Begrep og tilnærminger i risikohåndteringen

**Dette er et eksempel på en kort oversikt over sentrale begrep og tilnærminger i risikohåndteringen. Oversikten benyttes av personer som skal forberede seg til å delta i arbeid med å foreslå håndtering av risikoer.**

# Håndteringsalternativ

Når risikoer skal håndteres, har vi grovt sett fire alternativ – også kalt håndteringsalternativ. Disse er

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

Vi kan unngå en risiko ved å slutte å gjøre oppgaven som skaper risikoen eller ved å gjøre oppgaven på en annen måte eller med andre hjelpemidler.

Vi kan dele en risiko ved å kjøpe en forsikring der det er aktuelt. Vi kan også sette ut deler av virksomheten og inngå tjenesteavtaler (SLA). I slike avtaler kan det være klausuler om økonomisk erstatning ved tap av visse typer informasjon, eller det kan være avtalt økonomisk kompensasjon ved tjenesteavbrudd over en viss tid o.l.

Vi kan redusere en risiko ved å etablere sikkerhetstiltak. Dette er tiltak som etableres for å virke over tid.

Vi kan akseptere en risiko dersom kriteriene for å akseptere risiko er oppfylt.

# Formål med sikkerhetstiltak

Ved alternativet «redusere risiko», bør vi være bevisst formålet med ulike sikkerhetstiltak. Vi vil oftest være opptatt av ulike kombinasjoner av å

* forebygge
* oppdage
* reagere

Å **forebygge** innebærer å hindre at uønskede hendelser skjer. Å **oppdage** innebærer å oppdage at uønskede hendelser har skjedd. **Reagere** innebærer å reagere på og håndtere uønskede hendelser etter at de har skjedd, slik at konsekvenser kan unngås eller reduseres.

Uønskede hendelser er hendelser som kan gi uønskede konsekvenser. Alle tre formålene handler derfor om å redusere potensielle konsekvenser og/eller tilhørende sannsynlighet for at konsekvensene skal bli en realitet. Det er på den måten vi reduserer en risiko.

Noen sikkerhetstiltak er sammensatte og kan derfor virke inn på flere av formålene over.

# Virkeområde

Sikkerhetstiltak har forskjellige virkeområder – området hvor tiltaket har effekt.

Noen tiltak inngår i sentrale prosesser som gjelder for hele virksomheten, andre tiltak etableres for ett bestemt informasjonssystem. Tiltak kan etableres for en bestemt arbeidsoppgave, for en organisatorisk enhet, eller for å sikre en bestemt fysisk lokasjon. Det er viktig at man er bevisst hvilket virkeområde et tiltak har.

# Typer sikkerhetstiltak

Når tiltak skal identifiseres og velges, vil det ofte være nyttig å først ha en overordnet tilnærming til hvilken type tiltak som kan være hensiktsmessige. Vi grupperer derfor ofte tiltakene etter type, for eksempel slik:

* Organisatoriske tiltak (roller og ansvar, retningslinjer, prosedyrer og rutiner, mv.)
* Menneskelige tiltak (kompetanse og kultur)
* Tekniske tiltak (IKT-løsninger, skap, dører, rom, bygninger mv.)

Disse tiltakstypene over er generelle, og er ikke spesielle for informasjonssikkerhet. De er relevante for alle områder man ønsker at virksomhetens samlede internkontroll skal dekke. Ett tiltak kan virke inn på flere internkontrollområder.

I risikohåndteringen er det å tenke på tiltakstyper nyttig i forbindelse med den innledende refleksjonen over hvilke typer tiltak som er hensiktsmessig å velge, før man går ned på detaljerte tiltak.

Husk at flere tiltak, både av samme og av ulik type, kan være aktuelle for en og samme risiko.

# Tiltaksområder

Når en vurderer og velger tiltak er det nyttig å se på relevante tiltaksområder. Dette er «familier» av sikkerhetstiltak som henger sammen, ofte knyttet til en felles tiltaksleverandørs ansvarsområde.

Inndelingen kan gjøres på forskjellige måter. På overordnet nivå kan én slik inndeling være:

* føringer fra ledelsen (policy og retningslinjer)
* arbeidsrutiner hos dem som utfører oppgavene
* kompetanse og kultur hos dem som utfører oppgavene
* personaladministrasjon
* tilgangsstyring
* driften av IKT-løsningene
* fysiske forhold der arbeidsoppgavene utføres
* fysiske forhold der IKT-infrastruktur er plassert
* anskaffelser og oppfølging av leverandører
* beredskapsplaner og -rutiner

# Effekt, kostnad og negative sideeffekter

Ulike tiltak vil ha ulik innvirkning på risikoen (risikoreduserende effekt), ulik direkte økonomisk kostnad og ulike negative sideeffekter. Det er viktig å vurdere og veie alle disse tre forholdene opp mot hverandre ved vurdering av og valg av tiltak.