# Risikostyring

## Hvem har ansvar for risikostyring

Det er verdieier som er eier av risikoen og er ansvarlig for risikostyringen. Den sikkerhetsansvarlige skal bistå i den praktiske gjennomføringen av risikovurderingen og gi råd underveis. Verdieieren har ansvar for gjennomføring og oppfølging av tiltak. Det skal orienteres om gjennomførte risikovurderinger i ledergruppen, og særskilte risikoer og tiltak med vesentlig kostnad skal behandles.

## Risikovurdering

Risikovurdering består i å identifisere, analysere og evaluere risiko. Risikovurderinger gjennomføres systematisk, periodisk og ved vesentlige endringer i oppgaver eller omgivelsene. Risikovurderinger i *<virksomhet>* gjennomføres på grunnlag av NS 5832 «Samfunssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse» og veiledere i sikringsrisikoanalyse utgitt av Nasjonal Sikkerhetsmyndighet.

Arbeidet med risikovurderinger er initiert av:

* Årlige overordnede risikovurderinger
* Nye eller vesentlige endringer i tiltak, prosesser, IT-systemer, regulatoriske krav mv.
* Vesentlige endringer i trusselbildet
* Hendelser identifisert i og rapportert fra avvikshåndtering
* Status eller hendelser identifisert i og rapportert fra sikkerhetsrevisjon, egenkontroll og Ledelsens gjennomgang

## Risikohåndtering

Risikohåndtering er hvordan vi tar stilling til hvordan risikoer skal håndteres. Det skjer på bakgrunn av både resultatet fra risikovurderingene og ledelsens føringer for risikohåndteringen. Det er fire hovedmåter vi håndterer risiko på:

* Akseptere risiko
* Unngå risiko
* Overføre/flytte risiko
* Behandle/modifisere risiko

Hvordan risikoeier velger å håndtere risiko styres av eventuelle pålegg i form av lover og regler, føringer fra ledelsen, risikoens sannsynlighet og konsekvens, formålseffektiviteten til aktuelle tiltak, forventet kostnad og gevinst, samt kontraktuelle forhold.

Til sist i risikohåndteringen lages en plan for hvem som skal etablere valgte tiltak innen hvilke frister. Disse planene følges opp av risikoeier.

## Nivå og skala for risiko

*Eksempel:*

|  |
| --- |
| **Klassifisering av konsekvenser** |
|   |   | Lav | Moderat | Høy | Svært høy |
| **Virksomhet** | **Liv og helse for eget personell** | *Medfører ingen alvorlig personskade eller sykefravær* | *Mindre alvorlig personskade som ikke medfører varig uførhet* | *Alvorlig personskade som medfører varig uførhet* | *Dødsfall* |
| **Omdømme** | *Noe negativ publisitet, men ingen påviselig feil i <virksomhet>s leveranser eller rutiner.* | *Tidsbegrenset negativ publisitet og begrenset til enkelthendelse. Eventuelle konsekvenser berører enkeltpersoner.*  | *Negativ publisitet som fører til interne omorganiseringer og/eller endrede ansvarsforhold. Kan føre til rekrutterings-problemer.* | *Vedvarende negativ publisitet og omtale fører til omstrukturering og/eller reduserte rammebetingelser og/eller betydelige rekrutterings-problemer.* |
| **Økonomi** | *Direkte økonomiske tap inntill 0,1 mill. kr.*  | *Direkte økonomiske tap mellom 0,1 og 1 mill. kr.*  | *Direkte økonomiske tap mellom 1 og 5 mill. kr.* | *Direkte økonomiske tap over 5 mill. kr* |
| **Operativ drift** | *Mindre forsinkelser i tjeneste-leveranse*  | *Moderate forsinkelser i tjeneste-leveranse* | *Betydelig forsinkelse i tjenesteleveranse* | *Stopp i kritisk tjenesteleveranse. Tap av styring og kontroll.*  |
| **Brudd på kontrakt/****avtale** | *Mindre avvik* | *Kontraktsbrudd medfølgende erstatningskrav* | *Kontraktsbrudd medfølgende rettssaker og erstatninger* | *Alvorlige kontraktsbrudd medfølgende lange kostbare rettssaker og store erstatninger* |
| **Brudd på lovverk** | *Pålegg om utbedring* | *Forelegg eller påtale som relateres til enkelthendelse. Kan innebære endringer av praksis i <virksomhet>*  | *Dom med sanksjoner og/eller bøter. Kan innebære endringer av praksis i <virksomhet>.* | *Dom knyttet til strukturelle feil eller mangler. Betydelig økonomiske sanksjoner og/ eller bøter. Mulige konsekvenser for ansvarsforhold i <virksomhet>* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Samfunn** | **Nasjonal sikkerhet og suverenitet** | *Kan i noen grad medføre skadefølge.* | *Kan skade.* | *Alvorlig kan skade.* | *Helt avgjørende skadefølger.* |
| **Eksterne** | **Konsekvenser for behandlingsansvarlig** |   |   |   |   |
| **Konsekvenser for underleverandør** |   |   |   |   |
| **Konsekvenser for den registrerte**  |   |   |   |   |