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

*Dette eksempelet dekker internkontrollområdene informasjonssikkerhet og kvalitet. Eksempelet har denne formen for å synlig­gjøre hvordan vurdering av behov for risikovurderinger innen informasjons­sikkerhet kan integreres med andre områder der det er naturlig, jf.* [*eForvaltningsforskriften § 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».*

*Vurdering av behov for risikovurderinger mht. etterlevelse av kvalitetskrav, kan ha den tilnærmingen som er vist her. Det vil dessuten i flere sammenhenger kunne være hensikt­smessig å gjennomføre risiko­vurderinger for informasjons­sikkerhet og kvalitet samlet. Det kan da være nyttig å foreta en vurdering av behovene for slike risikovurderinger samlet. For andre internkontrollområder, som f.eks. HMS, må man ofte ha andre tilnærminger til å vurdere behov for mer konkrete risikovurderinger. De er derfor ikke omfattet i dette eksempelet.*

*Den enkelte virksomhet må selv vurdere om en retningslinje som dette bør dekke både informasjonssikkerhet og kvalitet. Dette er spesielt viktig for de som har et formelt kvalitetssystem, f.eks. etter ISO 9001. Blir vurderinger som dette ansett uhensiktsmessig eller dekket av kvalitetssystemet ellers, bør dokumentet avgrenses til informasjonssikkerhet.*

*Dersom man ønsker å avgrense dokumentet til kun informasjonssikkerhet, kan eksempelet enkelt snevres inn ved å ta bort enkelte punkter og spisse andre. Dette er kommentert under. Man bør uansett vurdere å spesifisere tittelen på dokumentet, slik at anvendelsesområdet kommer frem der. Det kan effektivisere forståelsen av når retningslinjen er relevant. Andre dokumenter som henviser til den, bør da også oppdateres.* ***De som gjenbruker sentrale deler av eksempelet, er selv ansvarlig for kvalitetssikring av innholdet og tilpasning til egen virksomhet****.*

*Gode støtteskjema og litt opplæring/veiledning er suksesskriterier. Det anbefales at virksomhetene prøver ut retningslinjen og støtteskjema og gjør justeringer ved behov, før retningslinjen eventuelt vedtas for hele virksomheten. Et forslag til støtteskjema er tilgjengelig fra Digitaliseringsdirektoratet som mal.)*

Innhold

[1. Innledning 1](#_Toc485057952)

[1.1 Målgruppe 1](#_Toc485057953)

[1.2 Formål 2](#_Toc485057954)

[1.3 Relaterte policyer og retningslinjer 2](#_Toc485057955)

[2. Gjennomføring 2](#_Toc485057956)

[2.1 Foranalyse 2](#_Toc485057957)

[2.2 Gruppere og dele opp ansvarsområdet 2](#_Toc485057958)

[2.3 Avdekke usikkerhet 2](#_Toc485057960)

[2.4 Ta beslutning ut fra beslutningskriteriene 3](#_Toc485057961)

[3. Dokumentere 3](#_Toc485057962)

[Vedlegg A: Støttespørsmål 4](#_Toc485057963)

[Vedlegg B: Beslutningskriterier 5](#_Toc485057964)

# Innledning

## Målgruppe

Dette dokumentet er en del av virksomhetens styrende dokumenter. Målgruppen er

* Risikoeiere, dvs. ledere med ansvar for oppgaveløsning, tjenesteutføring og egne IKT-system
* systemeiere for fellessystem[[1]](#footnote-1).

## Formål

Formålet er å gi føringer for hvordan man skal gå frem for å avgjøre behovet for nye eller oppdaterte risikovurderinger på operativt nivå innen informasjonssikkerhet og kvalitet. (Alternativt at dokumentet kun gjelder informasjonssikkerhet - dersom det er ønskelig.)

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

## Relaterte policyer og retningslinjer

Dokumentet må sees i sammenheng med følgende retningslinjer:

* Roller og ansvar
* Forstå, vurdere og håndtere risiko

# Gjennomføring

## Foranalyse av eget ansvarsområde

Alle risikoeiere skal utføre en foranalyse av eget ansvarsområde. Den bør omfatte både arbeidsoppgaver som utføres, informasjonen som behandles i oppgavene, IKT-system som benyttes og sentrale trusler, farer og sårbarheter.

Dersom foranalysen gjennomføres i ledergruppen over operativt nivå, vil det redusere omfanget av foranalyser og forenkle gjennomføringen. Eventuell slik organisering avgjøres av de enkelte organisatoriske enhetene.

Systemeiere for fellessystem bør få utført en forenklet foranalyse for fellessystemene de har ansvaret for. Disse bør baseres på foranalysene til risikoeierne.

## Gruppere og dele opp

Et ansvarsområde kan være enkelt og oversiktlig eller stort og komplekst. Når man skal avgjøre hvor og om det er behov for grundigere risikovurderinger, vil det ofte være hensiktsmessig eller nødvendig å slå noe sammen i større grupper eller dele det opp i delområder Vi kaller det å gruppere og dele opp.

På bakgrunn av foranalysen skal den ansvarlige vurdere om enkelthet, kompleksitet, rutiner, kompetanse eller andre forhold gjør at arbeidsoppgavene og IKT-systemene man har ansvaret for kan og bør slås sammen i større grupper eller deles opp i delområder.

## Avdekke usikkerhet for hvert delområde

For hvert delområde fra pkt. 2.2 skal den ansvarlige gå gjennom støttespørsmålene i vedlegg A. Spørsmålene skal relateres til det aktuelle området eller delområdet. Spørsmålslisten er ikke uttømmende. Den ansvarlige skal supplere med andre spørsmål og vurderinger der hun finner det relevant.

Målet med støttespørsmålene er å

* avdekke høyeste konsekvensnivå[[2]](#footnote-2) for området
* avdekke antatt høyeste risikonivå[[3]](#footnote-3) for området
* avdekke hvor usikker den ansvarlige er på om risikoene innen området kan aksepteres[[4]](#footnote-4) uten ytterligere risikovurdering og risikohåndtering. Nivåene stor, moderat og lav usikkerhet skal benyttes.

Referanserammen er virksomhetens kriterier for å akseptere risiko, samt normerende beskrivelser av risikonivå, konsekvensnivå og sannsynlighetsnivå, jf. vedlegg B, C, D og E i retningslinjen *Forstå, vurdere og håndtere risiko*.

Dersom man får stor variasjon i usikkerheten for ulike deler av det man vurderer, bør man gå tilbake til pkt. 2.2, foreta en ny oppdeling og gjenta pkt. 2.3 for aktuelle deler.

## Ta beslutning på hvert delområde ut fra beslutningskriteriene

Til sist skal den ansvarlige ta beslutninger i samsvar med denne retningslinjens vedlegg B. Beslutningene tas fortløpende for hvert delområde

Tidspunkt for konkrete risikovurderinger skal planlegges ut fra det.

# Dokumentere

Dokumentasjon av gjennomføringen foran skal som hovedregel skje skriftlig i de maler, støtteverktøy og arkivløsninger som er etablert for formålet.

Når risikovurderinger faktisk gjennomføres skal informasjonen over suppleres med

* Dato for gjennomført risikovurdering
* Referanse til dokumentasjon av risikovurderingen
* Høyeste risikonivå identifisert i risikovurderingen
* Kunnskapsstyrke for risikovurderingen samlet

Dette vil skape en helhetsoversikt og være til hjelp når man senere skal oppdatere behovsvurderingene.

# Vedlegg A: Støttespørsmål

Etter hvert temaområde i spørsmålene under, bør man fortløpende kort reflektere over, og ved behov notere, både antatt høyeste risikonivå og nivå på egen usikkerhet på om risikoene kan aksepteres som de er. Dette konkluderes det på til slutt i støttespørsmålene.

**Høyeste konsekvensnivå:**

1. Hva er høyeste konsekvensnivå innen området

* ved brudd på konfidensialitet, integritet og tilgjengelighet? (når risikoer ved informasjonssikkerhet er relevant for vurderingen)
* ved brudd på kvalitetskrav? (dersom det er relevant for vurderingen)

(Det siste kulepunktene fjernes dersom retningslinjen kun skal gjelde informasjonssikkerhet)

**Oversikt:**

1. Hvor god oversikt har vi over området?

* Mål for arbeidet eller tjenesten, system som benyttes og hvem som utfører arbeidet
* Trusler, farer og sårbarheter

**Tidligere risikovurderinger og risikohåndtering:**

1. Er det tidligere gjort gode risikovurderinger og en systematisk risikohåndtering på dette eller direkte sammenlignbare områder?
   * av oss eller andre vi har stor tillit til
2. I hvilken grad føler vi oss trygge på at tidligere arbeid med identifisering og valg rundt alternative arbeidsmåter og risikoreduserende sikkerhetstiltak, dekker våre risikoer og kravene rundt disse i våre kriterier for å akseptere risikoer?
   * gjennom bl.a. virksomhetens fellessikring og vår tilleggssikring
3. Er det vesentlige delområder eller risikoer som ikke er vurdert eller håndtert godt nok?
   * pga. manglende tid og kompetanse
   * pga. usikkerhet rundt sentrale deler av området eller usikkerhet rundt trusler, farer og sårbarheter

**Nye faktorer:**

1. Har det skjedd vesentlige endringer i oppgaveløsningen, tjenesteutformingen, informasjonsbehandlingen, trusler, farer eller rundt sårbarheter?
2. Har vi fått indikasjoner fra avviks- og hendelseshåndteringen, revisjonsrapporter e.l. som indikerer at tidligere risikovurderinger og risikohåndtering ikke lenger er gode nok?
3. Har vi fått tilbakemeldinger fra nøkkelpersonell om vesentlig usikkerhet på om risikovurderinger og tiltak er gode nok?

**Usikkerhet om risikoaksept:**

1. Hva antar vi er det høyeste risikonivået ut fra tidligere risikovurderinger og vurderingen over?
2. Hvor stor usikkerhet har vi om risikoene på området kan aksepteres i henhold til virksomhetens kriterier for å akseptere risiko? (Høy, moderat eller lav usikkerhet)

# Vedlegg B: Beslutningskriterier

**Velg prioriteringsgruppe for området** ut fra

* Høyeste konsekvensnivå fra spørsmål 1
* Nivå på usikkerhet fra spørsmål 10

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Usikkerhet om risikoene kan aksepteres** | |  | | | |
| **Nivå usikkerhet** |  | **Prioritetsgruppe for risikovurderinger** | | | |
| **Høy** | 5 | 4 | 2 | 1 |
| **Moderat** | 0 | 5 | 3 | 2 |
| **Lav** | 0 | 0 | 6 | 6 |
|  |  | **Lav** | **Moderat** | **Høy** | **Svært høy** |
|  | | **Konsekvensnivå** | | | |

(Man bør i arbeidet med retningslinjen systematisk vurdere innholdet i matrisen over og tabellen under, slik at man forstår hva de medfører, og kan vurdere om dette er hensiktsmessig for virksomheten. Begge kan justeres ut fra virksomhetens behov.)

**Planlegg risikovurderinger iht. tabellen under**

| **Prioritets-gruppe** | **Beslutning** |
| --- | --- |
| 0 | * Det er **ikke behov** for å gjennomføre nye eller oppdaterte risikovurderinger |
| 1 - 2 | * Ny/oppdatert risikovurdering skal gjennomføres **uten ugrunnet opphold** * Prioritering skal skje etter prioritetsgruppe * Nye arbeidsoppgaver skal ikke startes og nye system skal ikke tas i bruk før ny eller oppdatert risikovurdering er gjennomført og fulgt opp * Det skal straks vurderes om det er behov for eventuelle midlertidige ekstratiltak eller stopp i gjennomføring av oppgaver og bruk av IKT-system og annet utstyr. |
| 3 - 5 | * Ny/oppdatert risikovurdering skal gjennomføres **innen rimelig tid** * Prioritering skal skje etter prioritetsgruppe og ut fra kunnskapsstyrken[[5]](#footnote-5) på tidligere vurderinger * Nye arbeidsoppgaver kan startes og nye system kan tas i bruk dersom de etableres innen virksomhetens fellessikring og oppgaven som skal løses er svært viktig for å nå virksomhetens overordnede mål |
| 6 | * Ny/oppdatert risikovurdering skal **gjennomføres med intervall på maks 3 år, dersom ikke ny kunnskap tilsier gjennomføring tidligere** * Omfanget skal tilpasses kunnskapsstyrken4 på tidligere vurderinger * Nye arbeidsoppgaver kan startes og nye system kan tas i bruk dersom de etableres innen virksomhetens fellessikring og oppgaven som skal løses er svært viktig for å nå virksomhetens overordnede mål |

**Generelle krav:**

* Man skal alltid avslutningsvis for hvert område vurdere om man har spesielt høye risikoer (jf. spørsmål 9) og stor usikkerhet rundt disse. Dette kan kreve en skjønnsmessig høyere prioritering av området enn det som følger av tabellene over[[6]](#footnote-6). En annen prioritering enn i tabellene skal kort begrunnes i de skjema man benytter.
* Ressursinnsats og fokus i nødvendige risikovurderinger skal tilpasses områdets egenart, potensielt konsekvensnivå, antatt risikostørrelse og de foranalyser som er gjennomført.

1. Alle IKT-system og annet teknisk utstyr som benyttes av flere organisatoriske enheter kalles fellessystem. [↑](#footnote-ref-1)
2. «Høyeste konsekvensnivå» er det høyeste nivået på konsekvenser på området som man med en viss grad av sannsynlighet må regne med kan inntreffe. Urealistiske utfall holdes derfor utenfor. For støtte til å finne riktig nivå: Se vedlegg D i retningslinjen *Forstå, vurdere og håndtere risiko*. [↑](#footnote-ref-2)
3. For støtte til antatt høyeste risikonivå: Se eventuelt resultat fra tidligere risikovurderinger, vedlegg C, D og E i retningslinjen *Forstå, vurdere og håndtere risiko*, samt støttespørsmålene i vedlegg A her. [↑](#footnote-ref-3)
4. Kriterier for å akseptere risiko: Se vedlegg B i *Retningslinje: Forstå, vurdere og håndtere risiko*. [↑](#footnote-ref-4)
5. Kunnskapsstyrke et uttrykk for hvor god bakgrunnskunnskap og kvalitet vi har hatt i arbeidet med våre risikovurderinger og risikohåndtering, og dermed hvor sikre vi er på estimatene av konsekvens, sannsynlighet og risiko. Nivåene lav, moderat og høy skal benyttes på kunnskapsstyrke. [↑](#footnote-ref-5)
6. Tabellene baserer seg kun på høyeste konsekvensnivå i prioriteringen, ikke høyeste risikonivå. Den forenkling dette representerer gir en mulig feilkilde i prioriteringen som i stor grad skal rettes opp med dette generelle kravet. [↑](#footnote-ref-6)