

Forslag til skjema for risikovurdering – utfyllingsveiledning

Forhold og krav	Krav og forhold som er viktige for informasjonssikkerheten vurderes og føres inn først. Dette kan være lover, forskrifter, prosesser, rutiner/prosedyrer, system, arkiv, lokaler osv.
Trusselbeskrivelse	Kort beskrivelse av trusselbildet – hva kan skje? Uønskede mulige situasjoner, hendelser eller handlinger som kan oppstå og som kan representere en fare for informasjonssikkerheten. Mulige konsekvenser for brukere, økonomi, ansatte, omdømme osv beskrives kort. Kan uttrykkes i tekst eller kostnader.
Sannsynlighetsgradering (S)	Hvor stor sannsynlighet er det for at trusselen inntreffer (hvor ofte forventes den uønskede hendelsen å inntreffe -frekvens)? S=4: Svært sannsynlig (hendelsen inntreffer flere ganger hvert år) S=3: Meget sannsynlig (hendelsen inntreffer årlig eller sjeldnere) S=2: Sannsynlig (hendelsen inntreffer en gang pr 10 år eller sjeldnere) S=1: Lite sannsynlig (hendelsen inntreffer en gang per 50 år eller sjeldnere) Merk: Angivelsen av frekvens/antall må tilpasses virksomheten og tjenesten som vurderes. Bruken (volumet) av tjenesten som skal risikovurderes er sentralt.
Konsekvensgradering (K)	Hvor alvorlige vil konsekvensen/skaden kunne være? K=4; Katastrofalt K=3; Kritisk K=2; Farlig (kan være uheldig) K=1; Lite farlig (dette lever vi godt med) Et utgangspunkt for vurderingen kan være hva som skal til for å gjenopprette. Konsekvensgradering av at lover/forskrifter ikke blir oppfylt, settes alltid til høyt.
Tiltak	Risikoen er produktet av S og K. Akseptabelt risikonivå skal være nedfelt i virksomhetens sikkerhetspolicy. Dersom risikoen er større eller lik det akseptable nivå (for eksempel $K \times S \geq 8$) skal det iverksettes risikoreduserende tiltak (tiltak som reduserer sannsynligheten eller konsekvensene av uønsket hendelse). Gjennomføring av tiltak bør knyttes til en kost-nytte-vurdering. Når tiltaket skal være gjennomført og hvem som er ansvarlig, bør føres inn. Hvis tiltaket ikke er gjennomført innen fristen skal det registreres som avvik.
Forventet effekt av tiltak	Før inn forventet ny risiko etter at planlagt tiltak er gjennomført.
Opplevd effekt av tiltak	Før inn opplevd ny risiko etter at planlagt tiltak er gjennomført. Hvis tiltaket ikke har hatt den ønskede effekten, må nytt tiltak vurderes iverksatt.