**Risikovurdering <SYSTEMNAVN/PROSJEKTNAVN>**

**MARKEDSPLASS FOR SKYTJENESTER**

Mal for risikovurdering

V 1.0

|  |  |
| --- | --- |
| Navn | Navn på det som skal risikovurderes (system, arbeidsprosess, initiativ osv.) |
| Dato gjennomført | XX.XX.XXXX |
| Dato revidert | XX.XX.XXXX |
| Ansvarlig for gjennomføring | XXXXXXXXX  |

Innholdsfortegnelse

[Om malen for risikovurdering (fjernes ved utarbeidelse) 3](#_Toc83988675)

[Sammendrag 3](#_Toc83988676)

[Innledning 3](#_Toc83988677)

[Oppsummering fra foranalysen 3](#_Toc83988678)

[Avgrensninger og forutsetninger 3](#_Toc83988679)

[Metode 3](#_Toc83988680)

[Risikovurdering 4](#_Toc83988681)

[Risikoer 4](#_Toc83988682)

[Anbefalte tiltak 5](#_Toc83988683)

[Vedlegg 6](#_Toc83988684)

[Vedlegg 1 – Rollekart 6](#_Toc83988685)

[Vedlegg 2 – Sannsynlighetstabell 6](#_Toc83988686)

[Vedlegg 3 – Konsekvenstabell 6](#_Toc83988687)

[Vedlegg 4 – Risikomatrise 6](#_Toc83988688)

[Vedlegg 5 – Gjennomførte møter og intervjuer 6](#_Toc83988689)

# **Om malen for risikovurdering (fjernes ved utarbeidelse)**

Denne malen anvendes når det er besluttet at det skal anskaffes en skytjeneste og man skal gjennomføre en risikovurdering. Risikovurderingen danner grunnlaget blant annet for utarbeidelse av kravspesifikasjonen.

Risikovurderingen bør godkjennes av behovshaver. Se hvem som bør involveres i vurderingen i rollekartet i vedlegget.

Bruk av malen bør ses i sammenheng med veiledningen som finnes på Markedsplassen.

# **Sammendrag**

Lag en kortfattet oppsummering av innholdet i risikovurderingen slik at interessenter som behovshaver og leverandør får et raskt overblikk uten å måtte lese hele dokumentet.

Forslag til innhold:

* Bakgrunn
* Kort om tjenestene som skal anskaffes
* Konklusjon og noe overordnet rundt tiltak
* Om gjenværende risiko etter tiltak er akseptabel
* Skjermbilder av risikomatriser som viser risikoer før og etter tiltak

# **Innledning**

## Oppsummering fra foranalysen

Fortell kort om de viktigste funnene knyttet til verdier, trusler og sårbarheter fra foranalysen. Dette kan kopieres fra oppsummering i foranalysen.

## Avgrensninger og forutsetninger

Beskriv hva som er omfattet av risikovurderingen, samt det som bevisst er utelatt fra vurderingen.

Beskriv også eventuelle forutsetninger som er tatt.

## Metode

Det finnes flere metoder for å utføre risikovurderinger, beskriv derfor kort metoden som er lagt til grunn i vurderingen. Dersom dere velger å følge metoden som er brukt i malen, kan dere beholde teksten nedenfor.

Metoden i foranalysen baserer seg på det som kalles trefaktormodellen hvor man ser på verdi, trussel og sårbarheter. På bakgrunn av verdi-, trussel- og sårbarhetsvurderingene kan man utlede ulike risikoscenarier som knytter seg til skytjenestene man skal anskaffe.

* Når man skal vurdere risikoscenariene kan man se på følgende: Konsekvens(er) ved at en uønsket hendelse inntreffer. For å vurdere konsekvens kan man se på hva som er den mest trolige konsekvens ved hendelsen. Utgangspunktet for vurderingen er generell erfaring og tilgjengelig informasjon.
* Sannsynlighet for at en uønsket hendelse inntreffer. Sannsynlighet er ikke matematisk i denne sammenheng, men heller en praktisk og erfaringsbasert vurdering.

Når man sammenstiller konsekvens og sannsynlighet kommer man frem til om risikoen er:

* Akseptabel, i den forstand at virksomheten ikke trenger å foreta seg noe videre i form av tiltak
* Ikke akseptabel, i den forstand at virksomheten bør implementere bestemte tiltak for å redusere risikoen til et akseptabelt nivå.

Om risikoen er akseptabel eller ikke avhenger av hvordan virksomheten har definert risikoakseptnivå.

Ikke-akseptable risikoer må møtes med tiltak som er egnet til å redusere risikoen til et akseptabelt nivå. Man kan bruke risiko- og kravbanken som et utgangspunkt for å forstå hvilke tiltak som kan være egnet for den enkelte risikoen. En egen seksjon for “Anbefalte tiltak” finnes lengre ned i dokumentet. Risikovurderinger må gjøres kontinuerlig for å ha en reel oversikt over risikobildet.

Vedlegg 2, 3 og 4 viser tabeller med definisjon av de ulike nivåene for sannsynlighet, konsekvens og risiko som er brukt i vurderingen.

Gjennomføringen av risikovurderingen har vært basert på intervjuer, dokumentgjennomgang, workshops osv. Vedlegg 5 viser en oversikt over gjennomførte møter og deltagere.

# **Risikovurdering**

I de følgende tabellene kan virksomheten angi identifiserte risikoer og uønskede hendelser, og beskrive sannsynlighet, konsekvens og risiko.

## Risikoer

Her kan virksomheten bruke blant annet risikobanken som inspirasjon.

|  |  |
| --- | --- |
| **1** | **Kort navn på risiko** |
| **Beskrivelse av risiko** |  |
| **Beskrivelse av konsekvens** | Bruk innsikt fra foranalysen til å beskrive konsekvens. |
| **Beskrivelse av sannsynlighet** | Bruk innsikt fra foranalysen til å beskrive sannsynlighet. |
| **Risiko** | **Konsekvens** |  | **Sannsynlighet** |  | **Risiko** |  |  |
| **Mulige tiltak** | Referer til aktuelle tiltaks-ider fra tabellen i kapittelet «Anbefalte tiltak». |
| **Risiko etter tiltak** | **Konsekvens** |  | **Sannsynlighet** |  | **Risiko** |  |  |

|  |  |
| --- | --- |
| **2** | **Kort navn på risiko** |
| **Beskrivelse av risiko** |  |
| **Beskrivelse av konsekvens** | Bruk innsikt fra foranalysen til å beskrive konsekvens. |
| **Beskrivelse av sannsynlighet** | Bruk innsikt fra foranalysen til å beskrive sannsynlighet. |
| **Risiko** | **Konsekvens** |  | **Sannsynlighet** |  | **Risiko** |  |  |
| **Mulige tiltak** | Referer til aktuelle tiltaks-ider fra tabellen i kapittelet «Anbefalte tiltak». |
| **Risiko etter tiltak** | **Konsekvens** |  | **Sannsynlighet** |  | **Risiko** |  |  |

|  |  |
| --- | --- |
| **3** | **Kort navn på risiko** |
| **Beskrivelse av risiko** |  |
| **Beskrivelse av konsekvens** | Bruk innsikt fra foranalysen til å beskrive konsekvens. |
| **Beskrivelse av sannsynlighet** | Bruk innsikt fra foranalysen til å beskrive sannsynlighet. |
| **Risiko** | **Konsekvens** |  | **Sannsynlighet** |  | **Risiko** |  |  |
| **Mulige tiltak** | Referer til aktuelle tiltaks-ider fra tabellen i kapittelet «Anbefalte tiltak». |
| **Risiko etter tiltak** | **Konsekvens** |  | **Sannsynlighet** |  | **Risiko** |  |  |

## Anbefalte tiltak

Ettersom formålet med denne risikovurderingen er å komme frem til aktuelle krav som bør stilles til tjenesten eller leverandøren, er det naturlig at mange tiltak er krav, men noen tiltak kan gjelde internt i virksomheten. Tiltak vil bli endret og oppdatert etter hvert som den kontinuerlige risikoprosessen avdekker endringer i risikobildet.

|  |  |
| --- | --- |
| # | Beskrivelse av tiltak |
| T1 |  |
| T2 |  |
| T3 |  |
| T4 |  |

# **Vedlegg**

## Vedlegg 1 – Rollekart

Det anbefales at følgende roller deltar i risikovurderingen:

|  |  |  |
| --- | --- | --- |
| # | Rolle | Oppgave |
| 1 | Virksomhetsleder | Godkjenner risikovurderingen |
| 2 | Behovshaver / systemeier | Ansvarlig for at tjenesten som anskaffes er sikker og lovlig |
| 3 | Fagansvarlig informasjonssikkerhet og personvernombud | Fører risikovurderingen i pennenAnsvarlig for risikovurderingen |
| 4 | IKT-fagansvarlig  | Deltaker |
| 5 | Innkjøpere | Deltaker |
| 6 | Utviklere, arkitekter | Deltaker |

Merk at dette kun er et forslag og listen er ikke uttømmende.

## Vedlegg 2 – Sannsynlighetstabell

Sett inn sannsynlighetstabellen som er benyttet. Det finnes et eksempel på markedsplassen.

## Vedlegg 3 – Konsekvenstabell

Sett inn konsekvenstabellen som er benyttet. Det finnes et eksempel på markedsplassen.

## Vedlegg 4 – Risikomatrise

Sett inn risikomatrisen som er benyttet. Det finnes et eksempel på markedsplassen.

## Vedlegg 5 – Gjennomførte møter og intervjuer

|  |  |  |
| --- | --- | --- |
| Dato | Tema | Deltakere |
|  |  |  |
|  |  |  |
|  |  |  |