Plan for dagen

Klokkeslett	Tema
09:00	Intro om kurset og om Normen
09:45	Pause
10:00	Internkontroll
10:30	Pause
10:45	**Risikostyring**
11:30	Lunsj
12:00	Utvalgt personvern
12:45	Pause
13:00	Krav til informasjonssikkerhet
13:45	Gruppeoppgave- break out rooom
14:05	Kort pause
14:15	Normens krav i anskaffelser
14:45	Spørsmål og avslutning

Risiko: risikostyring og risikovurdering

10.01.24

Kurset «Intro om Normen»

Hvor i Normen er vi nå?

Kapittel 1: Om Normen

Kapittel 2: Ledelse og ansvar

Kapittel 3: Risikostyring

Kapittel 4: Grunnleggende krav til behandling av helse- og personopplysninger

Kapittel 5: Krav til informasjonssikkerhet

Vedlegg

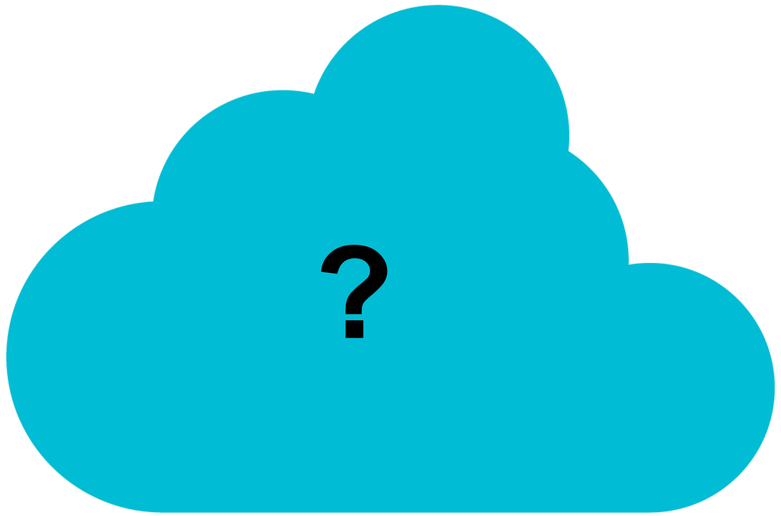
Læringsmål for tema risikostyring

Deltakeren skal ha grunnleggende kjennskap til hva risikostyring er og hvilken verdi det kan gi virksomheten

Deltakeren skal ha forståelse for forholdsmessighet mellom informasjonssikkerhet, personvern og pasientsikkerhet

Deltakeren skal ha kjennskap til styrende dokumenter som er relevante for risikovurdering

Deltakeren skal ha kjennskap til de mest nødvendige stegene i en risikovurdering



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 akseptabel risiko

Hensikten er å forebygge skade og tap på virksomhetens verdier -> opprettholde pasientens tillit til virksomheten og helsetjenesten

Risikostyring - en viktig del av internkontrollen

Hva bør vi minimum finne av styrende dokumenter i internkontrollen til virksomheten knyttet til risikostyring

- Overordnet risikostyringsprosess
- Prosess for gjennomføring av risikovurdering
- Nivå for akseptabel risiko
- Vurderingskriterier
- Fullmaktsmatrise
- (Overordnet sikkerhetsmål/prinsipper/sikkerhetsplan)

Oversikt over teknologi og behandling av helse- og personopplysninger

Virksomheten skal ha oversikt over:

- Behandlinger av helse- og personopplysninger, ofte kalt behandlingsprotokoll eller behandlingsoversikt; og

- IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten

Risikostyring av informasjonssikkerhet – som en del av virksomhetens prosesser

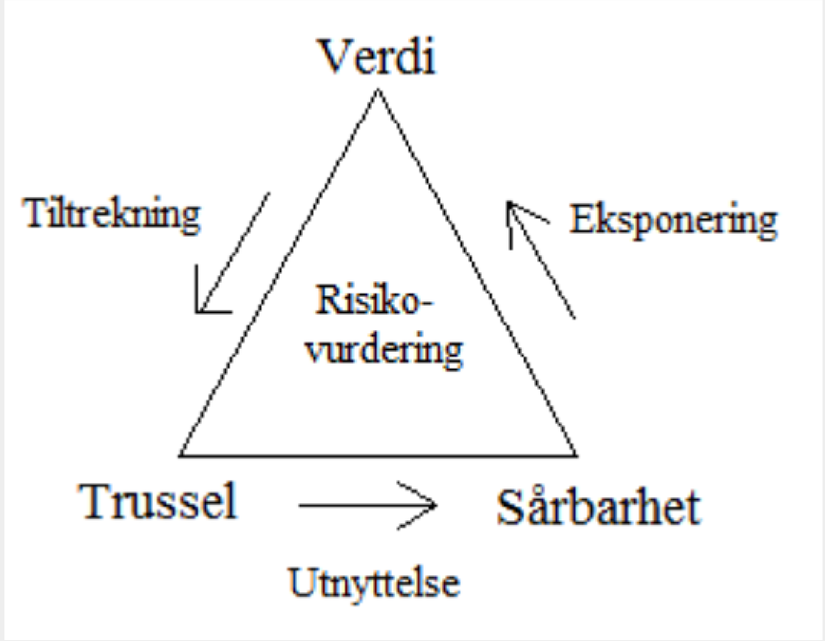
- Foranalyse av ansvarsområde
  - foranalyse hjelper systemeier/risikoeier å prioritere hvilke områder som behovet for risikovurdering er størst
  - støtte fra informasjonssikkerhetsressurser (som har best kjennskap til trusselbilde)

- Prosjekt og leveranseoppdrag – risikovurdering av informasjonssikkerhet og personvern som en delaktivitet i alle faser av prosjektet eller leveransen.
  - Kontinuerlige vurderinger- utfør tiltak og evt. justeringer på design og implementering

Hva er risikovurdering?

I en risikovurdering gjennomfører virksomheten nødvendige steg for å identifisere, vurdere og evaluere risiko knyttet til virksomhetens identifiserte verdier.

En risikovurdering er et beslutningsgrunnlag for ledere



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

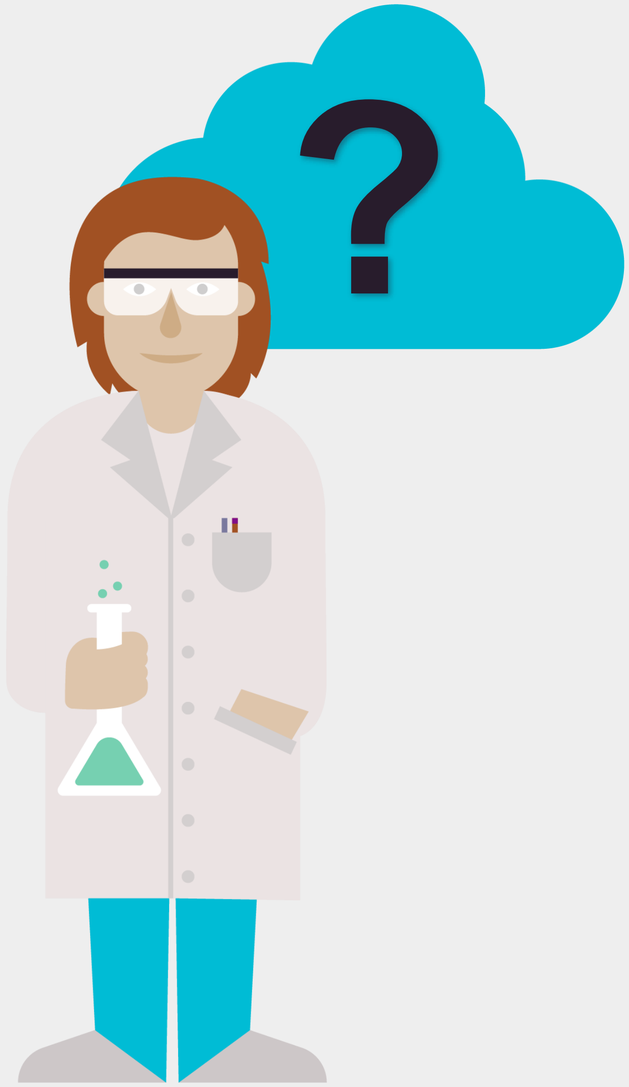
Risikovurdering bør oppdateres ved endring i trusselbildet

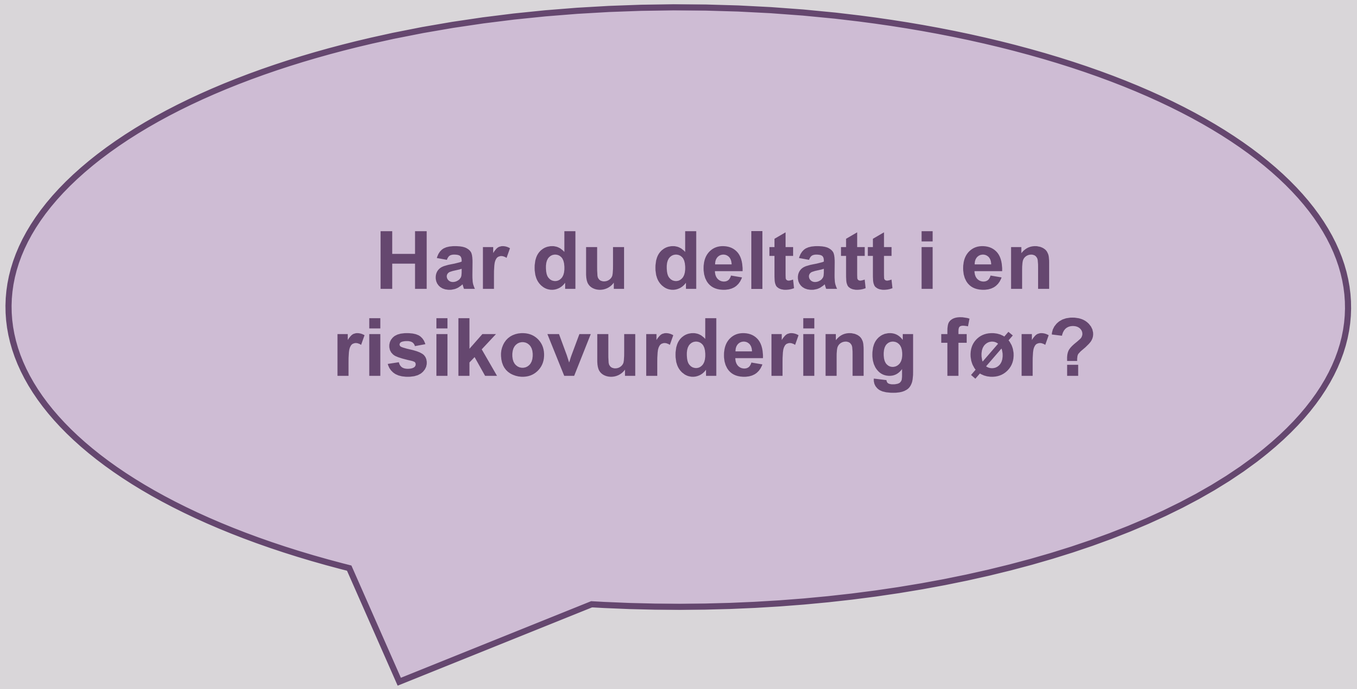
Hvordan risikovurderer vi?

Risikovurderingen bør være en strukturert prosess

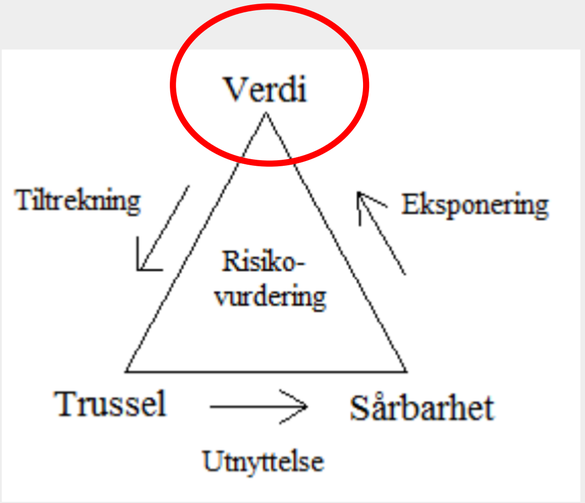
- Planlegging
- Forberede risikovurderingen
- Gjennomføre risikovurderingen
- Vurdering og anbefaling av nye tiltak

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.

Konfidensialitet

Tilgjengelighet (og robusthet)

Integritet

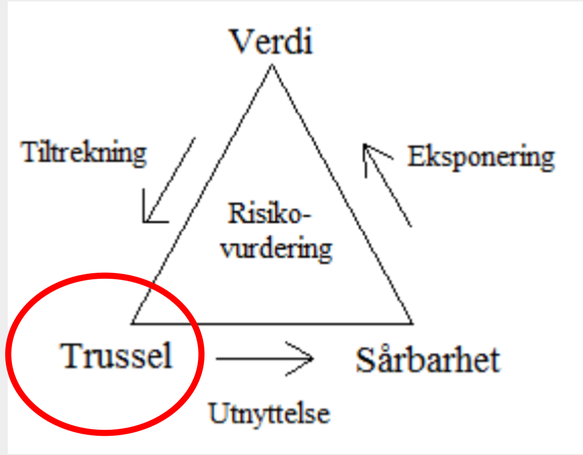
Eksempel:
Hjemmetjenesten i Normsund kommune går gjennom sine informasjonsverdier i forbindelse med risikovurdering av nytt EPJ-system.

Hva er den mest kritiske verdien?

Hvorfor?

Konfidensialitet
Integritet
Tilgjengelighet

Hvem skal vi beskytte oss mot?



- Trusselvurderingen 2023 for spesialisthelsetjenesten gir en grundig beskrivelse av det digitale trusselbildet mot spesialisthelsetjenesten.
- Bidrar med situasjonsforståelse og beslutningsstøtte
- Veldig relevant for risikovurderinger

Kilde: Utarbeidet av Sykehuspartner, Helse Nord IKT og HelseCERT, i samarbeid, og med støtte fra Helse Vest IKT og HEMIT.

KIT	Eksempel på scenario
K	Snoking, f.eks. helsepersonell som ser i journaler uten tjenstlig behov
K	Uautorisert tilgang til systemer med helse- og personopplysninger (tilsiktet, som følge av angrep eller lignende)
K	Uautorisert tilgang til systemer med helse- og personopplysninger (utilsiktet, pga. feil eller lignende)
K	Fysisk innbrudd/tyveri av opplysninger (utstyr)
K	Tilsiktet misbruk av sensitiv informasjon (for å presse/utnytte privatpersoner)
K	Tilsiktet misbruk av sensitiv informasjon (for å presse myndighetspersoner for politiske formål)
I	Uautorisert (mulighet for) endring av helse- og personopplysninger (tilsiktet, som følge av angrep eller lignende)
I	Uautorisert (mulighet for) endring av helse- og personopplysninger (utilsiktet, pga. feil eller lignende)
I	Helse- og personopplysninger knyttes til feil person i journal (feilføring)
I	Helse- og personopplysninger er ikke oppdaterte/feil i systemene
T	Tilsiktet og ikke-planlagte nedetider/utilgjengelighet på systemer (som følge av tjenestenektangrep, sabotasje, etc)
T	Utilsiktet nedetid på systemene (som følge av system- eller infrastrukturfeil, etc.)
T	Ikke tilgang til nødvendige helse- og personopplysninger eller annen kritisk informasjon (utilsiktet, som følge av feil etc.)
T	Ikke tilgang til nødvendige helse- og personopplysninger eller annen kritisk informasjon (tilsiktet, som følge av løsepengevirus eller andre typer angrep)
T	Brudd i kommunikasjon/funksjonalitet for sikker og rettidig deling av nødvendige helseopplysninger mellom samhandlende helsepersonell
T	Strømbrudd (fører til nedetid eller ødeleggelse)
T	Vannlekkasje (fører til nedetid eller ødeleggelse)
T	Naturkatastrofer og ekstremvær (fører til nedetid eller ødeleggelse)
KIT	Innsider benytter egne tilganger til andre formål (utro tjener)
KIT	Innsider benytter egne tilganger til andre formål som følge av press fra eksterne aktører (kriminelle, fremmede makter)
KIT	Innsider benytter egne tilganger til andre formål som følge av social engineering fra eksterne aktører (blir lurt, gjennom phishing eller andre teknikker)
KIT	Personell hos databehandler benytter tekniske tilganger til andre formål enn det som er regulert av databehandleravtalen
KIT	Menneskelig feil (utilsiktet)
	…

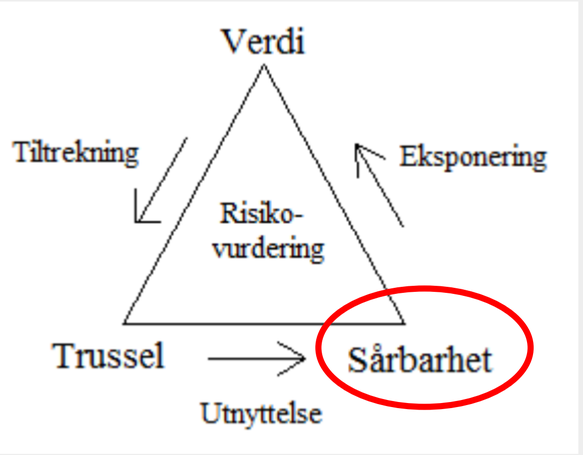
3.5 Eksempel på scenarioer i risiko-veilederen

NORMEN

Sårbarheter

- En sårbarhet er en svakhet, feil eller mangel som gjør at et trusselscenario kan gjennomføres, noe som dermed gjør det mer sannsynlig at en hendelse inntreffer.

- En sårbarhet kan også tolkes som en mangel på sikkerhetstiltak, dvs. at sårbarheten kan fjernes ved å innføre ett eller flere sikkerhetstiltak.



3.2 Eksempel på sannsynlighets-nivåer
i risikoveilederen

Eksempel på skala for sannsynlighet		
Sannsynlighets-nivå	**Frekvens** **(hvor ofte skjer det?)**	**Til støtte for vurdering av sannsynlighetsnivå: Tiltaksstyrke** **(hvor lett kan en uønsket hendelse skjer?)**
1 Usannsynlig	En gang hvert 5. år eller sjeldnere	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten • Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/ fullstendig kjennskap til tiltakene • Eksternt personell kan ikke omgå/bryte tiltaket
2 Mindre sannsynlig	En gang hvert år	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten • Tiltakene kan likevel omgås/brytes av egne medarbeidere med normale ressurser, som i tillegg har normal kjennskap til tiltakene • Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse
3 Mulig	En gang hver måned	• Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter fullt ut etter hensikten • Egne medarbeidere trenger kun normale ressurser for å omgå/bryte tiltakene – det er ikke nødvendig med kjennskap til tiltakene • Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke prosedyrer som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normale ressurser
4 Sannsynlig	En gang hver uke	• Sikkerhetstiltak er ikke etablert, eller • Det er kjent at tiltakene omgås/brytes av egne medarbeidere • Kan omgås/brytes av eksternt personell med normale ressurser og uten kjennskap til tiltakene
5 Svært sannsynlig	Daglig eller oftere	• Sikkerhetstiltak er ikke etablert, eller • Det er kjent at tiltakene omgås/brytes eksternt personell med normale ressurser uten kjennskap til tiltakene

NORMEN

3.3 Eksempel på konsekvens-nivåer *i risikoveilederen*

Eksempel på skala for konsekvens	
Konsekvensnivå	**Eksempler angitt for tilgjengelighet, konfidensialitet og integritet**
1 Ubetydelig/ ingen	• Stans i tjenesteleveranse forekommer ikke • Intet uautorisert innsyn i helse- og personopplysninger • Journal er komplett • Ingen påvirkning på pasienters helse • Ikke brudd på personvernet • Ikke økonomisk tap • Ikke tap av omdømme
2 Lav	• Stans i tjenesteleveranse opptil 30 minutter • Uautorisert innsyn i enkelte helse- og personopplysninger og lovbrudd • Noen mangler i journal slik at helse- og personopplysninger ikke er fullstendige og ajourført i forhold til behandlingen av opplysningene • Ingen påvirkning på pasienters helse • Brudd på personvernet for et lite antall pasienter • Gjenopprettelig økonomisk tap • Noe midlertidig tap av omdømme ovenfor pasienten eller virksomheten
3 Moderat	• Stans i tjenesteleveranse opptil 2 timer • Uautorisert innsyn i flere helse- og personopplysninger, mulighet for endring og brudd på lov • Informasjon mangler i journal og brudd på lov • Det gis tilgang til en bruker fra en ekstern virksomhet som ikke har tjenstlig behov for EPJ for en eller flere pasienter • Skade, velferdstap eller påvirkning på pasienters helse • Brudd på personvernet for et moderat antall pasienter • Alvorlig økonomisk tap • Midlertidig eller moderat tap av omdømme ovenfor pasienten eller omgivelsene
4 Alvorlig	• Stans i tjenesteleveranse opptil 5 timer • Uautorisert innsyn i store mengder helse- og personopplysninger, mulighet for endring og brudd på lov • Viktig informasjon mangler i journal og brudd på lov • Det gis tilgang til en bruker fra en ekstern virksomhet som ikke har tjenstlig behov for EPJ for en eller flere pasienter • Alvorlig skade, velferdstap eller påvirkning for pasienters helse • Brudd på personvernet for et stort antall pasienter • Alvorlig økonomisk tap • Alvorlig tap av omdømme overfor pasienten eller omgivelsene
5 Svært alvorlig	• Stans i tjenesteleveranse mer enn 5 timer • Fullt uautorisert innsyn i eller mulighet for endring av alle helse- og personopplysninger og brudd på lov • Kritisk informasjon mangler i journal og brudd på lov • Medikament, dosering eller behandlingstiltak blir feilregistrert • Helse- og personopplysninger knyttes til feil person og fører til svært alvorlig påvirkning på pasienters helse • Tilgang til behandlingsrettet helseregister (inkl. EPJ) og helse- og personopplysninger kommer på avveie • Tap av liv • Svært alvorlig økonomisk tap • Svært alvorlig tap av omdømme

NORMEN

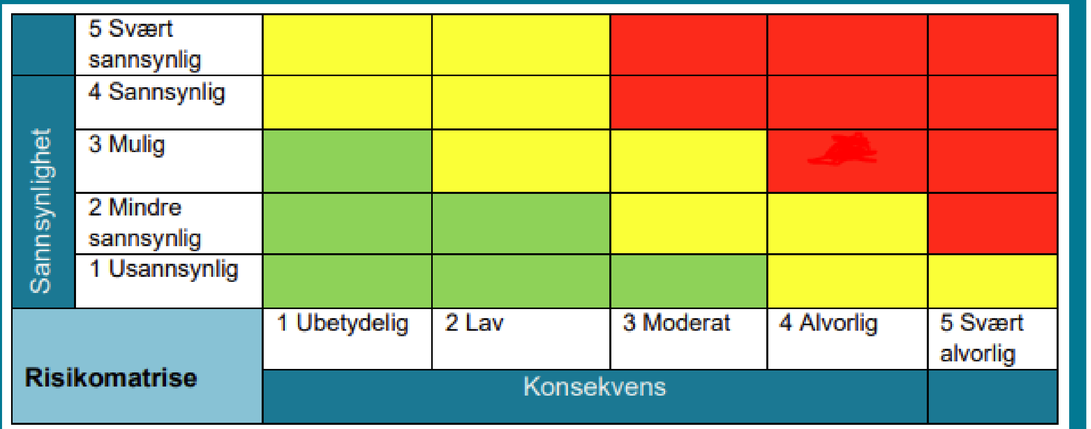
Eksempel:
Hjemmetjenesten i Normsund kommune gjennomfører risikovurdering av nytt EPJ-system.

De har blant annet valgt seg ut scenarioet «Løsepengevirus gjør EPJ-systemet utilgjengelig», og skal vurdere hvor sannsynlig det er at hendelsen inntreffer og hvor alvorlige konsekvenser den få for at de skal kunne levere forsvarlig helsehjelp.

Hvor sannsynlig er det?

Hvilke konsekvenser kan det få?

Hvor plasserer vi scenarioet i risikomatrisen?



2.3.6 Risiko i risiko-veilederen

2.3.7 Risiko-reduserende tiltak og risikoaksept i risikoveilederen

Eksempel:
Hjemmetjenesten i Normsund kommune gjennomfører risikovurdering av nytt EPJ-system. Scenarioet «Løsepengevirus gjør EPJ-systemet utilgjengelig» er vurdert å være en rød risiko.

Helse- og personopplysningene i hjemmetjenestens EPJ er sentral for å ivareta både informasjonssikkerhet, personvern og pasientsikkerhet. Kommunen benytter nivåer for akseptabel risiko i sin risikostyring, og for dette systemet skal risikoen være på grønt nivå. Derfor kan ikke hjemmetjenesten akseptere en risiko som er høyere enn grønn i matrisen kommunen deres bruker.

	5 Svært sannsynlig					
Sannsynlighet	4 Sannsynlig					
	3 Mulig				Risiko i scenarioet	
	2 Mindre sannsynlig		Akseptabel risiko			
	1 Usannsynlig					
Risikomatrise		1 Ubetydelig	2 Lav	3 Moderat	4 Alvorlig	5 Svært alvorlig
		Konsekvens				

Siden risikoen er rød, må beslutningen om eventuell risikoaksept eskaleres til kommunens øverste ledelse. Ledelsen får risikovurderingen presentert, og beslutter at det må gjennomføres tiltak for å redusere risikoen i dette scenarioet – den er for høy til at virksomheten kan akseptere den.

Det vil ikke være mulig å redusere denne risikoen til null, så tiltak av menneskelig, teknologisk og organisatorisk art må sikte på å redusere restrisikoen til et akseptabelt nivå. Merk at denne vurderingen er et eksempel for å illustrere metodikken, og ikke en fasit på hvilken risiko virksomheten kan akseptere i dette scenarioet.

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?
- Akseptabel risiko
- Hvilke tiltak kan få risikoen ned på et akseptabelt nivå?
  - Menneskelige, teknologiske, organisatoriske

Vurderinger

Ledelsen eier 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) og omvendt!
  - Ikke gitt hvilken rekkefølge – ofte i parallell – men anbefales aldri i samme prosess

- Det er en del av den dataansvarliges ansvar å gjennomføre egnede tekniske og organisatoriske tiltak
  - Disse kan blant annet finnes på grunnlag av risikovurderinger av informasjonssikkerheten

Hvor finner jeg mer om risiko?

- Normens kapittel 3 – Risikostyring
- Informasjon om relevante risikoscenarioer i spesifikke faktaark og veiledere på ulike temaer (som for eksempel i faktaark 54 om videokonsultasjon, MU-veilederen, skyveilederen)
- **Veileder om risikostyring for informasjonssikkerhet og personvern**

normen.no

NORMEN

Veileder om risikostyring for informasjonssikkerhet og personvern

Versjon 1.1
21. november 2022

Utarbeidet med støtte fra Direktoratet for e-helse
Vedtatt av Styringsgruppen for Normen