**Foranalyse <SYSTEMNAVN/PROSJEKTNAVN>**

**MARKEDSPLASS FOR SKYTJENESTER**

Mal for foranalyse

V 1.0

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

Innholdsfortegnelse

[Om malen for foranalyse (fjernes ved utarbeidelse) 3](#_Toc83988690)

[Sammendrag 3](#_Toc83988691)

[Kort om tjenesten som skal anskaffes 4](#_Toc83988692)

[Hvilke informasjonsverdier skal behandles 4](#_Toc83988693)

[Brukere av systemet 4](#_Toc83988694)

[Foranalyse 5](#_Toc83988695)

[Verdivurdering 5](#_Toc83988696)

[Trusselvurdering 6](#_Toc83988697)

[Sårbarhetsvurdering 8](#_Toc83988698)

[Vedlegg 9](#_Toc83988699)

[Rollekart 9](#_Toc83988700)

[Skalaer og nivåer for vurdering av verdi 9](#_Toc83988701)

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

Denne malen kan tas i bruk når det er besluttet at det skal anskaffes en skytjeneste. I så fall skal man gjennomføre en foranalyse. Foranalysen er et viktig innspill til risikovurderingen som igjen danner grunnlaget for utarbeidelse av kravspesifikasjonen.

Digitaliseringsdirektoratet (Digdir) har veiledning for hvordan man gjennomfører en foranalyse. Når Digdir snakker om foranalyse så er dette ment som en overordnet aktivitet for å skape oversikt over oppgaver, tjenester og informasjonsbehandling - slik at man kan prioritere hvor det trengs grundigere vurdering og håndtering av risiko. Hvis man har etablert dette som en aktivitet i egen virksomhet og den gir tilstrekkelig oversikt over tjenesten som skal anskaffes, er det ikke nødvendig å gjøre en ny foranalyse, men hente ut den relevante informasjonen til bruk i risikovurderingen. Denne malen tar utgangspunkt i Digdir sin veiledning, men er tilpasset slik at den egner seg til å gjøre en konkret risikovurdering. I tillegg er malene til Digdir forenklet og justert for å lettere kunne vurdere risiko ved en anskaffelse.

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

Hvis det er noen ord eller begreper du ikke forstår i denne malen, kan det være nyttig å se til Digdir sin utfyllende [veiledning](https://www.digdir.no/informasjonssikkerhet/ha-oversikt-over-et-ansvarsomrade/2642) for foranalyse.

Foranalysen bør godkjennes av behovshaver. Se hvem som bør involveres i en foranalyse i rollekartet i vedlegget.

# **Sammendrag**

Lag en kortfattet oppsummering av innholdet i foranalysen slik behovshaver og leverandør får et raskt overblikk uten å måtte lese hele dokumentet. Er dokumentet kort, kan oppsummeringen utelates.

Forslag til innhold:

* Bakgrunn
* Kort om systemet som skal anskaffes
* En oversikt over informasjonen somsystemet skal behandle
* En oppsummering av vurdering av konfidensialitet, integritet og tilgjengelighet
* Relevante trusler
* Relevante sårbarheter

# **Kort om tjenesten som skal anskaffes**

## Hvilke informasjonsverdier som skal behandles

List opp hvilke informasjonsverdier som behandles av tjenesten som skal anskaffes. Informasjonsverdier (eller bare verdier) er ressurser (enten fysiske eller logiske) som, hvis de blir utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som drar fordel av ressursen. Misbruk av informasjonsverdier skjer som regel ved brudd på konfidensialitet, integritet og tilgjengelighet på en måte som har negative innvirkninger på virksomhetens mål.

Hvis man skal anskaffe et informasjonssystem, er følgende typiske eksempler på verdier: brukerdata, kundedata, produktinformasjon, avtaler/kontrakter, personopplysninger, datamaskiner (f.eks. servere og databaser) og applikasjoner. Verdier kan også være fysiske dokumenter. Det er flere regelverk som setter krav til beskyttelse av informasjonsverdier, deriblant arkivloven, sikkerhetsloven, GDPR, for å nevne bare noen. En virksomhet må sette seg inn i hvilke regelverk som gjelder deres virksomhet.

Husk at informasjonen i et system inkluderer selve dataene som systemet *behandler*, så vel som logger, konfigurasjonsdata og sikkerhetskopiering som systemet *genererer*.

## Brukere av tjenesten

Det er nyttig å si noe om hvem som er brukere av tjenesten for å komme fram til hvilken verdi informasjonen har.

Beskriv hvem som skal bruke tjenesten og tiltenkt bruk. Husk å inkludere både interne og eksterne brukere dersom dette er relevant.

# **Foranalyse**

## Verdivurdering

Verdivurderingen er hjørnesteinen i risikovurderingen ettersom den avgjør hvilke verdier som kommer til å bli prioritert i risikovurderingsprosesser..

I tabellene nedenfor kan dere legge inn informasjonsverdiene som er identifisert og angi på en skala fra 1 til 4, hvilken konsekvens tap av konfidensialitet, integritet og tilgjengelighet (KIT) har for virksomheten din. Dette gjøres basert på en konsekvenstabell. Det finnes et eksempel på konsekvenstabell på Markedsplassen. Eksisterende eksempler på konsekvenstabeller kan bli brukt som utgangspunkt, men virksomheten din må lage en egen konsekvenstabell tilpasset virksomhetens situasjon.

* I tabellen vurderer man KIT innen ulike konsekvenskategorier. Kategoriene er bare et eksempel og er hentet fra konsekvenstabellen som finnes på Markedsplassen. Hver virksomhet må vurdere hvilke konsekvenskategorier de ønsker å bruke.
* Når dere vurderer verdi, velg høyeste verdi som er angitt for konfidensialitet, integritet og tilgjengelighet
  + **Konfidensialitet**: konsekvenser hvis informasjon kommer på avveie, blir kjent av uvedkommende og eventuelt misbrukt.
  + **Integritet**: konsekvenser hvis informasjon blir endret eller slettet av uvedkommende eller uten at det var etter hensikt.
  + **Tilgjengelighet**: konsekvenser hvis informasjon blir utilgjengelig.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Konsekvensnivå** | | | | **Merknad** |
| **Informasjonsverdi** | **Konsekvens-kategori** | **K** | **I** | **T** | **Verdi** |
|  | Liv og helse |  |  |  |  |  |
| Økonomi |  |  |  |  |  |
| Omdømme |  |  |  |  |  |
| Måloppnåelse |  |  |  |  |  |
| Lover og regler |  |  |  |  |  |
|  | Liv og helse |  |  |  |  |  |
| Økonomi |  |  |  |  |  |
| Omdømme |  |  |  |  |  |
| Måloppnåelse |  |  |  |  |  |
| Lover og regler |  |  |  |  |  |
|  | Liv og helse |  |  |  |  |  |
| Økonomi |  |  |  |  |  |
| Omdømme |  |  |  |  |  |
| Måloppnåelse |  |  |  |  |  |
| Lover og regler |  |  |  |  |  |
|  | Liv og helse |  |  |  |  |  |
| Økonomi |  |  |  |  |  |
| Omdømme |  |  |  |  |  |
| Måloppnåelse |  |  |  |  |  |
| Lover og regler |  |  |  |  |  |

K=Konfidensialitet, I=Integritet, T=Tilgjengelighet

## Trusselvurdering

Trusler kan defineres som uønskede hendelser som har en negativ konsekvens for virksomheten. Trusler kan ta form både som tilsiktede hendelser, slik som en cyberhendelse, eller utilsiktede hendelser, slik som naturkatastrofer eller feilkonfigurasjon av en løsning.

En trusselaktør er en person eller enhet som kan utføre en trussel. Når dere anskaffer en skytjeneste er det viktig å tenke på at trusler og trusselaktører kan ligge hos skytjenesteleverandøren.

#### Trusselaktører

Ved å benytte tabellen nedenfor kan dere vurdere trusselaktører.

Trusselaktør er en person, organisasjon eller et naturelement som kan forårsake en trusselhendelse mot virksomhetens verdier.

* Når dere vurderer motivasjon, vilje, kapasitet, trusselnivå og kunnskapsstyrke, bruk for eksempel kodene SH=Svært høy; H=Høy; M=Moderat; L=Lav; IA=ingen aning. Disse begrepene defineres på følgende måte:
  + Motivasjon er årsaken eller målet som fører trusselaktøren til å ønske å utføre en trussel
  + Vilje er drivkraften til å ville gjennomføre en trussel
  + Kapasitet er evnen og muligheten som trusselaktøren har til å faktisk gjennomføre en trussel
  + Trusselnivå beskriver i hvilken grad trusselen er vurdert å kunne inntreffe
  + Kunnskapsstyrke er kunnskapen som ligger til grunn for vurderingen
* Bruk eget skjønn på kodevalgene ut fra hva dere vet og tror om trusselaktørene. For å få økt innsikt kan anbefales å lese anerkjente rapporter om sårbarhet, for eksempel fra PST, NSM eller NorSIS
* Fyll ut merknadsfeltet ved behov
* Etter vurdering av aktørene kan virksomheten være tjent med å benytte seg av et system for å fremheve de høyeste trusselnivåene. Dette kan for eksempel gjøres ved bruk av fargekoder.

|  | Grunnlag | | | Konklusjon | | Merknad |
| --- | --- | --- | --- | --- | --- | --- |
|  | Intensjon | | Kapa­sitet | Trussel­nivå | Kunnskaps­styrke |
| Trusselaktør | Motiv | Vilje |
| Utro tjenere internt i virksomheten |  |  |  |  |  |  |
| Utro tjenere hos skyleverandør |  |  |  |  |  |  |
| Ansatte i egen virksomhet (utilsiktede hendelser, f.eks. feil) |  |  |  |  |  |  |
| Ansatte hos skyleverandør (utilsiktede hendelser, f.eks. feil) |  |  |  |  |  |  |
| Organiserte kriminelle |  |  |  |  |  |  |
| Konkurrenter |  |  |  |  |  |  |
| Enkeltkriminelle |  |  |  |  |  |  |
| Politisk motiverte aktører - «Hacktivister» |  |  |  |  |  |  |
| Fremmed stat – statssponsede aktører |  |  |  |  |  |  |
| Terrorister |  |  |  |  |  |  |
| Regulatoriske myndigheter |  |  |  |  |  |  |
| (Andre?) |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### Trusler

Ved å benytte tabellen nedenfor kan dere vurdere trusler. Truslene er utgangspunktet for risikovurderingen du skal gjennomføre etter at du har gjennomført foranalysen, hvor du altså skal vurdere konsekvens og sannsynlighet for de aktuelle truslene.

* Når dere vurderer trusler, tenk på hvilke uønskede hendelser som kan oppstå hos skyleverandør og i egen virksomhet knyttet til de(n) aktuelle tjenesten(e)
* Når dere vurderer hvor truslene kan oppstå, fokuser på trusselaktørene som ble identifisert ovenfor.
* Når dere vurderer sannsynlighet, forventet skadenivå og kunnskapsstyrke bruk for eksempel kodene SH=Svært høy; H=Høy; M=Moderat; L=Lav; IA=ingen aning. .
* Bruk eget skjønn på kodevalgene ut fra hva dere vet og tror om farekildene og stedene.
* Fyll ut merknadsfeltet med eventuelle spesielle forhold dere kjenner til som påvirker sannsynlighet og skadenivå.
* Etter vurdering av trusler og steder kan virksomheten være tjent med å benytte seg av et system for å fremheve radene med de høyeste kombinasjonene av innledende sannsynlighet og forventet skadenivå, dette vil legge til rette for lettere identifikasjon ved senere bruk. Dette kan for eksempel gjøres ved bruk av fargekoder.

| Trussel | Trusselaktør | Sannsynlighet | Forventet skadenivå | Kunnskaps­styrke | Merknad | |
| --- | --- | --- | --- | --- | --- | --- |
| Regelverksbrudd | Hos skyleverandør  I egen virksomhet |  |  |  |  |
| Løsepengevirus | Organiserte kriminelle |  |  |  |  | |
| Phishing |  |  |  |  |  | |
| ID-tyveri |  |  |  |  |  | |
| Datalekkasje |  |  |  |  |  | |
| Verdikjedeangrep |  |  |  |  |  | |
| Brann | Hos skyleverandør |  |  |  |  | |
| Brann | I eget serverrom |  |  |  |  | |
| Brann | I arbeidslokaler |  |  |  |  | |
| Vannlekkasje | Hos skyleverandør |  |  |  |  | |
| Vannlekkasje | I eget serverrom |  |  |  |  | |
| Vannlekkasje | I arbeidslokaler |  |  |  |  | |
| Jordskjelv | Hos skyleverandør |  |  |  |  | |
| Strømfeil | Hos skyleverandør |  |  |  |  | |
| Nettverksfeil | Hos skyleverandør |  |  |  |  | |
| (Andre?) |  |  |  |  |  | |
|  |  |  |  |  |  | |

## Sårbarhetsvurdering

En sårbarhet er en svakhet i en tjeneste som kan utnyttes av en trusselaktør for å tilgang til en verdi. Tjenester kan ha sårbarheter uten at det er koblet trusler til sårbarheten. Hvis du ikke finner sårbarheter som relaterer seg til truslene du har identifisert ovenfor, er trusselen mindre relevant og kan derfor nedprioriteres i risikovurderingen. Ved å benytte tabellene nedenfor kan du vurdere sårbarheter.

* Når dere vurderer sårbarhetsnivå og kunnskapsstyrke, bruk for eksempel kodene SH=Svært høy; H=Høy; M=Moderat; L=Lav; IA=ingen aning.
* Bruk eget skjønn på kodevalgene ut fra hva dere vet og tror. For å få økt innsikt kan anbefales å lese anerkjente rapporter om sårbarheter fra for eksempel fra PST, NSM, NorSIS eller kommersielle leverandører av teknologi.
* Fyll ut merknadsfeltet med eventuelle spesielle forhold dere kjenner til som påvirker deres vurdering av status og sårbarhetsnivå.

Tilsvarende vurderinger av sårbarhetsnivå og kunnskapsstyrke er ikke relevant for potensielle sårbarheter ettersom dette er tenkte sårbarheter man ønsker å unngå.

| Relevante sårbarheter i egen virksomhet som kan påvirke anskaffelsen | Sårbarhets-nivå | Kunnskaps­­styrke | Merknad |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| Potensielle sårbarheter i systemet/arbeidsprosessen som tjenesten skal være en del av | Merknad |
| --- | --- |
|  |  |
|  |  |
|  |  |

| Potensielle sårbarheter hos leverandøren | Merknad |
| --- | --- |
|  |  |
|  |  |
|  |  |

# **Vedlegg**

## Rollekart

Det anbefales at følgende roller deltar i foranalysen:

|  |  |  |
| --- | --- | --- |
| # | Rolle | Oppgave |
| 1 | Virksomhetsleder | Signerer og godkjenner foranalysen |
| 2 | Behovshaver/systemeier | Ansvarlig for at tjenesten som anskaffes er sikker og lovlig. |
| 3 | Fagansvarlig informasjonssikkerhet | Fører foranalysen i pennen  Ansvarlig for foranalysen |
| 4 | Personvernombud og/eller internjurist | Deltaker |
| 5 | IKT-fagansvarlig | Deltaker |
| 6 | Innkjøpere | Deltaker |
| 7 | Utviklere, arkitekter | Deltaker |

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

## Skalaer og nivåer for vurdering av verdi

Det finnes eksempler på markedsplassen.

## Begreper

**Integritet** omtaler konsekvenser ved at informasjon blir endret eller slettet

**Kapasitet** er evnen og muligheten som trusselaktøren har til å faktisk gjennomføre en trussel

**Konfidensialitet** omtaler konsekvenser ved at informasjon kommer på avveie, blir kjent av uvedkommende og eventuelt misbrukt

**Kunnskapsstyrke** er kunnskapen som ligger til grunne for vurderingen

**Motivasjon** er årsaken eller målet som fører trusselaktøren til å ønske å utføre en trussel

**Risiko** er forhold eller hendelser som kan inntreffe (men som ikke har inntruffet ennå) og som påvirker måloppnåelsen negativt

**Sårbarhet** er en svakhet i en tjeneste som kan utnyttes av en trusselaktør for å tilgang til en verdi

**Tilgjengelighet** omtaler konsekvenser hvis informasjon blir utilgjengelig

**Trussel** kan defineres som uønskede hendelser som har en negativ konsekvens for virksomheten

**Trusselaktør** er en person, organisasjon eller entitet (for eksempel et naturelement) som kan forårsake en trussel

**Trusselnivå** beskriver i hvilken grad trusselen er vurdert å kunne inntreffe.

**Verdi** inkluderer både informasjon og tilhørende støtteverdier. Misbruk av verdiene vil ha negative innvirkninger på virksomhetens mål.

**Vilje** er drivkraften til å ville gjennomføre en trussel.