INFORMATIONSSIKKERHED

INFORMATIONS-SIKKERHED I KOMMUNERNE

EN DREJEBOG OM AKTIVITETER, DER KAN UNDERSTØTTE DET KOMMUNALE ARBEJDE MED INFORMATIONSSIKKERHED

Informationssikkerhed i kommunerne
– en drejebog om aktiviteter, der kan understøtte det kommunale arbejde med informationssikkerhed

3. udgave, 1. oplag 2024

Produktion: Kommuneforlaget A/S
Design: e-Types
Foto: Colourbox

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne

Produktionsnr. 830874
ISBN 978-87-94514-11-8-pdf

INDHOLD

INDLEDNING

Afhængigheden af digitale løsninger vokser, og udfordringerne med at fastholde et acceptabelt sikkerhedsniveau øges og forandres med stor hast. Ligesom konsekvenserne af sikkerhedsbrud vokser. Borgernes tillid til kommunerne i en mere og mere digital tid, afhænger særligt af, at kommunerne kan beskytte data mod misbrug. Borgere og virksomheder skal fortsat kunne have tillid til og være trygge ved kommunernes håndtering, anvendelse og opbevaring af data og informationer. Kommunerne skal således øge og tilpasse indsatsen for informationssikkerhed.

I denne drejebog angives forslag til en måde at håndtere opgaverne på. Alle kommuner er forskellige i størrelse, kompleksitet og organisering, og derfor må hver kommune forholde sig konkret til egne forhold. Ledelsesmæssig styring af informationssikkerhed afhænger af den enkelte organisation, dens kultur og informationer. Indsatsen for informationssikkerhed skal planlægges, tilrettelægges og udvikles efter den enkelte kommune. Det er derfor vigtigt, at den enkelte kommune selv prioriterer og forholder sig til arbejdet med informationssikkerhed. Drejebogen giver konkret og direkte anvendelig inspiration til tilrettelæggelse af opgaven. Og vi håber den vil give værdi i samarbejdet om informationssikkerhed i den enkelte kommune.

Siden 2016 har der været fokus på i fællesskab – og på tværs af den offentlige sektor – at gøre en indsats ift. sikkerhedsarbejdet. Og at der arbejdes aktivt med risikobaseret håndtering af udfordringerne med informationssikkerhed med inspiration fra ISO27001 standarden. Det er aftalt, at alle myndigheder skal øge fokus på sikkerhed og at kommunerne skal følge principperne i standard for informationssikkerhed, ISO27001. Der følges årligt op på myndighedernes arbejde med informationssikkerhed.

Dette fokus er fortsat helt aktuelt og indgår også i den fællesoffentlige digitaliseringsstrategi 2022-2025, hvor fokus er på styrket forankring af cyber- og informationssikkerhed. Dette for at øge modenheden og opmærksomheden på cyber- og informationssikkerhed hos virksomheder, myndigheder og borgere, da behovet for en stærk cyber- og informationssikkerhed fortsat øges i takt med at kompleksiteten på området vokser.

ISO27001 er en sikkerhedsstandard, der arbejder med en risikobaseret tilgang til informationssikkerhed ud fra en række områder eller principper for, hvad der skal være fokus på, for et kvalificeret arbejde med informationssikkerhed. Denne tilgang passer godt med reglerne i databeskyttelsesforordningen, da der også her lægges op til en risikobaseret tilgang.

Med udgangspunkt i den risikobaserede tilgang, principperne for ISO27001 samt erfaringer fra kommuner, udarbejdede KL i 2017 denne opsamling, kaldet en drejebog, der kan anvendes i arbejdet med at få overblik over krav til informationssikkerhed og til at øge informationssikkerheden i den enkelte kommune. Siden da er der høstet yderligere erfaringer med informationssikkerhedsarbejdet i kommunerne, ligesom 43 kommuner sammen med KL i 2020-2022 har arbejdet sammen i et Partnerskab om informationssikkerhed, for at finde fælles løsninger og udnytte hinandens kompetencer i indsatsen for øget informationssikkerhed i kommunerne.

Dette er en opdateret version af drejebogen. Opdateringerne er foretaget på baggrund af ovenstående udvikling og aktiviteter siden 2017. Seneste opdatering er sket på baggrund af den opdaterede ISO27001-2023 standard.

Drejebogen er bygget op, så den beskriver en række opgaver, der skal udføres i arbejdet med informationssikkerhed og den risikobaserede tilgang. Disse opgaver er:

- Etablering af forretningsoverblik
- Ledelsens styring af informationssikkerhed, herunder rammerne for informationssikkerhed og organisering og bemanding
- Politik for informationssikkerhed
- Risikostyring, risikovurdering og håndtering, herunder dokumentation af kontroller/ foranstaltninger
- Årshjul

I drejebogen henvises der til en række materialer og skabeloner, der er udviklet i samarbejde mellem kommuner og KL. Disse kan være en støtte i arbejdet med informationssikkerhed og kan frit benyttes. Materialerne findes på KL's Videnscenter under punktet "Informationssikkerhed".

I drejebogen anvendes ligeledes en række fagudtryk om informationssikkerhed mv. som er søgt forklaret i en ordliste til slut i publikationen.

Målgruppe
Drejebogen er særlig henvendt til kommunens informationssikkerhedskoordinator og andre ansatte, der har ansvar for informationssikkerhed. Og til ledere, der ønsker viden om opgaver og ansvar ifm. arbejdet med informationssikkerhed. Her giver drejebogen mulighed for et hurtigt overblik.

01 / FORRETNINGS-OVERBLIK

Fundamentet for arbejdet med informationssikkerhed er, at der er etableret et overblik over forretningen og hvilke informationer og systemer, der er mest kritiske for opgaveløsningen. Herudover er det væsentligt, at man har kendskab til hvilke love og myndighedskrav, man er underlagt, da dette kan have indflydelse på de sikringstiltag, der kan eller skal etableres.

Uden dette overblik er der ikke garanti for, at arbejdet med informationssikkerhed har det rigtige fokus, da kritiske informationer kan være blevet overset, så de ikke får den nødvendige opmærksomhed og beskyttelse. Arbejdet med at etablere et forretningsoverblik, vil typisk resultere i et overblik over forretningsprocesser, arbejdsområder, interessenter og systemer m.v., som er essentielle for kommunen, herunder de ansvarlige for forretningsområderne (system- og risikoejere). Dette udgør endvidere grundlaget for risikovurderingen.

I det omfang dette forretningsoverblik allerede findes, anbefales det, at dette anvendes.

Anbefaling
Overblik over forretningen kan fx skabes gennem workshops med fagchefer og andre interne interessenter, som vil kunne bidrage med det forretningsmæssige indblik og medvirke til at skabe en fælles forståelse af vigtige prioriteringer.

Det er vigtigt, at der fokuseres bredt på informationer, og at det ikke kun kommer til at handle om "it-systemer".

Opgaven er kort sagt at gå fra at have fokus på it-sikkerhed til at have fokus på informationssikkerhed.

02 / LEDELSENS STYRING AF INFORMATIONS-SIKKERHEDEN

Den kommunale ledelse er ansvarlig for og skal styre arbejdet med informationssikkerhed, på samme måde som med de øvrige kommunale opgaver. Og der er her behov for at have en systematik for dette, som minder om de systematikker, som kommunen har ift. f.eks. økonomistyring eller arbejdsmiljø. Den ledelsesforankring, der er nødvendig ift. informationssikkerhed, adskiller sig ikke fra det, som ledelsen skal have ift. alle andre væsentlige områder i kommunen, hvor ledelsen konstant har et vågent øje.

I denne publikation er beskrivelsen af opgaverne omkring informationssikkerhed baseret på principperne i ISO27001. Dette ud fra, at det er de principper, som kommunerne er forpligtede til at følge, og fordi det er den standard, som mere og mere regulering og standardisering af krav til myndigheders arbejde med forskellige elementer af informationssikkerhed læner sig op ad. Det gælder f.eks. GDPR ift. den risikobaserede tilgang, krav til brugerstyring og EU reguleringer af netværk mv.

Ifølge ISO27001 er informationssikkerhed et ledelsesansvar. ISO27001 opererer med et ledelsessystem for informationssikkerhed – ofte benævnt 'ISMS' (Information Security Management System) – som indeholder alle de politikker, procedurer, retningslinjer og tilhørende ressourcer og aktiviteter, som en organisation administrerer for at beskytte sine informationsaktiver.

Både NSIS og NIS2 stiller krav om, at der findes et ledelsessystem svarende til principperne i ISO27001 eller en ISO27001 certificering.

Forankringen af informationssikkerhed i ledelsen kommer til udtryk i:

- Målfastsættelse: Ledelsen fastlægger niveauet for sikkerhed i organisationen, herunder accepterer risici, som fremkommer i arbejdet med informationssikkerhed
- Organisering: Ledelsen skal tage stilling til den praktiske organisering af informationssikkerhedsarbejdet. Det gælder fx udpegning af en eventuel informationssikkerhedskoordinator, DPO, informationssikkerhedsudvalg og formandskab, systemejere, brugernes ansvar mv.
- Ressourceallokering: Behov for at sikre tilstrækkelig ressourceallokering og prioritering, så der er de nødvendige ressourcer til at drive informationssikkerhedsarbejdet i kommunen.
- Kommunikation: Det er afgørende, at ledelsen, ved passende lejligheder, kommunikerer og understøtter kommunikation om vigtigheden af informationssikkerhedsarbejdet i hele kommunen.
- Fastsættelse af politikker og strategier: Ledelsen skal sikre udarbejdelse og fastlæggelse af en informationssikkerhedspolitik og strategi.

- Fastsættelse af roller og ansvar: Det er ledelsens ansvar, at der er klarhed over, hvem der gør hvad ift. informationssikkerhed og dermed at sikre uddelegering af det ansvar til medarbejdere, der er relevant for informationssikkerhedsarbejdets udførelse

- Opfølgning og forbedring: Det er ligeledes ledelsens ansvar at sikre, at der sker løbende evaluering og forbedring af arbejdet med informationssikkerhedsstyring.

I de fleste kommuner vil det i praksis ofte være informationssikkerhedsudvalget, der håndterer ovenstående punkter. Dog kræver dette, at der er den nødvendige beslutningskraft i udvalget. Det sikres f.eks. ved at formanden er fra den øverste ledelse. Det vil så være informationssikkerhedsudvalget, der orienterer topledelsen.

Anbefaling
Den risikobaserede og ledelsesforankrede tilgang er grundlaget for arbejdet med informationssikkerheden. En tilgang, hvor arbejdet med informationssikkerhed vurderes i forhold til betydningen for de kommunale opgaver, medarbejderne og borgerne. Mange steder vil det betyde, at prioriteringen af indsats flyttes ud af it-afdelingen og fra it-leverandøren over til forretningen.

Styringen af informationssikkerhed bør tilpasses og integreres i den eksisterende organisation, så der tages hensyn til eksisterende arbejdsgange, organisering og ansvarsfordeling m.v.

Den øverste ledelse bør etablere en organisation til koordinering af informationssikkerhedsarbejdet. Organisationen igangsætter aktiviteter, følger op på implementering af politikker og retningslinjer, måler effekt og rapporterer tilbage til ledelsen.

I den forbindelse er informationssikkerhedsudvalget en vigtig del af informationssikkerhedsorganisationen og det skal besidde den nødvendige beslutningskompetence. Det er eksempelvis sikkerhedsudvalget, der sætter mål for sikkerheden og sørger for at informationssikkerheden realiseres og efterleves.

Det anbefales derfor at informationssikkerhedsudvalget bemandes med IT- eller Digitaliseringschefen samt ledelsesrepræsentanter fra de vigtigste fagforvaltninger (set ud fra den risikobaserede tilgang). Formanden for udvalget bør være en repræsentant fra direktionen.

I stedet for at etablere et informationssikkerhedsudvalg kan man vælge at give et eksisterende udvalg, eksempelvis digitaliseringsudvalget, ansvaret som informationssikkerhedsudvalg.

Inspirationsmaterialer
Beskrivelse af informationssikkerhedsudvalgets organisering og samspil med organisationen kan findes på KL Videncenter under "Informationssikkerhedsudvalg".

Materialer til at øge viden om og kompetencer ift. informationssikkerhed for politikere og administrativ ledelse kan findes på KL Videncenter under "Kompetencer: Ledelse af informationssikkerhed".

Beskrivelse af funktioner og roller i arbejdet med informationssikkerhed kan findes på KL Videncenter under "Rejsefortællingen om roller og ansvar".

03 / POLITIK FOR INFORMATIONS-SIKKERHED

Alle kommuner har en sikkerhedspolitik. Denne skal transformeres til en informationssikkerhedspolitik. Det er topledelsens ansvar at informationssikkerhedspolitikken passer til kommunens opgavemæssige formål, indeholder målsætninger og rammer for sikkerhedsarbejdet og en forpligtigelse til løbende forbedringer af informationssikkerheden.

Informationssikkerhedspolitikken er et strategisk styringsredskab, hvor kommunens målsætning, afgrænsning, ansvarsplacering og rammer for styringen af arbejdet med informationssikkerhed fastsættes. Informationssikkerhedspolitikkerne kan også bidrage til at skabe en fælles forståelse i kommunen for, hvad informationssikkerhed indebærer, og hvilken tilgang man har til det.

Informationssikkerhedspolitikken skal godkendes af topledelsen og kommunikeres til medarbejderne, så de forstår hvilken betydning politikken har for dem.

Anbefaling
Ledelsen bør involveres i arbejdet med informationssikkerhedspolitikken, så det sikres, at ledelsens vurderinger og beslutninger indgår. Politikken kan evt. skrives ud fra en eksisterende skabelon i kommunen.

Det anbefales at indarbejde afsnit om etablering og vedligeholdelse af Informationssikkerhedsstyring.

Den løbende opdatering vil ofte være informationssikkerhedsudvalgets opgave, hvor der tages udgangspunkt i den aktuelle risikovurdering for kommunen.

04 / RISIKOSTYRING

Risikostyring er en tværorganisatorisk proces, hvori der indgår mange interessenter med forskellige opgaver og ansvarsområder. Planlægning, koordination og kommunikation ligger derfor hele tiden som et bagtæppe i risikostyringsprocessen – både før og efter gennemførelse af hovedaktiviteterne.

Ledelsesforankring er afgørende for en vellykket risikostyringsproces. Typisk vil det være informationssikkerhedsudvalget med deltagelse fra ledelsen, som skal godkende og afgrænse rammerne for risikostyringen. Herunder at risikovurderingsprocessen igangsættes, og at der afsættes ressourcer til, at den kan gennemføres. Dette skyldes bl.a. at de forskellige roller, fx data- og systemejere, skal medvirke til at vurdere risici og konsekvenser ved tab af fortrolighed, integritet og tilgængelighed. Denne medvirken tager tid og kræver deres deltagelse.

Informationssikkerhedsfunktionen har det praktiske og koordinerende ansvar for risikostyringen, mens data- og systemejere har ansvaret for identificering og håndtering af risici inden for eget område.

Risikovurdering
Risikovurderingen er omdrejningspunktet i risikostyringen. Her identificeres, analyseres og evalueres risici. Resultatet af risikovurderingen er en liste over risici.

En fremgangsmåde er at tage udgangspunkt i de primære og mest kritiske forretningsområder og deres tilhørende processer. En anden fremgangsmåde er at tage udgangspunkt i arket over behandlingsaktiviteter, som er udarbejdet af kommuner og KL ifm. udarbejdelse af materialer til risikovurdering ift. de registreredes rettigheder, som er beskrevet senere.

Risikohåndtering
Der er flere muligheder for at håndtere risici:

1. Kontroller/mitiger: risikoen styres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne.

2. Acceptér: risikoen accepteres, og der foretages ikke yderligere.

3. Undgå: risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen.

4. Flyt: risikoen overføres til en tredjepart, fx ved hjælp af forsikring, outsourcing eller lignende.

Formålet med implementering af foranstaltninger er at reducere risikoen. I ISO 27001 har foranstaltninger tidligere været benævnt som kontroller. Dette er ændret i ISO27001:2023 udgaven hvor kontroller nu benævnes foranstaltninger.

Foranstaltninger kan omfatte enhver proces, politik, plan, praksis eller andre handlinger, som ændrer risikoen. Foranstaltningerne kan udføres manuelt eller automatisk. Når der udvælges foranstaltninger til reducering af risici, skal det ske ud fra en businesscase, så foranstaltningernes effekt på risikoen vurderes i forhold til omkostningerne.

I forlængelse af risikohåndteringen bør SoA-dokumentet, der indeholder en formel beskrivelse af de sikkerhedstiltag, der udføres som led i håndteringen af risici, konsulteres. Dækkes eventuelle nye foranstaltninger allerede af de foranstaltninger, der er beskrevet i SoA-dokumentet eller skal der tilføjes nye? Se beskrivelse af SoA-dokumentet i kapitel 6.

Risikoaccept
For kritiske aktiver og processer bør risikoaccepten altid foretages af den øverste ledelse. En liste over risici, der skal kontrolleres/mitigeres kan i praksis benyttes som en anbefaling/indstilling til ledelsen. Her anføres de tiltag, som bør indføres, og hvilke risici som bør accepteres med udgangspunkt i de fastsatte kriterier for risikotolerance. Selvom risici kontrolleres ved at indføre yderligere foranstaltninger, vil der i de fleste tilfælde altid være en restrisiko. Det er vigtigt, at der foretages en vurdering af de valgte kontrollers effekt på risikoen, og at den tilbageværende risiko vurderes og beskrives.

Opfølgning på risici
Der bør løbende foretages opfølgning på risici. Dels bør det sikres, at de foranstaltninger og tiltag, der indføres som en del af risikohåndteringen rent faktisk også bliver implementeret og fungerer efter hensigten. Dels bør der løbende følges op på de forudsætninger, som ligger til grund for risikovurderingen. Aktiver, trusler, sårbarheder og konsekvenser kan hurtigt ændres og medfører tilsvarende ændringer i risikobilledet. Kommunens risikostyring bør derfor sikre, at der på en struktureret måde foretages en løbende opfølgning på risici, dvs. at kommunens risikostyring følger en planlagt og tilbagevendende proces, der gennemfører dokumenterede vurderinger ud fra den samme metode med henblik på at opnå sammenlignelige resultater.

Arbejdet med risikovurderingen skal munde ud i en vurdering af, hvilke trusler der synes mest oplagte i forhold til at kunne påvirke kommunen og "de registrerede" (borgerne, ansatte og andre samarbejdspartnere i form af fysiske personer). Dermed får ledelsen mulighed for at prioritere de indsatser, som giver kommunen et passende og ønsket niveau af informationssikkerhed, ligesom ledelsen kan prioritere ressourcerne i forhold til, hvor de gør mest gavn.

På baggrund af risikovurderingen udarbejdes en handlingsplan, der følger op på de risici, der vurderes som de vigtigste, og som ledelsen skal forholde sig til. Der skal foretages en organisatorisk, fysisk og teknisk afgrænsning af risikostyringens omfang, defineres risikotolerance og beskrives en metode for risikovurderingen.

Risikovurderingen og de aftalte aktiviteter i handlingsplanen skal godkendes af topledelsen eller informationssikkerhedsudvalget, hvis der her indgår en repræsentant fra topledelsen.

Anbefaling
I forbindelse med risikovurderingen anbefales det altid at gennemføre en konsekvensvurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed (FIT).

Risikovurdering bør tage udgangspunkt i de vigtigste aktiver, eksempelvis de vigtigste forretningsprocesser med anvendte it-systemer samt vigtigste tekniske aktiver (it-/digitaliseringsafdelingens ansvarsområde).

De vigtigste aktiver findes ved at inddrage fagforvaltningerne og få deres vurdering af, hvilke kritiske forretningsprocesser de har og er afhængige af. Eksempelvis lægge vægt på processer/arbejdsgange hvor sikkerhedsbrud kan have indvirkning på liv, ære og velfærd eller give økonomiske tab.

Det anbefales at informationssikkerhedsudvalget godkender hvilke aktiver, der skal gennemføres en risikovurdering på, så omfanget bliver styret.

Risikovurderingen bør dog ikke kun omfatte forretningsprocesser, it-systemer og de tekniske aktiver (it-afdelingens ansvarsområde), men alle de aktiver som indgår i et informationssystem. Det inkluderer også fysiske aktiver som fx papirarkiver, medarbejdere, immaterielle aktiver. I mange tilfælde kan de tekniske aktiver grupperes på en måde, hvor antallet begrænses, mens det stadig er muligt at knytte specifikke trusler til dem. For eksempel kan routere, switche, firewalls mv. grupperes som netværksudstyr eller infrastruktur. Aktiverne kan med fordel grupperes efter deres type for at lette identifikationen, eftersom der ofte vil være en sammenhæng med de relevante trusler.

Det anbefales at starte med risikovurderingen indenfor eksempelvis et fagforvaltningsområde for at opnå erfaringer med den valgte metode. Efterfølgende kan metoden tilpasses ift. erfaringer og udbredes til hele kommunen.

Deltagere
Risikovurderingen og risikohåndteringen vil ikke kunne foretages af sikkerhedskoordinatoren alene, men kræver at områdeleder, systemejer, superbruger eller andre medarbejdere, der kan vurdere konsekvenser og sandsynlighed, inddrages.

05 / KOM GODT I GANG MED RISIKOVURDERING

En risikovurdering består af en konsekvensvurdering og en sandsynlighedsvurdering.

Konsekvensvurderingen beskriver konsekvensen, hvis der sker et brud på fortrolighed, tilgængelighed eller integritet, mens sandsynlighedsvurderingen vurderer sandsynligheden for, at en trussel udnytter en sårbarhed og resulterer i et brud.

Risikovurdering i en ISO27001 kontekst og en GDPR kontekst – to forskellige vurderinger med samme metodik
I en ISO27001 kontekst er genstanden for risikovurderingerne kommunen selv – altså hvad sker der med kommunens økonomi og gode ry og rygte, hvis kommunen eksempelvis bliver hacket.

Det er absolut nødvendigt at have lavet sådanne risikovurderinger – men det er ikke tilstrækkeligt kun at lave denne ene type risikovurdering.

Databeskyttelsesforordningen (GDPR) stiller krav om, at der skal laves risikovurderinger ift. de registreredes rettigheder og frihedsrettigheder.

Her skal laves en vurdering af, hvilke risici kommunen som dataansvarlig udsætter borgere, medarbejdere og andre samarbejdspartnere i form af fysiske personer for.

Kommunen kan altså ikke nøjes med én risikovurdering, men er nødt til at lave en med kommunen i centrum og en med de registrerede i centrum. Til gengæld kan kommunen genbruge sit risikovurderingsframework, fordi metodikken ved de to risikovurderinger er ens.

Fastlæggelse af omfang
Inden selve risikovurderingen påbegyndes, skal omfanget og niveauet af den ønskede risikovurdering fastlægges. Der skal besluttes skala for konsekvens- og sandsynlighedsvurdering ligesom trusselskataloget skal beskrives.

De primære deltagere i arbejdet afhænger af, om der risikovurderes ift. den registrerede eller kommunen. Risikovurderes der ift. den registrerede deltager informationssikkerhedskoordinator og/eller DPO typisk sammen med forretningen. Risikovurderes der ift. kommunen deltager it-sikkerhedsfunktionen og forretningen typisk.

Trusselsvurdering
Identifikationen af relevante trusler er afgørende for, at man ikke overser risici. Derfor bør trusselsvurderingen ske på en systematisk måde. Ved at tage udgangspunkt i et katalog over mulige trusler kan man pejle sig ind på de trusler, der er relevante.

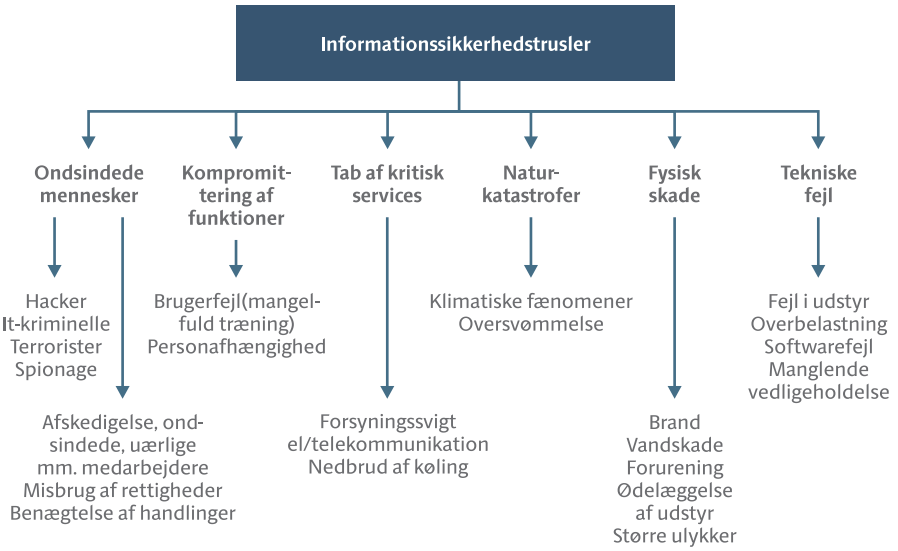
Der findes meget omfattende trusselskataloger, som indeholder enhver tænkelig situation, men man kan også anvende mere generiske kataloger. Ifølge National strategi for cyber- og informationssikkerhed er det et krav, at cybertrusler også indgår i myndighedernes risikovurderinger og risikoledelse.

I forbindelse med identifikationen af relevante trusler kan man med fordel se på egne historiske data. Hvilke trusler har faktisk resulteret i sikkerhedshændelser? Har kommunen været udsat for hacking, phishing eller ransomware, tyveri af personoplysninger, fejludsendelse af personoplysninger til forkert modtager eller har medarbejderne uploadet personoplysninger til private cloudtjenester?

Når man har lagt sig fast på, hvilke trusler der er relevante for kommunen, kan arbejdet med risikovurdering og -håndtering starte.

› Figur. Eksempel på det trusselsbillede ISO27005 tager udgangspunkt i

ISO27005: 2011 Risikoledelse



Konsekvensvurdering
En del af risikoanalysen er en identifikation af de konsekvenser, som et tab af fortrolighed, integritet og/eller tilgængelighed (FIT) vil medføre for et aktiv, eksempelvis for en forretningsproces/behandlingsaktivitet.

Afsættet for konsekvensvurderingen afhænger af, om man konsekvensvurderer ift. kommunen eller de registrerede, hvilket vil sige borgerne, ansatte og andre samarbejdspartnere i form af fysiske personer.

Hvis man konsekvensvurderer ift. kommunen tages der udgangspunkt i de forretningsmæssige konsekvenser et brud på informationssikkerheden vil have for kommunen. Her kan konsekvenserne eksempelvis være økonomisk tab, tab af omdømme, indflydelse på serviceniveau mv.

Hvis man konsekvensvurderer ift. de registreredes rettigheder tages der udgangspunkt i konsekvenserne for de registrerede, hvis der sker et brud på informationssikkerheden. Her kan konsekvenserne eksempelvis være økonomiske, fysisk og/eller psykisk påvirkning af helbred, stress, risiko for identitetstyveri mv.

Konsekvensvurderinger sker typisk efter en skala, hvor 1 = lav konsekvens, 2 = medium konsekvens, 3 = høj konsekvens og 4 = meget høj konsekvens.

Hvis konsekvensvurderingen resulterer i, at konsekvensen ved sikkerhedsbrud ikke vurderes højere end 2 (medium = mindre alvorlig/generende), kan man overveje ikke at risikovurdere dette aktiv yderligere, da den beregnede risiko aldrig vil blive højere end moderat.

Primære deltagere i afdækning af konsekvenser vil typisk være systemejere/sagsbehandlere.

› EKSEMPEL PÅ FORTROLIGHED

Brud på fortroligheden handler om, at data mister sin beskyttelse, og fremmede/uvedkommende dermed får adgang til data, som de ikke burde have adgang til.

Eksempler på brud på fortroligheden er:

› En bruger får ved en fejl adgang til en mappe på et fildrev, en sag eller et system, som personen ikke burde have adgang til, og dermed til data som personen ikke burde havde adgang til

› Et regneark bliver ved en fejl sendt til personer, som ikke skulle have haft det, og dermed får modtagerne adgang til data, som de ikke burde have haft

› Et brev med følsomme personoplysninger sendes ved en fejl til en forkert borger.

› EKSEMPEL PÅ INTEGRITET

Integritet handler om, at man kan stole på data, dvs. at de data som er f.eks. i et system, er de rigtige, og at man kan/tør træffe beslutninger på baggrund af dette.

Eksempler på brud på integriteten er:

› At der bliver indlæst gamle (ugyldige) data ind i et system, således at data ikke længere er de senest nye – og der dermed træffes beslutninger på et forkert grundlag

› At udefrakommende hacker sig ind på kommunens pc'er og foretager ændringer i it-systemer med personoplysninger eller i dokumenter indeholdende personoplysninger lagret på eksempelvis computerens drev eller fællesdrev

› At et regneark bliver overskrevet med en gammel version, og det dermed ikke længere er korrekt.

› EKSEMPEL PÅ TILGÆNGELIGHED (UNDER ½ DAG, 1 DAGE, 3 DAGE, EN UGE ELLER MERE)

Tilgængelighed handler om, at man kan få adgang til data.

Eksempler på brud på tilgængeligheden er:

› Systemet er brudt ned, og data er dermed ikke tilgængelige

› At data er blevet flyttet, eller der er blevet ændret ved muligheden for adgang, og de dermed ikke er tilgængelige

› Angreb af hackere med ransomware, hvor filer låses med krav om løsepenge for at åbne filerne igen.

Sandsynlighed/sårbarhed
Når konsekvensen ved et sikkerhedsbrud er vurderet, skal sandsynligheden for at det sker vurderes.

Ud fra trusselskataloget findes de trusler, der er relevante for aktiverne. Pr. aktiv vurderes sandsynlighed for, at truslerne udnytter en sårbarhed hos aktivet og dermed giver brud på fortrolighed, integritet og/eller tilgængelighed.

En trussel kræver en sårbarhed for at kunne resultere i en risiko. Sårbarheder kan for eksempel være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemer eller infrastruktur åbne for angreb. En god måde at få afdækket sårbarhederne på er ved at gennemgå de eksisterende foranstaltninger og vurdere deres effektivitet.

Primære deltagere i afdækning af sårbarheder og beskrivelse af sandsynlighed vil typisk være systemejere/superbrugere.

Sandsynlighed vurderes typisk efter samme skala som konsekvens, hvor 1 = usandsynlig, 2 = mindre sandsynligt, 3 = sandsynligt og 4 = forventet.

Beregning af risiko
På baggrund af sandsynlighedsvurderingen og konsekvensvurderingen kan risikoen beregnes. Der sker ved, at sandsynligheden sammenholdes med resultaterne af konsekvensvurderingen ud fra beregningsmetoden: konsekvens x sandsynlighed = risiko.

Risikoen beregnes for hver type konsekvens vurdering, det vil sige en med afsæt i konsekvenser for kommunen og en med afsæt i konsekvenser for de registrerede. Der vurderes for hver type for brud på fortrolighed, integritet, tilgængelighed, men det vil kun være den højeste konsekvens værdi, der anvendes i udregningen af risikoen.

Håndtering af risici
Sidste skridt i risikovurderingen er en håndtering af de fundne risici i forhold til de kriterier, som er fastlagt af ledelsen.

Håndtering af risici kan ske efter følgende principper (ovenstående tabel):

Risici i de grønne områder: Kan accepteres, ingen handlinger er nødvendige.

Risici i det gule område: Ledelsen kan beslutte at acceptere risikoen eller overveje at implementere tiltag, der kan reducere risikoen. Hvis man beslutter at acceptere risikoen, bør man løbende overvåge om risikoen indtræffer.

Risici i det orange område: Ledelsen bør ikke acceptere risikoen. Skal der sættes tiltag i værk eller kan risikoen overføres til tredje part via forsikring eller outsourcing?

› Eksempel på beregning af risiko

Konsekvens				
Meget høj	Under middel 4	Middel 8	Over middel 12	Høj 16
Høj	Lav 3	Under middel 6	Middel 9	Over middel 12
Medium	Lav 2	Under middel 4	Under middel 6	Middel 8
Lav	Lav 1	Lav 2	Lav 3	Under middel 4
Sandsynlighed	Usandsynligt	Mindre sandsynligt	sandsynligt	Forventet

	Lav - under middel: bør ikke give anledning til yderligere behandling
	Middel: bør give anledning til løbende overvågning
	Over middel: bør give anledning til håndtering
	Høj: bør håndteres med det samme

Risici i det røde område: Ledelsen bør ikke acceptere risikoen og der skal ageres umiddelbart. Skal der lukkes for services eller kan der sættes tiltag i værk, der kan nedbringe risikoen.

Når der risikovurderes ift. de registreredes rettigheder, så vær opmærksom på risici, hvor konsekvensen vurderes til at være meget høj. Her kan en usandsynlig eller mindre sandsynlig hændelse have alvorlige konsekvenser for den registrerede, hvis den indtræder. Selv om den beregnede risiko i disse situationer vil ligge på 4 eller 8, bør man overveje at lave en risikovurdering for at nedbringe risikoen for den registrerede.

Inspirationsmaterialer
I 2021/2022 er der i KL udarbejdet materiale til brug for risikovurdering ift. de registreredes rettigheder. Materialet er udarbejdet i et samarbejde mellem en række kommuner og KL. Materialet er udarbejdet med afsæt i KLE (KL's Emnesystematik), ud fra de KLE-numre der er GDPR opmærkede. Disse GDPR opmærkede KLE numre er grupperet i 90 behandlingsaktiviteter. Disse behandlingsaktiviteter er konsekvensvurderet i fællesskab ift. hvad konsekvensen vil være for den registrerede, hvis der sker et brud.

I materialet findes skabeloner til brug for den efterfølgende risikovurdering.

Der findes en videovejledning og en skrevet vejledning til materialet. Denne gennemgår materialet og viser et eksempel på en risikovurdering.

Materialet findes på KL videnscenter under "Risikostyring".

I materialet findes der et trusselskatalog, der også kan anvendes til risikovurdering med afsæt i konsekvenser for kommunen, ligesom man kan vælge at tilrette materialet, så det også kan dække denne risikovurdering.

06 / TIL- OG FRAVALG AF FORANSTALTNINGER – UDARBEJDELSE AF SoA-DOKUMENT

SoA står for Statement of Applicability, hvilket frit oversat kan forstås som en erklæring af, hvilket sikkerhedsniveau organisationens aktiv har besluttet sig for og hvorfor. SoA-dokumentet stammer fra ISO27001 og underbygger, hvorfor en organisation har gjort ét på et område og noget andet på et andet. Alt sammen begrundet i organisationens risikovurdering og risikoprofil. SoA-dokumentet kan ses som en statusopgørelse for organisationens arbejde med informationssikkerhed og som beslutningsdokumentation for dens til- og fravalg af sikkerhedsmæssige indsatser.

ISO27001 standarden indeholder et anneks A med sikringsforanstaltninger og kontroller. Standarden anbefaler, at organisationen som minimum forholder sig til disse i anneks A, når den udarbejder SoA-dokumentet. Desuden kan anneks A bruges som en tjekliste for, om egne risici er håndteret efter forskrifterne.

SoA-dokumentet er et krav i ISO27001 standarden og dermed ikke et krav at anvende for kommuner, men det kan anvendes som god inspiration.

Et SoA-dokument består af en liste med foranstaltninger, der kan være relevante for en organisation at implementere i forbindelse med organisationens risikohåndtering. Dette gælder også ift. håndtering af de risici, som vedrører den registrerede (GDPR). SoA-dokumentet vil dermed indeholde en samling over kontroller/foranstaltninger, kommunen har indført for at nedbringe risici og dermed sikre informationssikkerheden bedst mulig. Det kan være kontroller indført efter risikovurderingen ift. de registrerede, ift. infrastruktur, adgangskontrol etc.

SoA-dokument skal indeholde begrundelser for, hvorfor visse kontroller evt. er blevet valgt fra. De tilvalgte foranstaltninger indgår som grundlag for handlingsplaner for aktiviteter, der skal medføre en implementering af foranstaltningerne. Udover listen af foranstaltninger fra Anneks A, skal SoA-dokumentet også indeholde andre foranstaltninger som skønnes relevante for den enkelte kommune. Dette kan eksempelvis være lovkrav, best practice eller kontroller/foranstaltninger afledt af kommunens risikovurdering.

Resultatet af arbejdet med SoA-dokumentet skal godkendes af ledelsen, hvilket i praksis ofte vil være informationssikkerhedsudvalget.

Anbefaling
Udarbejdelse af SoA-dokumentet kan foregå enten i workshop- eller interviewform.

Anneks A foranstaltningerne kan med fordel gennemgås inden risikovurderingen starter, for at vurdere compliance ift. disse og dermed finde områder, der bør prioriteres.

Arbejdet ligger i forlængelse af de risici, man har identificeret under risikovurderingen. På baggrund af risikovurderingen besluttes det, hvilke muligheder man har for at håndtere de fundne risici, samt hvilke foranstaltninger man vil implementere.

Det er vigtigt, at en organisation identificerer sine sikkerhedskrav. Der er tre hovedkilder til sikkerhedskrav, som kan give anledning til at etablere foranstaltninger:

- Vurdering af risici i organisationen, idet der tages højde for organisationens overordnede forretningsstrategi og målsætninger.
- Lov-, myndigheds- og kontraktkrav, som en organisation, dens handelspartnere, leverandører og serviceudbydere skal opfylde.
- Best Practice – Sæt af principper, målsætninger og forretningskrav til informationshåndtering, -behandling, -lagring, -kommunikation og -arkivering, som en organisation har udviklet for at understøtte driften.

Husk at Anneks A ikke er udtømmende. Der kan være andre sikringsforanstaltninger og kontroller, som er relevante at få med i SoA-dokumentet.

Valg af foranstaltninger afhænger også af den måde, hvorpå foranstaltningerne supplerer hinanden og derved samlet udgør et solidt værn til beskyttelse af organisationens informationssikkerhed.

En foranstaltning kan fravælges ud fra den begrundelse, at den ikke er relevant eller at risikoen ved at fravælge den accepteres, undgås eller overføres til en tredje part.

Det udarbejdede SoA-dokuments tilvalg indgår som grundlag for handlingsplaner for konkrete aktiviteter, der skal implementere sikkerhedsforanstaltningerne.

SoA-dokumentet kan ligeledes anvendes som et systematisk værktøj til at opfylde dokumentationskravene fra NSIS (National Standard for Identiteters Sikringsniveauer).

07 / ÅRSHJUL

For at styre informationssikkerheden anbefales det, at gentage en række aktiviteter løbende år efter år. Dette er også ledelsens sikkerhed for, at kommunen har styr på informationssikkerheden, indenfor de risici man har accepteret.

Strukturering af planerne
Planer for tilbagevendende aktiviteter kan indgå i et årshjul, hvor alle elementer i arbejdet indgår. Aktiviteter, der afsluttes, og som ikke har behov for at blive gentaget, før der igen er identificeret et forbedringspotentiale, kan indføjes i en årsplan.

Forskellen på årshjulet og årsplanen
Årshjulet indeholder aktiviteter, der skal gentages med passende tidsintervaller. De er ikke i sig selv en sikkerhedsforanstaltning, men er ofte aktiviteter, der har karakter af opfølgning, evaluering, møder eller lignende. Alt sammen aktiviteter, der skal sikre, at den gennemførte indsats er tilstrækkelig. Det er ofte gennem disse aktiviteter, at der kan identificeres forbedringspotentialer og dermed opgaver til årsplanen eller risikohåndteringsplanen.

Årsplanen indeholder aktiviteter til forbedring af ledelsessystemet for informationssikkerhed, kontroller, sikringsforanstaltninger, processer eller lignende. En årsplan behøver ikke kun dække et år, den kan sagtens løbe over f.eks. tre eller fem år. Årsplanen og risikohåndteringsplanen kan med fordel slås sammen.

Der skal etableres planer for, hvornår aktiviteterne skal gennemføres. Planerne kan være udarbejdet i Excel, Word, et projektværktøj eller et Gantt-diagram, alt efter hvad der passer ind i den enkelte kommune. I planen bør deadline, ansvarlig og status fremgå under de enkelte aktiviteter.

Indhold i et årshjul
Opgaverne i et årshjul kan eksempelvis være:

- Opfølgning på dokumentation, beslutninger, risikovurderinger, beredskabsplan, awareness m.v. med det formål at vurdere, om der skal ske en opdatering
- Kontrol af brugerrettigheder, logninger, databehandlere, revision, test af beredskab m.v.
- Rapportering til informationssikkerhedsudvalget og direktionen

Hyppigheden vil typisk være angivet som årligt, halvårligt eller kvartårligt valgt ud fra opgavens kritikalitet ift. informationssikkerheden. Jo mere kritisk en opfølgning er for informationssikkerheden, jo hyppigere vil opgaven skulle foretages.

Afrapportering og fremdrift kan fx ske på møder i informationssikkerhedsudvalget.

Inspirationsmaterialer
Beskrivelse af Årshjul med eksempler på opfølgning og evaluering kan findes på KL Videncenter under "Årshjul".

ORDBOG

Aktiv
Ordet aktiver anvendes, som et fælles begreb for forretningsprocesser, it-systemer, teknisk infrastruktur, servere, pc'er etc. (Udtrykket stammer fra ISO27001).

Anneks A
Anneks A er en del af ISO27001 og indeholder en række foranstaltninger, der kan bruges som inspiration eller anvendes som tjekliste, for at sikre at relevante sikkerhedskrav er taget med i betragtning. Anneks A omtales ofte som SoA-dokumentet.

Dataejer
En chef/leder som har dispositionsret til data og ansvar for behandling af data. Dataejer kan også være systemejer. Se desuden KL Videncenter "En rejsefortælling om funktioner, roller og ledelse" hvor roller og opgaver for en data/systemejer er beskrevet.

FIT
Der bør altid gennemføres en konsekvensvurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed (FIT). Med fortrolighed menes, at uvedkommende får adgang til data, som de ikke burde have adgang til. Med integritet menes, at data, f.eks. i et system, er de rigtige, og at man kan træffe beslutninger på baggrund af dette. Med tilgængelighed menes, at man i organisationen kan tilgå nødvendige data.

ISO27001
ISO27001 standarden er udarbejdet med det formål at opstille krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS).

ISO27002
Kommunen vælger på basis af sin risikoprofil de foranstaltninger i ISO27001's Anneks A, der er relevante for at opnå en passende beskyttelse. Anneks A modsvarer indholdsfortegnelsen i ISO27002, der vejleder i hvorved kommunen bedre kan kvalificere og udpege handlinger, som anses for nødvendige.

Konsekvens
En del af risikoanalysen er en identifikation af de konsekvenser, som et tab af fortrolighed, integritet og/eller tilgængelighed vil medføre for et aktiv. Der kan være direkte økonomiske tab, tab af omdømme, indflydelse på serviceniveau mv.

Registreredes rettigheder og frihedsrettigheder
Databeskyttelsesforordningen (GDPR) stiller krav om, at der skal laves risikovurderinger ift. de registreredes rettigheder og frihedsrettigheder. Her skal laves en vurdering af, hvilke risici kommunen som dataansvarlig udsætter borgere, medarbejdere og andre samarbejdspartnere i form af fysiske personer for.

Risiko
En risiko kan opstå, hvis en trussel udnytter en sårbarhed, eksempelvis en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb.

Risikoejer
Risikoejer vil ofte være den, der har det økonomiske ansvar for risikoen. Kan eksempelvis være systemejer eller kontraktansvarlig.

Risikoprofil
Det fastlagte niveau for hvornår risici er acceptable. Niveauet i accept af risici kan hos informationssikkerhedsudvalget lægges forskelligt for eksempelvis økonomiske risici i forhold til risici på liv/ære/velfærdsområdet. Det samlede billede af risikovillighed udgør organisationens risikoprofil.

Risikovurdering
Risikovurdering handler om at identificere og analysere mulige trusler, sårbarheder overfor truslerne og sandsynligheden for de kan opstå samt tilhørende konsekvenser i forhold til risikoen for tab af fortrolighed, integritet og tilgængelighed.

Sandsynlighed
Når en trussel vurderes, vurderes sandsynligheden for at truslen udnytter en sårbarhed og dermed giver brud på fortrolighed, integritet og/eller tilgængelighed.

SoA
SoA står for 'Statement of Applicability'. SoA-dokumentet er en formel beskrivelse af udvalgte sikkerhedstiltag der udføres som et led i håndteringen af risici. SoA'en kaldes også beslutningsdokumentet og består konkret af en liste med kontroller/foranstaltninger. Anneks A kan anvendes til inspiration eller som basis for SoA dokumentet.

Systemejer
En chef/leder, der er ansvarlig for et eller flere systemer. Se desuden KL Videncenter "En rejsefortælling om funktioner, roller og ledelse" hvor roller og opgaver for en systemejer er beskrevet.

Sårbarhed
En trussel kræver en sårbarhed for at kunne resultere i en risiko. Sårbarheder kan være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb.

Trusler
Identifikationen af relevante trusler er afgørende for, at man ikke overser risici. Derfor bør trusselsvurderingen ske på en systematisk måde. Eksempler på trusler kan være hackerangreb, oversvømmelse, menneskelige fejl eks. deling af fortrolige oplysninger via mail, servernedbrud, spionage etc.

KL
Weidekampsgade 10
2300 København S
Tlf. 3370 3370
kl@kl.dk
www.kl.dk
@kommunerne

Produktionsnr. 830874
ISBN 978-87-94514-11-8