Kort sagt om...

NST
Nasjonalt senter for samhandling og telemedisin

Risikovurdering av informasjonssikkerhet

Risikovurdering er en prosess for å klarlegge sannsynlighet for og konsekvenser av uønskede hendelser. Ulike betegnelser blir brukt om en slik prosess: Risikoanalyse, risikovurdering, sårbarhetsanalyse, konsekvensanalyse, ROS-analyse.

Dette faktaarket beskriver en metode for risikovurdering basert på internasjonale standarder.

Man skiller gjerne mellom følgende hovedaspekter ved informasjonssikkerhet:

1. **Konfidensialitet:** beskytte mot innsyn fra uvedkommende.
2. **Tilgjengelighet:** sikre at tilstrekkelige og relevante opplysninger er til stede og kan nås ved behov.
3. **Integritet:** beskytte mot utilsiktet eller uautorisert endring av data eller systemer. I dette inngår også ikke-benekting, dvs. å sikre at den som har utført en handling, f.eks. stilt en diagnose, foreskrevet behandling, lest/hentet ut informasjon, ikke kan nekte for dette i ettertid.
4. **Kvalitet:** sikre at informasjonen til enhver tid er korrekt.

Krav om risikovurdering

Personopplysningsloven § 13 omhandler krav til informasjonssikkerhet ved behandling av personopplysninger, basert på tilsvarende bestemmelse i EUs personverndirektiv. Av personopplysningsforskriften § 2-4 følger at den ansvarlige for behandlingen av personopplysninger skal gjennomføre *risikovurdering* for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd.

Når bør risikovurdering gjennomføres?

Når nye løsninger utvikles og/eller før de settes i drift er det viktig å få en oversikt over risikoer og behovet for tiltak.
Risikovurdering bør startes så tidlig som mulig i et utviklingsløp. Slik kan tjenesten/produktet tilpasses kravene fra risikovurderingen i forkant.

Ved endringer internt eller eksternt som påvirker sikkerheten må risiko vurderes på nytt.

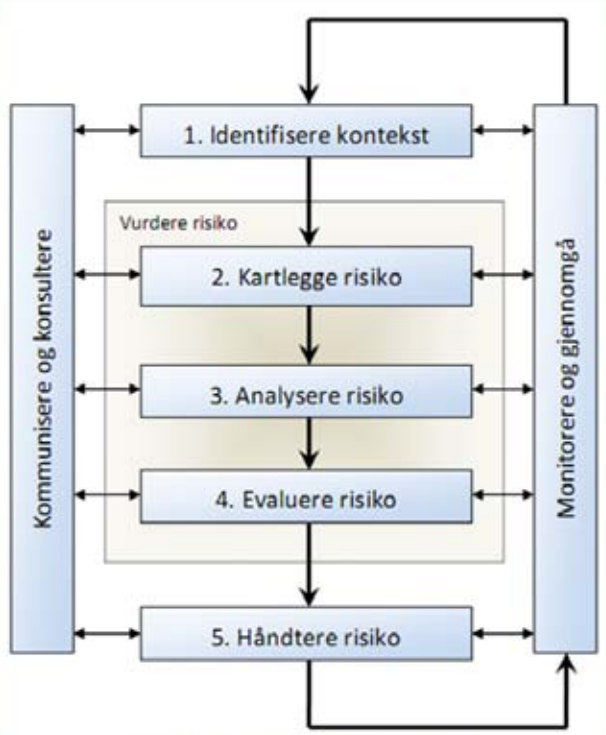
Metodikk i fem steg

Metoden for risikovurdering baserer seg på den internasjonale standarden ISO/IEC 27005:2011 Information security risk management. Denne standarden er basert på den mer overordnede standarden ISO/IEC 31000:2009 Risk management principles and guidelines.

Metoden omfatter følgende fem hovedtrinn:

1. **Identifisere kontekst:** Hva er det som skal analyseres og hvilke rammebetingelser gjelder?
2. **Kartlegge risikoer:** Verdier, trusler, sikkerhetstiltak, sårbarheter og type konsekvenser.
3. **Analysere risikoene:** Vurdere sannsynlighet og konsekvens for den enkelte trussel og beregne risikonivå ut fra sannsynlighet og konsekvens for de identifiserte truslene.
4. **Evaluere risikoene:** Sammenligne beregnet risikonivå med akseptabelt nivå for risiko.
5. **Håndtere risikoene:** Foreslå tiltak og planer for gjennomføring av tiltakene.

Disse punktene gjenspeiles i følgende figur, basert på ISOs standarder.



Figur 1: Prosess for risikostyring

Kartlegging og analyse av risiko kan med fordel foregå i en styrt idédugnad der alle relevante aktører deltar. I forkant av idédugnaden må konteksten og rammebetingelsene for risikovurderingen identifiseres (steg 1 i prosessen). Etter idédugnaden må risikoene evalueres og risikoreduserende tiltak foreslås (steg 4 og 5 i prosessen).

Steg 1: Identifisere kontekst

Forutsetninger for og omfang av risikovurderingen må fastsettes. Det omfatter på den ene siden planlegging av tids- og ressursbruk og økonomiske rammer for analysen. På den annen side må man enes om en tydelig beskrivelse og avgrensning av hva som skal analyseres. Denne bør inneholde en systemskisse som viser teknisk infrastruktur, eventuelle sikkerhetsmekanismer, systemets omgivelser, brukere og dataflyt.

Man må også beskrive tydelig:

- Hva skal beskyttes? Konkrete verdier, f.eks. maskiner, type informasjon (f.eks helseopplysninger) – og/eller konseptuelle verdier som "tilliten til norsk helsevesen".
- Sikkerhetskrav og -policy, lover og regler.
- Definisjon av sannsynlighetsnivå, konsekvensnivå og risikonivå (f.eks. Liten, Moderat, Stor), og hva disse nivåene innebærer.
- Akseptkriterier – hvilke nivå av risiko som kan aksepteres.

>>

Steg 2: Kartlegge risiko

Målet med dette steget er å kartlegge mulige trusler ved å:

- Identifisere potensielle uønskede hendelser
- Kartlegge mulige årsaker til slike hendelser
- Beskrive kjente sårbarheter/svakheter

Her er det viktig å involvere både ansvarlig ledelse, brukere av systemet/tjenesten, driftspersonell og personer med sikkerhets-kompetanse. Uønskede hendelser kan ha ulik opprinnelse. Det kan være både målrettede misbruk og uaktsomhet/brukerfeil, fra eksterne og interne aktører, menneskeskapte hendelser og eventuelle ytre påvirkninger fra omgivelsene (f.eks. strømbrudd, brann, oversvømmelse).

Ulike teknikker kan benyttes i kartleggingen av trusler. Vi benytter ofte styrt/strukturert idédugnad med en systematisk gjennomgang av systemet med hensyn på sikkerhetsaspektene konfidensialitet, integritet, tilgjengelighet og kvalitet. Dette kan suppleres med intervjuer og spørreskjema eller mer formelle teknikker (f.eks. FTA, FMECA, Hazop).

Trusselkartleggingen dokumenteres på en oversiktlig måte i en trusseltabell (se eksempel under steg 3 nedenfor). Her beskriver man de mulige uønskede hendelsene med mulige årsaker, og noterer viktige kommentarer som kommer fram i diskusjonen. Nødvendig rydding og strukturering av tabellen gjøres når steg 2 er avsluttet.

Steg 3: Analysere risiko

For hver av truslene som ble identifisert i steg 2 skal man vurdere konsekvens, sannsynlighet og risiko, og oppdatere trusseltabellen med verdier for disse.

Id	Trussel, hendelse	Årsak	Sannsynlighet	Konsekvens	Risiko	Kommentarer
k1	Uvedkommende får tilgang til sensitiv info	Brukernavn og passord på gul lapp under tastaturet	Stor "Halvparten i vår avd gjør det"	Stor Brudd på konfidensialitet	Høy	Bevisstgjøring, opplæring
k2	Pasientopplysninger sendt til feil mottaker	Feil mottaker registrert i journalsystemet, eller valgt feil fra adresseregister	Stor Skjer daglig	Stor Brudd på konfidensialitet	Høy	
t1	Journalsystemet utilgjengelig i én time	Server-krasj etter strømbrudd	Liten	Moderat	Lav	

Figur 2: Trusseltabell

Risiko defineres som produktet av **konsekvens** og **sannsynlighet**. Det kan framstilles i en todimensjonal matrise. Eksemplet fra trusseltabellen vil se slik ut:

Konsekvens / Sannsynlighet	Liten	Moderat	Stor	Alvorlig
Liten		t1		
Middels				
Stor			k1, k2	

Figur 3: Risikomatrise

Steg 4: Evaluere risiko

Resultatet av analysen i steg 3 skal evalueres i forhold til akseptansenivå og -kriterier man ble enige om i steg 1.
Man får da en oversikt over hvilke trusler som kan aksepteres og hvilke trusler som ikke har akseptabel risiko.

Her er det verdt å huske at:
*Å akseptere en **risiko***
er ikke det samme som
*å akseptere en uønsket **hendelse***

Steg 5: Håndtere risiko

Det er flere mulige måter å håndtere risiko:

1. Unngå risiko (risk avoidance)
   - Ikke utføre den risikable handlingen (f.eks. ikke gjøre endring, ikke bruke systemet)
2. Redusere risiko (risk reduction)
   - Iverksette tiltak for å redusere sannsynlighet og/eller konsekvens
3. Overføre/dele risiko (risk transfer, risk sharing)
   - F.eks. overføre til et forsikringsselskap
4. Beholde risiko (risk retention)
   - Leve med den risikoen som er der

I steg 5 vil det ofte være aktuelt å foreslå tiltak for å redusere risikonivået for de uakseptable truslene (pkt 2 over).

Risikovurderingen oppsummeres i en risikorapport.
Flere detaljer om metodikken finnes i NSTs veiledning og rapportmal for risikovurdering: www.telemed.no/sikkerhet, under overskrift "Risikovurdering".

Andre referanser:

- ISO 31000:2009: Risk management – Principles and guidelines
- ISO 27005:2011: Information security risk management
- LOV-2000-04-14-31: Personopplysningsloven
- FOR-2000-12-15-1256: Personopplysningsforskriften
- Faktaark nr. 7 til Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (www.normen.no)
- Datatilsynets veileder for risikovurdering: www.datatilsynet.no/upload/Dokumenter/veiledere/Risikoveileder_pdf.pdf
- Norsk Helsenetts veileder for risikovurdering: www.norsk-helsenett.no/informasjonssikkerhet/risikovurdering

Kontaktpersoner ved NST

Risikovurdering og datasikkerhet:
Eva Henriksen
eva.henriksen@telemed.no
Tlf: +47 957 31 836

Eva Skipenes
eva.skipenes@telemed.no
Tlf: +47 911 77 515

Juridiske spørsmål:
Ellen K. Christiansen
ellen.christiansen@telemed.no
Tlf: +47 416 84 705

Leif Erik Nohr
leif.erik.nohr@telemed.no
Tlf: +47 901 43 166

Se www.telemed.no/faktaark for andre faktaark i serien.