***(Kommentarar og nokre råd er skrivne i gult innleiingsvis og undervegs i dokumentet.***

*Dette dømet dekkjer «alle» internkontrollområde på operativt nivå. Det har denne forma for å synleggjere korleis føringar for risikostyring innan informasjonssikkerheit kan integrerast med andre operative område der det er naturleg. Dette tilrår vi som primær tilnærming, jf. efvlf. § 15, som seier at internkontrollen på informasjonssikkerheitsområdet* «bør være en integrert del av virksomhetens helhetlige styringssystem»

*Om ein ønskjer ei eiga retningslinje berre for informasjonssikkerheit eller for nokre færre område, kan dømet enkelt snevrast inn ved å justere pkt. 2 Bruk.* ***Dei som gjenbrukar sentrale delar av dømet, er sjølv ansvarlege for kvalitetssikring av innhaldet og tilpassing til eiga verksemd.***

*Merk at retningslinja berre dekkjer risikoar på* ***operativt nivå****. Det er desse som er dei sentrale i eit internkontrollarbeid innan informasjonssikkerheit. Operative risikoar omfattar uønskte hendingar og konsekvensar i den operative utføringa av oppgåver og tenester.*

*Sentrale føringar for operativ risikostyring kan skilje seg ein del frå føringar for risikostyring på strategisk og taktisk nivå i ei verksemd. Vi rår til at verksemdene vurderer å lage ei eiga retningslinje for å vurdere og handtere risiko på strategisk og taktisk nivå.* Dette fell utanfor fokuset til internkontroll informasjonssikkerheit. *Døme under bør likevel kunne gje inspirasjon også til delar av innhaldet for risikostyring på strategisk og taktisk nivå.)*

Innhald

[1. Innleiing 2](#_Toc90480922)

[1.1 Målgruppe 2](#_Toc90480923)

[1.2 Føremål 2](#_Toc90480924)

[1.3 Bruk 2](#_Toc90480925)

[1.4 Relaterte policyar og retningslinjer 2](#_Toc90480926)

[2. Risikoforståing 2](#_Toc90480927)

[3. Gjennomføre risikovurderingar og risikohandtering 2](#_Toc90480928)

[3.1 Hovudprosess 2](#_Toc90480929)

[3.2 Gjennomføring av hovudprosessen 3](#_Toc90480930)

[4. Førande prinsipp for handtering av risiko 3](#_Toc90480931)

[5. Førande prinsipp for risikoaksept 4](#_Toc90480932)

[6. Forenklingar i risikoarbeidet 4](#_Toc90480933)

[6.1 Konsekvenskategoriar 4](#_Toc90480934)

[6.2 Nivå som måleeining 5](#_Toc90480935)

[6.3 Normering av nivåa for konsekvens, sannsyn og risiko. 5](#_Toc90480936)

[7. Kommunisere risiko 5](#_Toc90480937)

[7.1 Risikoskildring 5](#_Toc90480938)

[7.2 Risikostorleik 6](#_Toc90480939)

[7.3 Uttrykke risiko 6](#_Toc90480940)

[Vedlegg A: Risikoforståing – sentrale omgrep og samanhengar 8](#_Toc90480941)

[Vedlegg B: Kriterium for å akseptere risiko 10](#_Toc90480942)

[Vedlegg C: Normerande skildringar av risikonivå 11](#_Toc90480943)

[Vedlegg D: Normerande skildringar av konsekvensnivå 12](#_Toc90480944)

[Vedlegg E: Normerande skildringar av sannsynsnivå 14](#_Toc90480945)

[Vedlegg F: Samanheng mellom normering av risikonivå og kriterium for å akseptere risiko 15](#_Toc90480946)

[Vedlegg G: Framgangsmåte for å estimere nivå på konsekvensen, sannsyn og risiko 16](#_Toc90480947)

[Vedlegg H: Støtte ved estimat av sannsynsnivå 18](#_Toc90480948)

# Innleiing

## Målgruppe

Dette dokumentet er ein del av verksemda sitt styrande dokument. Målgruppa er alle i verksemda som har behov for å estimere, handtere og kommunisere om risiko på operativt nivå.

## Føremål

Føremålet er å

1. etablere ei sams forståing i verksemda av kva risiko er
2. etablere ein effektiv og tilstrekkeleg einsarta måte å uttrykkje, estimere og handtere operative risikoar på

Operative risikoar omfattar uønskte hendingar og konsekvensar i den operative utføringa av oppgåver og tenester.

## Bruk

Dokumentet kjem til bruk på alle internkontrollområde som det ikkje er gjeve spesifikke alternative føringar for. (Alternativt at retningslinja berre gjeld informasjonssikkerheit eller nokre få operative område. Namnet på retningslinja bør også justerast om ein avgrensar bruksområdet)

## Relaterte policyar og retningslinjer

Dokumentet må sjåast i samanheng med følgjande

* Policy for informasjonssikkerheit
* (Eventuelt andre tilsvarande «toppdokument» for andre område)
* Retningslinja *Roller og ansvar*

# Risikoforståing

Ei skildring av sentrale omgrep og samanhengar rundt risikoforståing er gjeve i *Vedlegg A: Risikoforståelse - sentrale begrep og sammenhenger*. Dette vedlegget skal vere kjent og forstått av alle som har behov for å estimere, handtere og kommunisere om risiko hos oss.

# Gjennomføre risikovurderingar og risikohandtering

Relevante risikoar som kan hindre måloppnåing skal identifiserast og ved behov handterast. Dette er eit ansvar for risikoeigarar og systemeigarar fellessystem, jf. retningslinja *Roller og ansvar.*

## Hovudprosess

Konkrete risikovurderingar skal som minimum innehalde trinna identifisere, analysere og evaluere risikoar.

I trinnet identifisere, skal relevante risikoar identifiserast og gjevast ei risikoskildring. I trinnet analysere, skal dei enkelte risikoane analyserast og risikostorleiken reknast (estimerast). I trinnet evaluere, skal kvar risiko vurderast opp mot kriteria for å akseptere risiko.

Om evalueringa viser at nokre risikoar ikkje kan aksepterast som dei er, skal dei gjennom ein prosess for å vurdere og velje risikohandtering.

Om ein risiko framleis ikkje kan aksepterast, og det ikkje finst akseptable måtar å unngå risikoen på, skal ikkje oppgåva som skaper risikoen gjennomførast eller fortsetje.

Fokus, arbeidsinnsats og tiltak skal vere tilpassa risiko og vesentlegheit.

(Om ein behandlar informasjon eller forvaltar informasjonssystem (eller objekt og infrastruktur) etter sikkerhetsloven må ein syte for at elementa som inngår i vurdering av risiko inkluderer det som er påkravd i virksomhetsikkerhetsforskriften §12, for alle områda der dette regelverket kjem til bruk.)

## Gjennomføring av hovudprosessen

Undervegs i arbeidet skal vi normalt bruke dei forenklingane som er skildra i kapittel *6 Forenklingar i risikoarbeidet*.

Risikoar skal normalt uttrykkast slik det er skildra i kapittel

* *7.1 Risikoskildring*
* *7.2 Risikostørrelse*
* *7.3 Uttrykke risiko*

Ved estimering av risikostorleik skal ein stø seg på normeringane i

* *Vedlegg C: Normerande skildringar av risikonivå*
* *Vedlegg D: Normerande skildringar av konsekvensnivå*
* *Vedlegg E: Normerande skildringar av sannsynsnivå*

Det er under estimeringa tilrådd å stø seg på prosessen i *Vedlegg G: Framgangsmåte for å estimere nivå på konsekvensen, sannsyn og risiko*, samt *Vedlegg H: Støtte ved estimat av sannsynsnivå*.Tidsbruk på denne støtta bør tilpassast risikoen og eigenarten til risikovurderinga.

Ved evaluering av risikoar skal ein leggje til grunn *Vedlegg B: Kriterium for å akseptere risiko*.

I risikohandteringa skal ein følgje prinsippa i kapittel *4 Førande prinsipp for risikohandteringa*.

Om ikkje særlege grunnar tilseier noko anna, skal elles dei metodane, rettleiingane og støtteverktøya verksemda stiller til disposisjon for ulike typar risikovurderingar brukast.

# Førande prinsipp for handtering av risiko

Følgjande prinsipp skal leggjast til grunn i handtering av risiko hos oss.

Ressursinnsats og fokus

1. Ressursinnsatsen på å finne alternative arbeidsmåtar og risikoreduserande tiltak skal stå i samsvar med storleiken på risikoen.
2. Under identifisering av tiltak skal heile utfallsrommet for ein risiko vurderast, under dette alle råka konsekvenskategoriar.
3. For risikoar som inkluderer så høge konsekvensar eller sannsyn at dei går langt utanfor normale ytterpunkt i risikomatrisa vår, skal det alltid vurderast om risikoen i realiteten er så stor at han bør handterast som om han var på eit høgare risikonivå enn risikostorleiken indikerer.

Unngå risikoen

1. Alternative arbeidsmåtar som gjer at ein kan unngå risikoen, skal vurderast og eventuelt veljast ut frå kor føremålstenlege dei er, risikostorleik og kostnad.

Val av risikoreduserande tiltak

1. Aktuelle risikoreduserande tiltak skal vurderast opp mot nytte (risikoreduserande effekt), negative sideeffektar og kostnader elles.
2. Tiltak som reduserer risikoar som gjeld liv og helse, skal veljast og implementerast om det ikkje kan dokumenterast at tiltaka klart kostar meir enn nytta (ALARP-prinsippet).
3. Tiltak som reduserer risikoar som gjev andre konsekvensar enn liv og helse, skal veljast og implementerast om tiltaka har ei vesentleg positiv nytte/kost (nytte/kost-prinsippet).

Nye tiltak i eksisterande oppgåver og system

1. I påvente av implementering av valde tiltak, skal det straks vurderast om det er behov for eventuelle mellombelse ekstratiltak eller stopp i gjennomføring av pågåande oppgåver og bruk av system.

Tiltak i nye oppgåver og system

1. Nye arbeidsoppgåve og system skal som hovudregel ikkje startast eller takast i bruk før valde tiltak er implementerte.

# Førande prinsipp for risikoaksept

Følgjande prinsipp skal liggje til grunn i kriteria våre for å akseptere risiko:

1. Storleiken på aksepterte risikoar skal stå i eit rimeleg tilhøve til kor viktig og nyttig oppgåva/tenesta som skaper risikoen er.
2. Aksept av risikoar skal berre kunne skje når risikoen er låg eller at det er gjennomført ei risikohandtering i samsvar med kapittel 4 *Førande prinsipp for handtering* av risiko.
3. Aksept av risikoar skal skje på eit leiarnivå som står i samsvar med storleiken på risikoen.

Dette fører med seg dei kriteria for å akseptere risiko som er skildra i *Vedlegg B: Kriterium for å akseptere risiko*.Desse skal liggje til grunn for evalueringa av risikoar i risikovurderingar.

*Vedlegg F: Samanheng mellom normering av risikonivå og kriterium for å akseptere risiko* illustrerer korleis kriteria for å akseptere risiko heng saman med andre føringar for risikovurdering.

# Forenklingar i risikoarbeidet

## Konsekvenskategoriar

Konsekvenskategoriar er ei enkel gruppering av måla våre. Konsekvenskategoriar skal brukast som støtte i estimeringa av konsekvensar og der det er føremålstenleg som tilleggsinformasjon i kommunikasjonen om risiko.

Vi skal bruke følgjande sams konsekvenskategoriar i risikovurderingane våre.

* Tenestenivå
* Personvern
* HMS
* Regelverk (anna)
* Økonomien vår

Dette reknast som verksemdskritiske kategoriar.

(Det presiserast at kategoriane over er døme. Dei må vurderast og veljast ut frå eigenarten og behova til den enkelte verksemda. Om ein behandlar informasjon eller forvaltar informasjonssystem etter sikkerhetsloven vil det vere behov for ein kategori som dekkjer konsekvensar for grunnleggjande nasjonale funksjonar og nasjonale sikkerheitsinteresser.)

## Nivå som måleeining

Storleiken på konsekvensar, sannsyn og risiko er sentral i vurderinga vår av og kommunikasjon om risiko. Vi skal bruke ei forenkling av storleikane og har delt dei i nivå.

Følgjande nivånemningar skal som hovudregel brukast på både konsekvens, sannsyn og risiko.

* Svært høg
* Høg
* Moderat
* Låg
* Ubetydeleg

Det siste nivået «Ubetydeleg» brukast berre om ein skal vise storleiken på risikoskildringar som eigentleg ikkje representerer nokon risiko. Om noko har ubetydeleg konsekvens eller ubetydeleg sannsyn vil risikoen hos oss alltid vere ubetydeleg. Vi reknar ikkje dette som nokon risiko.

## Normering av nivåa for konsekvens, sannsyn og risiko.

Normerande skildringar av nivåa på konsekvens, sannsyn og risiko er gjevne i

* *Vedlegg C: Normerande skildringar av risikonivå*
* *Vedlegg D: Normerande skildringar av konsekvensnivå*
* *Vedlegg E: Normerande skildringar av sannsynsnivå*

Desse skal brukast som støtte i estimering av nivå på kvar av dei tre delane.

Det er i tillegg tilrådd å stø seg på prosessen i *Vedlegg G: Framgangsmåte for å estimere nivå på konsekvensen, sannsyn og risiko*, samt *Vedlegg H: Støtte ved estimat av sannsynsnivå*.

# Kommunisere risiko

## Risikoskildring

Alle risikoar vi vurderer skal gjevast ei risikoskildring som verbalt skildrar sentrale delar ved ei uønskt hending og tilhøyrande konsekvensar.

Innretning og detaljeringsnivå kan variere ut frå kontekst. I svært enkle samanhengar kan nokre få stikkord vere nok.

Ofte må likevel risikoskildringa utdjupast noko meir og dekkje heile hendingsforløpet. Der det ikkje er rekna som ueigna er følgjande tilrådd omfang på ei risikoskildring:

* nokre stikkord som karakteriserer:
  1. den innleiande hendinga i eitt eller fleire ledd
  2. kva som skaper sjølve målavviket (t.d. skade, informasjonssikkerheitsbrot e.l.)
  3. konsekvensane som kan oppstå

Døme:

|  |
| --- |
| *(1) Tilsette pratar om sosialsaker i kantina, naboar til klientar høyrer dette; (2) Brot på teieplikt; (3) Naboar snakkar om ting dei ikkje skulle vite, klientar opplever ubehag, barn blir stengde ute* |
| *(1) Organiserte kriminelle, sosial manipulering av tilsette via ekstern IKT-tilgang; (2) Kriminelle endrar beløp og utbetalingskonto i økonomisystem; (3) Feil utbetalingar, vi taper pengar, andre får ikkje det dei har krav på* |
| *(1) Brann i sørvarrom; (2) Alle system dett ned; (3) All aktivitet i verksemda ute av drift* |
| *(1) Tilsette arbeider på skjeremaskina; (2) Tilsette skjer seg; (3) Delar av hender kuttast, ulik grad av skade* |

## Risikostorleik

Alle risikoar vi vurderer skal vi gje ein risikostorleik. Han skal omfatte nivåa på konsekvens, tilhøyrande sannsyn og risiko.

For å forstå ein risiko må vi vere merksame på at ei risikoskildring kan ha eit stort utfallsrom, dvs. ei rekkje kombinasjonar av moglege konsekvensnivå og tilhøyrande sannsyn som kvar kan gje ulike risikonivå.

I risikovurderingane våre er vi spesielt opptekne av å identifisere kva risikoar som må handterast før dei eventuelt kan aksepterast. Då er høgaste nivå på risikoane for og etter risikohandtering sentralt. Samstundes ønskjer vi å gjennomføre effektive risikovurderingar.

Vi vel difor å forenkle kommunikasjonen og **avgrense omgrepet risikostorleik til eitt punkt i utfallsrommet** for ei risikoskildring. Det punktet skal vere den kombinasjonen av mogleg konsekvens og tilhøyrande sannsyn som gjev **det høgaste risikonivået.**

Dette vil **oftast** vere **det mest forventa konsekvensnivået og tilhøyrande sannsyn.** Den hypotesen bør likevel alltid vurderast og risikostorleiken eventuelt justerast til slutt i estimering av risikostorleik.

Det presiserast at sjølv om vi forenklar og vel eitt punkt i utfallsrommet som uttrykk for risikostorleik, så vil heile utfallsrommet vere viktig å forstå og relevant å vurdere under risikohandteringa og i kommunikasjon om risikoen.

## Uttrykke risiko

Minimum

Ein risiko skal hos oss som minimum uttrykkast ved hjelp av

* ei risikoskildring (jf. pkt. 7.1)
* ein risikostorleik (jf. pkt. 7.2)

Risikostorleiken skal uttrykke det høgaste risikonivået på risikoskildringa og innehalde nivå på

* 1. konsekvens
  2. tilhøyrande sannsyn (for det aktuelle konsekvensnivået)
  3. risiko (basert på kombinasjonen av konsekvens og tilhøyrande sannsyn)

Tillegg A (vanlege tillegg)

Det er rådd til at ein i tillegg alltid vurderer å uttrykkje følgjande frå analysen av risikoen

* råka konsekvenskategoriar (som følgje av risikoskildringa)
* sannsyn for at innleiande hending skjer og at målavvik[[1]](#footnote-2) oppstår
* konsekvenskategorien til risikostorleiken

Dette vil auke forståinga av risikoen for dei som les ei risikovurdering.

Tillegg B (utdjupande tillegg)

For komplekse risikoar bør ein også vurdere å supplere med utdjupande informasjon frå analysen. Dette kan vere omtale av sårbarheiter, spesielle dokumentasjonsteknikkar som skildrar risikoen, mv. Tilgjengeleg tid, storleiken og kompleksiteten på risikoen og nytta for dei som les risikovurderinga, bør avgjere kva ein eventuelt tar med.

Tillegg C (Kunnskapsstyrke)

Det det blir rekna som nyttig for avgjerdstakarar, bør ein alltid seie noko om kunnskapsstyrken[[2]](#footnote-3) bak dei analysar og estimat som er grunnlaget for uttrykka over. Det kan gjeras for ei risikovurdering samla, og for enkeltrisikoar eller som ein kombinasjon. I oppgjeving av kunnskapsstyrke skal ein bruke nivåa låg, moderat og høg. Det skal skje skjønsmessig.

Risikotabell og risikonotat

Minimumsdelen og tillegg A framføre, bør som hovudregel framstillast i ein risikotabell som kan sorterast på risikonivå. Alle vurderte risikoar bør gå fram av risikotabellen.

Ein risikotabell bør normalt vere eit vedlegg til eit risikonotat. Risikonotatet skal oppsummere viktige tilhøve rundt den gjennomførte risikovurderinga. Tillegg B og C framføre kan leggjast i risikonotatet eller i eigne vedlegg, avhengig av kva som reknast som føremålstenleg.

(Døma på vedlegga følgjer under)

# Vedlegg A: Risikoforståing – sentrale omgrep og samanhengar

Dette vedlegget gjev ei skildring av sentrale omgrep og samanhengar rundt risikoforståing. Vedlegget skal vere kjent og forstått av alle som har behov for å estimere, handtere og kommunisere om risiko hos oss.

Risiko, mål og usikkerheit

Risiko er moglege **avvik frå måla våre**, også kalla moglege avvik frå ønskte resultat eller ønskte tilstandar. Det er alltid knytt usikkerheit til moglege avvik. Usikkerheita er ein del av risikoen og kan i hovudsak uttrykkast som **sannsynet** for kvart avvik. Sannsynet er her eit uttrykk for kor truleg vi meiner det er at noko vil hende.

Vi kan i tillegg ha ulik grad av usikkerheit ved estimata våre – det vi trur. Den usikkeheita kan vi uttrykke ved å seie noko om graden vår av **kunnskapsstyrke**, dvs. kor god bakgrunnskunnskap og kvalitet vi har hatt i arbeidet med analysane våre, og på den måten kor sikre vi er på estimata av moglege avvik og sannsynet deira.

Mål og konsekvenskategoriar

Vi har ofte svært mange mål. For å forenkle risikovurderingar samstundes som vi har fokus på viktige målområde, brukar vi gjerne konsekvenskategoriar, t.d. tenestenivå, personvern, HMS, økonomi o.l. Konsekvenskategoriar er enkle grupperingar av sentrale mål. Dei moglege avvika (risikoane) ser ein då opp mot ein eller fleire av konsekvenskategoriane.

Positive og negative avvik

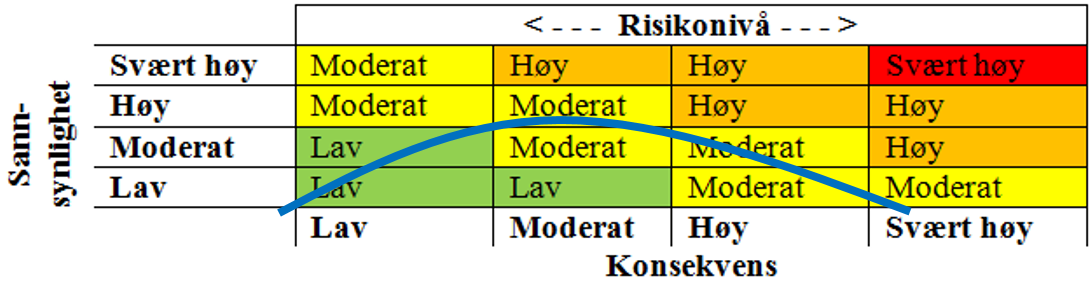
I ein del internasjonale standardar omfattar risiko både positive og negative avvik. Vi har hos oss valt å avgrense omgrepet risiko til negative avvik og kalle positive avvik for moglegheiter. Risiko og moglegheiter skal avvegast i verksemdsstyringa og i internkontrollarbeidet.

Konsekvensar og tilhøyrande sannsyn

Vi koplar ofte omgrepet risiko til **uønskte hendingar.** Vi kallar då moglege avvik frå mål for konsekvensar, og seier at risiko er **moglege konsekvensar og tilhøyrande sannsyn.** Orda «moglege» og «tilhøyrande» kan utelatast, men er då implisitte.

Utfallsrom

Ei uønskt hending kan ha mange forløp, og føre til ulike konsekvensar innan ulike konsekvenskategoriar. Kvar av desse vil som regel ha ulikt sannsyn.



Figuren viser ei risikomatrise med døme på sannsynsfordeling mellom ulike konsekvensnivå. Alle punkt på den blå streken, og området under streken, er moglege konsekvensnivå og tilhøyrande sannsyn for utfallet av ei hending. Vi kallar dette **utfallsrommet** for hendinga.

Vi delar opp i ei matrise med ruter og få nivå for å forenkle og effektivisere risikovurderingar og kommunikasjon om risiko.

Risikomatrise

For å forenkle analysen av risikoar delar ein ofte alle utfallsrom opp i ruter som representerer ulike nivå, slik det er gjort i figuren over. Det kallast ei **risikomatrise**.

Uttrykke risikostorleik

Omfanget av eller storleiken på ein risiko er eigentleg fordelinga av alle moglege konsekvensar og tilhøyrande sannsyn. Sidan ei risikoskildring kan ha eit stort utfallsrom med ei rekkje ulike konsekvensar som kvar har sine sannsyn, kan dette bli komplekst når det skal reknast ut eller uttrykkast. Vi vel difor ofte ei forenkling også når vi skal seie noko om storleiken på ein risiko.

I dei fleste risikovurderingar er ein spesielt oppteken av å identifisere kva risikoar som må handterast før dei eventuelt kan aksepterast. Då er høgaste nivå på risikoane for og etter risikohandtering sentralt.

Ein vel difor ofte å **avgrense omgrepet risikostorleik til eitt punkt i utfallsrommet for ei hending.** Det bør vere den kombinasjon av mogleg konsekvens og tilhøyrande sannsyn som gjev **det høgaste risikonivået.** Sjølv om det er ei forenkling, kallast dette punktet ofte «*risikoen*» ved ei hending eller «*risikostorleiken*».

Det **presiserast** at sjølv om vi forenklar og vel eitt punkt i utfallsrommet som uttrykk for risikostorleik, så vil **heile utfallsrommet vere viktig å forstå og relevant å vurdere** under risikohandteringa og i kommunikasjon om risikoen.

Mest forventa konsekvensnivå

Riskostorleiken med det høgaste risikonivået vil ofte inkludere **det mest forventa konsekvensnivået**, dvs. toppunktet i bogen over. Ein tar difor ofte utgangspunkt i det mest forventa konsekvensnivået når ein skal finne risikostorleiken. Deretter finn ein sannsynet som høyrer til.

Ein må likevel vere merksam på at andre kombinasjonar av konsekvensnivå og sannsyn som høyrer til i somme tilfelle kan gje eit høgare risikonivå. Det gjeld t.d. når det mest forventa konsekvensnivået og tilhøyrande sannsyn gjev ein risikostorleik på nivå låg. Då kan utfall med større konsekvens men mindre sannsyn samla gje eit høgare risikonivå. Dette kan gje ulike krav til risikohandtering og risikoaksept. Ein bør difor vere merksam på problemstillinga, vurdere det i sluttfasen av estimeringa, og eventuelt justere valet av både konsekvensnivå og sannsyn som høyrer til, slik at ein faktisk uttrykkjer den største risikostorleiken for hendinga.

Sannsyn for ulike ting

Det er også viktig å merke seg at ein ofte snakkar om **sannsyn for ulike ting.** Sannsynet for at ei **hending kan skje og gje målavvik** (t.d. skade, informasjonssikkerheitsbrot, vesentleg avvikande resultat) **er ein ting.** Sannsynet for at eit visst konsekvensnivå skal bli ein realitet, det vi kallar **tilhøyrande sannsyn, er noko anna.**

Det er den siste som er viktigast i risikovurderingar. Samstundes vil den siste byggje på den første og aldri vere høgare. Sannsynet for at ei innleiande hending skal hende og gje målavvik, vil på den måten kunne vere eit godt utgangspunkt i estimatet av tilhøyrande sannsyn til eit konsekvensnivå. Begge sannsyna er dessutan nyttige i den samla risikoforståinga og risikohandteringa.

# Vedlegg B: Kriterium for å akseptere risiko

|  |  |
| --- | --- |
| **Risikonivå** | **Kriterium for å akseptere risiko** |
| **Låg** | Kan aksepterast **utan å leite etter eller vurdere nytta av** alternative arbeidsmåtar eller fleire risikoreduserande tiltak. Merk at dette gjeld når heile utfallsrommet for ein risiko har risikostorleik på nivå låg innan alle råka konsekvenskategoriar. |
| **Kan aksepterast av leiarar på alle avgjerdsnivå.** |
| **Moderat** | Oppgåva/tenesta som utførast har **vesentleg betydning** for å nå **måla til verksemda**. |
| Det er gjennomført eit **systematisk arbeid** for å identifisere alternative arbeidsmåtar og risikoreduserande tiltak for denne eller direkte samanliknbare risikoar. |
| Alternative arbeidsmåtar som gjer at ein kan unngå risikoen **er ikkje føremålstenlege, gjev høgare risiko på dette eller andre område, eller er vesentleg meir kostbare.** |
| Tiltak er valde i samsvar med **prinsippa** for **ALARP** på liv og helse og **nytte/kost** på andre område (jf. kapittel *4 Førande prinsipp for handtering* av risiko) |
| Nytta ved at oppgåva/tenesta blir utført blir rekna som større enn risikoen. |
| **Kan aksepterast av leiarar på alle avgjerdsnivå.** |
| **Høg** | Oppgåva/tenesta som utførast er **naudsynt** for å nå **måla til verksemda**. |
| Det er gjennomført eit **systematisk og grundig** arbeid for å identifisere alternative arbeidsmåtar og risikoreduserande tiltak for denne eller direkte samanliknbare risikoar. |
| Alternative arbeidsmåtar som gjer at ein kan unngå risikoen **er svært lite føremålstenlege, gjev høgare risiko på dette eller andre område, eller er svært kostbare.** |
| Tiltak er valde i samsvar med **prinsippa** for **ALARP** på liv og helse og **nytte/kost** på andre område (jf. kapittel *4 Førande prinsipp for handtering* av risiko) |
| Nytta ved at oppgåva/tenesta blir utført er større enn risikoen. |
| **Kan berre aksepterast av leiarar på minimum avdelingssjefsnivå.** |
| **Svært**  **høg** | Oppgåva/tenesta som blir utført er **strengt naudsynt** for å nå **måla til verksemda.** |
| Det er gjennomført eit **systematisk og svært grundig** arbeid for å identifisere alternative arbeidsmåtar og risikoreduserande tiltak for denne eller direkte samanliknbare risikoar. |
| Alternative arbeidsmåtar som gjer at ein kan unngå risikoen **er totalt ikkje føremålstenlege, gjev høgare risiko på dette eller andre områder, eller er utanfor det økonomiske handlingsrommet til verksemda.** |
| Tiltak er valde i samsvar med **prinsippa** for **ALARP** på liv og helse og **nytte/kost** på andre område (jf. kapittel *4 Førande prinsipp for handtering* av risiko) |
| Nytta ved at oppgåva/tenesta blir utført er større enn risikoen. |
| **Kan berre aksepterast av direktør eller assisterande direktør.** |

# Vedlegg C: Normerande skildringar av risikonivå

Risikomatrisa under viser kva kombinasjonar av konsekvensnivå og tilhøyrande sannsynsnivå som skal gje kva slags risikonivå hos oss.

Om noko har ubetydeleg konsekvens eller ubetydeleg sannsyn vil risikoen hos oss alltid vere ubetydeleg. Vi reknar ikkje dette som nokon risiko.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sannsyns-nivå** |  |  | **< --- Risikonivå --- >** | | | |
| **Svært høg** | Ubetydeleg | Moderat | Høg | Høg | Svært høg |
| **Høg** | Ubetydeleg | Moderat | Moderat | Høg | Høg |
| **Moderat** | Ubetydeleg | Låg | Moderat | Moderat | Høg |
| **Låg** | Ubetydeleg | Låg | Låg | Moderat | Moderat |
| **Ubetydeleg** | Ubetydeleg | Ubetydeleg | Ubetydeleg | Ubetydeleg | Ubetydeleg |
|  |  | **Ubetydeleg** | **Låg** | **Moderat** | **Høg** | **Svært høg** |
|  |  | **Konsekvensnivå** | | | | |

*(Ein må sjå utforminga av vedlegg B, C, D og E i samanheng. Nivåskildringane i vedlegg D og E (konsekvensnivå og sannsynsnivå) avgjer til sjuande og sist krav til risikohandtering og kva risikoar som kan aksepterast av leiarar på ulike nivå, jf. vedlegg B (kriterium for å akseptere risiko. Vedlegg C her fungerer som kopling mellom vedlegg D og E i botn og vedlegg B på topp.*

*Vedlegga er normalt rimeleg enkle i bruk. Men for at dei skal fungere slik dei er meint, og for at ein skal ha ei målretta risikostyring i verksemda, må utforming og justeringar i vedlegga skje systematisk med eit medvite tilhøve til samanhengane.)*

# Vedlegg D: Normerande skildringar av konsekvensnivå

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Konsekvens-kategori** | **Indikatorar** |  | **Konsekvensnivå** | | | |
| **Ubetydeleg** | **Låg** | **Moderat** | **Høg** | **Svært høg** |
| Verksemdsnivå | Tenestenivå | Verknad [[3]](#footnote-4) | Ikkje merkbart | Eit lite merkbart økonomisk eller rettsmessig tap | Eit godt merkbart økonomisk eller rettsmessig tap | Påverkar fungering i samfunnet | Vesentleg hindrar fungering i samfunnet  (eller meir) |
| Regelverk[[4]](#footnote-5) | Verknad3 |
| Personvern | Verknad[[5]](#footnote-6) | Ikkje merkbart | Nokon kan føle seg krenkte | Dei fleste ville følt seg krenkte |
| HMS | Behandlingsbehov | Må ikkje behandlast | Må ikkje til lege e.l. | Krev lege eller  inntil 2 dg sjukehus e.l. | 2dg til 2 veker på sjukehus e.l. | Meir enn 2 veker sjukehus e.l. |
| Sjukmelding | Ingen | Maks 1 veke | Over 1,  maks 5 veker | Over 5,  maks 25 veker | Over 25 veker |
| Økonomien vår | Økonomisk tap [[6]](#footnote-7) | Tap <= 1.000 | Tap <= 5.000 | Tap <= 20.000 | Tap <= 80.000 | Tap > 80.000 |

*(****Det blir presisert at tabellen over er eit døme.*** *Kva slags kategoriar, indikatorar og* ***ikkje minst*** *nivåskildringar som faktisk skal brukast, må diskuterast i og tilpassast til den enkelte verksemda. Skildringane ein vel for ulike konsekvensnivå her i vedlegg D, må sjåast i samanheng med val og nivåskildringar av tilhøyrande sannsynskategoriar (jf. vedlegg E). Det er viktig at nivåskildringane i desse to skalaane er utforma* ***rimeleg proporsjonalt****, slik at faktoren ved auke langs den eine aksen i hovudsak har tilsvarande faktor i auke langs den andre aksen. Då vil dei reelle risikonivåa i vedlegg C bli rimeleg riktig framstilte. Samstundes må skildringane ha ei utforming som gjer dei effektive å bruke i estimeringa av nivå på konsekvens og tilhøyrande sannsyn.*

*Har ein behov for nye konsekvenskategoriar, t.d. «nasjonale sikkerheitsinteresser», må ein leggje inn nye rader i tabellen over (eller lage nye tabellar), og finne føremålstenlege indikatorar og nivåskildringar for desse kategoriane. Ein bør då også vurdere om ein treng ein ekstra sannsynskategori med eigne intervall i vedlegg E, slik at samanhengen mellom dei nye konsekvens- og sannsynsskildringane blir fornuftige, og ein får ønskt risikonivå og reaksjon på ulike kombinasjonar, jf. vedlegg C (risikonivå) og B (kriterium for å akseptere risiko).* [*Nasjonal sikkerheitsmyndigheit (NSM)*](https://nsm.stat.no/) *har rettleiingsansvaret for sikkerhetsloven. Vi viser til dei om ein treng råd om kva som kan vere føremålstenlege rettleiande nivåskildringar for «nasjonale sikkerheitsinteresser».)*

# Vedlegg E: Normerande skildringar av sannsynsnivå

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Bruksområde: | **Økonomien vår**  (+ evt. fleire konsekvenskategoriar) | | Eventuelt andre konsekvenskategoriar med andre intervallbehov |
| Sannsynstype: | **Hyppigheit**  **per år** | **Hyppigheit**  **per periode** |  |
| **Sannsynsnivå** |  |  |  |  |
| **Svært høg** | Over 50 gongar per år | Over 1 gong per veke |  |
| **Høg** | Inntil 50 gongar per år | Inntil 1 gong per veke |  |
| **Moderat** | Inntil 12 gongar per år | Inntil 1 gong per mnd. |  |
| **Låg** | Inntil 3 gongar per år | Inntil 1 gong kvar 4. mnd. |  |
| **Ubetydeleg** | Tilnærma 0 | Tilnærma 0 |  |

*(****Det blir presisert*** *at kva slags sannsynskategoriar og nivåskildringar som faktisk skal brukast, må diskuterast i og tilpassast den enkelte verksemda.*

***I dømet over*** *er det berre lagt inne hyppigheitsskala for konsekvenskategorien «Vår økonomi». Stigninga mellom nivåa følgjer i hovudsak same* ***faktor 4*** *som for kategorien økonomi i dømet i vedlegg D. For å få ein funksjonell bruk i praksis, er nivåa i både vedlegg D og E noko avrunda i høve til det prinsipielt riktige.*

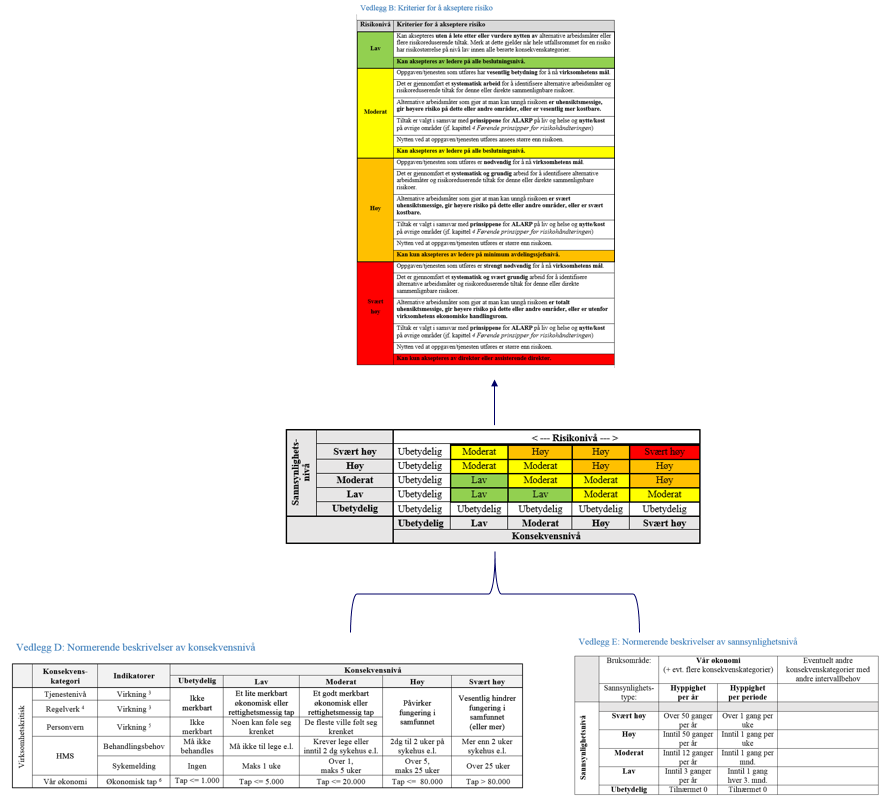
***Den enkelte verksemda må sjølv vurdere*** *kva slags faktor som bør brukast på «Vår økonomi» i vedlegg D og E. Same faktor bør brukast i begge vedlegga, med føremålstenleg avrunding.*

***Verksemda må også vurdere*** *om dei andre konsekvenskategoriane i vedlegg D skal bruke same hyppigheitshetsintervall som for «Vår økonomi», eller om dei må ha eigne intervall tilpassa eigenarten til kategorien. Det avgjerande er der ein ønskjer ulike kombinasjonar skal ende i vedlegg B (kriterium for å akseptere risiko).*

*Ein må difor først identifisere kva risikonivå (jf. vedlegg C) ulike kombinasjonar av konsekvensnivå og sannsynsnivå gjev (for dei enkelte konsekvenskategoriane), og deretter vurdere om den kombinasjonen bør føre med seg dei krava dette risikonivået gjev i vedlegg B (kriteria for å akseptere risiko).*

*For å få ein funksjonell bruk i praksis* ***rår vi til at ein er litt pragmatiske og ikkje lagar fleire intervallskalaar her i vedlegg E enn det som er naudsynt****. Om intervalla mellom sannsynsnivåa blir rekna som rimeleg riktige, bør ein bruke same intervallserie. Ein bør også vurdere om ein i staden for å lage eigne sannsynsintervall for ein konsekvenskategori, bør justere nivåskildringane for den aktuelle konsekvenskategorien i vedlegg D (konsekvensnivå).*

# Vedlegg F: Samanheng mellom normering av risikonivå og kriterium for å akseptere risiko



Figuren illustrerer korleis risikomatrisa fungerer som bindeledd mellom normering av konsekvens- og sannsynsnivå og kriteria for å akseptere risiko. (Figuren lesast nedanfrå og opp.)

# Vedlegg G: Framgangsmåte for å estimere nivå på konsekvensen, sannsyn og risiko

Framgangsmåten under er rådd til som støtte ved analyse og estimat av kvar risiko. Utgangspunktet er ei risikoskildring. Målgruppa er prosessleiarar for risikovurderingar.

**Generelt om punkta under**

Analyser ut frå behov ulike sider ved risikoskildringa. Vurder spesielt tilhøve rundt historisk hyppigheit, trugsmålsaktørar, sårbarheiter og trulege og moglege utviklingar av det som skjer undervegs i heile hendingsforløpet.

1. **Anslå «innleiande sannsyn»,** dvs. sannsynet for at innleiande hending vil skje og gje målavvik[[7]](#footnote-8).

* Bruk *Vedlegg H: Støtte ved estimat av sannsynsnivå* som hjelp. Ha fokus på den delen av hendinga som går fram mot at målavvik har skjedd.
* Noter ved behov anslått nivå på «innleiande sannsyn».

1. **Finn råka konsekvenskategoriar, mest forventa konsekvensnivå og førebels hovudkategori**

* Identifiser kva konsekvenskategoriar som i vesentleg grad råkast av risikoen. Noter ved behov namna på kategoriane.
* Anslå mest forventa konsekvensnivå på kvar av dei råka kategoriane. Bruk nivåskildringane i *Vedlegg D: Normerande skildringar av konsekvensnivå* som støtte.
* Kategorien med det høgaste av dei mest forventa konsekvensnivåa kan kallast førebels hovudkategori.

1. **Anslå tilhøyrande sannsyn og risikonivå på førebels hovudkategori**

* Ta utgangspunkt i førebels hovudkategori frå pkt. 2, denne sin mest forventa konsekvensnivå, samt «innleiande sannsyn» frå pkt. 1.
* Vurder om sannsynet som høyrer til dette konsekvensnivået er lågare enn «innleiande sannsyn»[[8]](#footnote-9).
* Anslå tilhøyrande sannsyn til det aktuelle konsekvensnivået ut frå dette. Bruk ved behov *Vedlegg H: Støtte ved estimat av sannsynsnivå* på nytt, for eventuelt å justere tilhøyrande sannsyn til eit lågare nivå enn «innleiande sannsyn».
* Bruk deretter *Vedlegg C: Normerande* skildringar av risikonivå som støtte. Anslå risikonivået ved å finne kryssingspunktet mellom mest forventa konsekvensnivå og tilhøyrande sannsyn.
* Noter konsekvenskategori samt konsekvensnivå, tilhøyrande sannsyn og risikonivå som førebels risikostorleik.
* Om tilhøyrande sannsyn ikkje er lågare enn «innleiande sannsyn»: Hopp over pkt. 4 [[9]](#footnote-10) og gå til pkt. 5.

1. **Anslå tilhøyrande sannsyn og risikonivå på alternative kategoriar**

* (Siste kulepunkt framføre avgjer om dette pkt. 4 skal gjennomførast)
* Vurder skjønsmessig om mest forventa konsekvensnivå frå nokre av dei andre råka kategoriane kan gje eit høgare risikonivå enn i pkt. 3.
* Anslå eventuelt tilhøyrande sannsyn og risikonivå for mest forventa konsekvensnivå i ein eller fleire av desse kategoriane. Bruk same framgangsmåte som i pkt. 3.
* Vel ein av desse kombinasjonane som ny førebels risikostorleik om den gjev høgast risikonivå.
* Noter eventuelt ny konsekvenskategori og konsekvensnivå, tilhøyrande sannsyn og risikonivå som ny førebels risikostorleik

1. **Vurder andre relevante kombinasjonar**

* Vurder skjønsmessig til slutt om andre relevante kombinasjonar av konsekvenskategori, konsekvensnivå og tilhøyrande sannsyn kan gje eit høgare risikonivå. Bruk *Vedlegg C: Normerande skildringar av risikonivå* som støtte.
  + Ver spesielt merksam på moglegheita for dette når førebels risikostorleik er låg, samstundes som det finst moglege utfall/konsekvensar ut mot høgre side av konsekvensaksen.
* Ved ja som vurderingssvar:
  + Vel antatt kategori og konsekvensnivå
  + Anslå tilhøyrande sannsyn til dette konsekvensnivået. Bruk ved behov *Vedlegg H: Støtte ved estimat av sannsynsnivå* som hjelp.
  + Anslå risikonivået ved hjelp av konsekvensnivå, tilhøyrande sannsyn og oppslag i *Vedlegg C: Normerande skildringar av risikonivå*
  + Vel dei nye kombinasjonane som endeleg riskostorleik om han gjev høgast risikonivå
* Ved nei:
  + Vel førebels risikostorleik frå pkt. 3 eller 4 som endeleg risikostorleik.

# Vedlegg H: Støtte ved estimat av sannsynsnivå

Dette vedlegget skal brukast som støtte ved estimat av sannsynsnivå (sjå også

Estimeringa av sannsynsnivåa skal skje skjønsmessig med støtte i dei normerande skildringane i tabellen under. Dei tre faktorane hyppigheit / % sannsynleg, trugsmålsaktørar og sårbarheit **skal ikkje brukast individuelt og isolert, men sjåast i samanheng.**

Følgjande framgangsmåte bør brukast (med støtte i tabellen under)

1. Ta utgangspunkt i historisk hyppigheit eller det vi veit om hyppigheit eller sannsyn
   * Anslå hyppigheitsintervall eller sannsynsprosent ut frå det som er kjent eller antatt om erfaringar hos eigen og hos klart samanliknbare verksemder
   * Identifiser kva sannsynsnivå dette gjev
2. Om ein trugsmålsaktør er involvert i risikoskildringa:
   * Vurdere nivået på intensjonen til aktøren (som kombinasjon av motivasjon og vilje)
   * Vurder nivået på kapasiteten til aktøren
   * Juster skjønsmessig sannsynsnivået frå førre hovudtrinn ut frå det nemnt over
3. Vurder sårbarheitsnivå
   * Vurder status i tiltaksetableringa
   * Vurder kor lett ein kan omgå etablerte tiltak
   * Vurder kor lett uhell eller aktløyse kan skje når det er relevant
   * Juster skjønsmessig sannsynsnivået frå førre hovudtrinn ut frå det nemnt over
4. Bruk det sannsynsnivået du no er kome fram til

| **Sannsynsnivå** | **Hyppigheit /**  **% sannsynleg** | **Trugsmålsaktørar** | | **Sårbarheit** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Intensjon** | **Kapasitet** | **Tiltaksetablering** | **Omgåing** | **Uhell og aktløyse** |
| **Svært høg** | Jf *Vedlegg E: Normerande skildringar av sannsynsnivå* | Det finst relevante aktørar med svært sterk motivasjon direkte mot verksemda vår og den aktuelle informasjonen og systema. Dei har svært stor vilje og inga vesentlege hemningar med tanke på å bryte reglar. | Relevante aktørar har kompetanse og ressursar til å overvinne svært avanserte tryggingstiltak. | Relevante tryggingstiltak er ikkje etablerte. | Alternativt kan dei omgåast/brytast av både interne og eksterne med små til normale ressursar. Det er ikkje naudsynt med kjennskap til tiltaka. | Uhell og aktløyse kan skje tilnærma uhindra. |
| **Høg** | Jf *Vedlegg E: Normerande skildringar av sannsynsnivå* | Det finst relevante aktørar med sterk motivasjon inn mot den typen verksemd vi er og den aktuelle typen informasjon og system. Dei har sterk vilje til å bryte reglar. | Relevante aktørar har kompetanse og ressursar til å overvinne mange avanserte tryggingstiltak. | Tryggingstiltak er etablerte, men i liten grad systematisk og risikobasert. Sentrale tiltak er ikkje ferdig etablerte eller fungerer ikkje etter føremålet. | Etablerte tiltak kan omgåast/brytast av både interne og eksterne med små til normale ressursar, men eksterne treng ein viss kjennskap til tiltaka. | Uhell og aktløyse kan skje ofte. |
| **Moderat** | Jf *Vedlegg E: Normerande skildringar av sannsynsnivå* | Det finst relevante aktørar med ein viss motivasjon mot den aktuelle typen informasjon og system. Dei har noko vilje til å bryte reglar. | Relevante aktørar har noko kompetanse og ressursar slik at dei kan overvinne enkle tryggingstiltak. | Tryggingstiltak er etablert systematisk og risikobasert. | Tiltaka kan likevel omgåast/brytast med små til normale ressursar av eigne medarbeidarar med normal kjennskap til tiltaka. Eksternt personell treng gode ressursar, og god/fullstendig kjennskap til tiltaka for å omgå/bryte desse. | Kjende uhell er dekte av tryggingstiltak, men grov aktløyse kan skje. |
| **Låg** | Jf *Vedlegg E: Normerande skildringar av sannsynsnivå* | Relevante aktørar har svært lita eller inga interesse i å gjere noko med vilje for å få uautorisert innsyn, gjere uautoriserte endringar eller hindre tilgjenge. | Relevante aktørar har låg kompetanse og ressursar til å gjennomføre villa handlingar som kan gje konsekvensar av betydning. | Tryggingstiltak er etablert systematisk og risikobasert og systematiske undersøkingar viser at dei fungerer slik dei er meint å gjere. | Tiltaka kan berre omgåast/brytast av eigne medarbeidarar med gode ressursar, og god/fullstendig kjennskap til tiltaka. Eksternt personell kan ikkje omgå/bryte tiltaka utan heilt spesielle føresetnader. | Alle kjende uhells- og aktløysetypar handterast effektivt. |
| **Ubetydeleg** | Jf *Vedlegg E: Normerande skildringar av sannsynsnivå* | Relevante aktørar har inga interesse | Relevante aktørar har ikkje kompetanse eller ressursar |  |  |  |

# 

1. Målavvik kan vere skade, informasjonssikkerheitsbrot, vesentleg avvikande resultat o.l. [↑](#footnote-ref-2)
2. Kunnskapsstyrke er eit uttrykk på kor god bakgrunnskunnskap og kvalitet vi har hatt i arbeidet med analysane våre, og på den måten kor sikre vi er på estimata av konsekvens, sannsyn og risiko. [↑](#footnote-ref-3)
3. Verknaden på kategoriane tenestenivå og regelverk gjeld verknad for både personar og verksemder. [↑](#footnote-ref-4)
4. Regelverk omfattar etterleving av lover, forskrifter, avtalar og interne reglar. Indikatoren verknad er her resultatet ved brot på desse. Regelverk som gjeld personvern og HMS er dekte i eigne konsekvenskategoriar. [↑](#footnote-ref-5)
5. Verknad på kategorien personvern gjeld personar. [↑](#footnote-ref-6)
6. Økonomisk tap dekkjer også effektivitetstap [↑](#footnote-ref-7)
7. Målavvik kan vere skade, informasjonssikkerheitsbrot, vesentleg avvikande resultat o.l. [↑](#footnote-ref-8)
8. Tilhøyrande sannsyn til eit konsekvensnivå vil aldri kunne vere høgare enn sannsynet for at den innleiande hendinga vil skje og gje målavvik (det vi her forenkla kallar «innleiande sannsyn») [↑](#footnote-ref-9)
9. Mest forventa konsekvensnivået i dei andre kategoriane vil då ikkje kunne gje eit høgare risikonivå. [↑](#footnote-ref-10)