***(Kommentarer og noen råd er skrevet i gult innledningsvis og underveis i dokumentet.***

*Dette eksempelet dekker «alle» internkontrollområder på operativt nivå. Det har denne formen for å synlig­gjøre hvordan føringer for risikostyring innen informasjons­sikkerhet kan integreres med andre operative områder der det er naturlig. Dette anbefaler vi som primær tilnærming, jf.* [*efvlf. §15*](https://lovdata.no/dokument/SF/forskrift/2004-06-25-988/KAPITTEL_2#KAPITTEL_3)*, som sier at internkontrollen på informasjonssikkerhetsområdet «bør være en integrert del av virksomhetens helhetlige styringssystem».*

*Dersom man ønsker en egen retningslinje kun for informasjons­sikkerhet eller for noen færre områder, kan eksempelet enkelt snevres inn ved å justere pkt. 2 Anvendelse.* ***De som gjenbruker sentrale deler av eksempelet, er selv ansvarlig for kvalitetssikring av innholdet og tilpasning til egen virksomhet****.*

*Merk at retningslinjen kun dekker risikoer på* ***operativt nivå****. Det er disse som er de sentrale i et internkontrollarbeid innen informasjonssikkerhet. Operative risikoer omfatter uønskede hendelser og konsekvenser i den operative utføringen av oppgaver og tjenester.*

*Sentrale føringer for operativ risikostyring kan skille seg en del fra føringer for risikostyring på strategisk og taktisk nivå i en virksomhet. Vi anbefaler at virksomhetene vurderer å lage en egen retningslinje for å vurdere og håndtere risiko på strategisk og taktisk nivå. Dette faller utenfor fokuset til internkontroll informasjons­sikkerhet. Eksempelet under bør likevel kunne gi inspirasjon også til deler av innholdet for risikostyring på strategisk og taktisk nivå.)*

Innhold

[1. Innledning 2](#_Toc517702312)

[1.1 Målgruppe 2](#_Toc517702313)

[1.2 Formål 2](#_Toc517702314)

[1.3 Anvendelse 2](#_Toc517702315)

[1.4 Relaterte policyer og retningslinjer 2](#_Toc517702316)

[2. Risikoforståelse 2](#_Toc517702317)

[3. Gjennomføre risikovurderinger og risikohåndtering 2](#_Toc517702318)

[3.1 Hovedprosess 2](#_Toc517702319)

[3.2 Gjennomføring av hovedprosessen 3](#_Toc517702320)

[4. Førende prinsipper for risikohåndteringen 3](#_Toc517702321)

[5. Førende prinsipper for risikoaksept 4](#_Toc517702322)

[6. Forenklinger i risikoarbeidet 4](#_Toc517702323)

[6.1 Konsekvenskategorier 4](#_Toc517702324)

[6.2 Nivåer som måleenhet 4](#_Toc517702325)

[6.3 Normering av nivåene for konsekvens, sannsynlighet og risiko 5](#_Toc517702326)

[7. Kommunisere risiko 5](#_Toc517702327)

[7.1 Risikobeskrivelse 5](#_Toc517702328)

[7.2 Risikostørrelse 6](#_Toc517702329)

[7.3 Uttrykke risiko 6](#_Toc517702330)

[Vedlegg A: Risikoforståelse - sentrale begrep og sammenhenger 8](#_Toc517702331)

[Vedlegg B: Kriterier for å akseptere risiko 10](#_Toc517702332)

[Vedlegg C: Normerende beskrivelser av risikonivå 11](#_Toc517702333)

[Vedlegg D: Normerende beskrivelser av konsekvensnivå 12](#_Toc517702334)

[Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå 13](#_Toc517702335)

[Vedlegg F: Sammenheng mellom normering av risikonivå og kriterier for å akseptere risiko 14](#_Toc517702336)

[Vedlegg G: Fremgangsmåte for å estimere nivå på konsekvens, sannsynlighet og risiko 15](#_Toc517702337)

[Vedlegg H: Støtte ved estimat av sannsynlighetsnivå 17](#_Toc517702338)

# Innledning

## Målgruppe

Dette dokumentet er en del av virksomhetens styrende dokumenter. Målgruppen er alle i virksomheten som har behov for å estimere, håndtere og kommunisere om risiko på operativt nivå.

## Formål

Formålet er å

1. etablere en felles forståelse i virksomheten av hva risiko er
2. etablere en effektiv og tilstrekkelig ensartet måte å uttrykke, estimere og håndtere operative risikoer på

Operative risikoer omfatter uønskede hendelser og konsekvenser i den operative utføringen av oppgaver og tjenester.

## Anvendelse

Dokumentet kommer til anvendelse på alle internkontrollområder som det ikke er gitt spesifikke alternative føringer for. (Alternativt at retningslinjen kun gjelder informasjonssikkerhet eller noen få operative områder. Navnet på retningslinjen bør også justeres dersom man avgrenser anvendelsesområdet)

## Relaterte policyer og retningslinjer

Dokumentet må sees i sammenheng med følgende

* Policy for informasjonssikkerhet
* (Eventuelt andre tilsvarende «toppdokumenter» for andre områder)
* Retningslinjen *Roller og ansvar*

# Risikoforståelse

En beskrivelse av sentrale begrep og sammenhenger rundt risikoforståelse er gitt i *Vedlegg A: Risikoforståelse - sentrale begrep og sammenhenger*. Dette vedlegget skal være kjent og forstått av alle som har behov for å estimere, håndtere og kommunisere om risiko hos oss.

# Gjennomføre risikovurderinger og risikohåndtering

Relevante risikoer som kan hindre måloppnåelse skal identifiseres og ved behov håndteres. Dette er et ansvar for risikoeiere og systemeiere fellessystem, jf. retningslinjen *Roller og ansvar.*

## Hovedprosess

Konkrete risikovurderinger skal som minimum inneholde trinnene identifisere, analysere og evaluere risikoer.

I trinnet identifisere, skal relevante risikoer identifiseres og gis en risikobeskrivelse. I trinnet analysere, skal de enkelte risikoene analyseres og risikostørrelsen anslås (estimeres). I trinnet evaluere, skal hver risiko vurderes opp mot kriteriene for å akseptere risiko.

Dersom evalueringen viser at noen risikoer ikke kan aksepteres som de er, skal de gjennom en prosess for å vurdere og velge risikohåndtering.

Dersom en risiko fortsatt ikke kan aksepteres, og det ikke finnes akseptable måter å unngå risikoen på, skal ikke oppgaven som skaper risikoen gjennomføres eller fortsette.

Fokus, arbeidsinnsats og tiltak skal være tilpasset risiko og vesentlighet.

(Dersom man behandler informasjon eller forvalter informasjonssystemer (eller objekter og infrastruktur) etter sikkerhetsloven må man sørge for at elementene som inngår i vurdering av risiko inkluderer det som er påkrevd i virksomhetsikkerhetsforskriften §12, for alle områder hvor dette regelverket kommer til anvendelse.)

## Gjennomføring av hovedprosessen

Underveis i arbeidet skal vi normalt benytte oss av de forenklinger som er beskrevet i kapittel *6 Forenklinger i risikoarbeidet.*

Risikoer skal normalt uttrykkes slik det er beskrevet i kapittel

* *7.1 Risikobeskrivelse*
* *7.2 Risikostørrelse*
* *7.3 Uttrykke risiko*

Ved estimering av risikostørrelse skal man støtte seg på normeringene i

* *Vedlegg C: Normerende beskrivelser av risikonivå*
* *Vedlegg D: Normerende beskrivelser av konsekvensnivå*
* *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå*

Det er under estimeringen anbefalt å støtte seg på prosessen i *Vedlegg G: Fremgangsmåte for å estimere nivå på konsekvens, sannsynlighet og risiko,* samt *Vedlegg H: Støtte ved estimat av sannsynlighetsnivå.* Tidsbruk på denne støtten bør tilpasses risikoen og risikovurderingens egenart.

Ved evaluering av risikoer skal man legge til grunn *Vedlegg B: Kriterier for å akseptere risiko*.

I risikohåndteringen skal man følge prinsippene i kapittel *4 Førende prinsipper for risikohåndteringen.*

Dersom ikke særskilte grunner tilsier noe annet, skal for øvrig de metoder, veiledninger og støtteverktøy virksomheten stiller til disposisjon for ulike typer risikovurderinger benyttes.

# Førende prinsipper for håndtering av risiko

Følgende prinsipper skal legges til grunn i håndtering av risiko hos oss:

Ressursinnsats og fokus

1. Ressursinnsatsen på å finne alternative arbeidsmåter og risikoreduserende tiltak skal stå i forhold til risikoens størrelse.
2. Under identifisering av tiltak skal hele utfallsrommet for en risiko vurderes, herunder alle berørte konsekvenskategorier
3. For risikoer som inkluderer så høye konsekvenser eller sannsynligheter at de går langt utenfor normale ytterpunkt i vår risikomatrise, skal det alltid vurderes om risikoen i realiteten er så stor at den bør håndteres som om den var på et høyere risikonivå enn risikostørrelsen indikerer.

Unngå risikoen

1. Alternative arbeidsmåter som gjør at man kan unngå risikoen, skal vurderes og eventuelt velges ut fra hensiktsmessighet, risikostørrelse og kostnad.

Valg av risikoreduserende tiltak

1. Aktuelle risikoreduserende tiltak skal vurderes opp mot nytte (risikoreduserende effekt), negative sideeffekter og kostnader for øvrig.
2. Tiltak som reduserer risikoer som gjelder liv og helse, skal velges og implementeres dersom det ikke kan dokumenteres at tiltakene klart koster mer enn nytten (ALARP-prinsippet).
3. Tiltak som reduserer risikoer som gir andre konsekvenser enn liv og helse, skal velges og implementeres dersom tiltakene har en vesentlig positiv nytte/kost (nytte/kost-prinsippet).

Nye tiltak i eksisterende oppgaver og system

1. I påvente av implementering av valgte tiltak, skal det straks vurderes om det er behov for eventuelle midlertidige ekstratiltak eller stopp i gjennomføring av pågående oppgaver og bruk av system.

Tiltak i nye oppgaver og system

1. Nye arbeidsoppgaver og system skal som hovedregel ikke startes eller tas i bruk før valgte tiltak er implementert.

# Førende prinsipper for risikoaksept

Følgende prinsipper skal ligge til grunn i våre kriterier for å akseptere risiko:

1. Størrelsen på aksepterte risikoer skal stå i et rimelig forhold til viktigheten og nytten av oppgaven/tjenesten som skaper risikoen.
2. Aksept av risikoer skal bare kunne skje når risikoen er lav eller etter at det er gjennomført en risikohåndtering i henhold til kapittel 4 *Førende prinsipper for risikohåndteringen.*
3. Aksept av risikoer skal skje på et ledernivå som står i forhold til risikoens størrelse.

Dette medfører de kriterier for å akseptere risiko som er beskrevet i *Vedlegg B: Kriterier for å akseptere risiko***.** Disse skal ligge til grunn for evalueringen av risikoer i risikovurderinger.

*Vedlegg F: Sammenheng mellom normering av risikonivå og kriterier for å akseptere risiko* illustrerer hvordan kriteriene for å akseptere risiko henger sammen med andre føringer for risikovurdering.

# Forenklinger i risikoarbeidet

## Konsekvenskategorier

Konsekvenskategorier er en enkel gruppering av våre mål. Konsekvenskategorier skal benyttes som støtte i estimeringen av konsekvenser og der det er hensiktsmessig som tilleggsinformasjon i kommunikasjonen om risiko.

Vi skal benytte følgende felles konsekvenskategorier i våre risikovurderinger:

* Tjenestenivå
* Personvern
* HMS
* Regelverk (for øvrig)
* Vår økonomi

Dette anses som virksomhetskritiske kategorier.

 (Det presiseres at kategoriene over er eksempler. De må vurderes og velges ut fra egenarten og behovene til den enkelte virksomhet. Dersom man behandler informasjon eller forvalter informasjonssystemer etter sikkerhetsloven vil det være behov for en kategori som dekker konsekvenser for grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser.)

## Nivåer som måleenhet

Størrelsen på konsekvenser, sannsynligheter og risiko er sentral i vår vurdering av og kommunikasjon om risiko. Vi skal benytte en forenkling av størrelsene og har delt dem i nivå.

Følgende nivåbetegnelser skal som hovedregel brukes på både konsekvens, sannsynlighet og risiko:

* Svært høy
* Høy
* Moderat
* Lav
* Ubetydelig

Det siste nivået «Ubetydelig» benyttes bare dersom man skal vise størrelsen på risikobeskrivelser som egentlig ikke representerer noen risiko. Dersom noe har ubetydelig konsekvens eller ubetydelig sannsynlighet vil risikoen hos oss alltid være ubetydelig. Vi anser ikke dette som noen risiko.

## Normering av nivåene for konsekvens, sannsynlighet og risiko

Normerende beskrivelser av nivåene på konsekvens, sannsynlighet og risiko er gitt i

* *Vedlegg C: Normerende beskrivelser av risikonivå*
* *Vedlegg D: Normerende beskrivelser av konsekvensnivå*
* *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå*

Disse skal benyttes som støtte i estimering av nivå på hver av de tre delene.

Det er i tillegg anbefalt å støtte seg på prosessen i *Vedlegg G: Fremgangsmåte for å estimere nivå på konsekvens, sannsynlighet og risiko,* samt *Vedlegg H: Støtte ved estimat av sannsynlighetsnivå.*

# Kommunisere risiko

## Risikobeskrivelse

Alle risikoer vi vurderer skal gis en risikobeskrivelse som verbalt beskriver sentrale deler ved en uønsket hendelse og tilhørende konsekvenser.

Innretning og detaljeringsnivå kan variere ut fra kontekst. I svært enkle sammenhenger kan noen få stikkord være nok.

Ofte må imidlertid risikobeskrivelsen utdypes noe mer og dekke hele hendelsesforløpet. Der det ikke anses uhensiktsmessig er følgende anbefalt omfang på en risikobeskrivelse:

* noen stikkord som karakteriserer:
	1. den innledende hendelsen i ett eller flere ledd
	2. hva som skaper selve målavviket (f.eks. skade, informasjonssikkerhetsbrudd e.l.)
	3. konsekvensene som kan oppstå

Eksempler:

|  |
| --- |
| *(1) Ansatte prater om sosialsaker i kantina, naboer til klienter overhører; (2) Brudd på taushetsplikt; (3) Naboer snakker om ting de ikke skulle vite, klienter opplever ubehag, barn utestenges* |
| *(1) Organiserte kriminelle, sosial manipulering av ansatte via ekstern IKT-tilgang; (2) Kriminelle endrer beløp og utbetalingskonto i økonomisystem; (3) Feil utbetalinger, vi taper penger, andre får ikke det de har krav på* |
| *(1) Brann i serverrom; (2) Alle system detter ned; (3) All aktivitet i virksomheten ute av drift* |
| *(1) Ansatte arbeider på skjæremaskinen; (2) Ansatte skjærer seg; (3) Deler av hender kuttes, ulik grad av skade* |

## Risikostørrelse

Alle risikoer vi vurderer skal gis en risikostørrelse. Den skal omfatte nivåene på konsekvens, tilhørende sannsynlighet og risiko.

For å forstå en risiko må vi være oppmerksom på at en risikobeskrivelse kan ha et stort utfallsrom, dvs. en rekke kombinasjoner av mulige konsekvensnivå og tilhørende sannsynligheter som hver kan gi ulike risikonivå.

I våre risikovurderinger er vi spesielt opptatt av å identifisere hvilke risikoer som må håndteres før de eventuelt kan aksepteres. Da er høyeste nivå på risikoene før og etter risikohåndtering sentralt. Samtidig ønsker vi å gjennomføre effektive risikovurderinger.

Vi velger derfor å forenkle kommunikasjonen og **avgrense begrepet risikostørrelse til ett punkt i utfallsrommet** for en risikobeskrivelse. Det punktet skal være den kombinasjon av mulig konsekvens og tilhørende sannsynlighet som gir **det høyeste risikonivået**.

Dette vil **oftest** være **det mest forventede konsekvensnivået og tilhørende sannsynlighet.** Den hypotesen bør imidlertid alltid vurderes og risikostørrelsen eventuelt justeres til slutt i estimering av risikostørrelse.

Det presiseres at selv om vi forenkler og velger ett punkt i utfallsrommet som uttrykk for risikostørrelse, så vil hele utfallsrommet være viktig å forstå og relevant å vurdere under risikohåndteringen og i kommunikasjon om risikoen.

## Uttrykke risiko

Minimum

En risiko skal hos oss som minimum uttrykkes ved hjelp av

* en risikobeskrivelse (jf. pkt. 7.1)
* en risikostørrelse (jf. pkt. 7.2)

Risikostørrelsen skal uttrykke det høyeste risikonivået på risikobeskrivelsen og inneholde nivå på

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

Tillegg A (vanlige tillegg)

Det anbefales at man i tillegg alltid vurderer å uttrykke følgende fra analysen av risikoen

* berørte konsekvenskategorier (som følge av risikobeskrivelsen)
* sannsynlighet for at innledende hendelse skjer og at målavvik[[1]](#footnote-2) oppstår
* konsekvenskategorien til risikostørrelsen

Dette vil øke forståelsen av risikoen for de som leser en risikovurdering.

Tillegg B (utdypende tillegg)

For komplekse risikoer bør man også vurdere å supplere med utdypende informasjon fra analysen. Dette kan være omtale av sårbarheter, spesielle dokumentasjonsteknikker som beskriver risikoen, mv. Tilgjengelig tid, størrelsen og kompleksiteten på risikoen og nytten for de som leser risikovurderingen, bør avgjøre hva man eventuelt tar med.

Tillegg C (Kunnskapsstyrke)

Der det anses nyttig for beslutningstakere, bør man alltid si noe om kunnskapsstyrken[[2]](#footnote-3) bak de analyser og estimat som er grunnlaget for uttrykkene over. Det kan gjøres for en risikovurdering samlet, for enkeltrisikoer eller som en kombinasjon. I angivelse av kunnskapsstyrke skal nivåene lav, moderat og høy benyttes. Det skal skje skjønnsmessig.

Risikotabell og risikonotat

Minimumsdelen og tillegg A foran, bør som hovedregel fremstilles i en risikotabell som kan sorteres på risikonivå. Alle vurderte risikoer bør fremgå av risikotabellen.

En risikotabell bør normalt være et vedlegg til et risikonotat.Risikonotatet skaloppsummere viktige forhold rundt den gjennomførte risikovurderingen. Tillegg B og C foran kan legges i risikonotatet eller i egne vedlegg, avhengig av hva som anses hensiktsmessig.

(Eksempel på vedleggene følger under)

# Vedlegg A: Risikoforståelse - sentrale begrep og sammenhenger

Dette vedlegget gir en beskrivelse av sentrale begrep og sammenhenger rundt risikoforståelse. Vedlegget skal være kjent og forstått av alle som har behov for å estimere, håndtere og kommunisere om risiko hos oss.

Risiko, mål og usikkerhet

Risiko er mulige **avvik fra våre mål**, også kalt mulige avvik fra ønskede resultater eller ønskede tilstander. Det er alltid knyttet usikkerhet til mulige avvik. Usikkerheten er en del av risikoen og kan i hovedsak uttrykkes som **sannsynligheten** for hvert avvik. Sannsynlighet er her et utrykk for hvor trolig vi mener det er at noe vil inntreffe.

Vi kan i tillegg ha ulik grad av usikkerhet ved våre estimat – det vi tror. Den usikkerheten kan uttrykkes ved å si noe om vår grad av **kunnskaps­styrke**, dvs. hvor god bakgrunnskunnskap og kvalitet vi har hatt i arbeidet med våre analyser, og dermed hvor sikre vi er på estimatene av mulige avvik og deres sannsynligheter.

Mål og konsekvenskategorier

Vi har ofte svært mange mål. For å forenkle risikovurderinger samtidig som vi har fokus på viktige målområder, benyttes gjerne konsekvenskategorier**,** f.eks. tjenestenivå, personvern, HMS, økonomi o.l. Konsekvenskategorier er enkle grupperinger av sentrale mål. De mulige avvikene (risikoene) sees da opp mot en eller flere av konsekvenskategoriene.

Positive og negative avvik

I en del internasjonale standarder omfatter risiko både positive og negative avvik. Vi har hos oss valgt å avgrense begrepet risiko til negative avvik og kalle positive avvik for muligheter. Risiko og muligheter skal avveies i virksomhetsstyringen og i internkontrollarbeidet.

Konsekvenser og tilhørende sannsynligheter

Vi kobler ofte begrepet risiko til **uønskede hendelser**. Vi kaller da mulige avvik fra mål for konsekvenser, og sier at risiko er **mulige konsekvenser og tilhørende sannsynligheter**. Ordene «mulige» og «tilhørende» kan utelates, men er da implisitte.

Utfallsrom

En uønsket hendelse kan ha mange forløp, og føre til ulike konsekvenser innen ulike konsekvenskategorier. Hver av disse vil som regel ha forskjellig sannsynlighet.

Figuren viser en risikomatrise med eksempel på sannsynlighetsfordeling mellom ulike konsekvensnivå. Alle punkter på den blå streken, og området under streken, er mulige konsekvensnivå og tilhørende sannsynligheter for utfallet av en hendelse. Vi kaller dette **utfallsrommet** for hendelsen.

Vi deler opp i en matrise med ruter og få nivåer for å forenkle og effektivisere risikovurderinger og kommunikasjon om risiko.

Risikomatrise

For å forenkle analysen av risikoer deler man ofte alle utfallsrom opp i ruter som representerer ulike nivå, slik det er gjort i figuren over. Det kalles en **risikomatrise**.

Uttrykke risikostørrelse

Omfanget av eller størrelsen på en risiko er egentlig fordelingen av alle mulige konsekvenser og tilhørende sannsynligheter. Siden en risikobeskrivelse kan ha et stort utfallsrom med en rekke ulike konsekvenser som hver har sine sannsynligheter, kan dette bli komplekst når det skal beregnes eller uttrykkes. Vi velger derfor ofte en forenkling også når vi skal si noe om størrelsen på en risiko.

I de fleste risikovurderinger er man spesielt opptatt av å identifisere hvilke risikoer som må håndteres før de eventuelt kan aksepteres. Da er høyeste nivå på risikoene før og etter risikohåndtering sentralt.

Man velger derfor ofte å **avgrense begrepet risikostørrelse til ett punkt i utfallsrommet for en hendelse**. Det bør være den kombinasjon av mulig konsekvens og tilhørende sannsynlighet som gir **det høyeste risikonivået**. Selv om det er en forenkling, kalles dette punktet ofte «*risikoen*» ved en hendelse eller «*risikostørrelsen*».

Det **presiseres** at selv om vi forenkler og velger ett punkt i utfallsrommet som uttrykk for risikostørrelse, så vil **hele utfallsrommet være viktig å forstå og relevant å vurdere** under risikohåndteringen og i kommunikasjon om risikoen.

Mest forventet konsekvensnivå

Risikostørrelsen med det høyeste risikonivået vil ofte inkludere **det mest forventede konsekvensnivået**, dvs. toppunktet i buen over. Man tar derfor ofte utgangspunkt i det mest forventede konsekvensnivået når man skal finne risikostørrelsen. Deretter finner man tilhørende sannsynlighet.

Man må likevel være oppmerksom på at andre kombinasjoner av konsekvensnivå og tilhørende sannsynlighet i enkelte tilfeller kan gi et høyere risikonivå. Det gjelder f.eks. når det mest forventede konsekvensnivået og tilhørende sannsynlighet gir en risikostørrelse på nivå lav. Da kan utfall med større konsekvens men mindre sannsynlighet samlet gi et høyere risikonivå. Dette kan gi ulike krav til risikohåndtering og risikoaksept. Man bør derfor være oppmerksom på problemstillingen, vurdere det i sluttfasen av estimeringen, og eventuelt justere valget av både konsekvensnivå og tilhørende sannsynlighet slik at man faktisk uttrykker den største risikostørrelsen for hendelsen.

Sannsynlighet for ulike ting

Det er også viktig å merke seg at man ofte snakker om **sannsynlighet for ulike ting**. Sannsynlig­heten for at en **hendelse kan skje og gi** **målavvik** (f.eks. skade, informasjons­sikkerhets­brudd, vesentlig avvikende resultat) **er en ting**. Sannsynligheten for at et visst konsekvensnivå skal bli en realitet, det vi kaller **tilhørende sannsynlighet, er noe annet**.

Det er den siste som er viktigst i risikovurderinger. Samtidig vil den siste bygge på den første og aldri være høyere. Sannsynlighet for at en innledende hendelse skal inntreffe og gi målavvik, vil dermed kunne være et godt utgangspunkt i estimatet av tilhørende sannsynlighet til et konsekvensnivå. Begge sannsynlighetene er dessuten nyttige i den samlede risikoforståelsen og risikohåndteringen.

# Vedlegg B: Kriterier for å akseptere risiko

|  |  |
| --- | --- |
| **Risikonivå** | **Kriterier for å akseptere risiko** |
| **Lav** | Kan aksepteres **uten å lete etter eller vurdere nytten av** alternative arbeidsmåter eller flere risikoreduserende tiltak. Merk at dette gjelder når hele utfallsrommet for en risiko har risikostørrelse på nivå lav innen alle berørte konsekvenskategorier. |
| **Kan aksepteres av ledere på alle beslutningsnivå.** |
| **Moderat** | Oppgaven/tjenesten som utføres har **vesentlig betydning** for å nå **virksomhetens mål**. |
| Det er gjennomført et **systematisk arbeid** for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer. |
| Alternative arbeidsmåter som gjør at man kan unngå risikoen **er uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er vesentlig mer kostbare.** |
| Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*) |
| Nytten ved at oppgaven/tjenesten utføres ansees større enn risikoen. |
| **Kan aksepteres av ledere på alle beslutningsnivå.** |
| **Høy** | Oppgaven/tjenesten som utføres er **nødvendig** for å nå **virksomhetens** **mål**. |
| Det er gjennomført et **systematisk og grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer. |
| Alternative arbeidsmåter som gjør at man kan unngå risikoen **er svært uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er svært kostbare.** |
| Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*) |
| Nytten ved at oppgaven/tjenesten utføres er større enn risikoen. |
| **Kan kun aksepteres av ledere på minimum avdelingssjefsnivå.** |
| **Svært****høy** | Oppgaven/tjenesten som utføres er **strengt nødvendig** for å nå **virksomhetens** **mål**. |
| Det er gjennomført et **systematisk og svært grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer. |
| Alternative arbeidsmåter som gjør at man kan unngå risikoen **er totalt uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er utenfor virksomhetens økonomiske handlingsrom.** |
| Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*) |
| Nytten ved at oppgaven/tjenesten utføres er større enn risikoen. |
| **Kan kun aksepteres av direktør eller assisterende direktør.** |

# Vedlegg C: Normerende beskrivelser av risikonivå

Risikomatrisen under viser hvilke kombinasjoner av konsekvensnivå og tilhørende sannsynlighetsnivå som skal gi hvilke risikonivå hos oss.

Dersom noe har ubetydelig konsekvens eller ubetydelig sannsynlighet vil risikoen hos oss alltid være ubetydelig. Vi anser ikke dette som noen risiko.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sannsynlighets-nivå** |  |  | **< --- Risikonivå --- >** |
| **Svært høy** | Ubetydelig | Moderat | Høy | Høy | Svært høy |
| **Høy** | Ubetydelig | Moderat | Moderat | Høy | Høy |
| **Moderat** | Ubetydelig | Lav | Moderat | Moderat | Høy |
| **Lav** | Ubetydelig | Lav | Lav | Moderat | Moderat |
| **Ubetydelig** | Ubetydelig | Ubetydelig | Ubetydelig | Ubetydelig | Ubetydelig |
|  |  | **Ubetydelig** | **Lav** | **Moderat** | **Høy** | **Svært høy** |
|  |  | **Konsekvensnivå** |

*(Utformingen av vedlegg B, C, D og E må sees i sammenheng. Nivåbeskrivelsene i vedlegg D og E (konsekvensnivå og sannsynlighetsnivå) avgjør til syvende og sist krav til risikohåndtering og hvilke risikoer som kan aksepteres av ledere på ulike nivå, jf. vedlegg B (kriterier for å akseptere risko. Vedlegg C her fungerer som kobling mellom vedlegg D og E i bunn og vedlegg B på topp.*

*Vedleggene er normalt rimelig enkle i bruk. Men for at de skal fungere etter hensikten, og for at man skal ha en målrettet risikostyring i virksomheten, må utforming og justeringer i vedleggene skje systematisk med et bevisst forhold til sammenhengene.)*

# Vedlegg D: Normerende beskrivelser av konsekvensnivå

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Konsekvens-kategori** | **Indikatorer** |  | **Konsekvensnivå** |
| **Ubetyde­lig** | **Lav** | **Moderat** | **Høy** | **Svært høy** |
| Virksomhetskritisk | Tjenestenivå | Virkning [[3]](#footnote-4) | Ikke merkbart | Et lite merkbart økonomisk eller rettighetsmessig tap | Et godt merkbart økonomisk eller rettighetsmessig tap | Påvirker fungering i samfunnet | Vesentlig hindrer fungering i samfunnet (eller mer) |
| Regelverk [[4]](#footnote-5) | Virkning 3  |
| Personvern | Virkning [[5]](#footnote-6) | Ikke merkbart | Noen kan føle seg krenket | De fleste ville følt seg krenket |
| HMS | Behandlingsbehov | Må ikke behandles | Må ikke til lege e.l. | Krever lege eller inntil 2 dg sykehus e.l. | 2dg til 2 uker på sykehus e.l. | Mer enn 2 uker sykehus e.l. |
| Sykemelding | Ingen | Maks 1 uke | Over 1, maks 5 uker | Over 5, maks 25 uker |  Over 25 uker |
| Vår økonomi | Økonomisk tap [[6]](#footnote-7) | Tap <= 1.000 | Tap <= 5.000 | Tap <= 20.000 | Tap <= 80.000 |  Tap > 80.000 |

*(****Det presiseres at tabellen over er et eksempel****. Hvilke kategorier, indikatorer og* ***ikke minst*** *nivåbeskrivelser som faktisk skal benyttes, må diskuteres i og tilpasses den enkelte virksomhet. Beskrivelsene man velger for ulike konsekvensnivå her i vedlegg D, må sees i sammenheng med valg og nivåbeskrivelse av tilhørende sannsynlighetskategorier (jf. vedlegg E). Det er viktig at nivåbeskrivelsene i disse to skalaene er utformet* ***rimelig proporsjonalt****, slik at faktoren ved økning langs den ene aksen i hovedsak har tilsvarende faktor i økning langs den andre aksen. Da vil de reelle risikonivåene i vedlegg C bli rimelig riktig fremstilt. Samtidig må beskrivelsene ha en utforming som gjør dem effektive å benytte i estimeringen av nivå på konsekvens og tilhørende sannsynlighet.*

*Har man behov for nye konsekvenskategorier, f.eks. «nasjonale sikkerhetsinteresser», må man legge inn nye rader i tabellen over (eller lage nye tabeller), og finne hensiktsmessige indikatorer og nivåbeskrivelser for disse kategoriene. Man bør da også vurdere om man trenger en ekstra sannsynlighetskategori med egne intervall i vedlegg E, slik at sammenhengen mellom de nye konsekvens- og sannsynlighetsbeskrivelsene blir fornuftig, og man får ønsket risikonivå og reaksjon på ulike kombinasjoner, jf. vedlegg C (risikonivå) og B (kriterier for å akseptere risiko).* [*Nasjonal sikkerhetsmyndighet (NSM)*](https://nsm.stat.no/) *har veilednings­ansvaret for sikkerhetsloven. Vi viser til dem dersom man trenger råd om hva som kan være hensiktsmessige veiledende nivåbeskrivelser for «nasjonale sikkerhetsinteresser».)*

# Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå

|  |  |  |  |
| --- | --- | --- | --- |
|  | Bruksområde: | **Vår økonomi** (+ evt. flere konsekvenskategorier) | Eventuelt andre konsekvenskategorier med andre intervallbehov |
| Sannsynlighets­type: | **Hyppighet** **per år** | **Hyppighet** **per periode** |  |
| **Sannsynlighetsnivå** |  |  |  |  |
| **Svært høy** | Over 50 ganger per år | Over 1 gang per uke |  |
| **Høy** | Inntil 50 ganger per år | Inntil 1 gang per uke |  |
| **Moderat** | Inntil 12 ganger per år | Inntil 1 gang per mnd. |  |
| **Lav** | Inntil 3 ganger per år | Inntil 1 gang hver 4. mnd.  |  |
| **Ubetydelig** | Tilnærmet 0 | Tilnærmet 0 |  |

*(****Det presiseres*** *at hvilke sannsynlighetskategorier og nivåbeskrivelser som faktisk skal benyttes, må diskuteres i og tilpasses den enkelte virksomhet.*

***I eksempelet over*** *er det bare lagt inne hyppighetsskala for konsekvenskategorien «Vår økonomi». Stigningen mellom nivåene følger i hovedsak samme* ***faktor 4*** *som for kategorien økonomi i eksempelet i vedlegg D. For å få en funksjonell bruk i praksis, er nivåene i både vedlegg D og E noe avrundet i forhold til det prinsipielt riktige.*

***Den enkelte virksomhet må selv vurder*** *hvilken faktor som bør benyttes på «Vår økonomi» i vedlegg D og E. Samme faktor bør benyttes i begge vedleggene, med hensiktsmessig avrunding.*

***Virksomheten må også vurdere*** *om de øvrige konsekvens­kategoriene i vedlegg D skal benytte samme hyppighetshetsintervall som for «Vår økonomi», eller om de må ha egne intervall tilpasset kategoriens egenart. Det avgjørende er hvor man ønsker ulike kombinasjoner skal ende i vedlegg B (kriterier for å akseptere risiko).*

*Man må derfor først identifisere hvilket risikonivå (jf. vedlegg C) ulike kombinasjoner av konsekvensnivå og sannsynlighetsnivå gir (for de enkelte konsekvens­kategoriene), og deretter vurdere om den kombinasjonen bør medføre de krav dette risikonivået gir i vedlegg B (kriteriene for å akseptere risiko).*

*For å få en funksjonell bruk i praksis* ***anbefaler vi at man er litt pragmatiske og ikke lager flere intervallskalaer her i vedlegg E enn det som er nødvendig****. Dersom intervallene mellom sannsynlighetsnivåene anses rimelig riktige, bør samme intervallserie benyttes. Man bør også vurdere om man i stedet for å lage egne sannsynlighetsintervall for en konsekvenskategori, bør justere nivåbeskrivelsene for den aktuelle konsekvenskategorien i vedlegg D (konsekvensnivå).*

# Vedlegg F: Sammenheng mellom normering av risikonivå og kriterier for å akseptere risiko

Figuren illustrerer hvordan risikomatrisen fungerer som bindeledd mellom normering av konsekvens- og sannsynlighets nivå og kriteriene for å akseptere risiko. (Figuren leses nedenfra og opp.)

# Vedlegg G: Fremgangsmåte for å estimere nivå på konsekvens, sannsynlighet og risiko

Fremgangsmåten under anbefales som støtte ved analyse og estimat av hver risiko. Utgangspunktet er en risikobeskrivelse. Målgruppen er prosessledere for risikovurderinger.

**Generelt om punktene under**

Analyser ut fra behov ulike sider ved risikobeskrivelsen. Vurder spesielt forhold rundt historisk hyppighet, trusselaktører, sårbarheter og trolige og mulige utviklinger av det som skjer underveis i hele hendelsesforløpet.

1. **Anslå «innledende sannsynlighet»,** dvs. sannsynligheten for at innledende hendelse vil skje og gi målavvik[[7]](#footnote-8).
* Bruk *Vedlegg H: Støtte ved estimat av sannsynlighetsnivå* som hjelp. Ha fokus på den delen av hendelsen som går frem mot at målavvik har skjedd.
* Noter ved behov anslått nivå på «innledende sannsynlighet».
1. **Finn berørte konsekvenskategorier, mest forventede konsekvensnivå og foreløpig hovedkategori**
* Identifiser hvilke konsekvenskategorier som i vesentlig grad berøres av risikoen. Noter ved behov navnene på kategoriene.
* Anslå mest forventet konsekvensnivå på hver av de berørte kategoriene. Bruk nivå­beskrivelsene i *Vedlegg D: Normerende beskrivelser av konsekvensnivå* som støtte.
* Kategorien med det høyeste av de mest forventede konsekvensnivåene kan kalles foreløpig hovedkategori.
1. **Anslå tilhørende sannsynlighet og risikonivå på foreløpig hovedkategori**
* Ta utgangspunkt i foreløpig hovedkategori fra pkt. 2, dens mest forventede konsekvensnivå, samt «innledende sannsynlighet» fra pkt. 1.
* Vurder om tilhørende sannsynlighet til dette konsekvensnivået er lavere enn «innledende sannsynlighet»[[8]](#footnote-9).
* Anslå tilhørende sannsynlighet til det aktuelle konsekvensnivået ut fra dette. Bruk ved behov *Vedlegg H: Støtte ved estimat av sannsynlighetsnivå* på nytt, for eventuelt å justere tilhørende sannsynlighet til et lavere nivå enn «innledende sannsynlighet».
* Benytt deretter *Vedlegg C: Normerende* beskrivelser av risikonivå som støtte. Anslå risikonivået ved å finne krysningspunktet mellom mest forventet konsekvensnivå og tilhørende sannsynlighet.
* Noter konsekvenskategori samt konsekvensnivå, tilhørende sannsynlighet og risikonivå som foreløpig risikostørrelse.
* Dersom tilhørende sannsynlighet ikke er lavere enn «innledende sannsynlighet»: Hopp over pkt. 4 [[9]](#footnote-10) og gå til pkt. 5.
1. **Anslå tilhørende sannsynlighet og risikonivå på alternative kategorier**
* (Siste kulepunkt foran avgjør om dette pkt. 4 skal gjennomføres)
* Vurder skjønnsmessig om mest forventet konsekvensnivå fra noen av de andre berørte kategoriene kan gi et høyere risikonivå enn i pkt. 3.
* Anslå eventuelt tilhørende sannsynlighet og risikonivå for mest forventet konsekvens­nivå i en eller flere av disse kategoriene. Bruk samme fremgangsmåte som i pkt. 3.
* Velg en av disse kombinasjonene som ny foreløpig risikostørrelse dersom den gir høyest risikonivå.
* Noter eventuelt ny konsekvenskategori og konsekvensnivå, tilhørende sannsynlighet og risikonivå som ny foreløpig risikostørrelse
1. **Vurder andre relevante kombinasjoner**
* Vurder skjønnsmessig til slutt om andre relevante kombinasjoner av konsekvenskategori, konsekvensnivå og tilhørende sannsynlighet kan gi et høyere risikonivå. Bruk *Vedlegg C: Normerende beskrivelser av risikonivå* som støtte.
	+ Vær spesielt oppmerksom på muligheten for dette når foreløpig risikostørrelse er lav, samtidig som det finnes mulige utfall/konsekvenser ut mot høyre side av konsekvensaksen.
* Ved ja som vurderingssvar:
	+ Velg antatt kategori og konsekvensnivå
	+ Anslå tilhørende sannsynlighet til dette konsekvensnivået. Bruk ved behov *Vedlegg H: Støtte ved estimat av sannsynlighetsnivå* som hjelp.
	+ Anslå risikonivået ved hjelp av konsekvensnivå, tilhørende sannsynlighet og oppslag i *Vedlegg C: Normerende beskrivelser av risikonivå*
	+ Velg den nye kombinasjonene som endelig risikostørrelse dersom den gir høyest risikonivå
* Ved nei:
	+ Velg foreløpig risikostørrelse fra pkt. 3 eller 4 som endelig risikostørrelse.

# Vedlegg H: Støtte ved estimat av sannsynlighetsnivå

Dette vedlegget skal benyttes som støtte ved estimat av sannsynlighetsnivå (se også

Estimeringen av sannsynlighetsnivåene skal skje skjønnsmessig med støtte i de normerende beskrivelsene i tabellen under. De tre faktorene hyppighet / % sannsynlig, trusselaktører og sårbarhet **skal ikke brukes individuelt og isolert, men sees i sammenheng.**

Følgende fremgangsmåte bør benyttes (med støtte i tabellen under)

1. Ta utgangspunkt i historisk hyppighet eller det vi vet om hyppighet eller sannsynlighet
	* Anslå hyppighetsintervall eller sannsynlighetsprosent ut fra det som er kjent eller antatt om erfaringer hos egen og hos klart sammenlignbare virksomheter
	* Identifiser hvilket sannsynlighetsnivå dette gir
2. Dersom en trusselaktør er involvert i risikobeskrivelsen:
	* Vurdere nivået på aktørens intensjon (som kombinasjon av motivasjon og vilje)
	* Vurder nivået på aktørens kapasitet
	* Juster skjønnsmessig sannsynlighetsnivået fra forrige hovedtrinn ut fra ovennevnte
3. Vurder sårbarhetsnivå
	* Vurder status i tiltaksetableringen
	* Vurder hvor lett etablerte tiltak kan omgås
	* Vurder hvor lett uhell eller uaktsomhet kan skje når det er relevant
	* Juster skjønnsmessig sannsynlighetsnivået fra forrige hovedtrinn ut fra ovennevnte
4. Benytt det sannsynlighetsnivå du nå er kommet frem til

| **Sannsynlighets­nivå** | **Hyppighet /****% sannsynlig** | **Trusselaktører** | **Sårbarhet** |
| --- | --- | --- | --- |
| **Intensjon** | **Kapasitet** | **Tiltaksetablering** | **Omgåelse** | **Uhell og uaktsomhet** |
| **Svært høy** | Jf. *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå* | Det finnes relevante aktører med svært sterk motivasjon direkte mot vår virksomhet og den aktuelle informasjonen og systemene. De har svært stor vilje og ingen vesentlige hemninger mht. å bryte regler. | Relevante aktører har kompetanse og ressurser til å overvinne svært avanserte sikkerhetstiltak. | Relevante sikkerhetstiltak er ikke etablert. | Alternativt kan de omgås/brytes av både interne og eksterne med små̊ til normale ressurser. Det er ikke nødvendig med kjennskap til tiltakene. | Uhell og uaktsomhet kan skje tilnærmet uhindret. |
| **Høy** | Jf. *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå* | Det finnes relevante aktører med sterk motivasjon inn mot den type virksomhet vi er og den aktuelle typen informasjon og systemer. De har sterk vilje til å bryte regler. | Relevante aktører har kompetanse og ressurser til å overvinne mange avanserte sikkerhetstiltak. | Sikkerhetstiltak er etablert, men i liten grad systematisk og risikobasert. Sentrale tiltak er ikke ferdig etablert eller fungerer ikke etter hensikten. | Etablerte tiltak kan omgås/brytes av både interne og eksterne med små til normale ressurser, men eksterne trenger en viss kjennskap til tiltakene. | Uhell og uaktsomhet kan skje ofte. |
| **Moderat** | Jf. *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå* | Det finnes relevante aktører med en viss motivasjon mot den aktuelle typen informasjon og systemer. De har noe vilje til å bryte regler. | Relevante aktører har noe kompetanse og ressurser slik at de kan overvinne enkle sikkerhetstiltak. | Sikkerhetstiltak er etablert systematisk og risikobasert. | Tiltakene kan likevel omgås/brytes med små̊ til normale ressurser av egne medarbeidere med normal kjennskap til tiltakene. Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse. | Kjente uhell er dekket av sikkerhetstiltak, men grov uaktsomhet kan skje. |
| **Lav** | Jf. *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå* | Relevante aktører har svært liten eller ingen interesse i å gjøre noe med vilje for å få uautorisert innsyn, gjøre uautoriserte endringer eller hindre tilgjengelighet. | Relevante aktører har lav kompetanse og ressurser til å gjennomføre villede handlinger som kan gi konsekvenser av betydning. | Sikkerhetstiltak er etablert systematisk og risikobasert og systematiske undersøkelser viser at de fungerer etter hensikten. | Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/fullstendig kjennskap til tiltakene. Eksternt personell kan ikke omgå/bryte tiltakene uten helt spesielle forutsetninger. | Alle kjente uhells- og uaktsomhets­typer håndteres effektivt. |
| **Ubetydelig** | Jf. *Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå* | Relevante aktører har ingen interesse | Relevante aktører har ikke kompetanse eller ressurser |  |  |  |

#

1. Målavvik kan være skade, informasjonssikkerhetsbrudd, vesentlig avvikende resultat o.l. [↑](#footnote-ref-2)
2. Kunnskapsstyrke er et uttrykk hvor god bakgrunnskunnskap og kvalitet vi har hatt i arbeidet med våre analyser, og dermed hvor sikre vi er på estimatene av konsekvens, sannsynlighet og risiko. [↑](#footnote-ref-3)
3. Virkning på kategoriene tjenestenivå og regelverk gjelder virkning for både personer og virksomheter. [↑](#footnote-ref-4)
4. Regelverk omfatter etterlevelse av lover, forskrifter, avtaler og interne regler. Indikatoren virkning er her resultatet ved brudd på disse. Regelverk som gjelder personvern og HMS er dekket i egne konsekvenskategorier. [↑](#footnote-ref-5)
5. Virkning på kategorien personvern gjelder personer. [↑](#footnote-ref-6)
6. Økonomisk tap dekker også effektivitetstap [↑](#footnote-ref-7)
7. Målavvik kan være skade, informasjonssikkerhetsbrudd, vesentlig avvikende resultat o.l. [↑](#footnote-ref-8)
8. Tilhørende sannsynlighet til et konsekvensnivå vil aldri kunne være høyere enn sannsynligheten for at den innledende hendelsen vil skje og gi målavvik (det vi her forenklet kaller «innledende sannsynlighet») [↑](#footnote-ref-9)
9. Mest forventede konsekvensnivået i de andre kategoriene vil da ikke kunne gi et høyere risikonivå [↑](#footnote-ref-10)