Omgrep og tilnærmingar i risikohandteringa

**Dette er eit døme på ei kort oversikt over sentrale omgrep og tilnærmingar i risikohandteringa. Oversikta kan nyttast av personar som skal førebu seg til å delta i arbeid med å foreslå handtering av risikoar.**

# Handteringsalternativ

Når risikoar skal handterast, har vi grovt sett fire alternativ – også kalla handteringsalternativ. Desse er

* unngå risiko
* dele risiko
* redusere risiko
* akseptere risiko

Vi kan unngå ein risiko ved å slutte å gjere oppgåva som skaper risikoen eller ved å gjere oppgåva på ein annan måte eller med andre hjelpemiddel.

Vi kan dele ein risiko ved å kjøpe ei forsikring der det er aktuelt. Vi kan også setje ut delar av verksemda og inngå tenesteavtalar (SLA). I slike avtalar kan det vere klausular om økonomisk erstatning ved tap av visse typar informasjon, eller det kan vere avtalt økonomisk kompensasjon ved tenesteavbrot over ei viss tid o.l.

Vi kan redusere ein risiko ved å etablere tryggingstiltak. Dette er tiltak som vert etablerte for å verke over tid.

Vi kan akseptere ein risiko dersom kriteria for å akseptere risiko er oppfylte.

# Føremål med sikkerheitstiltak

Ved alternativet «redusere risiko», bør vi vere medvitne føremålet med ulike sikkerheitstiltak.  Vi vil oftast vere opptekne av ulike kombinasjonar av å

* førebygge
* oppdage
* reagere

Å **førebygge** inneber å hindre at uønskte hendingar skjer. Å **oppdage** inneber å oppdage at uønskte hendingar har skjedd. **Reagere** inneber å reagere på og handtere uønskte hendingar etter at dei har skjedd, slik at konsekvensar kan unngåast eller reduserast.

Uønskte hendingar er hendingar som kan gje uønskte konsekvensar. Alle tre føremåla handlar derfor om å redusere potensielle konsekvensar og/eller tilhøyrande sannsyn for at konsekvensane skal verte ein realitet. Det er på den måten vi reduserer ein risiko.

Nokre tryggingstiltak er samansette og kan derfor verke inn på fleire av føremåla over.

# Verkeområde

Tryggingstiltak har forskjellige verkeområde – området der tiltaket har effekt.

Nokre tiltak inngår i sentrale prosessar som gjeld for heile verksemda, andre tiltak vert etablerte for eitt bestemt informasjonssystem. Tiltak kan etablerast for ei bestemt arbeidsoppgåve, for ei organisatorisk eining, eller for å sikre ein bestemt fysisk lokasjon. Det er viktig at ein er medviten om kva verkeområde eit tiltak har.

# Typar tryggingstiltak

Når tiltak skal identifiserast og veljast, vil det ofte vere nyttig å først ha ei overordna tilnærming til kva type tiltak som kan vere føremålstenlege. Vi grupperer derfor ofte tiltaka etter type, til dømes slik:

* Organisatoriske tiltak (rollar og ansvar, retningslinjer, prosedyrar og rutinar, mv.)
* Menneskelege tiltak (kompetanse og kultur)
* Tekniske tiltak (IKT-løysingar, skap, dører, rom, bygningar mv.)

Desse tiltakstypane over er generelle, og er ikkje spesielle for informasjonssikkerheit. Dei er relevante for alle område der ein ønsker at den samla internkontrollen i verksemda skal dekke. Eitt tiltak kan verke inn på fleire internkontrollområde.

I risikohandteringa er det å tenke på tiltakstypar nyttig i samband med den innleiande refleksjonen over kva typar tiltak som er føremålstenlege å velje, før ein går ned på detaljerte tiltak.

Hugs at fleire tiltak, både av same og av ulik type, kan vere aktuelle for ein og same risiko.

# Tiltaksområde

Når ein vurderer og vel tiltak er det nyttig å sjå på relevante tiltaksområde. Dette er «familiar» av tryggingstiltak som heng saman, ofte knytt til ein felles tiltaksleverandør sitt ansvarsområde.

Inndelinga kan gjerast på forskjellige måtar. På overordna nivå kan éi slik inndeling vere:

* føringar frå leiinga (policy og retningslinjer)
* arbeidsrutinar hjå dei som utfører oppgåvene
* kompetanse og kultur hjå dei som utfører oppgåvene
* personaladministrasjon
* tilgangsstyring
* drifta av IKT-løysingane
* fysiske tilhøve der arbeidsoppgåvene vert utførte
* fysiske tilhøve der IKT-infrastruktur er plassert
* anskaffingar og oppfølging av leverandørar
* beredskapsplanar og -rutinar

# Effekt, kostnad og negative sideeffektar

Ulike tiltak vil ha ulik innverknad på risikoen (risikoreduserande effekt), ulik direkte økonomisk kostnad og ulike negative sideeffektar. Det er viktig å vurdere og vege alle desse tre tilhøva opp mot kvarandre ved vurdering av og val av tiltak.