NOTAT

Haderslev Kommune
IT og Digitalisering
Østergade 48, 1. sal
6100 Haderslev

www.haderslev.dk

Dir. tlf. 20284637
anjus@haderslev.dk

13. april 2023 • Sagsident: 23/8330 • Sagsbehandler: Anders Juel Sørensen

Retningslinjer for risikostyring

Formål

Formålet med en risikovurdering er at definere behovet for sikringstiltag samt at identificere kritiske processer og systemer, som organisationen er afhængig af. Desuden hjælper risikovurderingen med at identificere kontroller, der skal implementeres i fremtidige informationssikkerhedsprojekter, og gøre det muligt at prioritere disse projekter.

Metode

Risikovurderingen gennemføres gennem interviews med medarbejdere og ledere i Haderslev Kommune. Interviewdeltagerne skal repræsentere både systemejere og systemansvarlige for at sikre, at risikovurderingen er så bredt funderet og omfattende som muligt.
Risikovurderinger skal altid indeholde en vurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed. Risikovurderinger skal altid følge metodikken fra ISO27005.

Roller og ansvar

Informationssikkerhedsansvarlige har ansvaret for, at der udarbejdes løbende samlede risikorapporter for Haderslev Kommune. Informationssikkerhedsansvarlige skal derudover vurdere og rådgive i forbindelse risikohåndteringsplaner forelagt af systemansvarlige eller procesejere i det omfang det er nødvendigt.
Informationssikkerhedsansvarlige kan videresende bekymrende risikohåndteringsrapporter til behandling i Styregruppen for Digital Fremtid.
Informationssikkerhedsansvarlige har endeligt ansvar for at udarbejdet et samlet risikoregister for Haderslev Kommune.
Informationssikkerhedsansvarlige skal både kunne vejlede ud fra tekniske og juridiske kompetencer.
Styregruppen for Digital Fremtid har ansvar for at være orienteret om risikobilledet for Haderslev Kommune generelt og træffe de nødvendige beslutninger for at nedbringe risici til et acceptabelt niveau.
Det er derudover Styregruppen for Digital Fremtids ansvar, at Direktionen orienteres om alvorlige risici, således at de har mulighed for at handle, med henblik på at risici nedbringes.
Styregruppen for Digital Fremtid er ansvarlig for at tværgående projekter, der sigter mod at nedbringe samlede risici på tværs af Haderslev Kommune.
Databeskyttelsesrådgiveren skal inddrages, hvis der inficeres en høj risiko for de registrerede med henblik på at vurdere om der skal udarbejdes en konsekvensanalyse, jf. art 35.
Databeskyttelsesrådgiveren fører derudover kontrol med at risikovurderinger udarbejdes.
Databeskyttelsesrådgiverens rolle er alene rådgivende og kontrollerende.

Systemansvarlige har ansvaret for der altid forelægger en aktuel risikovurdering, samt at identificere og håndtere risiko inden for eget system. Systemansvarlige skal mindst en gang årligt gennemgå egne risikovurderinger. Systemansvarlige har mulighed for at uddelegere opgaven. Ved identifikation af alvorlige risici forbundet med et system, er Systemansvarlige ansvarlig for at udarbejde risikohåndteringsrapporter. Hvis systemansvarlige ikke i tilfredsstillende omfang kan nedbringe risici, skal der forelægges en risikohåndteringsrapport for Informationssikkerhedsansvarlige.
IT-afdelingen, eller en repræsentant med de nødvendige tekniske kompetencer, skal bidrage med teknisk indsigt som baggrund for risikovurderinger. IT-afdelingen skal alene forholde sig til Haderslev Kommunes infrastruktur. Ved cloud/SaaS-løsninger træder den ansvarlige leverandør i stedet for IT-afdelingen.
IT-afdelingen har derudover ansvaret for risikovurdering af Haderslev Kommunes IT-infrastruktur.
Det er endeligt IT-afdelingens ansvar at sikre løbende opfølgning på den generelle IT-sikkerhedssituation og de trusler, der kan have påvirkning på Haderslev Kommunes informationssikkerhed som helhed.
Processejer har ansvaret for at identificere og håndtere risiko inden for eget område. Den enkelte chef er procesejer i det de er ansvarlige for det data der behandles indenfor eget område. Procesejeren skal som minimum sikre risikovurdering af alle processer omfattet af KL's 90 behandlingsaktiviteter hjemhørende under eget område. I tilfælde hvor en behandlingsaktivitet vurderes at medføre høj risiko for den registrerede er procesejer ansvarlig for at der udarbejdes en konsekvensanalyse (DPIA).
Risikovurderingsopgaven kan uddelegeres. Det er procesejers ansvar at behandling af data foretages i tilstrækkeligt sikrede systemer.
Informationssikkerhedskonsulenter
Informationssikkerhedskonsulenterne deltager i og faciliterer risikovurderinger indenfor egen forvaltning. Informationssikkerhedskonsulenten bidrager med den nødvendige forståelse for risikovurderinger, der sikrer den nødvendige kvalitet og struktur. Informationssikkerhedskonsulenten sikrer et samlet overblik over alle systemer og processer, samt deres dertilhørende risikovurderinger inden for egen forvaltning, Informationssikkerhedskonsulenten kan vurdere forholdet mellem foranstaltninger og risici. Informationssikkerhedskonsulenten er ikke ansvarlig for udførsel af risikovurderinger eller opfølgende handling. Informationssikkerhedskonsulenten skal have de nødvendige kompetencer til at udføre systematiske risikovurderinger.

Afgrænsning af risikovurderingen

Det første trin i risikovurderingsprocessen er at identificere de kritiske processer og systemer, der indeholder den information, som risikovurderingen skal omfatte. Rammen for risikovurderingen skal defineres og de forskellige interviews planlægges.
En risikovurdering består af seks trin:

1. Identifikation af forretningskritiske processer og systemer
2. Vurdering af trusselsniveauet
3. Vurdering af konsekvensen for organisationens processer og muligvis systemer ved brud på fortrolighed, integritet og tilgængelighed
4. Vurdering af sårbarhed eller sandsynlighed for sikkerhedshændelser
5. Udarbejdelse af en risikohåndteringsplan
6. Udarbejdelse af en risikorapport

Identifikation af forretningskritiske processer og systemer

Formålet med denne aktivitet er at skabe et overblik over de behandlingsaktiviteter(processer)[1] der foretages i Haderslev Kommune. Behandlingsaktiviteterne skal være i overensstemmelse med kravene i Persondataforordningens artikel 30, men kan tage udgangspunkt i de 90 behandlingsaktiviteter identificeret af KL's Partnerskab om informationssikkerhed, Som en del af oversigten identificeres behandlingsaktiviteter og systemer, der anses for at have en væsentlig indflydelse på organisationens evne til at udføre kerneopgaverne. Opgaven identificerer og beskriver, hvordan den samlede IT-arkitektur består af IT-systemer, der understøtter behandlingsaktiviteter. Oversigten er baseret på de forretningskritiske processer, disses afhængighed af systemer og forholdet mellem de forskellige elementer.
Ved gennemgang af processer skal der identificeres, hvilke aktiver der understøtter behandlingsaktiviteterne. Et aktiv (eksempelvis et IT-system) kan f.eks. anvendes af flere behandlingsaktiviteter til forskellige formål og med forskellige konsekvenser, hvis der sker en hændelse. Behandlingsaktiviteter defineres i denne sammenhæng som værende sammenhængende med de opgaver som en given afdeling udfører. Arbejdsmarkeds behandlingsaktivitet kan f.eks. være "Behandling af personoplysninger i forbindelse med sygesikring".

Risikovurdering

Formålet med risikovurderingen er at vurdere sårbarhedens risikoniveau ud fra sandsynlighed og konsekvens. På denne måde skal der gives et billede af den samlede risiko for et aktiv eller en behandlingsaktivitet.
De praktiske risikovurderinger udarbejdes og behandles i Haderslev Kommunes ISMS.
Risikovurderinger skal udarbejdes efter ISO27005 og "Plan-Do-Check-Act"-modellen som beskrevet i ISO27001.
Ved udarbejdelse af risikovurderinger skal vejledningen "Risikostyring- og vurdering" følges.
Den samlede risiko regnes ud fra en vurdering af sandsynlighed og konsekvens ud fra 4x4-matriksen som beskrevet i vejledningen.
Risikovurderinger omfatter ikke kun IT-systemer og processer, men alle de aktiver som indgår i et informationssystem. Det inkluderer også fysiske aktiver som f.eks. papirarkiver.

Vurdering af trusselsniveauet

Trusselskataloget I ISMS-systemet er udarbejdet for at skabe overblik over hændelser i form af trusler, der kan påvirke organisationens informationer og påvirke risikobilledet. Kun trusler, der er relevante for organisationen, skal medtages i trusselskataloget. Informationssikkerhedsansvarlige har ansvar for at identificere relevante trusler i trusselskataloget.

Vurdering af konsekvens

Effekten af brud på informationssikkerheden skal vurderes af den procesejer, der er ansvarlige for eller har kendskab til Behandlingsaktiviteten. Det forventes, at procesejer har kendskab til de systemer, der understøtter deres egne behandlingsaktiviteter.
Konsekvens vurderes ud fra:

- Fortrolighed
- Integritet

[1] Processer i Haderslev Kommunes benævnes som behandlingsaktiviteter hvad end der er tale om behandlingsaktiviteter jf. Persondataforordningen eller ISO27001/5.

- Tilgængelighed

Risikoskalaerne kan opdateres og ændres efter ønske fra Informationssikkerhedsansvarlige. Eventuelle ændringer af risikoskalaerne skal forelægges Styregruppen for Digital Fremtid.
Konsekvensvurderinger skal tage hensyn til forretningskonsekvens. Konsekvensen for de registrerede vurderes i tilfælde af, at der behandles personoplysninger i aktivet.

Vurdering af sårbarhed eller sandsynlighed

Sårbarhed
Sårbarhed er et udtryk for, hvor sårbar organisationen er over for de relevante trusler. For at vurdere de kritiske systemers sårbarhed og dermed sandsynligheden for hændelser, er det nødvendigt at vurdere de kontroller, der er implementeret for at beskytte mod de specifikke trusler. Disse vurderinger kan foretages Informationssikkerhedskonsulenten.
Sårbarheder kan opstå i mange forskellige sammenhænge. Det kan for eksempel være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør at IT-systemet er åbent for angreb. De identificerede sårbarheder gør at en trussel kan realiseres. Manglende eller utilstrækkelig adgangsstyring kan f.eks. vurderes som værende årsag til at en trussel om misbrug af et system kan realiseres.

Sandsynlighed
Sandsynlighedsvurderinger er en enklere måde at udføre risikovurderingen på, hvor en leverandør vurderes ud fra tidligere erfaringer. Informationssikkerhedskonsulenten kan vælge at vurderer sandsynligheden for brud på fortrolighed, integritet og tilgængelighed eller en specifik trussel.
Sandsynlighedsvurderinger bør kun anvendes i tilfælde, hvor en teknisk gennemgang ikke er mulig og der ikke sker behandling af personoplysninger.

Udarbejdelse af risikohåndteringsplan og -rapport
Baseret på resultaterne af risikovurderingen udarbejdes risikohåndteringsplaner og en risikorapport.

Risikohåndteringsplaner
Formålet med risikohåndteringsplaner er at behandle de identificerede risici, der ligger over det ønskede niveau for risikoaccept.
Det er et krav, at der udarbejdes en risikohåndteringsplan af risikoejeren, der er ejer af et system eller en behandlingsaktivitet, når den samlede risiko overstiger 10 på 4x4-scalaen.

Risikohåndteringsplaner skal som minimum beskrive:
1. Formål – hvilken risiko håndteres
2. Ansvarlig – Risikoejer
3. Risikohåndteringstiltag – mitigerende handlinger
4. Restrisici – hvilke risici håndteres ikke
5. Ressourcer – omkostninger
6. Tidsplan – hvornår forventes risici håndteret

Risikohåndteringsplaner skal forelægges Informationssikkerhedsansvarlige.
Informationssikkerhedsansvarlige har ansvaret for den endelige godkendelse af risikohåndteringsplanenerne.

Informationssikkerhedsansvarlige har der udover mulighed for at afkræve at ejeren af et aktiv udarbejder en risikohåndteringsplan, hvis dette findes nødvendigt af grundet andre forhold.
Informationssikkerhedsansvarlige har mulighed for at videresende risikohåndteringsplaner til Styregruppen for Digital Fremtid. Den ansvarlige risikoejer har ligeledes mulighed for at appellere Informationssikkerhedsansvarliges afgørelser til Styregruppen for Digital Fremtid.
Styregruppen for Digital Fremtid har den endelige beslutning ret, men kan vælge at høre Direktionen i alvorlige tvivlsspørgsmål.
Baseret på risikoresultaterne og den godkendte risikohåndteringsplan, skal der udarbejdes en Statement of Applicability (SoA)

.

Risikorapporter
Der udarbejdes årligt en risikorapport. Risikorapporten skal forelægges Styregruppen for Digital Fremtid én gang årligt.
Formålet med risikorapporten er at fremhæve resultaterne af risikovurderingen og udarbejdes med henblik på, at ledelsen, ud fra rapporten, træffer endelig beslutning om risikohåndteringsplanen

.

Risikohåndtering

Når risikovurderingerne er udarbejdet, dannes der et risikobillede. Risikobillede skal være medvirkede til at sikre optimal brug af ressourcer i forhold til informationssikkerheden.
Systemejer har ansvaret for at der handles på baggrund af risikovurderingerne.
Der er fire muligheder for handling i forhold til risici:

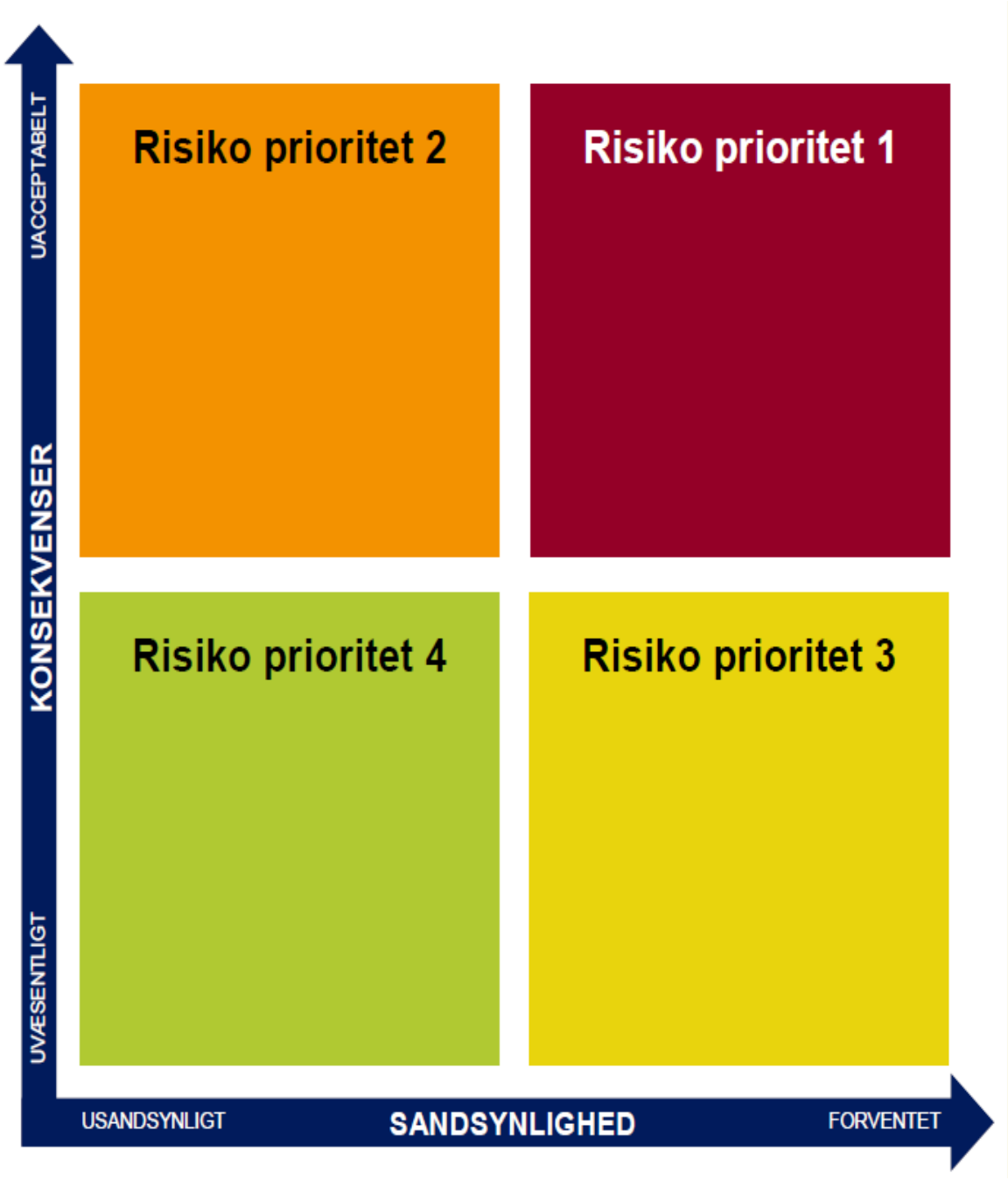
1. Reducer – Risikoen reduceres ved at indføre kontroller eller foranstaltninger, som fjerne eller reducerer sandsynligheden eller konsekvensen.
Indførsel af kontroller eller foranstaltninger med henblik på at reducere risiko bør ske efter en cost/benefit-vurdering, for at sikre bedst mulig effekt i forhold til omkostninger. Risiko kan reduceres ved enten at indføre forebyggende eller udbedrende tiltag.
Forebyggende tiltag har til formål at mindsker sandsynligheden for sikkerhedshændelser, mens udbedrende tiltag har til formål at mindske konsekvensen.

2. Undgå - Risikoen undgås ved at stoppe eller ændre aktiviteten som er årsag til risikoen.
Informationssikkerhedsansvarlige har mulighed for at pålægge et aktivs ejer at stoppe behandlingen af person- eller forretningsdata i et givne system. Det er derudover muligt at pålægge f.eks. et systemskifte som følge af alvorlige risiko.

3. Del – Risikoen overføres til en tredjepart, f.eks. forsikring, outsourcing eller lignende
Systemejer har mulighed for at reducere risici for et aktiv ved f.eks. at outsource driften af et system. I tilfælde hvor Haderslev Kommune er dataansvarlig for persondata, er det ikke muligt at dele det endelige ansvar.

4. Accepter – Risikoen accepteres og der foretages ikke yderligere
Accept af risiko for kritiske processer og systemer kan kun foretages af Informationssikkerhedsansvarlige, hvis der er tale om risici over 10 ud fra 4x4-modellen.
Alle håndteringer af risici over 10 af skalaen, skal følges op med en forklaring af hvorfor en risiko accepteres.

Kriterier for risikohåndtering
Alle risici under 5 kan automatisk accepteres.
Informationssikkerhedsansvarlige har mulighed for at vælge en tærskel for behandling af aktiver med risiko mellem 5 og 10. Der kan f.eks. kræves risikohåndteringsplaner fra alle systemer med en risiko over 7 eller udvælges særligt kritiske systemer som, så afkræves en risikohåndteringsplan.
Alle risici over 10 skal afføde en risikohåndteringsplan, der skal behandles og godkendes af Informationssikkerhedsansvarlige.
Prioriteringen af risikohåndtering bør fokuseres efter sandsynlighed og konsekvens.
Højeste prioritet er således aktiver, hvor sandsynligheden for f.eks. databrud er stor, samtidig med at konsekvensen er stor (Se illustration nedenfor).



Opfølgning på risici

Der skal mindst en gang årligt ske opfølgning på risikohåndteringsplaner.
Informationssikkerhedsansvarlige har ansvar for løbende at holde sig orienteret i forhold til generelle IT-sikkerhedsrisici, der kan påvirke eller ændre forudsætningerne for risikobilledet for de enkelte aktiver.

Godkendelse og opfølgning på retningslinjer for risikohåndtering

Rammerne og metoden for risikohåndtering revideres og godkendes årligt af Styregruppen for Digital Fremtid, efter indstilling f Informationssikkerhedsansvarlige.

9.1. Versioner

Version	Ændringsbeskrivelse	Forfatter	Dato
1.0	Første udgave	Anders Juel Sørensen	2023-05-09

9.2. Godkendelse

Dokumentet er godkendt i følgende version:

Politisk / direktionen	Version	Dato
Styregruppen for Digital Fremtid	1.0	2023-05-09