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

*Dette dømet dekkjer internkontrollområda informasjonssikkerheit og kvalitet.* Dømet har denne forma for å synleggjere korleis vurdering av behov for risikovurderingar innan informasjonssikkerheit kan integrerast med andre område der det er naturleg, jf. [eForvaltningsforskriften § 15](https://lovdata.no/dokument/SF/forskrift/2004-06-25-988/KAPITTEL_2#KAPITTEL_3), som seier at internkontrollen på informasjonssikkerheitsområdet *«bør være en integrert del av virksomhetens helhetlige styringssystem».*

*Vurdering av behov for risikovurderingar med tanke på etterleving av kvalitetskrav, kan ha den tilnærminga som er vist her. Det vil dessutan i fleire samanhengar kunne vere føremålstenleg å gjennomføre risikovurderingar for informasjonssikkerheit og kvalitet samla. Det kan då vere nyttig å gjere ei vurdering av behova for slike risikovurderingar samla. For andre internkontrollområde, som t.d. HMS, må ein ofte ha andre tilnærmingar til å vurdere behov for meir konkrete risikovurderingar. Dei er difor ikkje omfatta i dette dømet.*

*Den enkelte verksemd må sjølv vurdere om ei retningslinje som dette bør dekkje både informasjonssikkerheit og kvalitet. Dette er spesielt viktig for dei som har eit formelt kvalitetssystem, t.d. etter ISO 9001. Blir vurderingar som dette rekna som føremålstenlege eller dekte av kvalitetssystemet elles, bør dokumentet avgrensast til informasjonssikkerheit.*

*Om ein ønskjer å avgrense dokumentet til berre informasjonssikkerheit, kan dømet enkelt snevrast inn ved å ta bort enkelte punkt og spisse andre. Dette er kommentert under. Ein bør uansett vurdere å spesifisere tittelen på dokumentet, slik at bruksområdet kjem fram der. Det kan effektivisere forståinga av kva tid retningslinja er relevant. Andre dokument som tilviser til henne, bør då også oppdaterast.* Dei som gjenbrukar sentrale delar av dømet, er sjølv ansvarlege for kvalitetssikring av innhaldet og tilpassing til eiga verksemd.

*Gode støtteskjema og litt opplæring/rettleiing er suksesskriterium. Det er rådd til at verksemdene prøver ut retningslinja og støtteskjema og gjer justeringar ved behov, før retningslinja eventuelt vedtakast for heile verksemda. Eit framlegg til støtteskjema er tilgjengeleg frå Digitaliseringsdirektoratet som mal.)*

Innhald

[1. Innleiing 1](#_Toc90481632)

[1.1 Målgruppe 1](#_Toc90481633)

[1.2 Føremål 2](#_Toc90481634)

[1.3 Relaterte policyar og retningslinjer 2](#_Toc90481635)

[2. Gjennomføring 2](#_Toc90481636)

[2.1 Foranalyse av eige ansvarsområde 2](#_Toc90481637)

[2.2 Gruppere og dele opp 2](#_Toc90481638)

[2.3 Avdekkje usikkerheit for kvart delområde 2](#_Toc90481639)

[2.4 Gjer vedtak på kvart delområde ut frå avgjerdskriteria 3](#_Toc90481640)

[3. Dokumentere 3](#_Toc90481641)

[Vedlegg A: Støttespørsmål 4](#_Toc90481642)

[Vedlegg B: Vedtakskriterium 5](#_Toc90481643)

# Innleiing

## Målgruppe

Dette dokumentet er ein del av verksemda sine styrande dokument. Målgruppa er

* Risikoeigarar, dvs. leiarar med ansvar for oppgåveløysing, tenesteutføring og eigne IKT-system
* systemeigarar for fellessystem[[1]](#footnote-1).

## Føremål

Føremålet er å gje føringar for korleis ein skal gå fram for å avgjere behovet for nye eller oppdaterte risikovurderingar på operativt nivå innan informasjonssikkerheit og kvalitet. (Alternativt at dokumentet berre gjeld informasjonssikkerheit - om det er ønskeleg.)

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

## Relaterte policyar og retningslinjer

Dokumentet må sjåast i samanheng med følgjande retningslinjer:

* Roller og ansvar
* Forstå, vurdere og handtere risiko

# Gjennomføring

## Foranalyse av eige ansvarsområde

Alle risikoeigarar skal utføre ein foranalyse av eige ansvarsområde. Denne bør omfatte både arbeidsoppgåver som utførast, informasjonen som blir behandla i oppgåvene, IKT-system som brukast og sentrale trugsmål, farar og sårbarheiter.

Om foranalysen blir gjennomført i leiargrupper over operativt nivå, vil det redusere omfanget av foranalysar og forenkle gjennomføringa. Eventuell slik organisering avgjerast av dei enkelte organisatoriske einingane.

Systemeigarar for fellessystem bør få utført ein forenkla foranalyse for fellessystema dei har ansvaret for. Desse bør baserast på foranalysane til risikoeigarane.

## Gruppere og dele opp

Eit ansvarsområde kan vere enkelt og oversiktleg eller stort og komplekst. Når ein skal avgjere kvar og om det er behov for grundigare risikovurderingar, vil det ofte vere føremålstenleg eller naudsynt å slå noko saman i større grupper eller dele det opp i delområde. Vi kallar det å gruppere og dele opp.

På bakgrunn av foranalysen skal den ansvarlege vurdere om enkelheit, kompleksitet, rutinar, kompetanse eller andre tilhøve gjer at arbeidsoppgåvene og IKT-systema ein har ansvaret for kan og bør slåast saman i større grupper eller delast opp i delområde.

## Avdekkje usikkerheit for kvart delområde

For kvart delområde frå pkt. 2.2 skal den ansvarlege gå gjennom støttespørsmåla i vedlegg A. Spørsmåla skal relaterast til det aktuelle området eller delområdet. Spørsmålslista er ikkje uttømande. Den ansvarlege skal supplere med andre spørsmål og vurderingar der ho finn det relevant.

Målet med støttespørsmåla er å

* avdekkje høgaste konsekvensnivå[[2]](#footnote-2) for området
* avdekkje antatt høgaste risikonivå[[3]](#footnote-3) for området
* avdekkje kor usikker den ansvarlege er på om risikoane innan området kan aksepterast[[4]](#footnote-4) utan ytterlegare risikovurdering og risikohandtering. Nivåa stor, moderat og låg usikkerheit skal brukast.

Referanseramma er verksemda sine kriterium for å akseptere risiko, samt normerande skildringar av risikonivå, konsekvensnivå og sannsynsnivå, jf. vedlegg B, C, D og E i retningslinja *Forstå, vurdere og handtere risiko.*

Om ein får stor variasjon i usikkerheita for ulike delar av det ein vurderer, bør ein gå tilbake til pkt. 2.2, gjere ei ny oppdeling og gjenta pkt. 2.3 for aktuelle delar.

## Gjer vedtak på kvart delområde ut frå avgjerdskriteria

Til sist skal den ansvarlege gjere vedtak i samsvar med vedlegg B i denne retningslinja. Vedtaka takast fortløpande for kvart delområde

Tidspunkt for konkrete risikovurderingar skal planleggjast ut frå det.

# Dokumentere

Dokumentasjon av gjennomføringa framføre skal som hovudregel skje skriftleg i dei malar, støtteverktøy og arkivløysingar som er etablerte for føremålet.

Når risikovurderingar faktisk gjennomførast skal informasjonen over supplerast med

* Dato for gjennomført risikovurdering
* Referanse til dokumentasjon av risikovurderinga
* Høgaste risikonivå identifisert i risikovurderinga
* Kunnskapsstyrke for risikovurderinga samla

Dette vil skape ei heilskapsoversikt og vere til hjelp når ein seinare skal oppdatere behovsvurderingane.

# Vedlegg A: Støttespørsmål

Etter kvart temaområde i spørsmåla under, bør ein fortløpande kort reflektere over, og ved behov notere, både antatt høgaste risikonivå og nivå på eiga usikkerheit på om risikoane kan aksepterast som dei er. Dette konkluderast det på til slutt i støttespørsmåla.

**Høgaste konsekvensnivå:**

1. Kva er høgaste konsekvensnivå innan området

* ved brot på konfidensialitet, integritet og tilgjenge? (når risikoar ved informasjonssikkerheit er relevant for vurderinga)
* ved brot på kvalitetskrav? (om det er relevant for vurderinga)

(Det siste kulepunktet fjernast om retningslinja berre skal gjelde informasjonssikkerheit)

**Oversikt:**

1. Kor god oversikt har vi over området?

* Mål for arbeidet eller tenesta, system som brukast og kven som utfører arbeidet
* Trugsmål, farar og sårbarheiter

**Tidlegare risikovurderingar og risikohandtering:**

1. Er det tidlegare gjort gode risikovurderingar og ei systematisk risikohandtering på dette eller direkte samanliknbare område?
   * av oss eller andre vi har stor tillit til
2. I kva grad kjenner vi oss trygge på at tidlegare arbeid med identifisering og val rundt alternative arbeidsmåtar og risikoreduserande tryggingstiltak, dekkjer risikoane og krava våre rundt desse i kriteria våre for å akseptere risikoar?
   * gjennom m.a. verksemda si fellessikring og vår tilleggssikring
3. Er det vesentlege delområde eller risikoar som ikkje er vurderte eller handterte godt nok?
   * pga. manglande tid og kompetanse
   * pga. usikkerheit rundt sentrale delar av området eller usikkerheit rundt trugsmål, farar og sårbarheiter

**Nye faktorar:**

1. Har det skjedd vesentlege endringar i oppgåveløysinga, tenesteutforminga, informasjonsbehandlinga, trugsmål, farar eller rundt sårbarheiter?
2. Har vi fått indikasjonar frå avviks- og hendingshandteringa, revisjonsrapportar e.l. som indikerer at tidlegare risikovurderingar og risikohandtering ikkje lenger er gode nok?
3. Har vi fått tilbakemeldingar frå nøkkelpersonell om vesentleg usikkerheit på om risikovurderingar og tiltak er gode nok?

**Usikkerheit om risikoaksept**

1. Kva går vi ut frå er det høgaste risikonivået ut frå tidlegare risikovurderingar og vurderinga over?
2. Kor stor usikkerheit har vi om risikoane på området kan aksepterast i samsvar med verksemda sine kriterium for å akseptere risiko? (Høg, moderat eller låg usikkerheit)

# Vedlegg B: Vedtakskriterium

**Vel prioriteringsgruppe for området** ut frå

* Høgaste konsekvensnivå frå spørsmål 1
* Nivå på usikkerheit frå spørsmål 10

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Usikkerheit om risikoane kan aksepterast** | |  | | | |
| **Nivå usikkerheit** |  | **Prioritetsgruppe for risikovurderingar** | | | |
| **Høg** | 5 | 4 | 2 | 1 |
| **Moderat** | 0 | 5 | 3 | 2 |
| **Låg** | 0 | 0 | 6 | 6 |
|  |  | **Låg** | **Moderat** | **Høg** | **Svært høg** |
|  | | **Konsekvensnivå** | | | |

(Ein bør i arbeidet med retningslinja systematisk vurdere innhaldet i matrisa over og tabellen under, slik at ein forstår kva dei medfører, og kan vurdere om dette er føremålstenleg for verksemda. Begge kan justerast ut frå behova til verksemda.)

**Planlegg risikovurderingar i høve til tabellen under**

| **Prioritets-gruppe** | **Vedtak** |
| --- | --- |
| 0 | * Det er **ikkje behov** for å gjennomføre nye eller oppdaterte risikovurderingar. |
| 1 - 2 | * Ny/oppdatert risikovurdering skal gjennomførast **utan ugrunna opphald** * Prioritering skal skje etter prioritetsgruppe * Nye arbeidsoppgåver skal ikkje startast og nye system skal ikkje takast i bruk før ny eller oppdatert risikovurdering er gjennomført og følgt opp * Det skal straks vurderast om det er behov for eventuelle mellombelse ekstratiltak eller stopp i gjennomføring av oppgåver og bruk av IKT-system og anna utstyr. |
| 3 - 5 | * Ny/oppdatert risikovurdering skal gjennomførast **innan rimeleg tid** * Prioritering skal skje etter prioritetsgruppe og ut frå kunnskapsstyrken[[5]](#footnote-5) på tidlegare vurderingar * Nye arbeidsoppgåver kan startast og nye system kan takast i bruk om dei blir etablerte innan verksemda si fellessikring og oppgåva som skal løysast er svært viktig for å nå verksemda sitt overordna mål |
| 6 | * Ny/oppdatert risikovurdering skal **gjennomførast med intervall på maks 3 år, om ikkje ny kunnskap tilseier gjennomføring tidlegare** * Omfanget skal tilpassast kunnskapsstyrken4 på tidlegare vurderingar * Nye arbeidsoppgåver kan startast og nye system kan takast i bruk om dei blir etablerte innan verksemda si fellessikring og oppgåva som skal løysast er svært viktig for å nå verksemda sitt overordna mål |

**Generelle krav:**

* Ein skal alltid avslutningsvis for kvart område vurdere om ein har spesielt høge risikoar (jf. spørsmål 9) og stor usikkerheit rundt desse. Dette kan krevje ei skjønsmessig høgare prioritering av området enn det som følgjer av tabellane over[[6]](#footnote-6). Ei anna prioritering enn i tabellane skal kort grunngjevast i dei skjemaa ein brukar.
* Ressursinnsats og fokus i naudsynte risikovurderingar skal tilpassast eigenarten til området, potensielt konsekvensnivå, antatt risikostorleik og dei foranalysane som er gjennomførte.

1. Alle IKT-system og anna teknisk utstyr som brukast av fleire organisatoriske einingar kallast fellessystem. [↑](#footnote-ref-1)
2. «Høgaste konsekvensnivå» er det høgaste nivået på konsekvensar på området som ein med ei viss grad av sannsyn må rekne med kan hende. Urealistiske utfall blir difor haldne utanfor. For støtte til å finne riktig nivå: Sjå vedlegg D i retningslinja *Forstå, vurdere og handtere risiko.* [↑](#footnote-ref-2)
3. For støtte til antatt høgaste risikonivå: Sjå eventuelt resultat frå tidlegare risikovurderingar, vedlegg C, D og E i retningslinja *Forstå, vurdere og handtere risiko*, samt støttespørsmåla i vedlegg A her. [↑](#footnote-ref-3)
4. Kriterium for å akseptere risiko: Sjå vedlegg B i *Retningslinje: Forstå, vurdere og handtere risiko*. [↑](#footnote-ref-4)
5. Kunnskapsstyrke er eit uttrykk for kor god bakgrunnskunnskap og kvalitet vi har hatt i arbeidet med risikovurderingane og risikohandteringa vår, og dermed kor sikre vi er på estimata av konsekvens, sannsyn og risiko. Nivåa låg, moderat og høg skal brukast på kunnskapsstyrke. [↑](#footnote-ref-5)
6. Tabellane baserer seg berre på høgaste konsekvensnivå i prioriteringa, ikkje høgaste risikonivå. Den forenklinga dette representerer gjev ei mogleg feilkjelde i prioriteringa som i stor grad skal rettast opp med dette generelle kravet. [↑](#footnote-ref-6)