

INFORMATIONSSIKKERHED OG RISIKOSTYRING

TOPLEDERENS ANSVAR

Ved du, hvad konsekvenserne for jer er i tilfælde af utilgængelige systemer, tab af fortrolig information eller mistet tillid til korrekte data? Og hvad vil du som leder gøre ved det?

I bund og grund er risikostyring netop at stille de spørgsmål og handle på svarene.

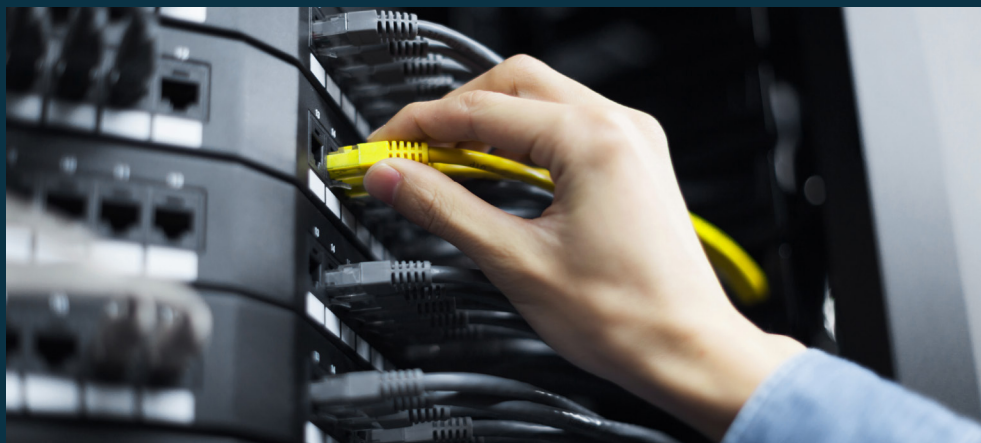
Når det gælder informationssikkerhed, er risikostyring ikke kun en teknisk opgave. Det er en vigtig del af topledelsens ansvar.

I en tid med stadigt flere trusler og voksende uforudsigelighed er risikostyring et nødvendigt værktøj både for at beskytte din organisation og for at sikre, at I når jeres mål. Det er sjældent muligt at fjerne risici helt. Men det er muligt at forstå dem, prioritere sine indsatser og systematisk reducere dem.

Denne pjece sætter fokus på toplederens rolle og ansvar i risikostyring inden for informationssikkerhed.



Styrelsen for
Samfundssikkerhed



Derfor er risikostyring vigtigt

Alle organisationer bruger it-systemer og håndterer data, hvilket indebærer risici. God risikostyring skaber overblik og sikrer, at organisationens ressourcer bliver brugt der, hvor de gør mest gavn.

Risikostyring hjælper bl.a med at:

- ✓ Identificere de største risici i processer og systemer
- ✓ Øge robustheden mod trusler
- ✓ Træffe bedre beslutninger og anvende ressourcer effektivt
- ✓ Opnå større driftssikkerhed og sikkerhed i myndighedens leverancer
- ✓ Styrke organisationens omdømme

Risikostyring er ikke en engangsopgave. Det kræver en løbende indsats, og at du som leder tager ejerskab over det og gør det til en del af ledelsesopgaven.

DIT ANSVAR I RISIKOSTYRING

Som topleder har du det overordnede ansvar for risikostyring.

Det betyder, at du skal:



Sætte retning og prioritere ressourcer

Du skal sikre, at der er tid, kompetencer og processer til at håndtere risici. Det gælder f.eks. organisering, acceptkriterier og bemanning.



Godkende og følge op

Du skal godkende væsentlige risikovurderinger og sikre, at der bliver fulgt op på dem, fx på sikkerhedsudvalgmøder.



Fremme en risikobevidst kultur

Du skal vise engagement og gå forrest ved at anvende den risiko-baserede tilgang som grundlag for beslutninger. På den måde er du med til at skabe en kultur, hvor risici tænkes ind i det daglige arbejde.



Holde dig opdateret

Du skal kende det aktuelle trusselsbillede. Det kan f.eks. gøres gennem SAMSIK's trusselsvurderinger eller andre relevante kilder.

NIS2 og risikostyring

I organisationer omfattet af NIS 2-loven skærpes ledelsens ansvar i arbejdet med risikostyring. Det betyder bl.a., at ledelsen har ansvaret for styringen af cybersikkerhed og skal godkende og føre tilsyn med sikkerhedsforanstaltninger. Se NIS 2-vejledningen Ledelsens rolle og opgaver på samsik.dk.

Arbejder din organisation efter sikkerhedsstandarden ISO 27001, er risikostyring et centralt krav.



Styrelsen for
Samfundssikkerhed

Læs mere og hent inspiration

Som topleder skal du sikre, at der er det rette fokus og den rette tilgang til arbejdet med risikostyring i din organisation.

Styrelsen for Samfundssikkerhed har i efteråret 2025 udgivet en opdateret vejledning og en ny skabelon til risikostyring inden for informationssikkerhed. Vejledningen henvender sig til informationssikkerhedsfunktionen i organisationen.

Du og din organisation kan finde inspiration, vejledning og værktøjer på **sikkerdigital.dk/myndighed** og på **samsik.dk**.

Hvis I har spørgsmål, behov for rådgivning eller brug for sparring om arbejdet med informationssikkerhed, er I velkomne til at kontakte **samsik@samsik.dk**.

Nyttige links:

www.samsik.dk

www.sikkerdigital.dk/myndighed

[Nationalt Risikobillede 2025](#)

[Trusselsvurderinger på cyberområdet](#)



Styrelsen for
Samfundssikkerhed