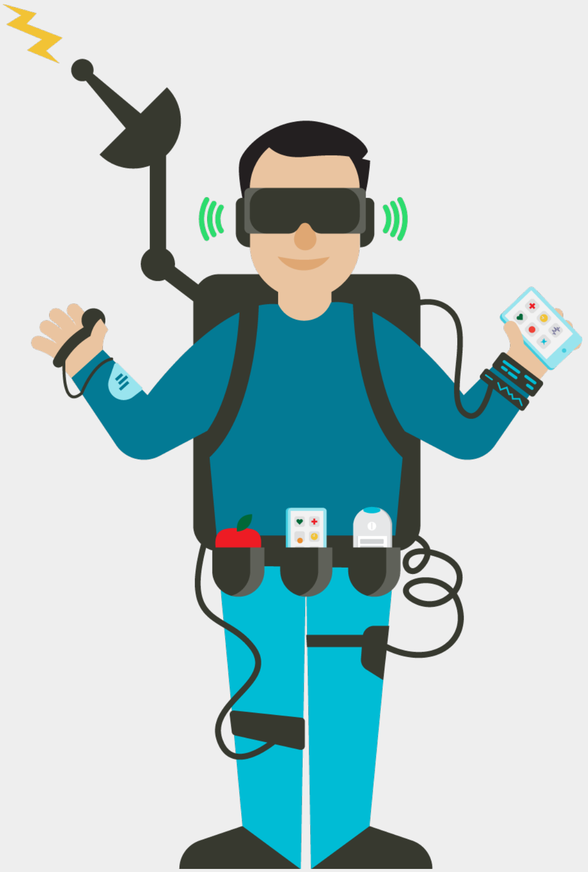
La oss jobbe litt praktisk!

SCENARIO – uønsket hendelse

- Uvedkommende får tilgang til spørsmålene som stilles til Normsekretariatet i webinarverktøyet

Informasjonsverdier

- Personopplysninger (navn og virksomhetstilhørighet) til spørsmålsstiller
- Potensielt sensitiv informasjon som deles med webinarets organisatorer
- …



Sannsynlighet – eksempel på hvordan det kan vurderes

	Tiltaksstyrke	Frekvens
4 – Sannsynlig	Det er ikke iverksatt sikkerhetstiltak. Det er kjente kjente/sårbarheter, og det er identifisert ytterligere tiltak.	>365/1 Daglig eller oftere
3 – Mulig	Sikkerhetstiltak er iverksatt, men de er ikke effektive nok. Det er kjente svakheter/sårbarheter, og det er identifisert ytterligere tiltak.	12/1 En gang hver måned
2 – Mindre sannsynlig	Ett eller flere effektive sikkerhetstiltak er iverksatt, men tiltakene kan omgås av aktører med store ressurser eller med god kjennskap til sikkerhetstiltakene. Det er kjente svakheter/sårbarheter, men det er ikke identifisert ytterligere tiltak.	1/1 En gang hvert år
1 – Usannsynlig	Flere effektive sikkerhetstiltak er iverksatt. Ingen kjente svakheter/sårbarheter som medfører ytterligere tiltak.	1/5 En gang hvert 5. år eller sjeldnere

Konsekvens – eksempel på hvordan det kan vurderes

	Liv og helse	Personvern	Økonomi	Omdømme
4 – Svært høy	Tap av liv og/eller stor, varig helseskade	Langvarig tap av anseelse eller personlig integritet som er krenkende og som kan medføre tap av liv	Uopprettelig økonomisk konsekvens	Langvarig negativ omtale på riksplan
3 – Høy	Varig helseskade	Tap av anseelse eller personlig integritet som er krenkende og/eller påvirker helse på en alvorlig måte	Alvorlig økonomisk konsekvens	Kortvarig negativ omtale på riksplan
2 – Moderat	Forbigående helseskade	Tap av anseelse eller personlig integritet som kan oppfattes som krenkende og/ eller påvirker helse	Mindre alvorlig økonomisk konsekvens.	Kortvarig negativ omtale lokalt
1 – Lav	Ubetydelig helseskade	Ubetydelig tap av anseelse eller personlig integritet	Ubetydelig økonomisk konsekvens	Ubetydelig omdømmetap

NORMEN

menti.com

6223 6071

Hvilken risiko har scenarioet vårt?

Hva gjør vi nå?

Sannsynlighet					
	4 – Sannsynlig				
	3 – Mulig				
	2 – Mindre sannsynlig				
	1 – Usannsynlig				
		1 – Lav	2 – Moderat	3 – Høy	4 – Svært høy
	Konsekvens				

Hvor høy risiko kan virksomheten akseptere?

Husk at en enkelt risikovurdering er en del av en helhet!

- Ledelsens ansvar
- Ha et bevisst forhold til egen risikoappetitt
  - Hvor mye risiko kan vi leve med?
- Fastsette nivå for akseptabel risiko – akseptkriterier
- Hvilke tiltak kan få risikoen ned på et akseptabelt nivå?
  - Menneskelige, teknologiske, organisatoriske

Vurderinger

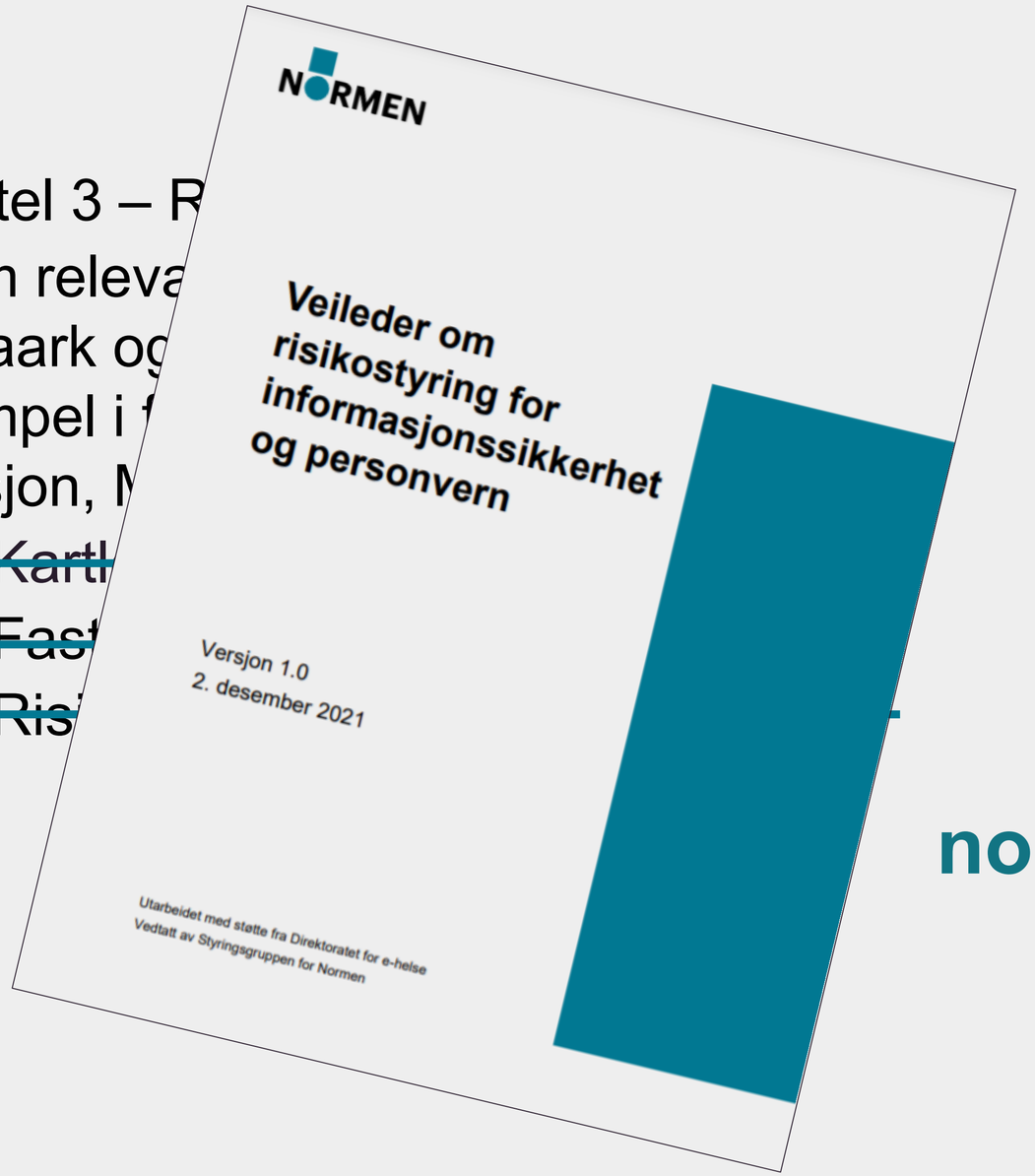
Ledelsen må ha «eierskap» til vurderingene og hvilke tiltak som eventuelt implementeres

Hvordan henger dette sammen med personvernforordningen?

- Risikobasert tilnærming og forholdsmessighet
- Risikovurderinger som underlag for vurdering av personvernkonsekvenser (DPIA)
- Det er en del av den dataansvarliges ansvar å gjennomføre egnede tekniske og organisatoriske tiltak
  - Disse kan finnes på grunnlag av risikovurderinger

Hvor finner jeg mer om risiko?

- Normens kapittel 3 – R
- Informasjon om releva
  spesifikke faktaark og
  (som for eksempel i f
  videokonsultasjon, M
- ~~Faktaark 04 – Kartl~~
- ~~Faktaark 05 – Fast~~
- ~~Faktaark 07 – Risi~~



normen.no