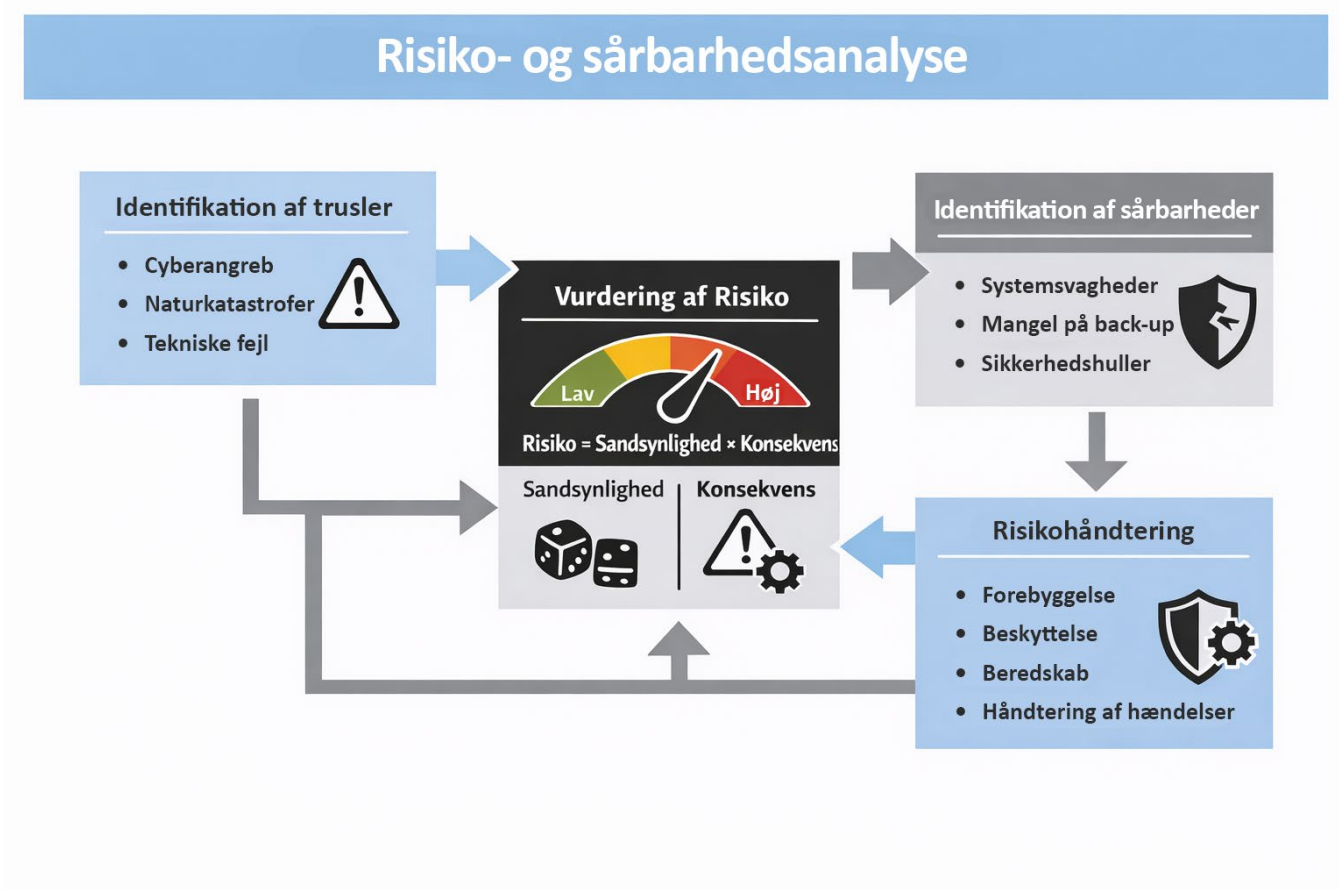
Risiko- og sårbarhedsanalyse



Værktøjet er tilvejebragt i projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), der er støttet med midler fra Industriens Fond. Dato for publicering: 09.01.2026

Fremgangsmåde

1. **Forberedelse**
   - Definer formål og scope: Beslut hvilke forretningsområder, processer og IT-systemer analysen skal dække.
   - Etabler styringsgruppe: Involver ledelse og nøglepersoner fra kritiske funktioner (økonomi, IT, produktion, salg).
   - Saml relevant data: Tidligere hændelser, systemdokumentation, leverandøroplysninger, kontrakter og sikkerhedspolitikker.
2. **Identifikation af forretningskritiske processer og aktiver**
   - Kortlæg alle forretningsprocesser og vurder, hvilke der er kritiske for virksomhedens overlevelse.
   - Identificer tilknyttede aktiver: IT-systemer, medarbejdere, lokationer, forsyningskæde og leverandører.
   - Vurder afhængigheder mellem processer og aktiver.
3. **Identifikation af trusler og sårbarheder**
   - Trusler: Hændelser, som kan påvirke virksomhedens drift (f.eks. cyberangreb, strømudfald, brand, naturkatastrofer, pandemier).
   - Sårbarheder: Svagheder i virksomhedens processer eller systemer, f.eks. mangel på backup, utilstrækkelig IT-sikkerhed, afhængighed af enkeltleverandører og afhængighed af enkeltkunder.
4. **Risikovurdering**
   - For hver kombination af trussel og sårbarhed vurderes:
     1. Sandsynlighed: Hvor sandsynligt er det, at hændelsen indtræffer? (Lav = 1, Middel = 2, Høj = 3).
     2. Konsekvens: Hvad bliver effekten på kritiske processer (økonomisk, operationelt, omdømme)? (Lav = 1, Middel = 2, Høj = 3).
     Udregn risiko, f.eks. Risiko = Sandsynlighed × Konsekvens.
     3. Prioriter risici baseret på høj risiko først.

Fremgangsmåde (fortsat)

5. **Analyse af konsekvenser (Business Impact)**
   - Identificer den maksimale tolerable nedetid for kritiske processer.
   - Kvantificer potentielle tab (økonomi, drift, kundetilfredshed).
   - Brug resultaterne til at fastlægge, hvilke processer der skal prioriteres i kontinuitetsplaner.
6. **Udarbejdelse af handlingsplaner**
   - Udarbejd risikohåndteringstiltag: Forebyggelse, beskyttelse, beredskab, genopretning.
   - Overvej alternative løsninger for kritiske afhængigheder: backup-leverandører, midlertidige lokationer, redundante IT-systemer.
7. **Implementering og træning**
   - Implementér handlingsplaner og sikkerhedsforanstaltninger.
   - Gennemfør træning og øvelser, så medarbejdere ved, hvordan de reagerer i tilfælde af hændelser.
8. **Overvågning og opdatering**
   - Følg op på risici og sårbarheder løbende.
   - Opdater analysen mindst én gang årligt eller ved større ændringer i forretningsprocesser, teknologi eller leverandørforhold.

Fokus bør også være på *single point of failure*, der er en sårbarhed i et system, hvor et svigt her vil medføre, at hele systemet holder op med at fungere.