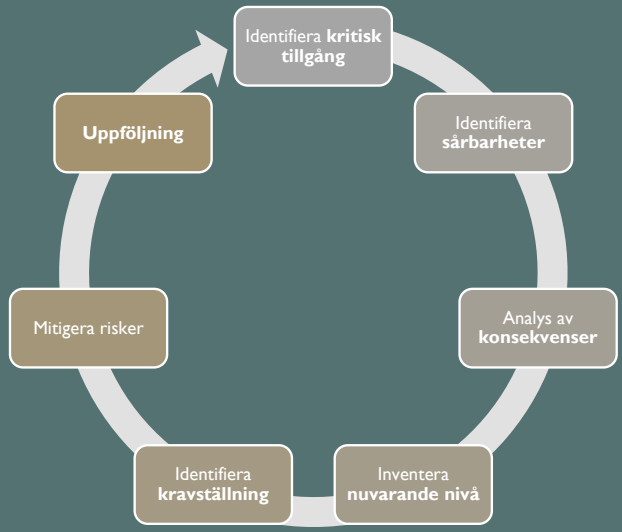
SYSTEMATISKT SÄKERHETSARBETE

I detta materiel beskrivs processarbetets sju steg samt hur genomfarande utförs. Det systematiska säkerhetsarbetet syftar till att identifiera de mest kritiska sårbarheterna, analysera och kvantifiera dem samt arbeta för att konsekvenserna om de skulle inträffa är hanterbara eller att de inte inträffar alls.

PROAKTIV SÄKERHET



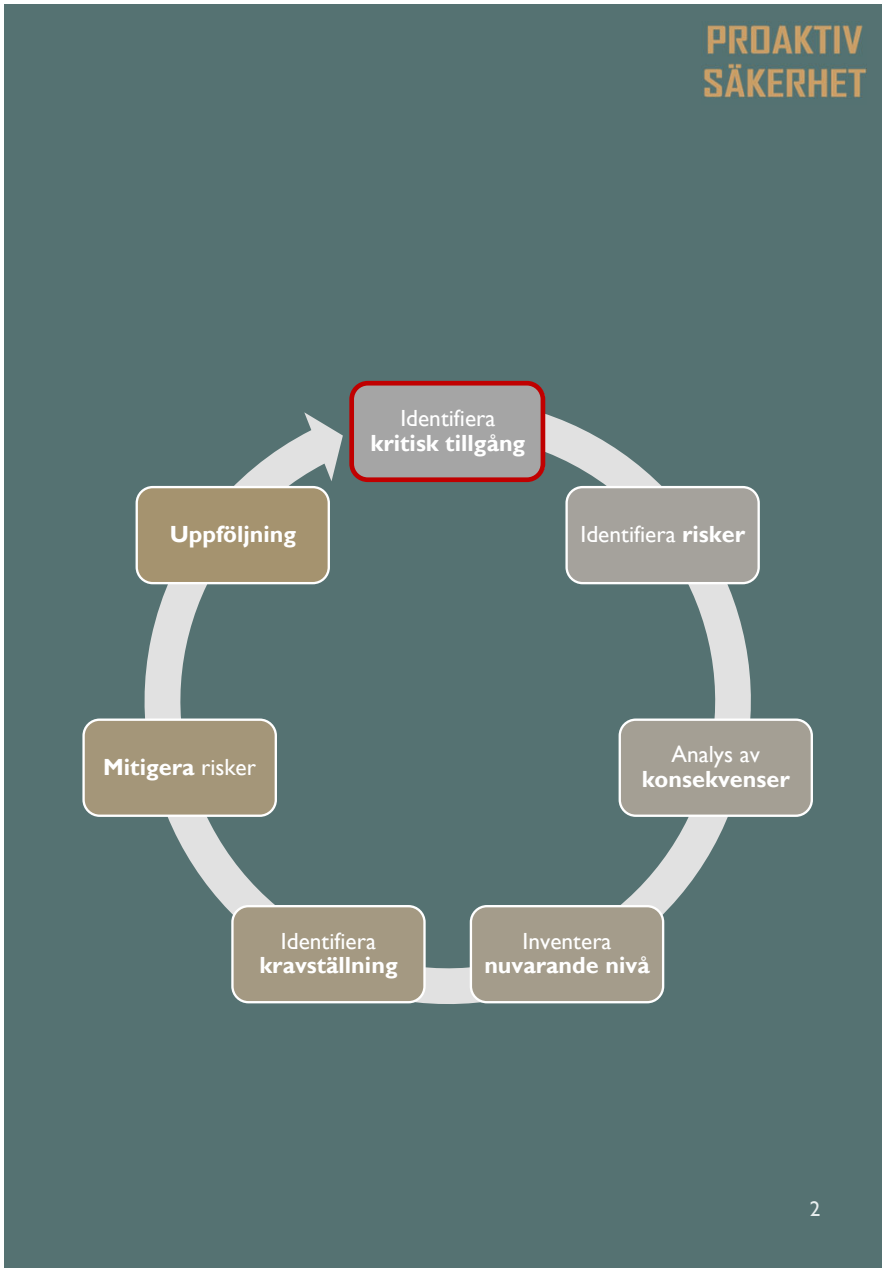
IDENTIFIERA KRITISK TILLGÅNG

Genomförs som workshops med beslutsfattare, specialister, controllers mm identifiera den kritiska tillgången.

Vilka tillgångar har vi i verksamheten som måste skyddas?

Kritisk tillgång kan vara:

- Kritisk infrastruktur (IT, el, vatten, ånga, väg)
- Unik inventarier (testutrustning, dyr i inköp)
- Personal (unik kompetens)



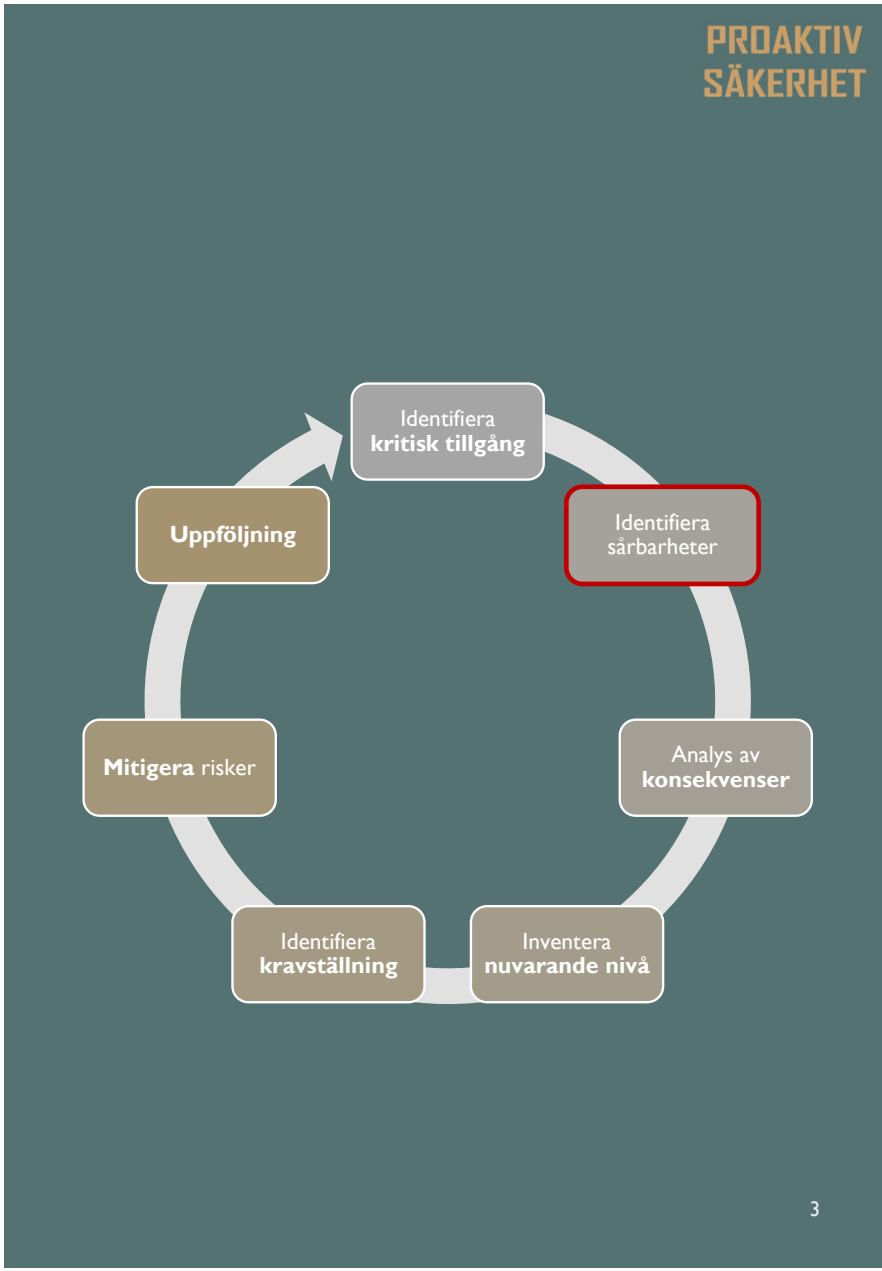
IDENTIFIERA SÅRBARHETER

Identifiera sårbarheterna som är kopplade till den identifierade kritiska tillgången

Vilka eventuella hot, sårbarheter eller risker finns mot de identifierade kritiska tillgångarna?

Sårbarheter kan vara:

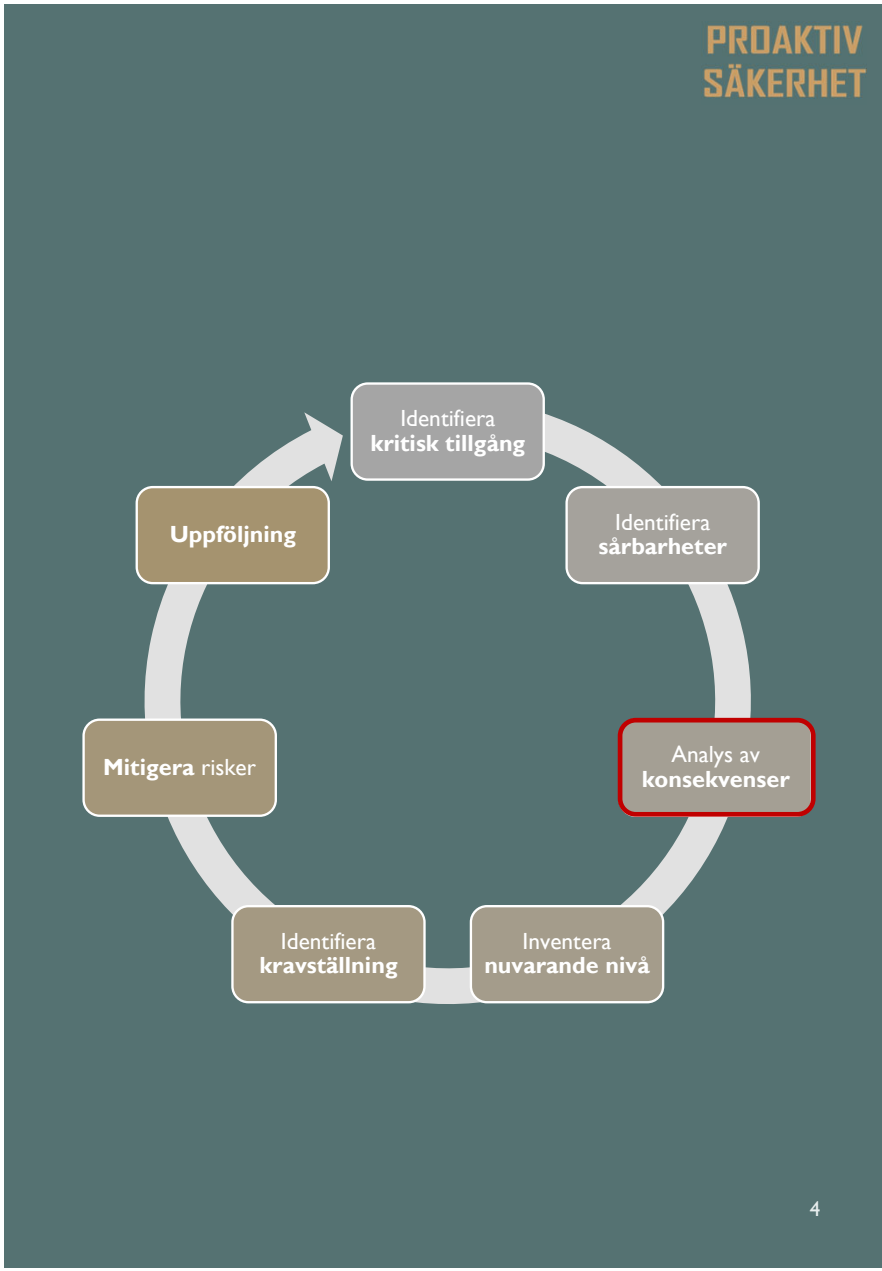
- Förlust av inkomst
- Förlust av kompetens
- Förlorat tilltro till varumärket.



ANALYS AV KONSEKVENSER

Analysera konsekvenserna som de identifierade riskerna kan leda till

Uppskatta konsekvenserna för verksamheten om de identifierade riskerna inträffar.

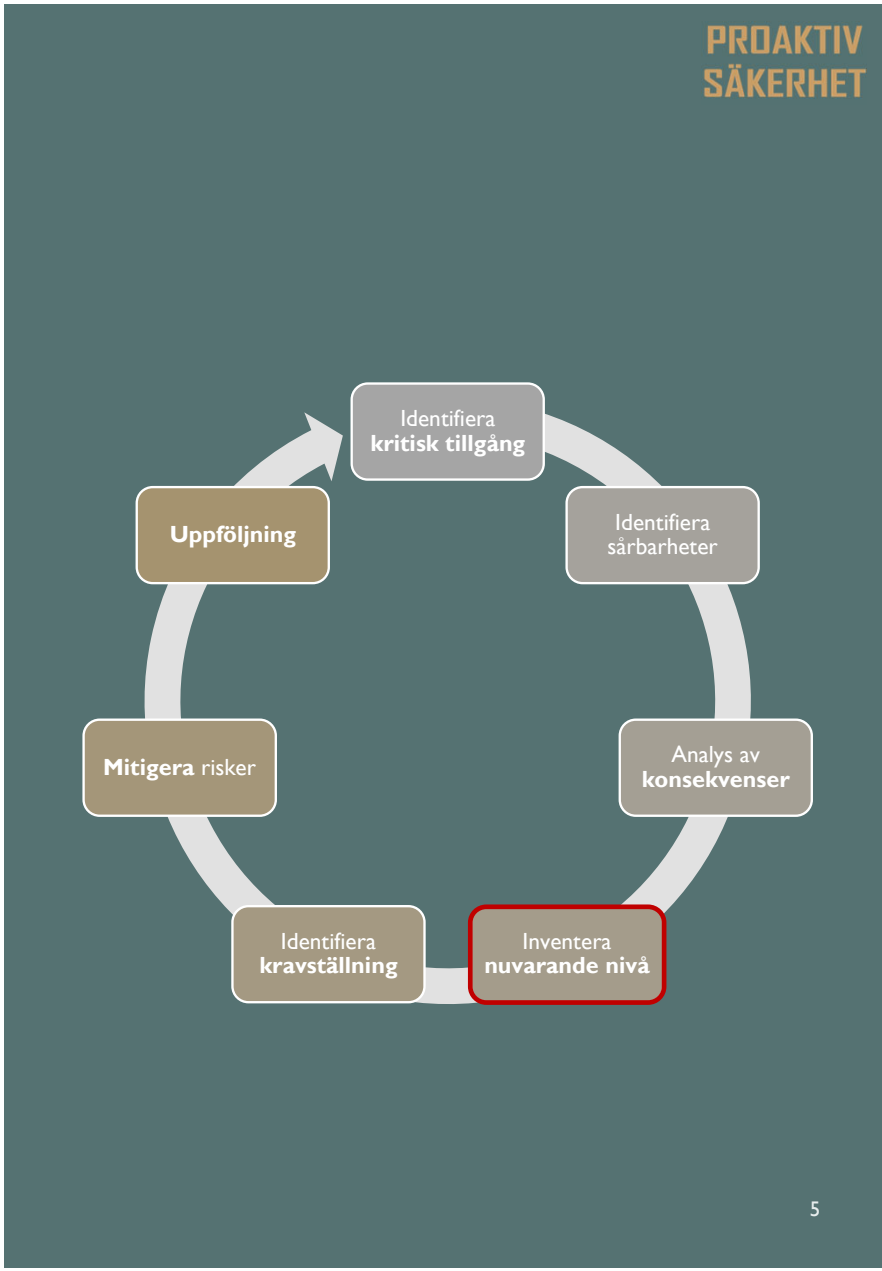


INVENTERA NUVARANDE NIVÅ

Inventera den befintliga skyddsnivån på varje identifierad kritisk tillgång

Hur ser skyddet för verksamheten ut i stort och specifikt mot de identifierade kritiska tillgångarna?

- Fysiskt
  - Omslutningsyta
  - Punktskydd
  - Zonindelning
- Elektroniskt
  - Larm
  - Passagekontrollsystem
  - CCTV
- Kulturellt
  - Regelverk
  - Clean desk
  - Efterlevnad av regelverk
  - Ordning och reda

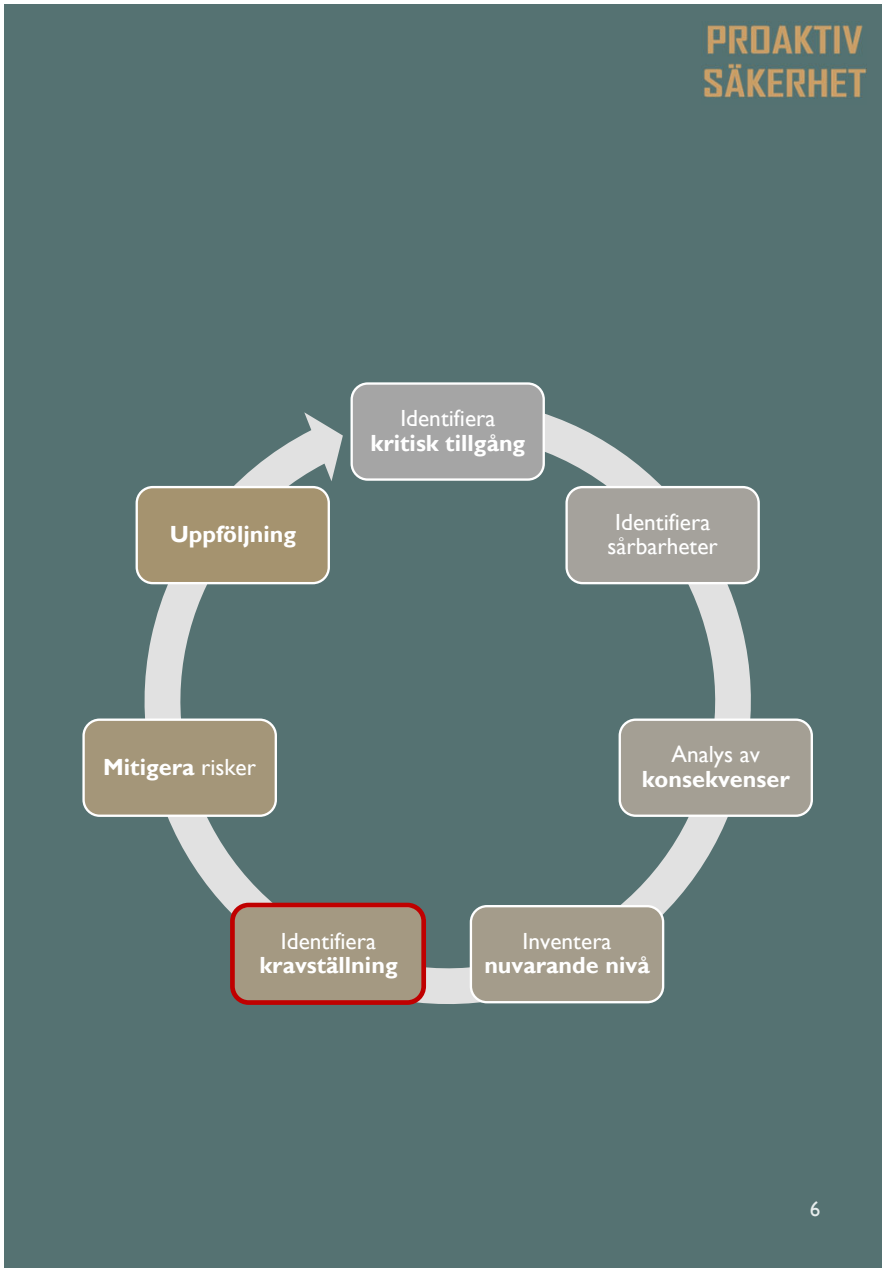


IDENTIFIERA KRAVSTÄLLNING

Identifiera de interna och/eller externa krav som ställs på typen av kritisk tillgång

Utifrån de bedömda riskerna, finns det några krav (interna och/eller externa) att ta hänsyn till?

- Polices
- Instruktioner
- Guidelines
- Lagstiftning
- Myndigheter (författningssamlingar)

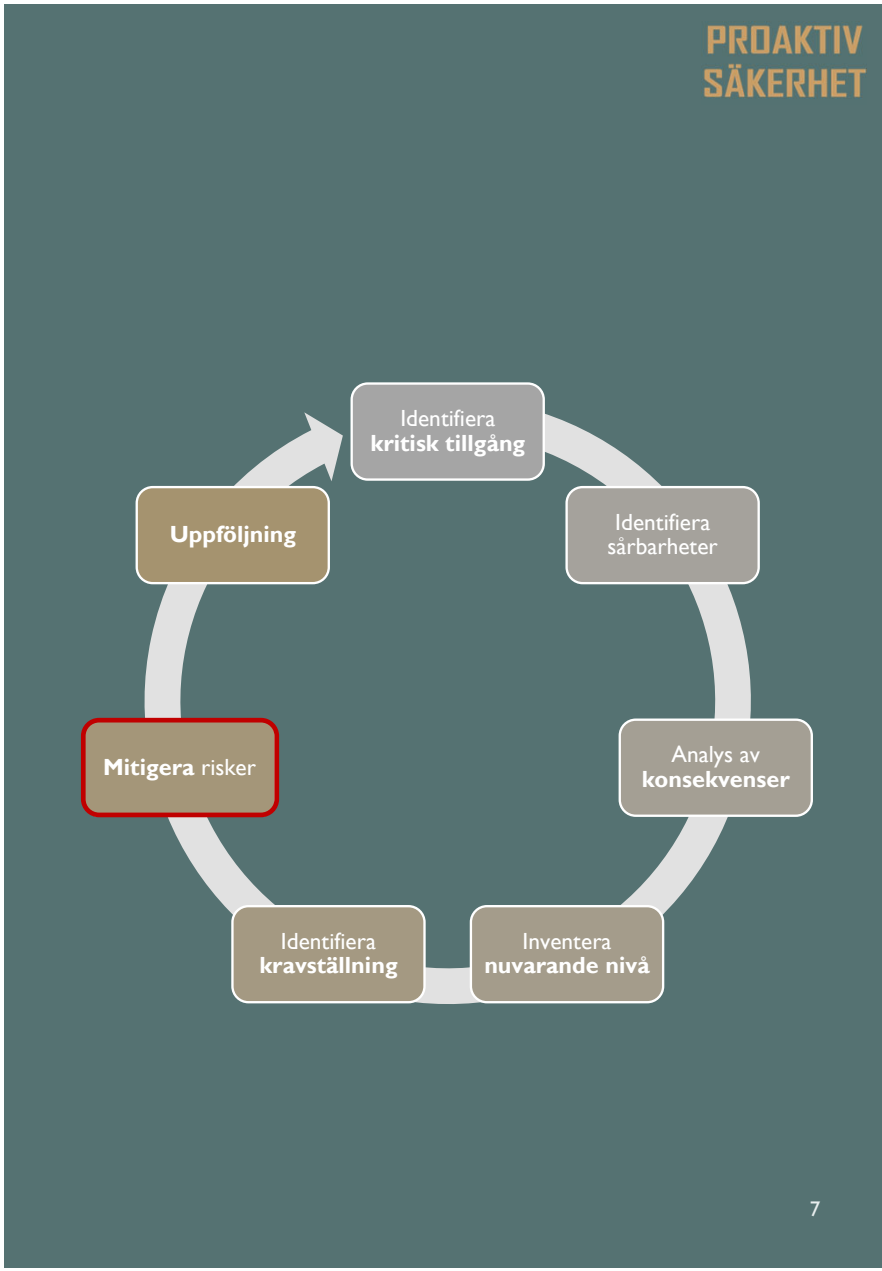


MITIGERA RISKER

Justera skyddet så det uppfyller kraven (interna/externa) som ställs

Hur hanterar och lindrar vi effekterna av de identifierade riskerna och sårbarheterna?

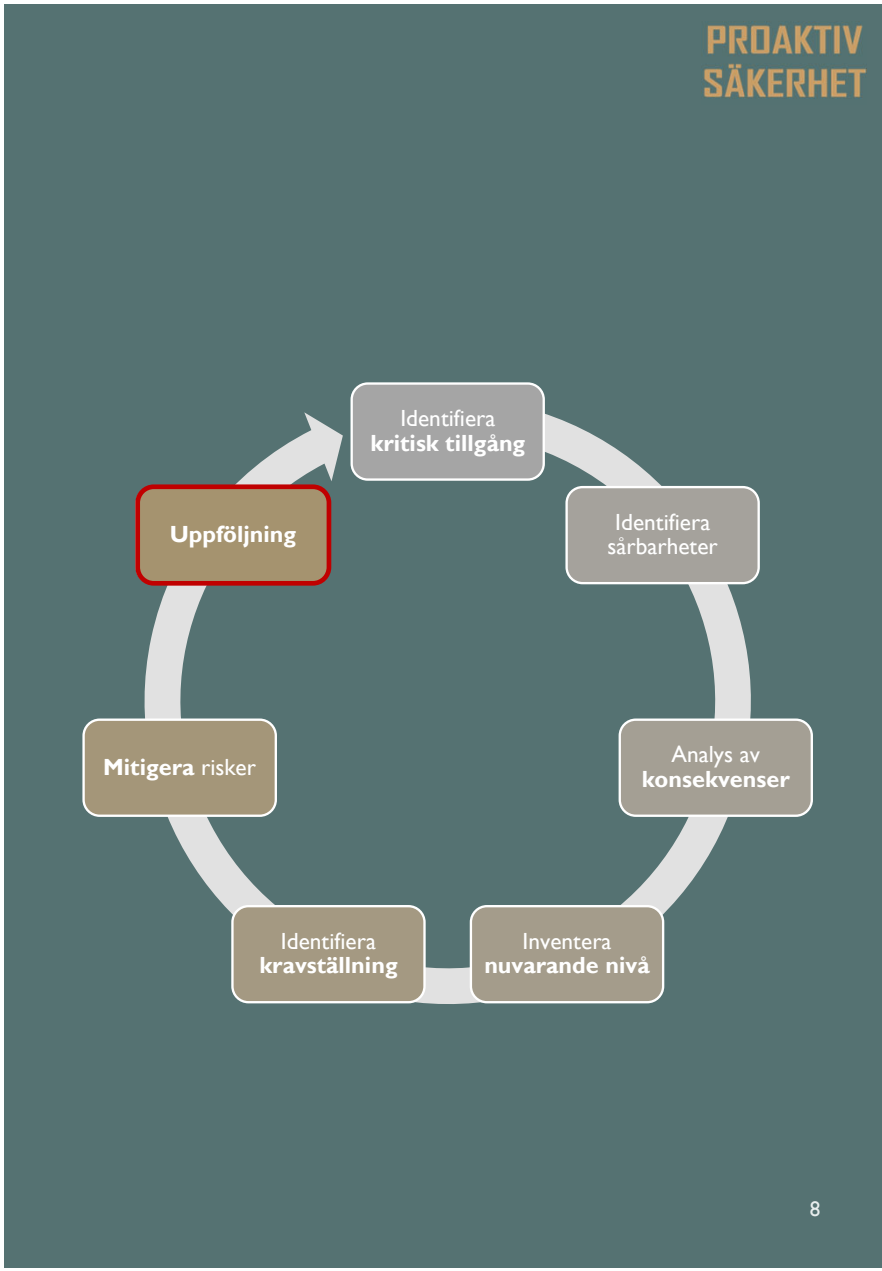
- Ignorerar
- Försäkringar
- Fysiska åtgärder
- Elektroniska åtgärder
- Kulturella åtgärder



UPPFÖLJNING

Följ upp så att alla delar i processen har genomförts och att de åtgärder som är beslutade är genomförda och att tidsplanen har följts.

Finns det något i processen att förbättra?



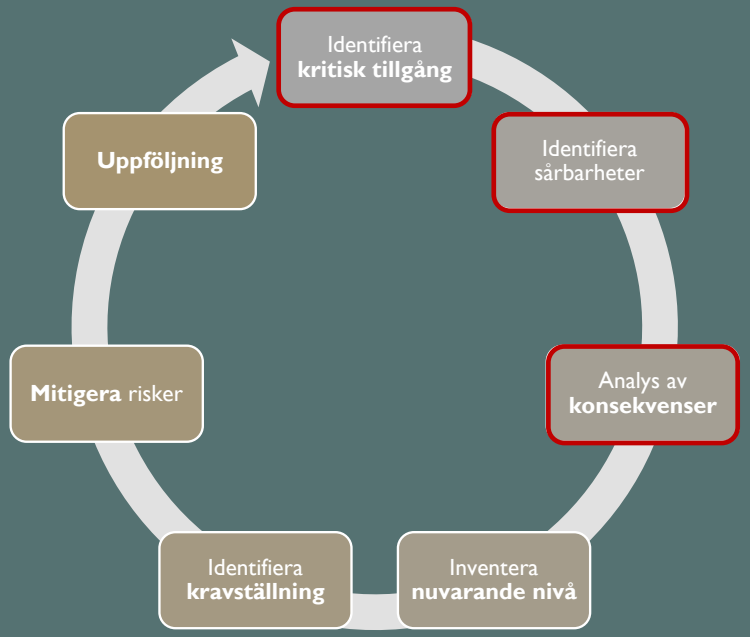
GENOMFÖRANDE – WORKSHOP ENLIGT CARVER

En workshop hanterar de tre första stegen i processen.

Workshopen (CARVER metodiken används) leds av säkerhetskonsulten med olika kompetenser från verksamheten som deltagare:

- Operations
- Finans
- Facility Management
- Security
- Logistik

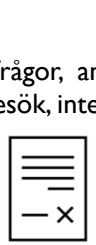
Protokoll, frågor, analysverktyg - Workshop

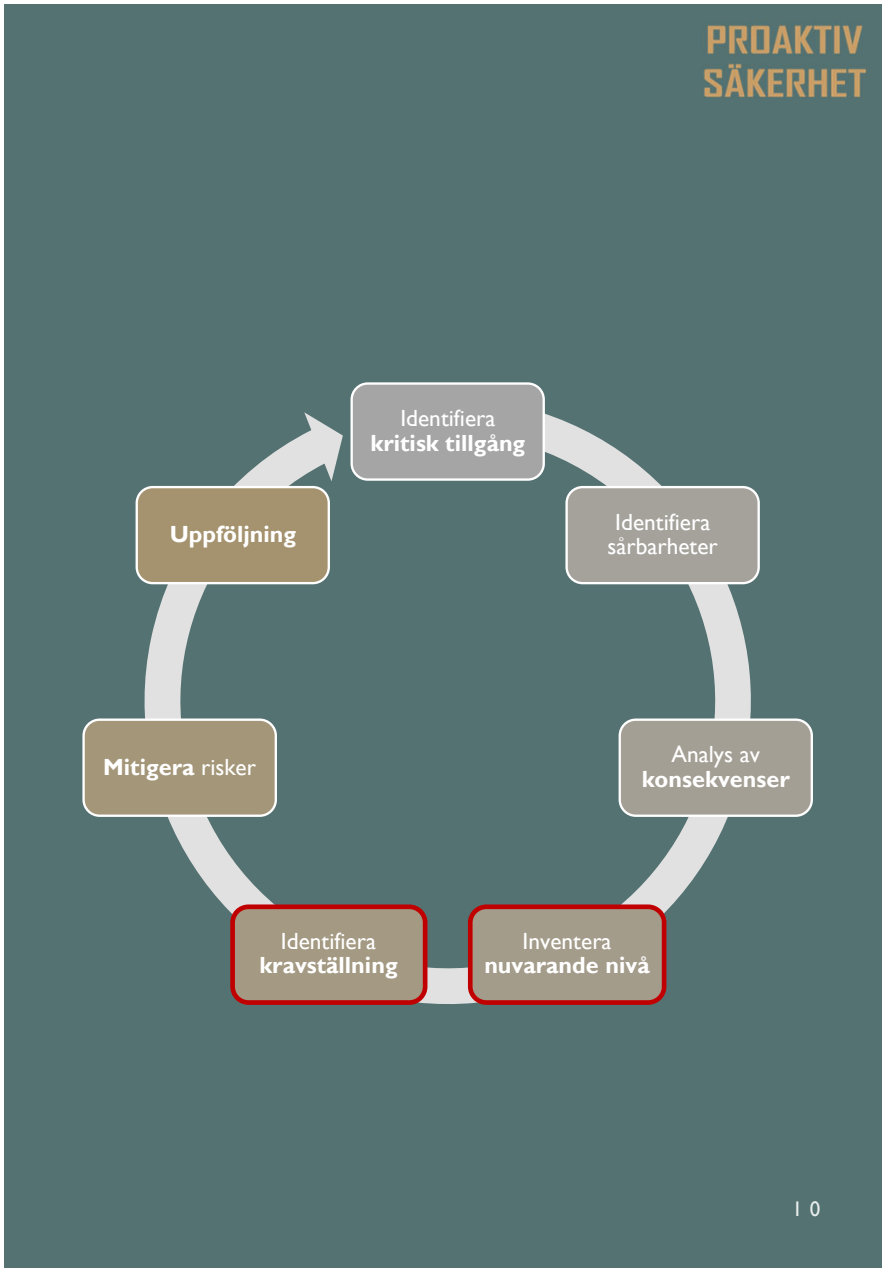


GENOMFÖRANDE - INFORMATIONSINHÄMTNING

Steg fyra och fem innebär inhämtning av information. Detta för att bedöma hur verksamheten eller tillgången ser ut idag samt vilka skyddskrav som ställs.

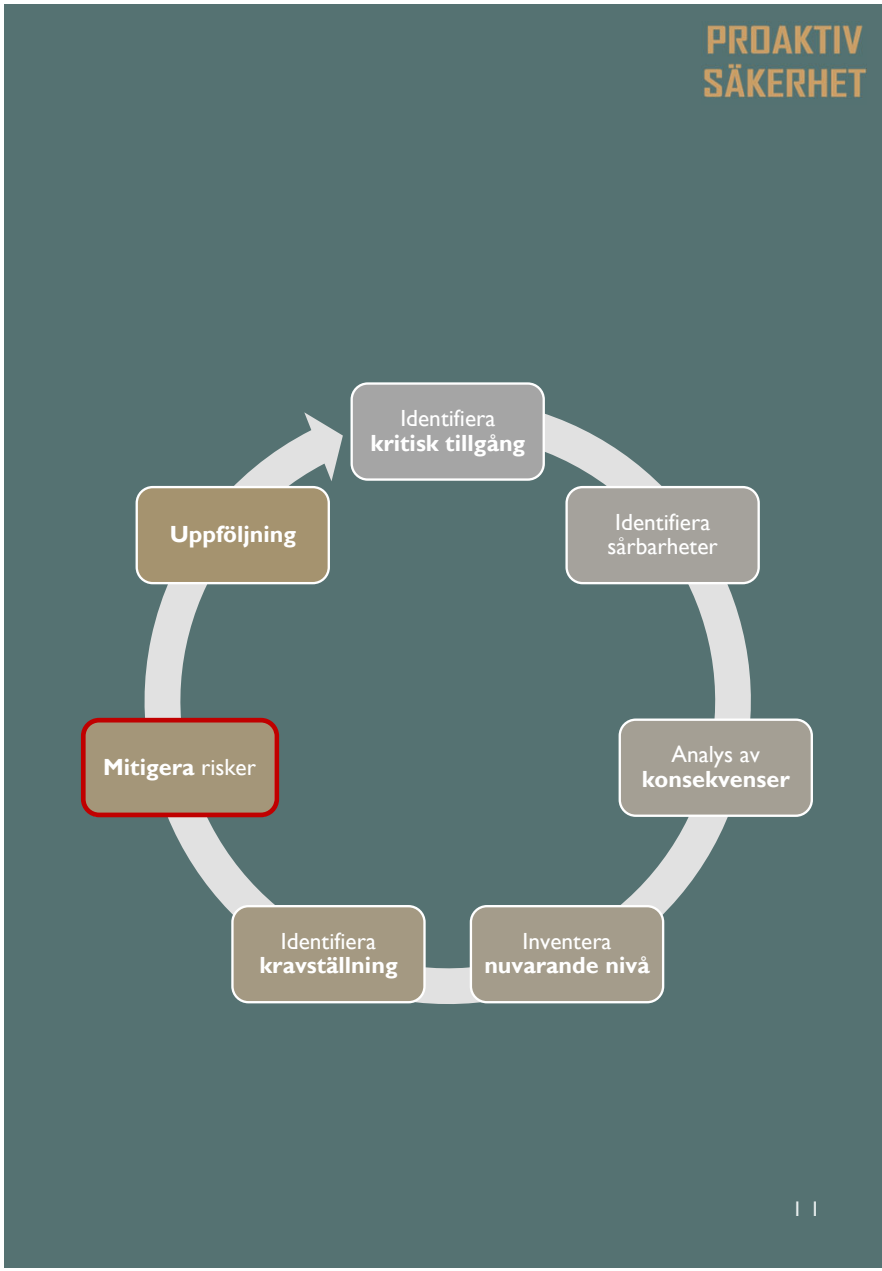
Protokoll, frågor, analysverktyg
Platsbesök, intervjuer





GENOMFÖRANDE - REDUCERA RISKERNA

Ta fram en plan för hur de identifierade riskerna skall reduceras och minskas.



GENOMFÖRANDE - UPPFÖLJNING

Genomförs med de verktyg som verksamheten redan har definierat.