

## Riskanalys

En risk och riskåtgärd per blankett!

**1. Identifiera hot och sårbarheter** – Ange de hot och/eller sårbarheter som finns

**2. Riskbeskrivning** – Ange en kortare beskrivning av risken. Vad kan hända?

**3. Konsekvensbeskrivning** – Ange en kortare beskrivning av den troliga konsekvensen om hotet inträffar

**4. Konsekvenskategorier** – Ange vilken eller vilka konsekvenskategorier som är aktuella för denna risk

- ekonomisk förlust (*t.ex. minskade intäkter, ökade kostnader, skada på tillgångar*)
- verksamhetsavbrott (*negativ påverkan på, eller avbrott i den operativa verksamheten*)
- IT - eller systembortfall
- överträdelse eller bristande lagefterlevnad
- personskada
- skada för miljö – och hälsa, inklusive arbetsmiljö
- skada på organisation eller samhället i stort
- negativ påverkan på kommunen (*skadat varumärke, minskat förtroende*)

**5. Konsekvens** – Hur stor blir konsekvensen om det händer?

- 1** - försumbar konsekvens
- 2** - måttlig konsekvens
- 3** - betydande konsekvens
- 4** - allvarlig konsekvens

**Motivera konsekvensvärdet**

**6. Sannolikhet** – Hur stor är sannolikheten att det händer?

- 1 (*osannolikt, mindre än en gång på 10-20 år*)
- 2 (*liten sannolikhet, sällan, en gång på 5-10 år*)
- 3 (*stor sannolikhet, inträffar en gång per år*)
- 4 (*mycket stor sannolikhet, inträffar flera gånger per år*)

**Motivera sannolikhetsvärdet**

**7. Riskvärde** – konsekvens x sannolikhet

**8. Riskrespons** – Ange hur risken ska hanteras<sup>1</sup>

- Acceptera (ska dokumenteras och godkännas av behörig, se delegationsordning)
- Överför
- Reducera
- Undvik

**Motivera riskresponsen**

---

<sup>1</sup> Acceptera: Risken anses vara tillräckligt låg för att den ska vara värd att ta, risken kan alltså accepteras som den är och man väljer att inte göra någonting åt den. T.ex. saknas sätt att hantera risken eller så är kostnaden för åtgärder större än eventuell konsekvens OBS! En riksacceptans behöver dokumenteras!

Överför: Någon annan tar risken och dess riskåtgärder. T.ex. IT-centrum, leverantör om risken som fastställts ligger hos dem.

Reducera: **Minska/minimera** risken genom att införa en eller flera säkerhetsåtgärder så att risken blir så låg som det rimligtvis är möjligt.

Undvik: Välja att inte göra det som man tänkt, t.ex. att inte införa/använda ett system.

## Riskhantering

- 1. Ange åtgärd** – Vad kan göras för att få bort, begränsa eller bevaka de identifierade riskerna och dess sårbarheter?
- 2. Riskägare** – Ange vem eller vilka som har övergripande ansvar för att åtgärden genomförs
- 3. Ansvarig för åtgärd**, om det är känt – ange vem eller vilka som ska utföra åtgärden
- 4. Slutdatum** – När ska åtgärden vara genomförd?
- 5. Påverkan på riskvärde** – Beskriv vilken påverkan som åtgärden kommer att ha på riskens värde

**Datum:**

**Utförd av:**

**Informationsägare:**

Kopia skickas till [infosakerhet@osthammar.se](mailto:infosakerhet@osthammar.se)

Vid innehåll av känsliga uppgifter, kolla med informationssäkerhetsteamet vilken säker kanal som kan användas.