IM_

Medarbejderkompetencer på området for informations- og cybersikkerhed

Analyse udarbejdet af Implement Consulting Group for Fremfærd Borger med projektledelse af HK Kommunal og KL

Implement Consulting Group • 10. april 2024

Indholdsfortegnelse

Ledelsesresumé	3
Projektets baggrund, formål og tilrettelæggelse	5
Rammevilkår for kommuners arbejde med informations- og cybersikkerhed	8
Kompetencebehov for gruppen af administrative medarbejdere	10
Målgruppen for kompetenceudviklingen	16
Forslag til kompetenceudviklingstilbud	21
Andre opmærksomhedspunkter	28
Bilag	30

Ledelsesresumé

Analysen afdækker behov og potentiale for at udvikle administrative medarbejderes kompetencer på informations- og cybersikkerhedsområdet i kommunerne

Kommuner har en central rolle inden for informations- og cybersikkerhed. Men der er behov for at øge kompetencerne i takt med, at behov og krav stiger.

- **Analysen bygger på eksisterende viden på området ved at samle op på allerede udarbejdede analyser, rammevilkår og bedste-praksis for arbejdet med informations- og cybersikkerhed i kommunerne.**
- **Analysen peger på, hvilke områder inden for informations- og cybersikkerhed der er særligt relevant at udvikle kompetenceudviklingstilbud inden for, så de matcher målgruppens nuværende kompetenceniveau og understøtter fremadrettede behov.**
- **Endelig kommer analysen med anbefalinger til, hvordan et attraktivt kompetenceudviklingstilbud kan sammensættes.**

Formål

Danske kommuners opgavevaretagelse understøttes i stigende grad af digitale løsninger. Det skaber nye muligheder og bidrager til effektivt at levere services af høj kvalitet til borgere. Men samtidig står danske kommuner ligesom resten af samfundet overfor et stadigt skærpet trusselsbillede, hvor de nye digitale løsninger også kan skabe nye sårbarheder og angrebsflader, som potentielt kan udnyttes.

Hvis trusselsaktører lykkes med at sabotere en kommunes systemer og services kan det forstyrre driften af kritiske funktioner, og det kan betyde, at kommunen ikke kan løse de samfundsvigtige opgaver, de har som fx drikke-/spildevand, madudbringning eller borgernær sundhedspleje. I tillæg kan det have store økonomiske konsekvenser for en kommune at genoprette stabil drift i de kritiske funktioner, ligesom borgernes tillid til den kommunale opgaveløsning og det politiske system kan lide last.

Derfor er der behov for, at medarbejdere i kommuner rustes endnu bedre til at varetage opgaven med at sikre kommuners systemer, processer, opgaver og services mod potentielle angreb fra IT-kriminelle og fjendtligsindede, såvel som fejl forårsaget af medarbejdere – intentionelt eller uvidende.

Denne analyse skaber et afsæt for netop at løse dette.

Analysens resultater skaber fundamentet for, at kursus- og uddannelsesudbydere kan tilrettelægge kompetenceudviklingstilbud på området for informations- og cybersikkerhed målrettet administrative medarbejdere i kommunerne.

Gennem en tæt inddragelse af kommunale eksperter og repræsentanter fra målgruppen af administrative medarbejdere kortlægger analysen, hvordan et effektfuldt og engagerende kompetenceudviklingstilbud kan skabes for at bidrage til at løse den opgave, som kommuner og samfundet som helhed står over for.

Analysens konklusioner og produkter

Analysen konkluderer overordnet, at der er et behov for at løfte kompetencerne inden for informations- og cybersikkerhed blandt administrative medarbejdere i kommuner, så de er bedre rustet til at løfte den vigtige opgave med at sikre stabil drift og opgavevaretagelse.

Udgangspunktet for målgruppens kompetencebehov er de lovmæssige og bedste praksis rammevilkår, som er relevante for kommuner inden for informations- og cybersikkerhed. Hertil er udviklet et **kompetencehjul** med fire dimensioner, som hver især udgør en kerneopgave i arbejdet med informations- og cybersikkerhed i kommuner. Kompetencehjulet forventes at være kernen i indholdet af et kompetenceudviklingstilbud til målgruppen, men kan ligeledes benyttes som et dialogværktøj i kommuner ang. kompetenceudvikling.

For at sikre at kompetenceudviklingstilbuddet målrettes de helt rigtige medarbejdere og deres hverdag, er der udviklet **tre profiler** inden for målgruppen administrative medarbejdere, som forventes at have en rolle i kommuners fremadrettede arbejde med informations- og cybersikkerhed. Profilerne er beskrevet med en 'kompetencestatus' samt 'læringsbehov', hvilket giver en indikation af, hvor stort et udviklingspotentiale der er for profilerne på de respektive områder inden for informations- og cybersikkerhed.

På baggrund af kompetencehjulet og de identificerede profilers behov og udviklingspotentiale fremsætter analysen en **anbefaling til tre kompetenceudviklingstilbud**, der forventes at kunne løfte niveauet for informations- og cybersikkerhed væsentligt blandt administrative medarbejdere og dermed kommuner og samfund samlet set – præcis dér hvor de største behov er identificeret. Yderligere beskrives de erfaringer og ønsker, målgruppen har, når det kommer til kompetenceudvikling samt nogle af de produkter og ressourcer, som kursus- og uddannelsesudbydere forventes at bruge som afsæt, når de(t) endelige kompetenceudviklingstilbud udvikles.

God læselyst!

Projektets baggrund, formål og tilrettelæggelse

Baggrunden for projektet er øgede krav til kommuner i forhold til håndtering af opgaver på informations- og cybersikkerhedsområdet. Her kan administrative medarbejder med de rette kompetenceudviklingstilbud til rådighed spille en nøglerolle i fremtiden.

Analysen tager afsæt i øgede krav til kommunernes håndtering af opgaver inden for informations- og cybersikkerhed. Her kan administrative medarbejdere spille en nøglerolle.

Baggrund og formål

Øgede krav

Forvaltningsloven og GDPR har i en årrække sat rammerne for det kommunale arbejde med informations- og cybersikkerhed, men flere krav følger fx som følge af NIS2, hvis nationale implementering stadig (under analysens færdiggørelse) er under udarbejdelse.

Danske kommuner er som resten af samfundets institutioner potentielt sårbare overfor IT-sikkerhedshændelser, der risikerer at forstyrre driftskontinuiteten i kritiske funktioner og opgaver. IT-sikkerhedshændelser kan også lede til kompromittering af datas fortrolighed, integritet eller tilgængelighed. Hændelserne kan skyldes angreb fra fx IT-kriminelle, fjendtligtsindede nationer eller en medarbejder, der enten intentionelt eller som fejl kommer til forsage skade. Det kan have store økonomiske omkostninger for kommunerne at genoprette stabil drift i kritiske funktioner og infrastruktur efter nedbrud, ligesom borgernes tillid til den kommunale opgaveløsning og det politiske system kan lide last.

Grundet det forsat mere alvorlige og skærpede trusselsbillede følger derfor flere og flere lovgivningsmæssige krav, som sætter barren for arbejdet med informations- og cybersikkerhed højere og højere.

Behov for at bygge videre på eksisterende indsatser

For at øge kommunernes robusthed ift. bl.a. cyberangreb og skærpe indsatsen for at højne det kommunale IT-sikkerhedsniveau generelt er der behov for at sætte ind på flere fronter. Det er ikke nogen let opgave. Det kræver ledelsesfokus, og en indsats fra alle. Et af redskaberne i værktøjskassen er kompetenceudvikling, hvor særligt administrative medarbejdere kan spille en nøglerolle i fremtiden. I den forbindelse har Implement med projektledelse hos HK og KL og midler fra Fremfærd Borger gennemført en analyse af administrative medarbejderes behov for kompetenceudvikling på området. Som en del af Fremfærdsprojekterne hjælper analysen KL og HK Kommunal med at få viden om, hvordan kompetenceudviklingstilbud bedst tilrettelægges, så administrative medarbejdere i fremtiden bliver bedre klædt på til at støtte et højt IT-sikkerhedsniveau i kommunerne.

Kompetenceudvikling

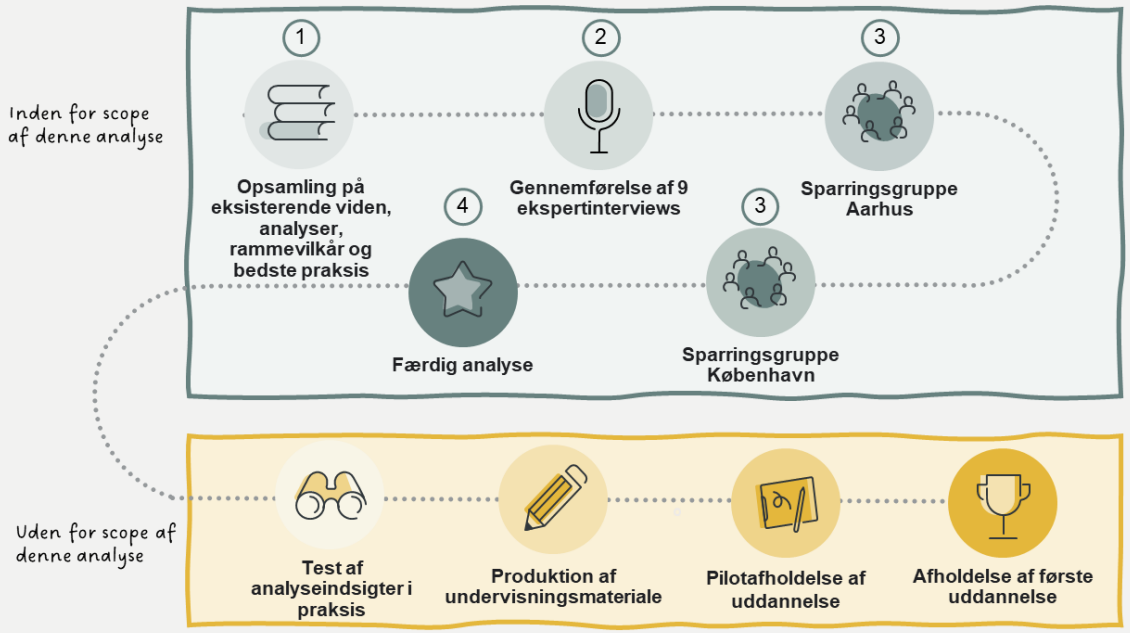
På baggrund af analysen vil det være muligt at efterspørge og tilrettelægge kompetenceudviklingstilbud på informations- og cybersikkerhedsområdet rettet mod administrative medarbejdere i kommunerne. Hvad enten det drejer sig om e-læring, kortere kompetenceudviklingstilbud eller uddannelser på akademi- og diplomniveau kan indsigterne fra analysen indgå som et redskab i designet af tilbuddene, der skal etableres og udbydes af kursusudbydere og uddannelsesinstitutioner.

Analysens resultater hviler på inddragelse af eksperter, medarbejdere og ledere i kommuners arbejde med informations- og cybersikkerhed

Analysen er første skridt på vejen til kompetenceudviklingstilbud

Analysen er første skridt på vejen mod at tilbyde kompetenceudviklingstilbud til målgruppen af administrativt personale i kommunerne. Analysen er gennemført i en iterativ proces og hviler på inddragelse af henholdsvis eksperter i kommunalt arbejde med informations- og cybersikkerhed samt af medarbejdere og ledere med ansvar for kommunale administrative opgaver.

Analysens resultater indgår som fundament for, at forskellige kursus- og uddannelsesudbydere kan tilrettelægge kompetenceudviklingstilbud på området for informations- og cybersikkerhed målrettet administrative medarbejdere i kommunerne. Tilbuddene skal udvikles af uddannelsesinstitutioner og kursusudbydere. Nedenstående figur viser processen fra nærværende analyse til udvikling af kompetenceudviklingstilbud.



Analysen er gennemført i fire iterative trin

1 Opsamling af eksisterende viden via desk-research

Bagtæppet for analysen er allerede udarbejdet litteratur og rapporter på området for kommunalt arbejde med informations- og cybersikkerhed samt analyser udarbejdet om målgruppen og deres kompetencer inden for digitalisering som helhed og mere specifikt inden for informations- og cybersikkerhed. Dernæst er der en række lovgivningsmæssige rammevilkår, som også er inkluderet i analysen. Endelig er der trukket på viden om bedste-praksis for arbejdet med informations- og cybersikkerhed fx ISO 2700x-serien[1].

2 Ekspertinterviews til kvalificering af hypoteser om kompetencebehov i fremtiden

Der er afholdt 9 ekspertinterviews[2] for at kvalificere hypoteser, der er kommet frem via desk-researchen. Eksperterne er udvalgt, fordi de har særlig indsigt i:

1. Rammevilkår og kommunal opgaveløsning på informations- og cybersikkerhedsområdet
2. Kompetenceudvikling
3. Målgruppen og deres behov

3 Kommunale sparringsworkshops

Med henblik på at afdække kompetencebehovene blandt de administrative medarbejdere, er der afholdt to sparringsworkshops med bred repræsentation af forskellige medarbejdertyper inden for kommunal administration[3]. Deltagerne er udvalgt med henblik på at sikre bred inddragelse og indfange indsigter og tendenser ift. målgruppens behov set fra deres perspektiv. Deltagerne er ligeledes udvalgt for at sikre repræsentation på tværs af størrelse, geografi, organisatorisk set-up på sikkerhedsområdet og anciennitet på sikkerhedsområdet.

4 Færdig analyse

På baggrund af ovenstående tre skridt er analysen færdiggjort og kvalificeret af HK Kommunal og KL.

1) For liste over materiale i desk-resarch se bilag 1
2) For liste over eksperter se bilag 1
3) For liste over funktioner se bilag 1

Rammevilkår for kommuners arbejde med informations- og cybersikkerhed

Kommunerne har i lang årrække arbejdet med at højne sikkerheden[1]. På tværs af kommunerne er der ikke én måde at gøre det på, men fælles for arbejdet er, at der er en række rammevilkår, som danner bagtæppet for arbejdet.

Rammevilkårene er udgangspunkt for kompetenceudviklingsindsatsen blandt administrative medarbejdere.

1: Se side 27

Rammevilkår (standarder, lovkrav mm.) stiller krav til de administrative medarbejderes kompetencer indenfor informations- og cybersikkerhed

Den kommunale opgaveløsning går på tværs

Den kommunale opgaveløsning er særlig i den forstand, at kommunens ansvarsområde går på tværs af mange forskellige sektorer. I kommunerne arbejdes der tværgående på den samme infrastruktur og i systemer, som i tillæg tilgås af mange forskellige medarbejdertyper. Kommunerne har nærhed med borgerne og en væsentlig del af kommunen er decentrale institutioner fra skoler, daginstitutioner samt forskellige dag- og døgntilbud til borgere samt en lang række øvrige opgaver også inden for bl.a. teknik og miljø.

Den tværgående opgaveløsning stiller selvfølgelig også særlige krav til kommuners arbejde med informations- og cybersikkerhed.

Rammevilkår tegner kompetencebehovet hos administrative medarbejdere

Via ekspertinterviews har vi identificeret en række rammevilkår, som er med til at forme de kompetencebehov vi ser i dag og i fremtiden for administrative medarbejdere. Nogle rammevilkår er lovgivning, som selvfølgelig implementeres og efterleves. Andre rammevilkår er udtryk for bedste praksis i arbejdet med informations- og cybersikkerhed for at sikre systematik og effektivitet i arbejdet.

Listen til højre er ikke udtømmende, men flere af rammevilkårene er gået igen både i desk-research og i flere ekspertinterviews, og disse rammevilkår anses derfor i denne analyse, som værende de vilkår, der i højest grad danner bagtæppet for kompetencebehovene hos administrative medarbejdere, når det kommer til informations- og cybersikkerhed.

Oversigt over eksempler på rammevilkår

- NIS2
- GDPR
- Forvaltningsretlige principper
- ISO 27001
- Tekniske minimumskrav

Disse rammevilkår er betonet i både desk research og flere ekspertinterviews, hvorfor de anses som væsentlige for administrative medarbejderes kompetencebehov. Derfor er de uddybet i bilag 2.

- NSIS
- AI act
- Data act
- Data governance act
- CIS 18
- NIST CSF
- IEC 62443

Disse rammevilkår er dukket op i desk-research og nævnt i ekspertinterviews – dog uden væsentlige gentagelser. De er relevante for informations- og cybersikkerhed men anses ikke som afgørende for administrative medarbejderes kompetencebehov.

Kompetencebehov for gruppen af administrative medarbejdere

På baggrund af de identificerede rammevilkår mm. er der udviklet et kompetencehjul, som illustrerer, hvilke kompetencer der kan understøtte det kommunale arbejde med informations- og cybersikkerhed.

Vi har udviklet et kompetencehjul med fire dimensioner for at konkretisere kompetencebehov på informations- og cybersikkerhedsområdet for administrative medarbejdere i kommunerne

Kompetencehjul med fire forskellige dimensioner

På baggrund af desk-research, interviews og workshops har vi udarbejdet et kompetencehjul på området for informations- og cybersikkerhed rettet mod administrative medarbejdere i kommunerne. Hjulet er inddelt i fire dimensioner, som hver især udgør en kerneopgave i arbejdet med informations- og cybersikkerhed for de administrative medarbejdere i kommunerne. Dimensionerne tager udgangspunkt i:

- Kommunale rammevilkår for arbejdet med cyber og informationssikkerhed, herunder retslige forpligtelser
- Bedste-praksis standarder
- De kommunale arbejdsopgaver

I tabellen til højre summerer vi, hvilke kilder de forskellige dimensioner er udviklet på baggrund af for at sikre sporbarhed i analysen. Nedenfor er de fire dimensioner kort summeret. På de kommende sider dykker vi mere ned i hver dimension samt underdimensioner.

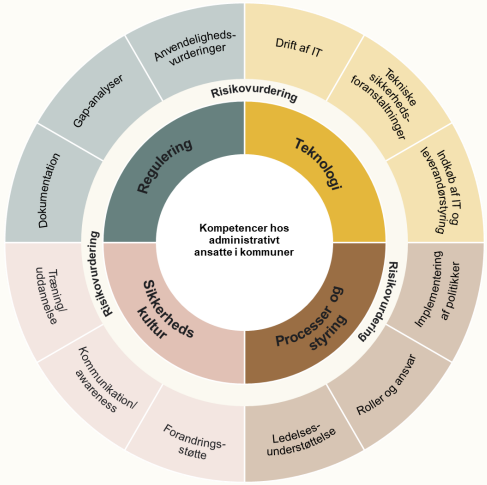
Kernen i sikkerhedsarbejdet er risikovurdering. Derfor er risikovurdering ikke en selvstændig disciplin i hjulet, men en grundlæggende forudsætning, der er udgangspunkt for de øvrige aktiviteter og opgaver.

Regulering

Bidrage til at love, krav og standarder er overholdt og dokumenteret i overensstemmelse med krav.

Sikkerhedskultur

Understøtte en stærk sikkerhedskultur i overensstemmelse med kommunale kerneværdier.



Teknologi

Bidrage til implementering af tekniske foranstaltninger på systemer og data samt indkøb og løbende drift.

Processer og styring

Understøtte implementering og forbedring af processer, procedurer og organisering af sikkerhedsarbejdet.

Oversigt over kompetenceområder og begrundelse for at tage det med*

Område	Begrundelse og baggrund for området
Teknologi	**Begrundelse:** Administrative medarbejdere kan være bindeled mellem IT-afdelingen og kommunens kerneopgaver samt indgå i driften – også når det kommer til sikkerhed. **Baggrund:** • ISO 27002, 27005 • Tekniske minimumskrav for kommuner • NIST's NICE (National Initiative for Cybersecurity Education) • HK Kommunal & KL: Kommunernes IT- og Digitaliseringsfunktion, 2017
Processer og styring	**Begrundelse:** Administrative medarbejdere kan hjælpe med at understøtte processer relateret til sikkerhed samt sagsbehandling og ledelsesunderstøttelse. **Baggrund:** • ISO 27001 • NIS2 • Forvaltningsretlige principper • GDPR
Sikkerheds-kultur	**Begrundelse:** Administrative medarbejdere kan bidrage til at ændre kommunens sikkerhedskultur i overensstemmelse med kerneværdierne. **Baggrund:** • ISO 27001, 27002 • NIS2 • NIST's NICE (National Initiative for Cybersecurity Education)
Regulering	**Begrundelse:** Administrative medarbejdere kan have opgaver relateret til de reguleringsmæssige aspekter af sikkerhed, herunder love, krav, standarder og anbefalinger. **Baggrund:** • GDPR • NIS2 • Forvaltningsretlige principper • NIST's NICE (National Initiative for Cybersecurity Education) • HK Kommunal & KL: Kommunernes IT- og Digitaliseringsfunktion, 2017

* Opdelingen af det respektive baggrundsmateriale på forskellige dimensioner er selvfølgelig lettere fortegnet, og flere af kilderne vil selvfølgelig gøre sig gældende i alle dimensioner. Uagtet er de dog opdelt her for indikere en prioritering.

Fokus på kompetencehjulet: Teknologi

Kompetencehjul med fire forskellige dimensioner

Oversigt over indholdet i dimensionen

Teknologi

Administrative medarbejdere kan være bindeled mellem IT-afdelingen og kommunens kerneopgaver samt indgå i driften – også når det kommer til sikkerhed.

Dimensionen indeholder generelt kompetencer med at understøtte implementering af tekniske sikkerhedsforanstaltninger på systemer og data. Dette kræver generel forståelse for IT-landskabet og sikkerhedsarkitektur. Yderligere at bidrage til kravstillelse ved indkøb og løbende opfølgning på leverandører.

Drift af IT

- Understøtte stabil og sikker drift af f.eks. servere, netværk, systemer og IT-udstyr, herunder patching, rettighedsstyring, back-up og monitorering.
- Hjælpe kommunens medarbejdere med sikker brug af IT, apps, software mm.

Tekniske sikkerhedsforanstaltninger

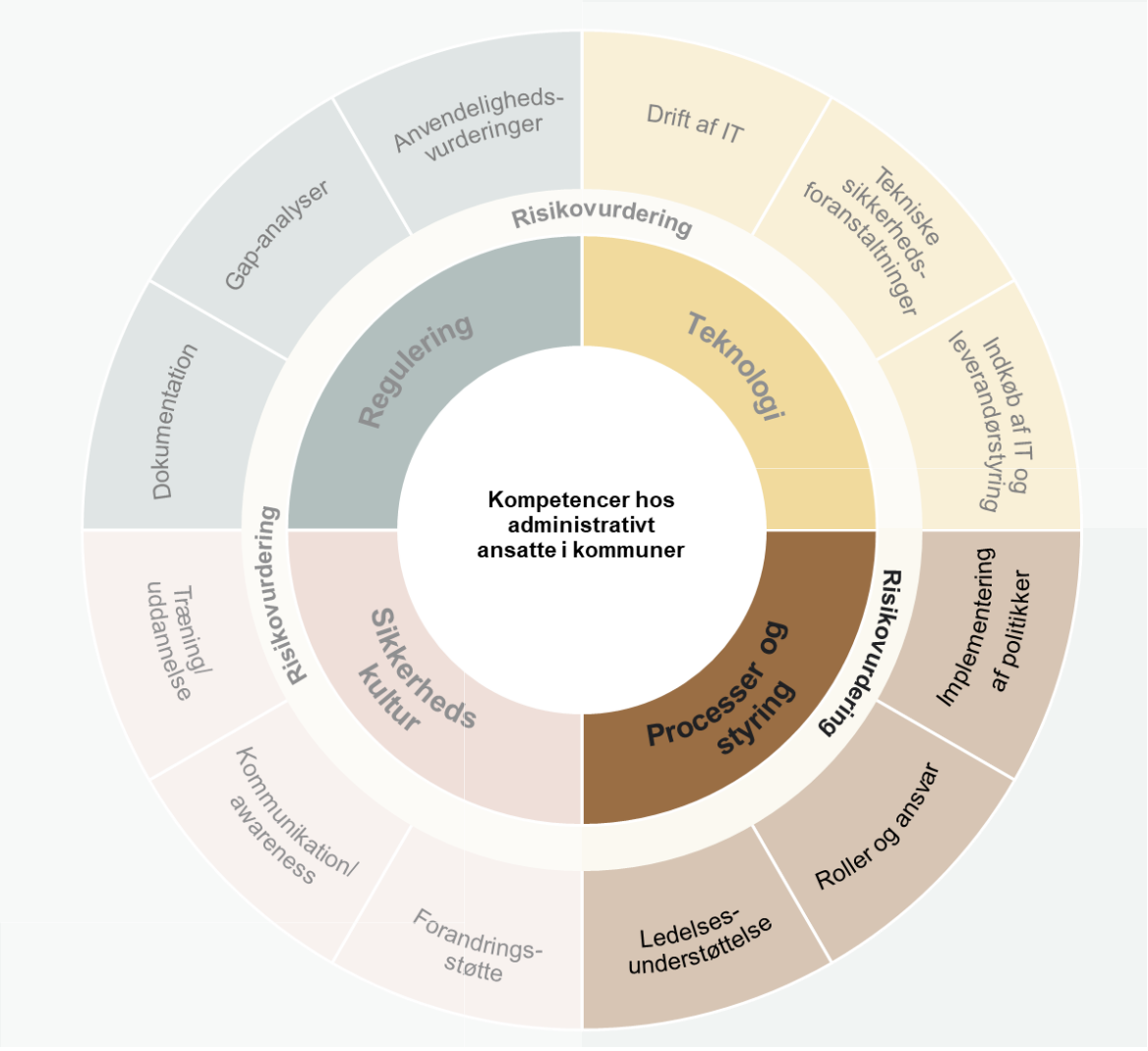
- Bidrage til konkret implementering af minimumskrav, tekniske standardforanstaltninger mv.
- Hjælpe med implementering af firewalls, kryptering af harddiske, logning og MFA på enheder. Implementeringen sker enten på egen hånd eller via samarbejde med ekstern leverandør.

Indkøb af IT og leverandørstyring

- Hjælpe med at beskrive kommunens sikkerhedsbehov ifm. indkøb af IT, herunder udformning af funktionelle og non-funktionelle krav.
- Understøtte løbende kontraktstyring for at sikre sig, at der er overensstemmelse mellem krav og implementeringsgrad fra leverandørens side.

Fokus på kompetencehjulet: Processer og styring

Kompetencehjul med fire forskellige dimensioner



Oversigt over indholdet i dimensionen

Processer og styring

Administrative medarbejdere understøtter processer relateret til sikkerhed samt sagsbehandling og ledelsesunderstøttelse.

Dimensionen indeholder generelt kompetencer med at understøtte vedligeholdelsen og forbedringen af processer, procedurer og organiseringen af sikkerhedsarbejdet. Dette kræver evner inden for koordinering, interessentinddragelse, solid sagsbehandling og understøttelse af godkendelsesprocesser. Yderligere at bidrage til at ledelsen kan arbejde effektivt.

Implementering af politikker

- Understøtte processen med at implementere og følge op på kommunens informationssikkerhedspolitik og –retningslinjer.
- Koordinering, interessentinddragelse, indhentning af input, understøttelse af godkendelsesprocesser og ledelsesrapportering.

Roller og ansvar

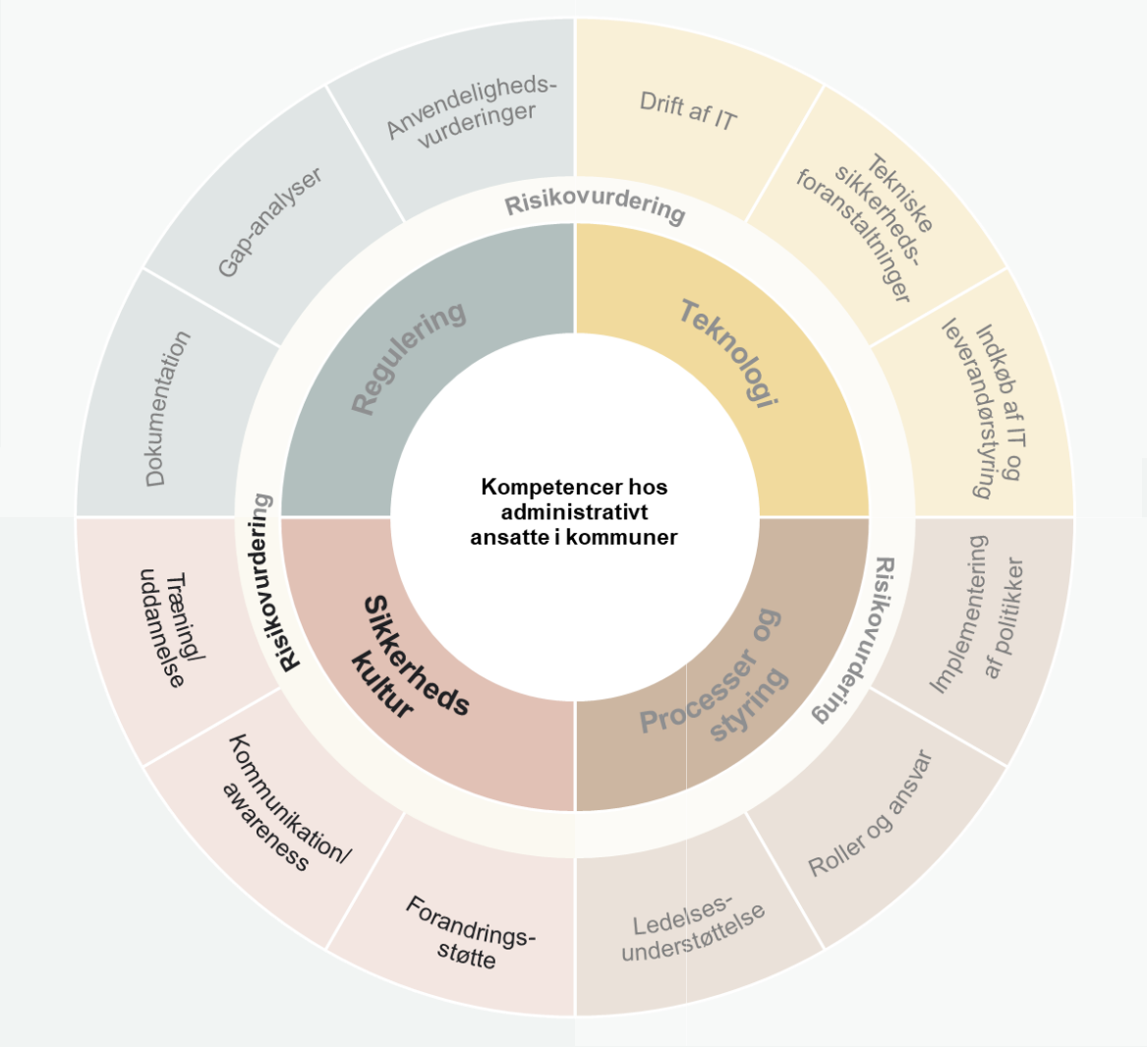
- Understøtte at kommunen har de roller, som et effektivt sikkerhedsarbejde kræver.
- Holde overblik over sikkerhedsorganisationen og koordinere mellem medarbejdere og afdelinger, så alle er klar over deres roller og ansvar.

Ledelsesunderstøttelse

- Bidrage med information til ledelsen, så de kan sætte den strategiske og taktiske retning for kommunens informations- og cybersikkerhed.
- Sortere i store mængder af data og kunne fremstille en sag klart og tydeligt med beslutningspunkter.

Fokus på kompetencehjulet: Sikkerhedskultur

Kompetencehjul med fire forskellige dimensioner



Oversigt over indholdet i dimensionen

Sikkerhedskultur

Administrative medarbejdere kan bidrage til at ændre kommunens sikkerhedskultur i overensstemmelse med kerneværdierne.

Dimensionen indeholder generelt kompetencer med at bidrage til formidling af budskaber, inddrage de rigtige personer og understøtte at der er blik for, at en forandring af vaner og processer typisk møder modstand hos medarbejdere og ledere. Yderligere at kunne understøtte den praktiske del af kurser og arrangementer.

Forandringsstøtte

- Bidrage til den overordnede sikkerhedstransformation/konsolidering, som kommunen skal igennem.
- Kommunikations- og koordinationsevner og at støtte specialister i håndtering af evt. modstand blandt medarbejdere i forbindelse med transformationen.

Kommunikation/awareness

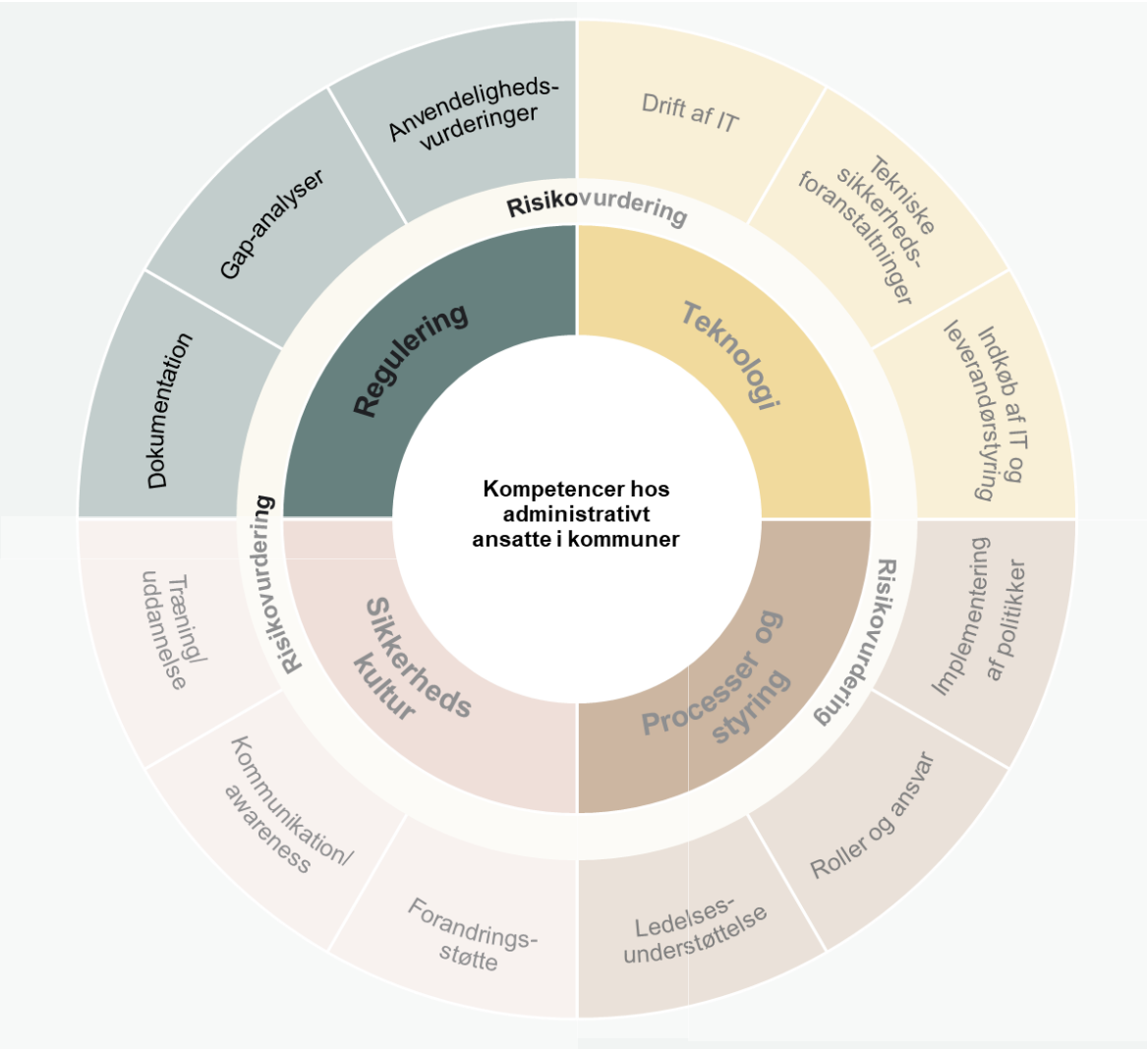
- Kommunikere internt og eksternt om retningslinjer vedrørende informations- og cybersikkerhed, så de bliver implementeret.
- Arrangere tiltag/producere materialer til kollegaer så information kommer ud til alle.

Træning/uddannelse

- Understøtte uddannelse af kommunens ansatte – ledelse såvel som medarbejdere.

Fokus på kompetencehjulet: Regulering

Kompetencehjul med fire forskellige dimensioner



Oversigt over indholdet i dimensionen

Regulering

Administrative medarbejdere kan have opgaver relateret til de reguleringsmæssige aspekter af sikkerhed.

Dimensionen indeholder generelt kompetencer med at systematisere og dokumentere viden ift. love, standarder, krav mv. Yderligere at bidrage til at vurdere om og hvordan kommunen er omfattet ift. kommunens kontekst samt at hjælpe med at vurdere hvilke nødvendige tiltag, der skal implementeres, for at komme i fuld overensstemmelse med et krav eller en lovgivning.

Dokumentation

- Bidrage til at kommunen kan gennemføre effektive audit og tilsyn.
- Dokumentation, kategorisering og journalisering af kommunens sikkerhedsrelaterede processer som f.eks. rettighedsstyring, databehandling, risikostyring og beredskabsprocesser.

Gap-analyser

- Hjælpe med at vurdere omfanget af mangler i processer og organisation, så kommunen kan overholde en standard, et krav eller en lovgivning tilfredsstillende.
- Hjælpe med at dokumentere den nuværende modenhed og at kunne synliggøre vejen til den ønskede modenhed.

Anvendelighedsvurderinger

- Vurdere om og hvordan kommunen er omfattet af lovkrav, rammevilkår eller standarder.
- Sætte sig ind i lovgivningen/kravet/standarden og at hjælpe med at vurdere, hvordan det passer ind i kommunens kontekst og opgaveløsning.

Målgruppen for kompetenceudviklingen

Administrative medarbejdere i kommunerne udfører en lang række forskelligartede opgaver. For at tilrettelægge kompetenceudviklingstilbud målrettet dem er der udviklet tre forskellige profiler, som både nu og i fremtiden kan have gavn af at udvikle deres kompetencer inden for informations- og cybersikkerhed for at styrke sikkerheden i kommunerne.

Analysen peger på tre kompetenceprofiler inden for målgruppen af administrative medarbejdere i kommunerne

De tre profiler har forskellige behov for kompetenceudvikling

Arbejdet med informations- og cybersikkerhed er organiseret forskelligt fra kommune til kommune. Her præsenteres tre kompetenceprofiler. De er ikke tænkt som jobprofiler, men skal ses som et bud på, hvilke kompetencer det er nødvendigt at tænke ind, når kommunale administrative medarbejdere i fremtiden skal have endnu bedre forudsætninger for at bidrage til et højt sikkerhedsniveau i kommunen.

Profilerne er tænkt som arketyper, og derfor vil der selvfølgelig være profiler i den "rigtige" kommunale virkelighed, der går på tværs af disse tre, når det kommer til opgaver og ansvar i hverdagen.

På baggrund af de gennemførte analyseaktiviteter peger analysen på, at særligt tre kompetenceprofiler kan være relevante at kende, når der skal udvikles kompetenceudviklingstilbud. Det være sig administrative medarbejdere:

1. **Uden specifikke opgaver** inden for informations- og cybersikkerhed
2. **Med specifikke organisatoriske opgaver** inden for informations- og cybersikkerhed
3. **Med specifikke tekniske opgaver** inden for informations- og cybersikkerhed

Profilernes behov for kompetenceudvikling varierer og afhænger af, hvor dyb deres berøring er med opgaver relateret til informations- og cybersikkerhed. I bilag 3 findes en uddybning af eksempler på typiske arbejdsopgaver og sikkerhedsrelaterede opgaver, som de forskellige profiler har.

Kompetenceprofilerne er tænkt som et værktøj til at overveje, hvordan indholdet på et kompetenceudviklingstilbud bedst tilrettelægges, så det understøtter behovet i kommunerne. Fremadrettet kan kompetenceprofilerne også evt. bruges som et fælles udgangspunkt ved MUS, hvor såvel leder som medarbejder overvejer kompetencebehov.

De tre kompetenceprofiler – kort fortalt

Profil 1: Administrativ medarbejder **uden specifikke opgaver** inden for informations- og cybersikkerhed

Hovedparten af administrative medarbejdere kommunerne udfører dagligt deres kerneopgave som kan omfatte alt borgerserviceopgaver til controlling til sekretærarbejde på skolerne. Fælles for dem er, at de har ansvar for at udføre egen praksis, så sikkerheden opretholdes. De har ikke yderligere specifikke opgaver inden for informations- og cybersikkerhed.

Profil 2: Administrativ medarbejder **med specifikke organisatoriske opgaver** inden for informations- og cybersikkerhed

Administrative medarbejdere som har fået specifikke organisatoriske opgaver inden for informations- og cybersikkerhed. Medarbejderne kan være placeret forskellige steder i kommunen både centralt på rådhusene og i decentrale forvaltninger, tilbud og institutioner som fx på skolerne, bibliotekerne eller i borgerservice. De udfører en lang række forskelligartede opgaver, som er deres kerneopgave, men har også fået en specifik rolle inden for informations- og cybersikkerhed. Det kan fx være, at de er GDPR-ansvarlige, har systemansvar eller er med i et udvalg af informationssikkerhedskoordinatorer.

Profil 3: Administrativ medarbejder **med specifikke tekniske opgaver** inden for informations- og cybersikkerhed

Medarbejdere som har fået tildelt specifikke tekniske opgaver inden for informations- og cybersikkerhed. De er ofte placeret i eller tæt på IT-afdelinger eller deciderede sikkerhedsfunktioner i kommunerne. De udfører en række opgaver, der understøtter sikker daglig drift og vedligehold af kommunens IT-systemer og -infrastruktur. Deres arbejde varierer fx afhængigt af størrelsen på IT-afdelingen samt kommunens specifikke behov.

De tre kompetenceprofiler arbejder sammen på tværs og har brug for hinanden for at løfte deres kommunes samlede sikkerhed. **Profil 1** har en vigtig opgave med understøtte profil 2 og 3's arbejde. **Profil 2** forventes at arbejde tæt sammen med profil 1. **Profil 3** forventes at have en kerneopgave med sikkerhed og at arbejde tæt sammen med profil 2.

Ledelsen er en vigtig aktør uanset profilen, da de sætter retningen og prioriterer ressourcerne.

Profil 1: Administrativ medarbejder **uden specifikke opgaver** inden for informations- og cybersikkerhed

Behov for basale kompetencer inden for informations- og cybersikkerhed, så egen praksis kan udføres inden for rammerne af kommunens sikkerhedskrav

Kompetencestatus

I denne gruppe indgår administrative medarbejdere bredt set. De udgør langt hovedparten af målgruppen som helhed, og de er kendetegnet ved, at de ikke er tildelt specifikke opgaver inden for informations- og cybersikkerhed.

De udfører dagligt deres kerneopgave, som kan omfatte alt fra borgerserviceopgaver til controlling til sekretærarbejde på skolerne.

I forhold til informations- og cybersikkerhed har de brug for at vide, hvad der skal til for at kunne udføre egen praksis på en sikker måde. De skal vide, at de også har en rolle i at opretholde kommunens sikkerhed.

De har også behov for viden om kommunens grundlæggende krav til informationssikkerhed og håndtering af data, så datas integritet, tilgængelighed eller fortrolighed ikke kompromitteres.

Informationssikkerhed i egen opgavevaretagelse/praksis

”Vi har brug for basale kompetencer til at styrke vores daglige arbejde med sikkerhed og understøtte vores kollegaer med sikkerhedsopgaven”

Læringsbehov

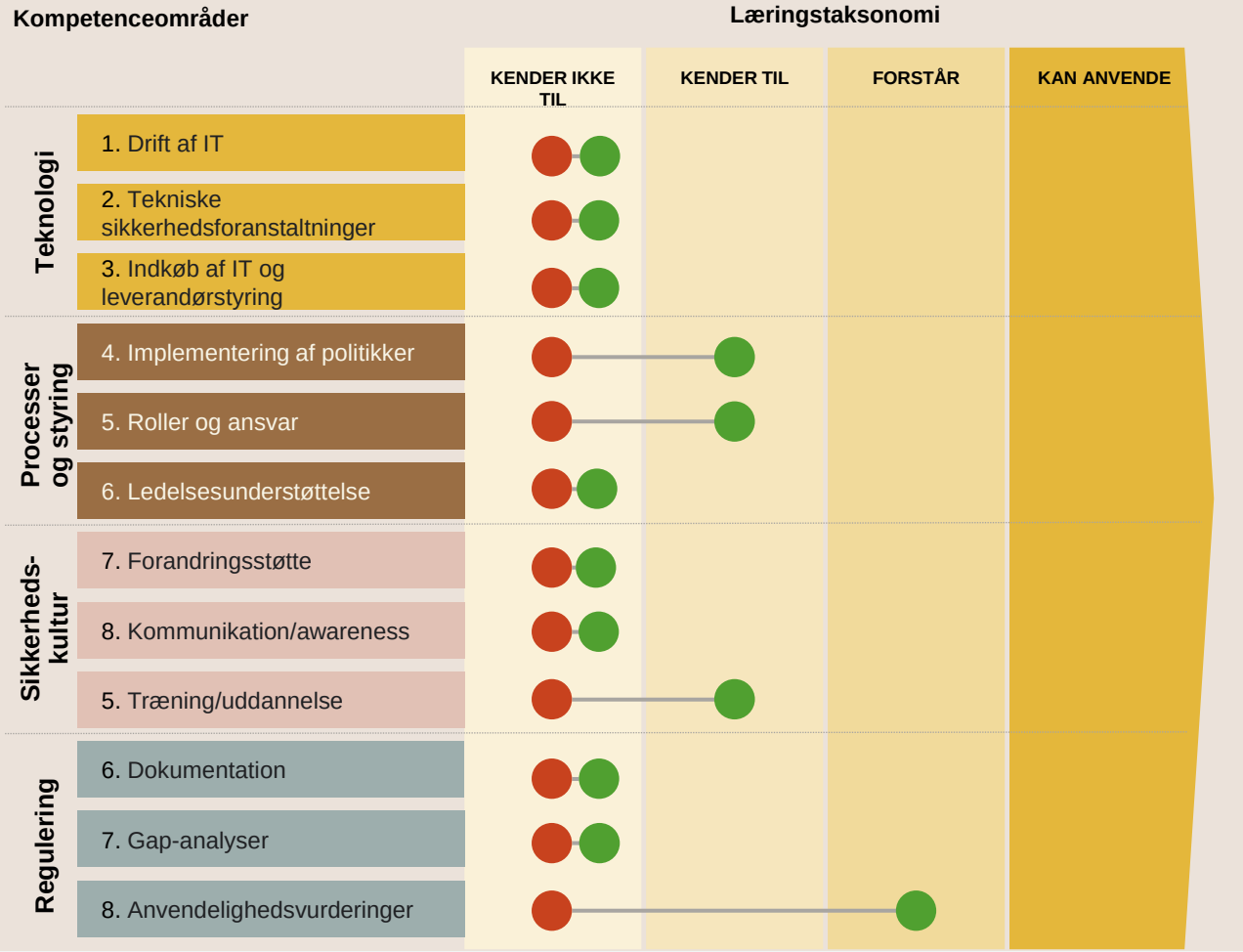
Teknologi:
- Ingen særlige behov for kompetencer inden for kategorien teknologi.

Processer og styring:
- Har behov for overordnet kendskab til kommunens sikkerhedspolitik.
- Har behov for kendskab til, at de spiller en rolle i forhold til at opretholde informations- og cybersikkerhed i kommunen.

Sikkerhedskultur:
- Skal kende til mulighed for fx obligatoriske basale kurser i informations- og cybersikkerhed.
- De er aftagere af awareness-aktiviteter

Regulering:
- Skal kunne forstå sektorlovning inden for egen praksis, og hvilke krav det stiller til sikker håndtering af data.

Læringsrejse



Profil 2: Administrativ medarbejder **med specifikke organisatoriske opgaver** inden for informations- og cybersikkerhed

Behov for grundlæggende forståelse for at opretholde informations- og cybersikkerhed i hverdagen med særligt fokus på kompetencer inden for processer og styring samt sikkerhedskultur.

Kompetencestatus

I denne profil indgår administrative medarbejdere, der ud over deres kerneopgave er tildelt en specifik opgave inden for informations- og cybersikkerhed. Det kan fx være, at de hjælper med at opretholde informationssikkerhed eller krav til sikker håndtering af persondata. De kan arbejde i centrale funktioner på rådhuse, i forvaltninger/centre eller i tilbud eller institutioner.

De arbejder fx med systemforvaltning, risikostyring, brugerstyring eller har en rolle som ambassadører for god sikkerhed lokalt på deres arbejdsplads.

Der kan fx være tale om medarbejdere med et specifikt ansvar inden for GDPR, systemforvaltning eller informations-sikkerhedskoordinatorer centralt og lokalt.

Informationssikkerhed i hverdagen

”Vi har brug for redskaber til at hjælpe med at opretholde sikkerheden i vores hverdag – der hvor vi arbejder”.

Læringsbehov

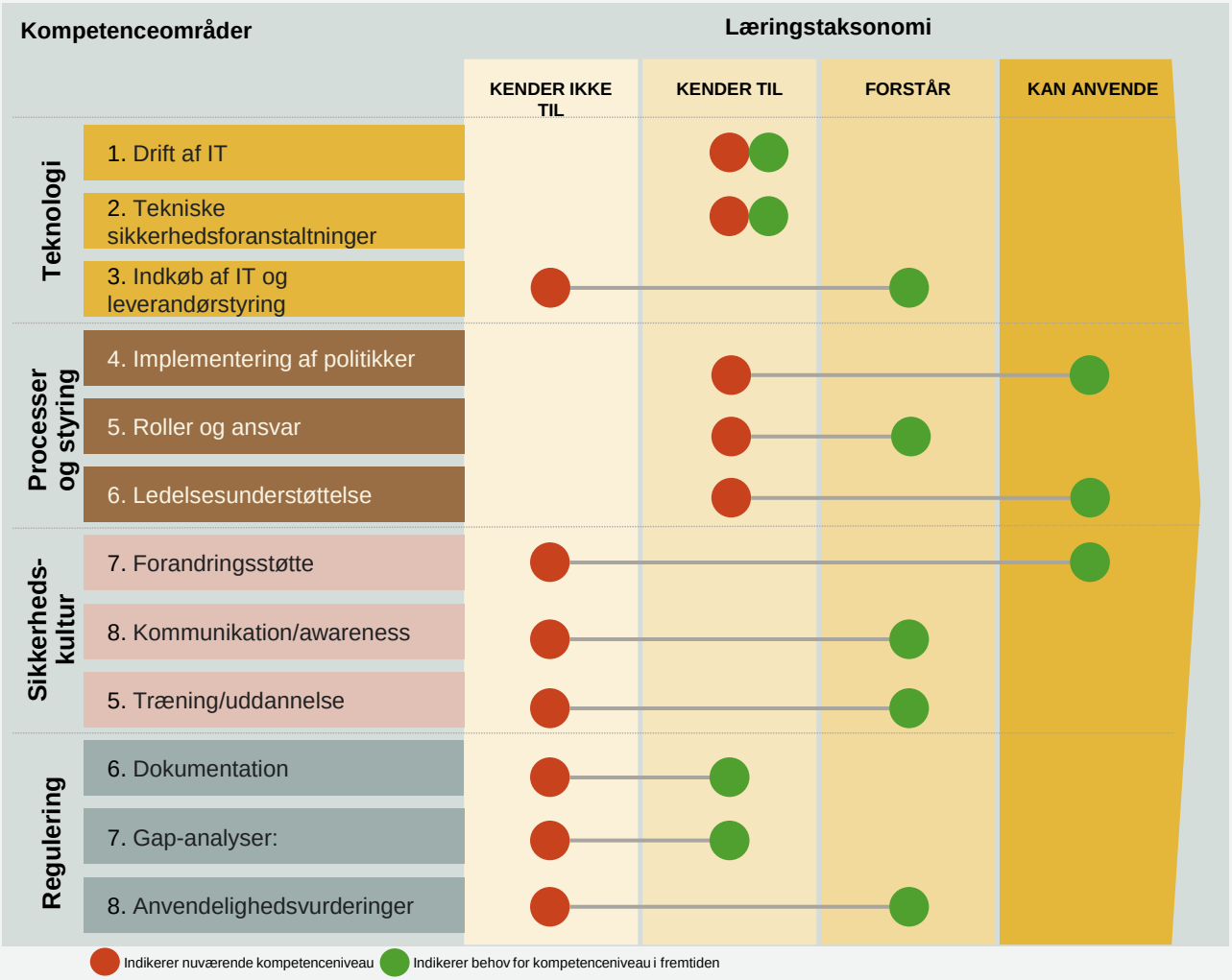
Teknologi:
- Grundlæggende kendskab til sikker drift af IT-løsninger.
- Behov for at kunne forstå, hvordan IT-løsninger indkøbes, så det lever op til kommunens politik på området.

Processer og styring:
- Behov for at kunne anvende kommunens sikkerhedspolitik og forstå den grundlæggende terminologi inden for informations- og cybersikkerhed fx med udgangspunkt i ISO 2700x-standarderne.
- Forstå egen roller og ansvar i sikkerhedsarbejdet og kunne støtte op om ledelsen på området.

Sikkerhedskultur:
- Behov for at kunne forstå, hvordan sikkerhedskultur implementeres lokalt i organisationerne.

Regulering:
- Kende til regulering inden for området og også hvilke krav, det sætter til eget arbejde.

Læringsrejse



Profil 3: Administrativ medarbejder **med specifikke tekniske opgaver** inden for informations- og cybersikkerhed

Behov for at kunne forstå eller anvende koncepter inden for alle fire kompetenceområder: Teknologi, processer og styring, sikkerhedskultur og regulering

Kompetencestatus

Administrative medarbejdere, der arbejder i kommunerne og har specifikke tekniske arbejdsopgaver inden for informations- og cybersikkerhed. Det kunne være systemadministratorer, systemansvarlige, medarbejdere i IT- og digitaliseringsafdelinger eller medarbejdere i sikkerhedsafdelinger.

Målgruppen har ikke altid formel træning eller uddannelse inden for informations- og cybersikkerhed, men har behov for grundlæggende viden om sikkerhedsområdet fx baseret på ISO 27001-standarden og også teknisk viden fx med udgangspunkt i bl.a. tekniske sikkerhedsforanstaltninger og tekniske minimumskrav.

Teknisk IT-sikkerhed i praksis

”Vi vil gerne have konkrete redskaber og værktøjer til at kunne arbejde med teknisk IT-sikkerhed i praksis for at understøtte vores kommunes mål på sikkerhedsområdet”

Læringsbehov

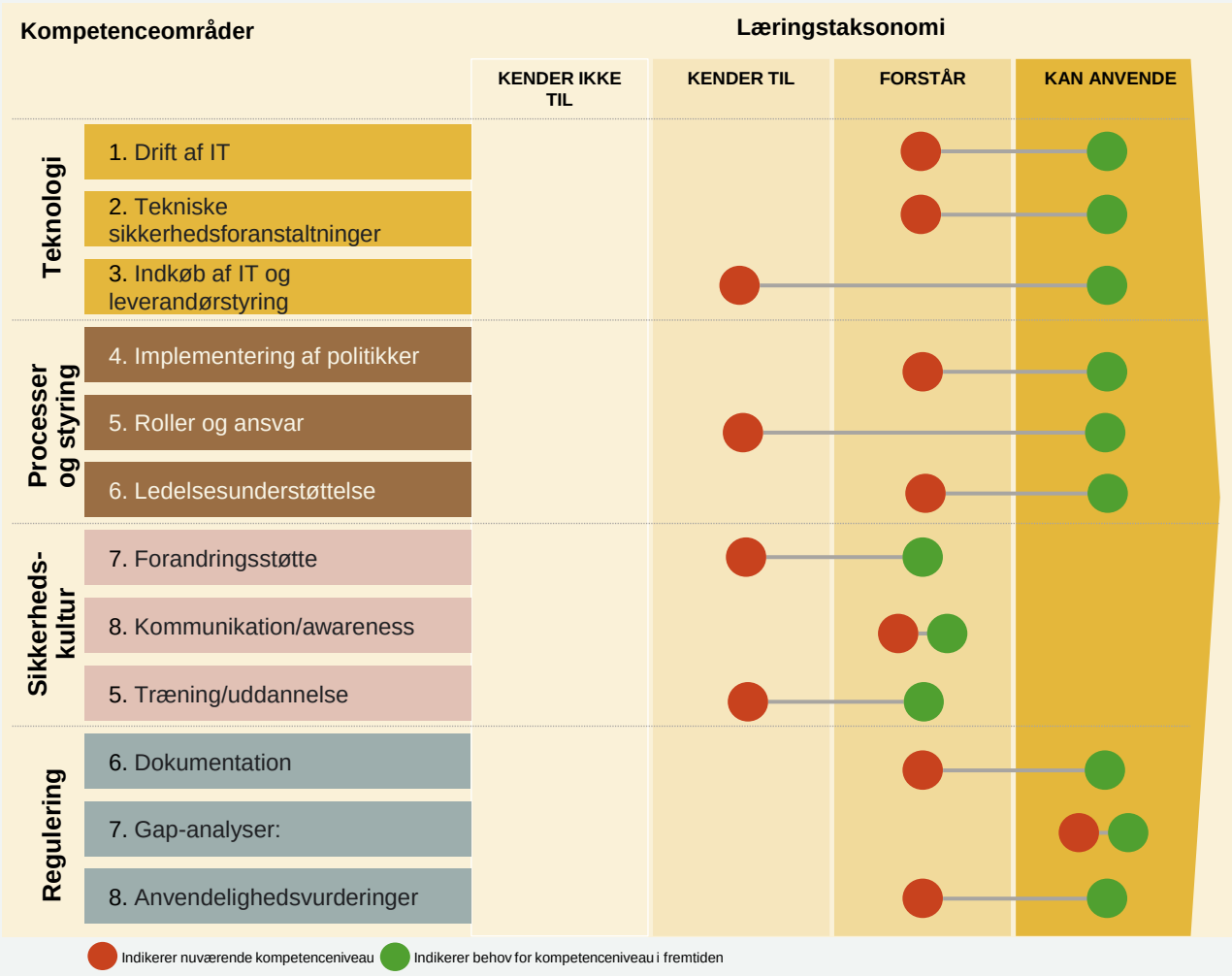
Teknologi:
- Behov for viden om tekniske minimumskrav og sikkerhedsforanstaltninger fx fra ISO 27002.
- Grundlæggende IT-teknisk forståelse til at kunne indgå i kritisk dialog med leverandører af IT-løsninger.

Processer og styring:
- Behov for viden i forhold til organisering af sikkerhedsarbejdet, herunder roller og ansvar.
- Viden om implementering af sikkerhedspolitikker, og hvordan man arbejder ud fra dem.

Sikkerhedskultur:
- Grundlæggende viden om, hvad god sikkerhedskultur er, og hvordan man arbejder med det.

Regulering:
- Viden til at kunne forstå og anvende regulering på området, så kommunens arbejde med at være lovmedholdelig støttes.

Læringsrejse



Forslag til kompetenceudviklings-tilbud

På baggrund af de skitserede kompetenceprofiler peger analysen på, at der kan udvikles forskellige kompetenceudviklingstilbud, som matcher profilernes behov. Forslagene skal ses som udgangspunkt for, at uddannelsesinstitutioner eller kursusudbydere kan udvikle kompetenceudviklingstilbud.

Målgruppen har forskelligt behov for dybden af kompetencer

Ekspertinterviews og sparringsgrupper peger alle på, at administrative medarbejdere er en ganske broget målgruppe med ganske forskellige behov for dybden af kompetencer inden for informations- og cybersikkerhed.

Derfor foreslår vi en trappetilgang til at løfte administrative medarbejderes kompetencer inden for informations- og cybersikkerhed. Der er tre niveauer i trappen, som matcher de tre kompetenceprofiler, der er beskrevet tidligere i afrapporteringen.

Trin et: Kompetenceudvikling med fokus på det mest basale om informations- og cybersikkerhed

Her er alle de administrative medarbejdere, som ikke har en specifik opgave inden for informations- og cybersikkerhed. De har et lille og rimeligt afgrænset behov. Dvs. at de i overvejende grad ”blot” skal kende til de vigtigste begreber og processer med henblik på at udøve en generel sikker adfærd i deres hverdag og egen praksis. Måske skal de kunne støtte enkelte processer relateret til informations- og cybersikkerhed i deres arbejde. Disse medarbejdere vil have gavn af et rimelig grundlæggende basalt kompetenceudviklingstilbud.

Trin to: Kompetenceudvikling med fokus på de væsentligste værktøjer og processer inden for informations-, cyber- og IT-sikkerhed

På dette niveau finder vi administrative medarbejdere, som har brug for at forstå og mestre de væsentligste værktøjer og processer i deres daglige arbejde relateret til informations- og cybersikkerhed. Disse medarbejdere vil have gavn af et mere dybdegående kompetenceudviklingstilbud.

Trin tre: Kompetenceudvikling med fokus på tekniske aspekter af informations-, cyber- og IT-sikkerhed: Disse medarbejdere har brug for at styrke og mestre også de mere tekniske aspekter af informations- og cybersikkerhed. De har overordnet set det største behov for mere dybdegående træning og uddannelse i informations- og cybersikkerhed.

Formatet på de forskellige tilbud på hvert trappetrin er til inspiration og er baseret på indsigter fra ekspertinterviews og sparringsgrupper. Formaterne kan dermed med fordel efterprøves i pilotudgaver af kompetenceudviklingstilbud(ene), lige så vel som de kan bygge ovenpå eksisterende tilbud. På de følgende slides har vi uddybet de tre forslag til kompetenceudviklingstilbud yderligere.

Trin et: Basal sikkerhed

Formål: Forstå det mest basale om informations- og cybersikkerhed

Målgruppe: Alle administrative medarbejdere

Format: Kort læringstilbud (fx e-læring mv.)

Trin to: Cyber- og informations-sikkerhed i kommunerne

Formål: Forstå og mestre de væsentligste værktøjer og processer inden for informations-, cyber- og IT-sikkerhed

Målgruppe: Administrative medarbejdere med en specifik organisatorisk opgave inden or informations- og cybersikkerhed

Format: Mellemlangt læringstilbud (fx 4+1 dages tilbud)

Trin tre: Teknisk cyber- og informationssikkerhed i kommunerne

Formål: Forstå og mestre de tekniske aspekter af informations-, cyber- og IT-sikkerhed

Målgruppe: Administrative medarbejdere med en specifik teknisk opgave inden for informations- og cybersikkerhed

Format: Langt læringstilbud (fx 8+2 dages tilbud)

Trin et: Kompetenceudvikling med fokus på **det mest basale** om informations- og cybersikkerhed

Overordnet beskrivelse

Kompetenceudviklingstilbuddet skal klæde administrative medarbejdere i kommunerne på til at kunne varetage egen praksis på sikker vis. Det gælder grundlæggende cyber-hygiejne og kendskab til sikkerhedspolitikken i kommunen. Endelig kunne deltagerne blive klædt på til at kende til egen rolle i forhold til at opretholde kommunens sikkerhed.

Udbytte af kompetenceudviklingstilbud for kommunerne

- Grundlæggende forståelse for basal sikkerhed for en stor medarbejdergruppe i kommunen
- Understøtte basal informations- og cybersikkerhed

Udbytte af kompetenceudviklingstilbud for kursisterne

- Blive klædt på til at vide, at der er krav til alle administrative medarbejdere i forhold til at opretholde kommunens digitale sikkerhed

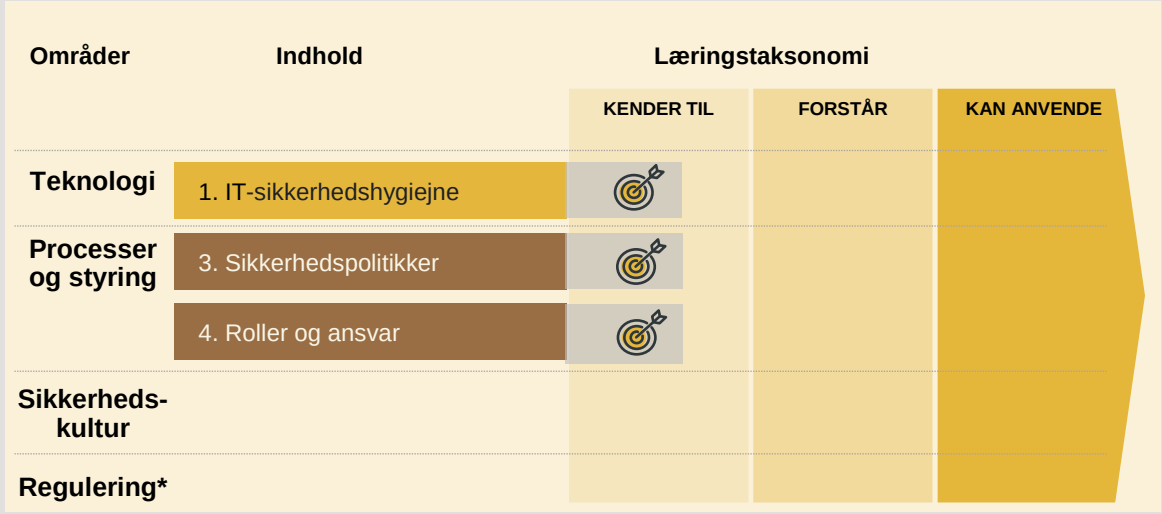
Kompetenceudviklingen skal fx give kursisterne

- Kendskab til grundlæggende IT-sikkerhedshygiejne og kommunens krav hertil
- Kendskab til overordnede principper i kommunens sikkerhedspolitik

Kompetenceudviklingen kunne være relevant for

Alle administrative medarbejdere.

Forslag til indhold og læringstaksonomi: Basal sikkerhed



* Der er behov for at medarbejdergruppen forstår den sektorlovgivning, der er relevant for at medarbejderne kan løse deres kerneopgave. Ofte vil være krav til behandling af data. Fordi der er stor variation på kravene på tværs af særlovgivninger, vil det være mere relevant at kompetenceopbygningen sker på anden vis end ved et basal kompetenceudviklingstilbud på området for informations- og cybersikkerhed.

Forslag til format: E-læring evt. suppleret med kampagner omkring digital svindel.

Varighed: For eksempel 30-45 minutter.

Forslag til udbydere: Uddannelsesinstitutioner eller private udbydere af kompetenceudvikling.

Trin to: Kompetenceudvikling med fokus på at **de væsentligste værktøjer og processer** inden for informations-, cyber- og IT-sikkerhed

Overordnet beskrivelse

Kompetenceudviklingstilbuddet skal give konkrete redskaber og værktøjer til at kunne understøtte arbejdet med informations- og cybersikkerhed i kommunerne i hverdagen. Kompetenceudviklingen kunne med fordel klæde deltagerne på til at kunne arbejde med konkrete værktøjer og metoder til at styrke sikkerheden lokalt i kommunerne.

Udbytte af kompetenceudviklingstilbud for kommunerne

- Fælles sprog omkring arbejdet med informations- og cybersikkerhed
- Flere medarbejdere vil kunne supportere og understøtte arbejdet med sikkerhed og styrke samarbejdet på tværs af administrative og tekniske faggrupper
- Løft af sikkerheden

Udbytte af kompetenceudviklingstilbud for kursisterne

- Blive fagligt klædt på til at varetage opgaver inden dagligdagsarbejde med informations- og cybersikkerhed. Det kunne fx være med udgangspunkt i ISO 27001-standarden.
- Få et netværk blandt kollegaer inden for feltet enten i egen kommune eller på tværs af kommunegrænser
- Blive inspireret til at arbejde med sikkerhed på en ny måde

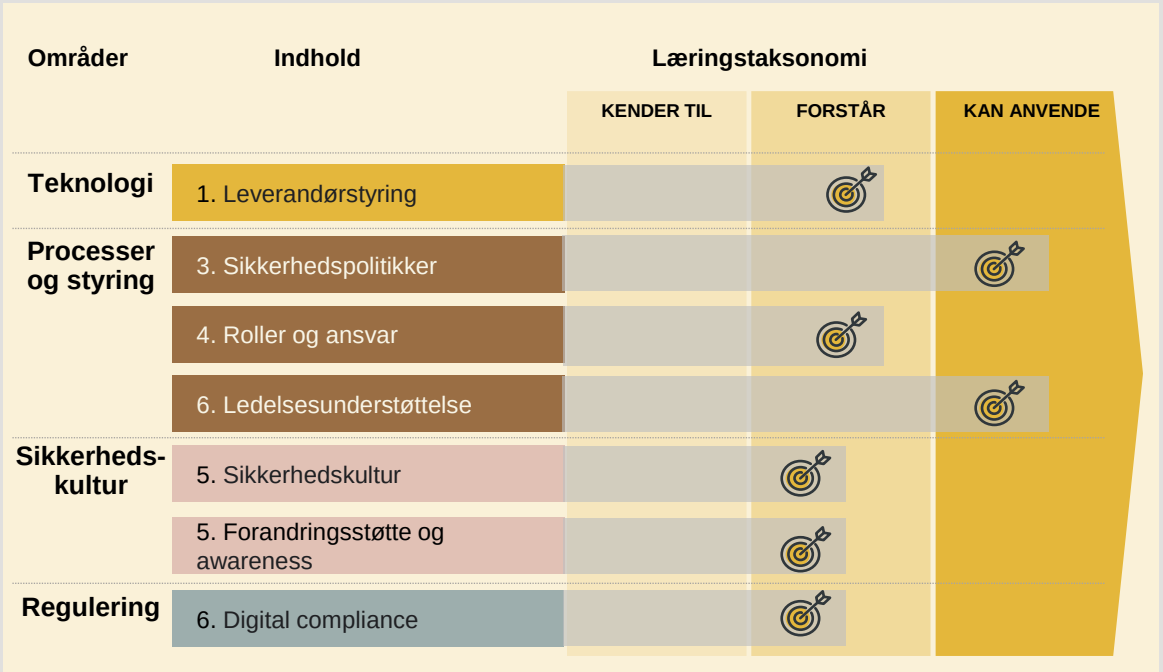
Kompetenceudviklingen skal fx give kursisterne

- Indblik i teori, metoder og værktøjer til at arbejde med informations- og cybersikkerhed i kommunerne
- Forståelse for organisering og hovedaktiviteter inden for fx risikostyring og beredskabsplanlægning
- Indsigt i hvordan man understøtter forandringsledelsesinitiativer lokalt på sin arbejdsplads

Kompetenceudviklingen kunne være relevant for

Administrative medarbejdere, der arbejder i kommunerne, som har specifikke organisatoriske arbejdsopgaver inden for informations- og cybersikkerhed. Det kunne være medarbejdere med et specifikt ansvar inden for GDPR, systemforvaltning eller informationssikkerhedskoordinatorer lokalt i forvaltninger, centre, institutioner eller tilbud.

Forslag til indhold og læringstaksonomi: Cyber- og informationssikkerhed i kommunerne



Forslag til format: Kompetenceudvikling på diplom eller akademiniveau med 5 ETCS-point. Alternativt kunne private kursusudbydere udbyde kurser med samme indholdsmæssige niveau dog uden, at kompetenceudviklingen giver deltagerne ETCS-point.

Varighed: For eksempel 4-10 dage

Forslag til udbydere: Uddannelsesinstitutioner eller private udbydere af kompetenceudvikling

Trin tre: Kompetenceudvikling med fokus på **de tekniske aspekter** af informations-, cyber- og IT-sikkerhed

Overordnet beskrivelse

Kompetenceudviklingstilbuddet skal give konkrete redskaber og værktøjer til at kunne understøtte det tekniske arbejde med informations- og cybersikkerhed i kommunerne. Kompetenceudviklingen kunne med fordel gå i dybden med de tekniske aspekter af sikkerhedsarbejdet og evt. tage udgangspunkt i de tekniske minimumskrav.

Udbytte af kompetenceudviklingstilbud for kommunerne

- Fælles sprog omkring arbejdet med teknisk sikkerhed
- Flere medarbejdere vil kunne supportere og understøtte arbejdet med teknisk sikkerhed og styrke samarbejdet på tværs af administrative og tekniske faggrupper
- Løft af sikkerheden

Udbytte af kompetenceudviklingstilbud for kursisterne

- Blive fagligt klædt på til at varetage opgaver inden for de tekniske discipliner af arbejdet med informations- og cybersikkerhed
- Få et netværk blandt kollegaer inden for feltet enten i egen kommune eller på tværs af kommunegrænser
- Blive inspireret til at arbejde med sikkerhed på en ny måde

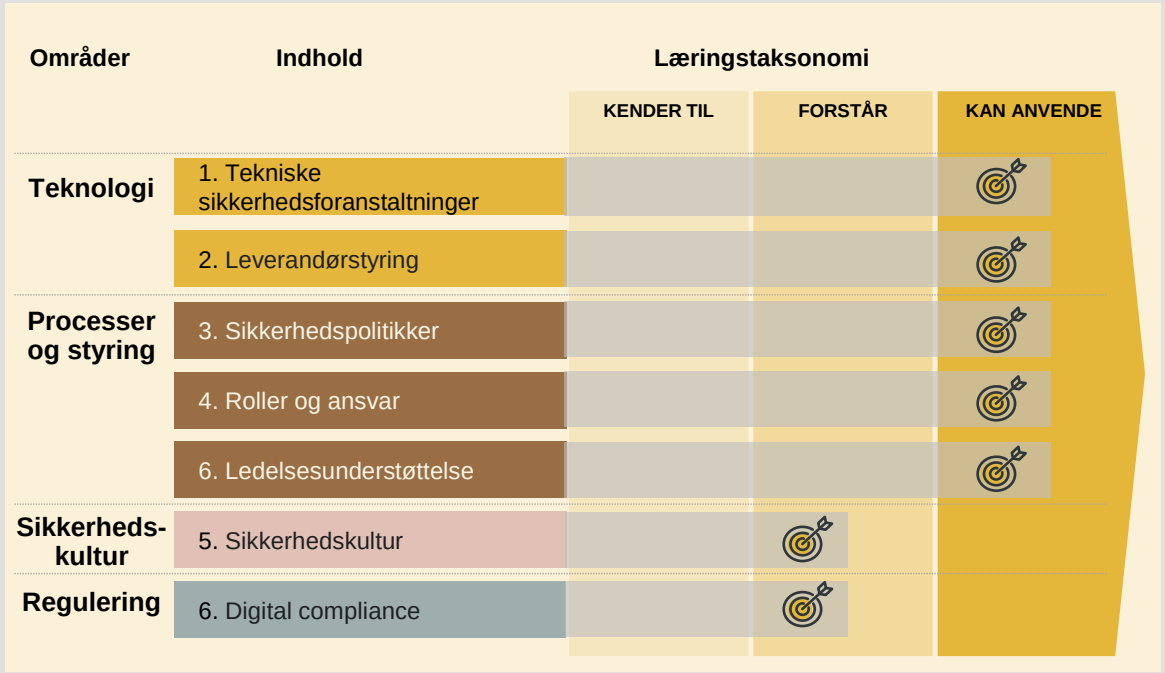
Kompetenceudviklingen skal fx give kursisterne

- Indblik i trusler og risikostyring
- Forståelse for organisering og hovedaktiviteter inden for beredskabsplanlægning
- Indsigt i IT-tekniske foranstaltninger såsom brugerstyring og tekniske minimumskrav

Kompetenceudviklingen kunne være relevant for

Administrative medarbejdere, der arbejder i kommunerne, som har specifikke tekniske arbejdsopgaver inden for informations- og cybersikkerhed. Det kunne være systemadministratorer, systemansvarligere, medarbejdere i IT- og digitaliseringsafdelinger eller medarbejdere i sikkerhedsafdelinger.

Forslag til indholdsområder og læringstaksonomi:
Teknisk cyber- og informationssikkerhed i kommunerne



Forslag til format: Kompetenceudviklingen kunne udbydes som på diplom eller akademiniveau med 5 eller 10 ETCS-point. Alternativt kunne private kursusudbydere udbyde kurser med samme indholdsmæssige niveau dog uden, at kompetenceudviklingen giver deltagerne ETCS-point.

Varighed: For eksempel 4-10 dage

Forslag til udbydere: Uddannelsesinstitutioner eller private udbydere af kompetenceudvikling.

Målgruppen peger på, at formatet for kompetenceudviklingstilbuddene er afgørende for deres succes

Målgruppebeskrivelse

Når uddannelsesinstitutioner eller kursusudbydere udarbejder kursusbeskrivelser, har deltagere i sparringsgrupperne peget på, at følgende kan være relevant at medtage eller tænke over:

- Fokus på GDPR og informationssikkerhed.
- Brede formuleringer som ”administrative medarbejdere” kan være svære at forholde sig til, derfor kan det ramme bedre med ord som systemadministratorer, systemejere, de der behandler personoplysninger.
- Fokus på, at man arbejder med kommunal drift.
- ”Fylder GDPR for meget hos jer?”
- Cybersikkerhed kan være svært at forstå. Derfor er det bedre at bruge ord som informationssikkerhed eller IT-sikkerhed.
- Det kan også yderligere være godt at gøre opmærksom på, at der er tale om andet og mere end et GDPR-kursus.
- En cathcy overskrift
- Få styr på lovgivning og regler
- ”Vil du være med til at passe på borgerne?”
- Tal ind i at man uddanner sig til at være fremtidens administrative medarbejder – en uddannelse til morgendagens jobs.
- Det er vigtigt, at målgruppen kan se sig selv i beskrivelserne, og at det er nært til deres hverdag og lokation.

Form på kompetencetilbuddet

Når uddannelsesinstitutioner eller kursusudbydere udbyder uddannelser eller kurser på området for informations- og cybersikkerhed, har sparringsgrupperne peget på, at det er værd at være opmærksom på følgende i forhold til formen på kompetenceudviklingstilbuddet:

- Fysisk undervisning foretrækkes, hvis det kan styrke et netværk med kollegaer, der arbejder inden for samme område og/eller inspirere til, hvordan andre arbejder med samme område som en selv.
- Blanding af virtuel og fysisk undervisning
- Det er godt med case-arbejde, hvis case-arbejdet er målrettet en kommunal kontekst.
- Der må gerne være en blanding af teori og praksis.
- Individuel forberedelse kan være fint, men det kan være svært at finde tid til.
- Eksamen kan afskrække. De fleste har peget på, at det er godt med en case-baseret eksamensform.
- Eksamen er vigtig for tilbuddet, men det skal ikke være én stor eksamen, så hellere flere små i løbet af forløb – gerne gruppeeksamen.
- Ikke krav om forudgående kompetencer.

Varighed

Når uddannelsesinstitutioner eller kursusudbydere udbyder uddannelser eller kurser på området for informations- og cybersikkerhed, har sparringsgrupperne peget på, at følgende kan indtænkes i forhold til varighed:

- Det er godt at undgå de store ferieperioder
- Generelt er det godt, hvis kompetenceudviklingen ligger i efteråret
- Det er fint, hvis kursusdagene er spredt ud. Det kan være svært at få tid til at tage flere dage ud på én uge.
- Der skal helst ikke være overnatning.
- Det må gerne følge den almindelige åbningstid i kommunen fx fra 8-15:30.
- Gerne halve dage

Andet

Når uddannelsesinstitutioner eller kursusudbydere udbyder uddannelser eller kurser på området for informations- og cybersikkerhed, har sparringsgrupperne peget på, at følgende andre perspektiver kan indtænkes:

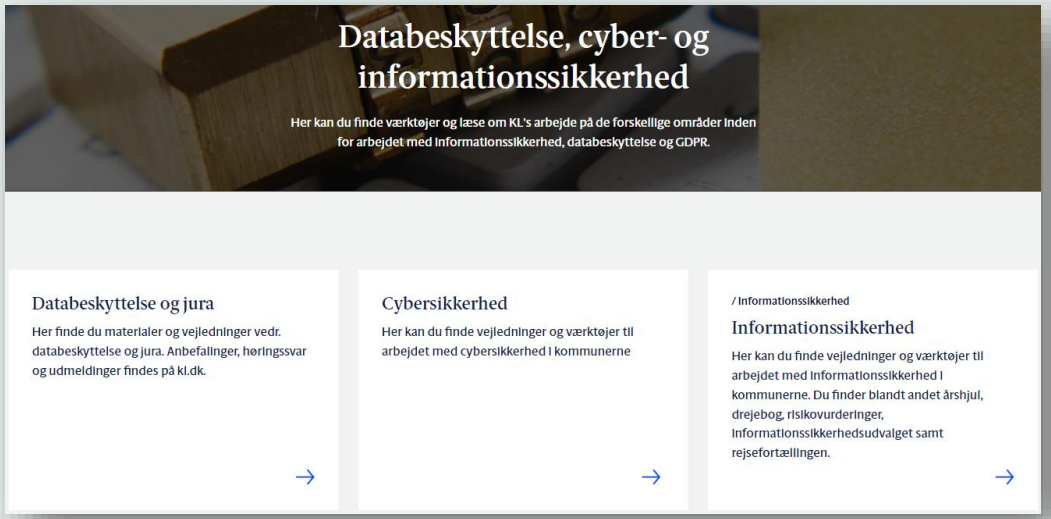
- Undervisningen må meget gerne være i et let forståeligt sprog, relaterbart og ikke ”jurasprog”.
- Undervisningen må meget gerne foregå lokalt – det skal være underviserne, der er de rejsende.
- Gerne to-delt forløb med overbygning afhængigt af målgruppe – foundation og practitioner
- Det er at foretrække, hvis undervisningen også understøtter dannelse af et netværk inden for området
- Pris er vigtigt (8000 DKK er for meget)
- Tid og ressourcer er mest afgørende for, om man kommer afsted
- ECTS-point kan godt spredes over længere periode, gerne modulopbygget
- ECTS-point kan både være plus og minus
- Der skal være mere viden til ledere, om hvordan de kan finansiere undervisningen.
- Mulighed for både åbne og lukkede kurser (for egen afdeling eller kommune)
- Vigtigt at tilbud er kompetencegivende/karrierefremmende

Kompetenceudviklingstilbud til administrative medarbejdere bør tage afsæt i allerede eksisterende materialer fra det fælleskommunale sikkerhedsprogram

Der er visse rammevilkår, som gælder for kommuner, når det kommer til informations- og cybersikkerhed. Det være sig lovgivning som fx GDPR og de forvaltningsretlige principper, men også rammevilkår i form af bedste praksis standarder og anbefalinger som fx ISO 27001 og de kommunale tekniske minimumskrav. Se bilag 2 for yderligere uddybning af rammevilkår.

Yderligere har kommunerne et særligt vilkår i at gå på tværs af sektorer og infrastrukturer for at kunne levere de nødvendige tilbud til borgerne samt at være organiseret i mange decentrale institutioner.

Derfor har KL i dialog med kommuner udviklet en række materialer i regi af det fælleskommunale sikkerhedsprogram, som er tilgængelige på KL's Videnscenter[1]. Det er afgørende, at fremtidige kompetenceudviklingstilbud tager afsæt i og bygger videre på det materiale, der er tilgængeligt her.



Særligt vigtige materialer fra det fælleskommunale sikkerhedsprogram

Databeskyttelsesforordningens dokumentationskrav[2]:

Anbefalinger til hvordan kommunerne lever op til de nye påvisnings- og dokumentationskrav i databeskyttelsesforordningen for at undgå over- eller underimplementering af kravene.

Tekniske minimumskrav[3]:

Anbefalinger til et sæt af minimumskrav, der bør implementeres i kommuner. Kravene er inspireret af de statslige tekniske minimumskrav, men er tilpasset kommunernes tætte kontakt med borgerne.

Drejebog: Beredskab for informationssikkerhed[4]:

Drejebogen giver en overordnet beskrivelse af, hvad et beredskab er og hvordan det styres, testes og implementeres. Der findes desuden en række skabeloner til dette.

1: https://videncenter.kl.dk/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed
2: https://videncenter.kl.dk/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed/databeskyttelse-og-jura/databeskyttelsesforordningens-dokumentationskrav
3: https://videncenter.kl.dk/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed/cybersikkerhed/tekniske-minimumskrav
4: https://videncenter.kl.dk/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed/cybersikkerhed/beredskab-for-cyber-og-informationssikkerhed

Andre opmærksomheds-punkter

Analysen har foruden opgavens kernefokus identificeret en række områder, som kan have relevans for succesen af kommunernes arbejde med informations- og cybersikkerhed fremadrettet. Det er fx at ledelserne på alle niveauer skal klædes på til at forstå og drive sikkerhedsarbejdet samt at organiseringen omkring sikkerhedsarbejdet med fordel kan være mere klart.

Analysen har foruden opgavens kernefokus identificeret en række områder, som kan have relevans for succesen af kommunernes arbejde med informations- og cybersikkerhed fremadrettet

Ledelsen skal med

Flere respondenter peger på, at ledelsen i en kommune er den mest afgørende faktor for, at informations- og cybersikkerhed behandles på tilfredsstillende manér.

I en virkelighed hvor ressourcerne i kommunerne er knappe, og der er mange vigtige dagsordener, der kæmper om opmærksomheden, bliver ledelsesopmærksomhed afgørende for, at medarbejderne kan prioritere at bruge deres tid på informations- og cybersikkerhed, herunder deltage i et kompetenceudviklingstilbud.

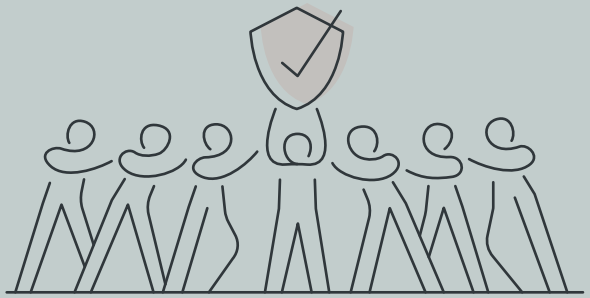
De peger også på, at opgaven med at understøtte ledelsen i at kunne involvere sig i informations- og cybersikkerhed, så ledelsen kan træffe de nødvendige beslutninger og prioriteringer, er vigtig og muligvis ikke højt nok prioriteret i dag. Flere respondenter peger på, at ledelsen mangler viden og kompetencer til at kunne spille den nødvendige aktive rolle på området.

Sikkerheden i kommunen er en fælles opgave

Flere respondenter nævner ønsket om en højere grad af sparring og samarbejde på tværs af kommuneskel, når det kommer til informations- og cybersikkerhed. Især udtrykkes der ønsker om fælles ressourcer.

Arbejdet med informations- og cybersikkerhed går i sin natur på tværs af systemer og infrastrukturer og dermed kommunegrænser, og det er derfor i en vis udstrækning en fælles opgave, at det samlede niveau for informations- og cybersikkerhed blandt kommuner er tilfredsstillende. Der er en høj grad af forbundethed og afhængighed af hinandens processer, systemer og modenhed, og derfor er samarbejde vigtigt.

Samtidig er der en tendens til, at medarbejdere på området oplever at sidde alene med opgaven, og at den er drevet af ildsjæle i kommunerne. Samarbejde kan dermed være med til at fostre det nødvendige netværk og sparring samt sikre et bedre fælles niveau for informations- og cybersikkerhed.

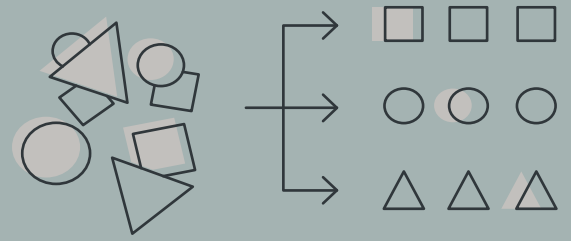


Mere klarhed om organisering, roller og ansvar

Arbejdet med informations- og cybersikkerhed i kommunerne har ifølge flere respondenter en tendens til at være organiseret en uformelt og på ad hoc basis. Det vil sige, at arbejdet til tider er drevet af ildsjæle, og at det har en høj grad af personafhængighed.

Flere respondenter peger derfor på, at et stærkere fælles sprog om informations- og cybersikkerhed samt mere fokus på formel organisering af sikkerhedsarbejdet ville styrke niveauet for informations- og cybersikkerhed i kommunerne og dermed for borgerne væsentligt.

Samtidig ville det give medarbejderne, der i dag har rollen med sikkerhed på mere uformel vis, lidt mere slagkraft over for organisationen og medarbejderne. Den mere formelle organisering og tildeling af rolle kunne reducere følelsen af at påtage sig ”politimand”-rollen på sin arbejdsplads og styrke dem i at støtte arbejdet bedst muligt.



Bilag 1. Oversigt over deltagere i projektet og materiale til erfaringsopsamling

Oversigt over deltagere i ekspertinterviews og sparringsgrupper

Projektet har fået input fra hele landet

Følgende funktioner har deltaget i sparringsgrupper

- Juridiske konsulenter
- Borgerservicemedarbejdere
- GDPR-koordinatorer
- I-sikkerhedskoordinatorer
- Informationssikkerhedskoordinatorer
- Fællestillidsrepræsentanter
- Skolesekretærer
- IT-chefer
- Lektorer
- Uddannelsesansvarlige
- IT-controllere
- IT-konsulenter
- PPR-medarbejdere

I alt har 29 personer deltaget i sparrings-grupperne

Følgende personer har deltaget i ekspertinterviews

Jette Larsson, Konsulent, KL
Christian Christensen, Programleder, KL
Thøger Terp, Chefkonsulent, Komponent
Lene Daugaard, HR-leder, Fredericia kommune
Anne C. Dandanell, Digitaliserings- og IT-chef, Kalundborg kommune
Bjarne Østergaard, Informationssikkerhedskoordinator, Kalundborg kommune
André Barsøe Jensen, Faglig studieansvarlig, UCL
Henning Mortensen, Formand, Rådet for Digital Sikkerhed
Morten Eeg Ejrnæs Nielsen, Sikkerhedsrådgiver, Globeteam

Materiale inkluderet i erfaringsopsamling, desk research

Materiale	Opdragsgiver
Arbejdsmarkedet for informationssikkerhed i Danmark (https://digst.dk/media/28840/arbejdsmarkedet-for-informationssikkerhedskompetencer-i-danmark-rapport.pdf)	Digitaliseringsstyrelsen, Erhvervsstyrelsen og Center for Cybersikkerhed
Model for digitale kompetencer i staten (https://digst.dk/styring/statens-digitaliseringsakademi/model-for-digitale-kompetencer/)	Digitaliseringsstyrelsen
Fremtidens digitale kompetencer (https://kl.digitalekompetencer.dk/)	KL
Fremtidens kompetencer til et digitalt arbejdsliv i kommunerne (https://www.kl.dk/media/0hilzgtl/fremtidens-kompetencer-til-et-digitalt-arbejdsliv-i-kommunerne.pdf)	KL
Digitalt kompetencebarometer fra Digitalt Dogme (https://media.graphassets.com/puAVA5vRcK1HR8iK31iw)	Digitalt Dogme
KL og COK's kompetenceprogram for digitale kompetencer (https://www.kl.dk/videncenter/viden-og-vaerktoejer/digital-transformation/kompetencer-og-digitalt-mindset/kl-og-coks-kompetenceprogram-for-digitale-kompetencer)	KL og Center for Offentlig Kompetenceudvikling (Komponent)
Kompetencer til et digitalt arbejdsliv i kommunerne (https://videnscenterportalen.dk/vtoe/wp-content/uploads/sites/5/2018/07/Kompetencekatalog.pdf)	Videnscenterportalen
Kommunernes IT- og digitaliseringsfunktion (https://vpt.dk/sites/default/files/2017-08/IT_kompetencer_KL_HK_rapport%20%28002%29.pdf)	HK kommunal og KL
ISO 27001, ISO 27002, ISO 27005	ISO/IEC
NIS2-direktivet, GDPR-forordningen	EU
NIST NICE-framework (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions)	NIST
NIST CSF-framework (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)	NIST
IDA-rapport "Cyber- IT- og informationssikkerhed - Har Danmark de rigtige kompetencer?" https://ida.dk/media/14371/ida-ekspertgruppe-rapport_cybersikkerhed_a4.pdf	IDA
D-mærket og NIS2 https://d-maerket.dk/events-og-artikler/brug-d-maerket-og-bliv-klar-nar-eu-strammer-reglerne-for-cybersikkerhed-med-nyt-nis2-direktiv/	D-mærket
Statens tekniske minimumskrav https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav	Digitaliseringsstyrelsen og Center for Cybersikkerhed
Kommuners tekniske minimumskrav https://www.kl.dk/videncenter/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed/cybersikkerhed/tekniske-minimumskrav	KL
Materialer fra KL's Sikkerhedsprogram https://videncenter.kl.dk/viden-og-vaerktoejer/databeskyttelse-cyber-og-informationssikkerhed	KL

Bilag 2. Uddybning af rammevilkår

Fokus på GDPR

Indhold

Hvad er GDPR?

GDPR* er en forordning vedtaget af EU for at beskytte fysiske personers personlige oplysninger og privatliv.

GDPR blev implementeret i maj 2018 og pålægger organisationer at sikre, at personoplysninger kun indsamles og behandles på en lovlig og gennemsigtig måde.

GDPR giver borgere ret til at indgive klager over databeskyttelsesovertrædelser og kræver, at organisationer rapporterer persondataretlige brud til Datatilsynet.

Overtrædelse af GDPR kan føre til store bøder; op til 20 millioner euro eller op til 4% af den årlige omsætning for en virksomhed, afhængigt af hvilket beløb der er størst.

Datatilsynet kan indstille både private aktører og offentlige myndigheder til bødestraf, dog er bødeniveauet for offentlige myndigheder generelt lavere end for private aktører.

Hvorfor er GDPR relevant for kommuner?

GDPR og Datatilsynets afgørelser har betydet en markant omvæltning for, hvordan kommuner arbejder og udfører deres opgaver.

Datatilsynet har i flere tilfælde truffet konkrete afgørelser i sager omkring kommuners brud på persondatasikkerhed[1].

Der kan derfor ikke være tvivl om, at GDPR har afgørende betydning for, hvordan kommuner arbejder og hvilke kompetencer, der dermed er behov for blandt medarbejderne.

* General Data Protection Regulation
1: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jan/tilsyn-med-kommuner-om-sikkerheden-i-aula og https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/sep/nye-afgoerelser-16-tilsyn-med-kommuners-og-bankers-haandtering-af-brud-

Oversigt over krav

Hvilke krav stiller GDPR?

- Organisationen skal udarbejde en fortegnelse over behandlinger af personoplysninger
- Organisationen skal risikovurdere deres behandlingsaktiviteter og foretage særlige konsekvensanalyser, hvor der er en høj risiko for de fysiske personer (de registrerede)
- Der skal være et lovligt formål (et hjemmelsgrundlag) for samtlige behandlingsaktiviteter
- Organisationen skal i visse tilfælde sikre, at der indhentes samtykke fra de fysiske personer, før deres personlige oplysninger behandles
- Organisationen skal sikre tilstrækkelig beskyttelse af personoplysninger gennem passende organisatoriske og tekniske sikkerhedsforanstaltninger
- Fysiske personer skal informeres om, hvordan deres data vil blive behandlet
- Fysiske personer har ret til at få indsigt i behandlingen, få berigtiget oplysninger og slettet deres personoplysninger
- Databrud skal rapporteres til Datatilsynet inden for 72 timer
- Organisationens medarbejdere skal trænes, så de GDPR-retlige forpligtelser kan overholdes

Fokus på forvaltningsretlige principper

Indhold

Hvad er de forvaltningsretlige principper ?

Forvaltningsretten er det juridiske område, der regulerer forholdet mellem borgere og offentlige myndigheder.

De forvaltningsretlige principper er grundlæggende for at sikre en ansvarlig og transparent offentlig forvaltning. Principperne gælder for alle forvaltningsmyndigheder såsom kommuner.

Principperne omfatter bl.a. retssikkerhed, lighed, proportionalitet, saglighed og god forvaltningsskik.

Hvis myndigheder bryder med principperne kan det resultere retlige konsekvenser såsom retssager, erstatningsansvar eller kritik fra Folketingets Ombudsmand.

Folketingets Ombudsmand kan kritisere og anbefale myndigheder at behandle en sag igen og eventuelt ændre deres afgørelse, men Ombudsmanden kan ikke selv træffe afgørelser.

Hvorfor er de forvaltningsretlige principper relevante for kommuner, når det kommer til sikkerhed?

Forvaltningsretten og dermed de forvaltningsretlige grundprincipper udgør rygraden i dansk offentlig forvaltning og er afgørende for, hvordan kommuners arbejde er struktureret og styret.

Ombudsmanden har ved mange lejligheder har udtalt, at IT-systemer skal overholde de forvaltningsretlige principper, hvilket understreger vigtigheden af at arbejde systematisk med IT-sikkerhed og infromationssikkerhed[1].

I en virkelighed hvor kommunernes arbejde og services gennemgår en øget grad af digitalisering, og hvor nye angrebsflader og trusler opstår, vil de forvaltningsretlige grundprincipper også være styrende for, hvordan kommuner indretter deres arbejde med informations- og cybersikkerhed ift. borgerne.

1: https://www.ombudsmanden.dk/findviden/fob-artikler/it-loesninger/

Oversigt over krav

Hvilke principper er væsentlige ift. sikkerhed?

- **Retssikkerhedsprincippet** kan indebære, at myndigheder skal sikre, at borgerne er informeret om sikkerhedspolitikker og -procedurer relateret til håndtering af persondata og andre følsomme oplysninger.
- **Lighedsprincippet** kan forpligte myndighederne til at sikre, at cybersikkerhedstiltag beskytter alle borgere lige og uden forskelsbehandling, og at alle har lige adgang til at få deres informationer beskyttet af offentlige sikkerhedsprotokoller.
- **Proportionalitetsprincippet** kan kræve, at sikkerhedsforanstaltninger, myndighederne iværksætter, står i forhold til de trusler, de er designet til at imødegå. Dette betyder, at sikkerhedsforanstaltningerne ikke må være mere indgribende end nødvendigt og skal balancere behovet for sikkerhed med borgernes rettigheder og friheder.
- **God forvaltningsskik** indebærer, at myndighederne udøver deres handlinger med en høj grad af kompetence, retfærdighed og respekt for borgernes digitale rettigheder, herunder retten til privatliv og datasikkerhed.
- **Saglighedsprincippet** betyder, at myndighederne skal basere deres handlinger og beslutninger vedrørende cybersikkerhed på et sagligt og lovmæssigt grundlag, hvor personlige data og systemintegritet beskyttes i henhold til relevante love og bestemmelser.

Fokus på NIS2

Indhold

Hvad er NIS2?

NIS 2-direktivet* er et EU-dækkende direktiv på informations- og cybersikkerhedsområdet, som medfører nye juridiske krav til at fastsætte et minimumsniveau for cybersikkerhed i EU.

NIS 2-direktivet erstatter og ophæver det oprindelige EU direktiv NIS**.

NIS 2 etablerer en risikobaseret tilgang til cybersikkerhed og opstiller væsentlige sanktioner for overtrædelser.

Direktivet trådte i kraft den 16. januar 2023, og omfattede organisationer skal efterleve det senest den 18. oktober 2024.

Hvorfor er NIS2 relevant for kommuner?

Forsvarsministeriet meldte 5. feb. 2024 ud[1], at de danske regler vedr. NIS2 bliver forsinket med ca. to måneder efter EU's frist for implementering i dansk ret. Det er derfor usikkert, hvornår de danske regler præcist gælder fra.

Ligeledes er det ikke afgjort, i hvilken udstrækning danske kommuner vil være omfattet af direktivet. Dog vil NIS 2 under alle omstændigheder berøre enheder, der leverer tjenester eller udfører aktiviteter på tværs af en lang række sektorer – herunder fx spildevand, offentlig administration og sundhed. I det omfang kommunen udfører sådanne opgaver, bliver i hvert fald disse dele af forvaltningen omfattet.

Selv hvis kommuner ikke vil være formelt omfattet, vil det være at anse som best practice, at kommunerne følger kravene fra NIS 2 meget nært. Dette grundet naturen af kommunernes opgaver og services. Disse digitaliseres i øget grad, hvilket betyder nye typer af trusler og angrebsflader, som medarbejdere i kommuner skal arbejde struktureret og effektivt med.

En risikobaseret tilgang – som NIS2 foreskriver – sikrer, at kommunerne arbejder effektivt med de sikkerhedsudfordringer, der opstår. Det sikrer, at der hverken over- eller underimplementeres sikkerhedsforanstaltninger.

* Direktiv 2022/2555 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen.
** Direktiv 2016/1148/EF om netværks- og informationssystemer
1: https://www.fmn.dk/da/nyheder/2024/nye-regler-om-cybersikkerhed-bliver-forsinkede/

Oversigt over krav

Hvilke krav stiller NIS2?

- Risikoanalyse og informationssystemsikkerhedspolitikker
- Hændelseshåndtering
- Forretningskontinuitet, såsom backupstyring, reetablering efter en katastrofe og krisestyring
- Sikkerhed i forsyningskæden, herunder hver enheds direkte leverandører eller tjenesteudbydere
- Sikkerhed ved erhvervelse, udvikling og vedligeholdelse; sårbarhedshåndtering og offentliggørelse
- Politikker og procedurer til at vurdere effektiviteten af risikostyringsforanstaltninger
- Grundlæggende computerhygiejnepraksis og cybersikkerhedstræning
- Politikker og procedurer for brug af kryptografi og kryptering
- Personalesikkerhed, adgangskontrolpolitikker og asset management
- MFA eller kontinuerlige autentificeringsløsninger; sikret stemme-, video- og tekstkommunikation
- Ledelsen skal følge regelmæssig færdigheds- og videnbaseret træning i cybersikkerhedsrisici

Fokus på ISO 27001

Indhold

Hvad er ISO 27001?

ISO 27001* er en international standard til etablering af et ledelsessystem for styring af informationssikkerhed i en organisation.

ISO 27001 er en del af 27000-serien, som består af en række standarder med indbyrdes relationer. Eksempelvis indeholder ISO 27002 en liste af foranstaltninger, der kan bruges som hjælp ved udvælgelsen og implementeringen af de kontroller, der er nødvendige for at opnå passende informationssikkerhed i en given organisation. ISO 27005 indeholder retningslinjer for risikovurdering og styring.

ISO 27001 lægger vægt på en risikobaseret og struktureret tilgang til sikkerhedsarbejdet.

Organisationer kan blive certificeret efter ISO 27001.

Hvorfor er ISO 27001 relevant for kommuner?

Statslige myndigheder har siden 2016 været forpligtet til at implementere ISO 27001. Kommuner har ikke samme forpligtelse men er jf. Den fællesoffentlige digitaliseringsstrategi forpligtet til at følge principperne i ISO 27001[2].

Således bliver kommuner ikke formelt målt på deres implementering med tilsyn til følge.

Dog har flere kommuner af egen drift valgt at implementere ISO 27001 i deres daglige arbejde, da standarden kan anses som en best practice tilgang til sikkerhedsarbejdet. For selvom kommuner ikke er formelt forpligtede stiller kommunernes øgede digitalisering krav til, at der arbejdes systematisk med sikkerhedsudfordringer.

Den strukturerede og risikobaserede tilgang, som ISO 27001 lægger vægt, sikrer at kommuner arbejder systematisk med deres risici og kommer hele vejen rundt.

Oversigt over krav

Hvilke kravområder indeholder ISO 27001[3]?

- Organisations kontekst
- Lederskab
- Planlægning
- Support
- Drift
- Evaluering
- Løbende forbedringer
- Leverandørstyring
- Beredskabsplaner

* ISO/IEC 27001:2023
1: https://fm.dk/media/25359/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf
2: https://digst.dk/media/12023/71-styr-paa-informationssikkerhed-i-alle-myndigheder-aftalepapir.pdf
3: ISO 27001 indeholder 10 klausuler og 93 foranstaltninger. De summerede områder er taget fra spørgeområderne i den årlige statslige ISO 27001-modenhedsmåling. De er primært udarbejdet pba. kapitel 4-9 og anneks a.

Fokus på de tekniske minimumskrav

Indhold

Hvad er de tekniske minimumskrav?

De tekniske minimumskrav til kommuner udgør nogle anbefalinger til tekniske tiltag, som kan give basis for god beskyttelse af kommunens IT-infrastruktur og borgernes oplysninger.

De kommunale minimumskrav er inspireret af de tekniske minimumskrav til statslige myndigheder, men er i samarbejde med en række kommuner tilpasset kommunernes tætte kontakt med borgerne.

De oprindelige statslige minimumskrav tager afsæt i vejledninger fra Digitaliseringsstyrelsen, Center for Cybersikkerhed og Datatilsynet eller er udtryk for alment anerkendt best practice.

Hvorfor er de tekniske minimumskrav relevante for kommuner?

Anbefalingerne er et værktøj, der kan støtte kommuner i at vurdere, hvad der er et tilstrækkeligt minimumsniveau for teknisk sikkerhed, herunder beskyttelse af IT-udstyr og netværk.

Anbefalingerne kan dermed bidrage til kommunens arbejde med at beskytte medarbejdere og borgeres oplysninger mod at blive kompromitteret eller misbrugt.

Anbefalingerne er minimumsstandarder, og derfor er det stadig relevant, at den enkelte kommune går risikobaseret til værks ift. det daglige sikkerhedsarbejde og evt. implementerer yderligere tekniske sikkerhedstiltag.

Oversigt over krav

Hvad er de overordnede kategorier for de tekniske minimumskrav?

- PC'er/klienter
- Mail
- Autentifikation
- Mobile enheder
- Logning
- Domæner
- Netværk
- Diverse

Bilag 3. Uddybning af kompetenceprofiler

Kompetenceprofil 1:

Administrativ medarbejder **uden specifikke opgaver** inden for informations- og cybersikkerhed

Eksempler på typiske arbejdsopgaver

Administrative medarbejdere uden specifikke opgaver inden for informations- og cybersikkerhed kan være ansat i forskellige tilbud, institutioner eller enheder og udføre forskellige funktioner afhængigt af deres specifikke rolle og ansvarsområder. De udfører en bred vifte af opgaver, der understøtter den daglige drift og service til borgere. Her er listet nogle typiske eksempler

Indirekte borgerbetjening:

- Understøtter at der kan leveres service til kommunens borgere ved at besvare spørgsmål, håndtere henvendelser og yde vejledning om kommunale tjenester, programmer og procedurer.

Administrativ støtte:

- Giver administrativ støtte og assistance på skoler, biblioteker, plejehjem og sociale tilbud.
- Håndterer indgående og udgående korrespondance, koordinering af møder og arrangementer og opdaterer dokumenter.

Budget- og regnskabsstyring:

- Assisterer med budget- og regnskabsstyring inden for deres enhed eller afdeling.
- Behandler fakturaer og udlæg.
- Opdaterer budgetdata og hjælper med rapportering af finansielle oplysninger.

Personaleadministration:

- Behandler ansættelsesdokumenter, registrerer fravær og opdaterer personalesager for medarbejdere i deres enhed.

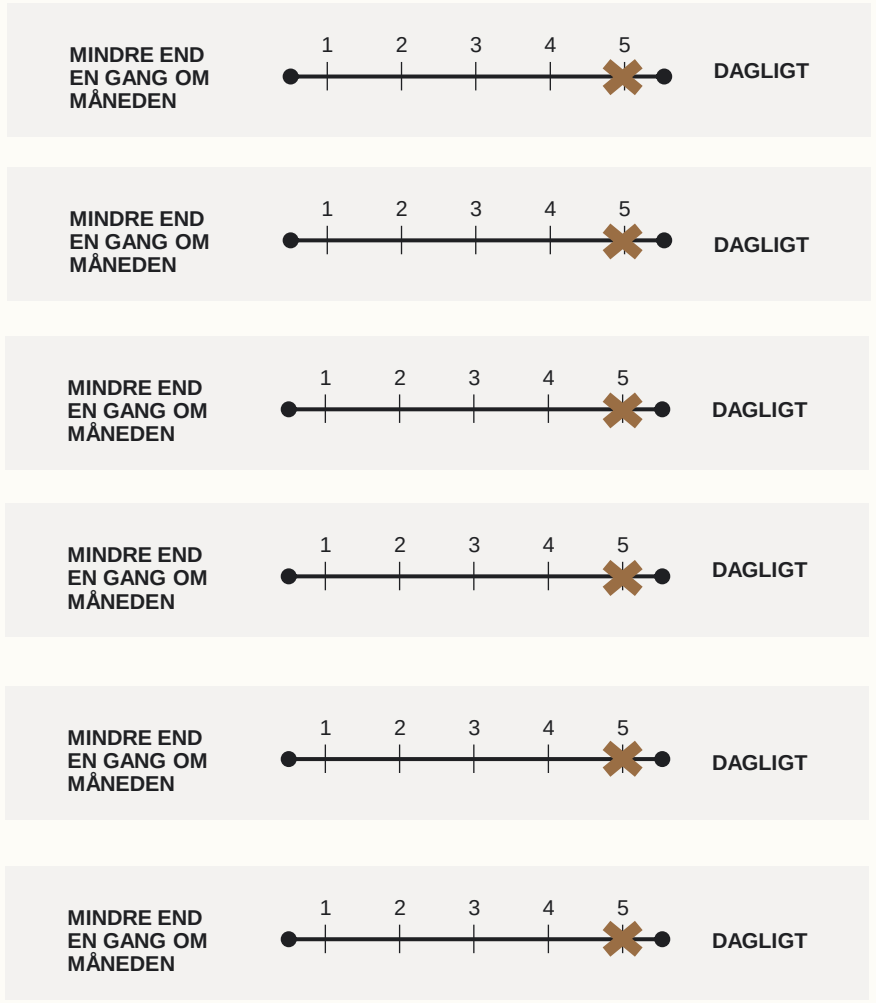
Direkte borgerbetjening:

- Sagsbehandling og afgørelser inden for specifikke fagområder som fx miljø-/teknikområdet, beskæftigelsesområdet og socialområdet.

Kommunikation og information:

- Bidrager til kommunikation og information ved at opdatere hjemmesider, sociale medier og informationsmaterialer med relevante oplysninger om kommunale tilbud, begivenheder og nyheder.

Hvor ofte arbejder profilen med arbejdsopgaven?



Kompetenceprofil 1:

Administrativ medarbejder **uden specifikke opgaver** inden for informations- og cybersikkerhed

Eksempler på typiske sikkerhedsrelaterede opgaver

Administrative medarbejdere i uden specifikke opgaver på området for informations- og cybersikkerhed har ansvar for at udføre egen praksis så det lever op til kommunens krav om sikkerhed. Det omfatter også almindelig god praksis for cyber-hygiejne. Nogle af disse opgaver inkluderer:

Databeskyttelse og fortrolighed:

- Håndterer følsomme oplysninger, korrespondancer og dokumenter på vegne af kommunens ledelse.
- Sikrer at fortrolige oplysninger behandles og opbevares sikkert i overensstemmelse med gældende regler og politikker.

Fysisk sikkerhed:

- Skal bidrage til at opretholde fysisk sikkerhed på kontoret eller i de institutioner, de arbejder i. Dette kan omfatte at overholde kommunens retningslinjer, når det kommer til adgangskontrol og brug af egne devices som PC'er og mobiltelefoner.

Cyber-hygiejne:

- Skal overholde kommunens retningslinjer om god cyber-hygiejne. Det kan fx være at deltage i obligatoriske kurser i grundlæggende sikkerhed, holde adgangskoder sikre, bruge multifaktorgodkendelse, opdatere computere regelmæssigt, holde øje med digital svindel eller være opmærksomme på brug af wifi uden for arbejdspladsen.

Hvor ofte arbejder profilen med arbejdsopgaven?

MINDRE END EN GANG OM MÅNEDEN 1 2 3 4 5 **DAGLIGT**

MINDRE END EN GANG OM MÅNEDEN 1 2 3 4 5 **DAGLIGT**

MINDRE END EN GANG OM MÅNEDEN 1 2 3 4 5 **DAGLIGT**

Kompetenceprofil 2:

Administrativ medarbejder **med specifikke organisatoriske opgaver** inden for informations- og cybersikkerhed

Eksempler på typiske arbejdsopgaver

Administrative medarbejdere med specifikke organisatoriske opgaver inden for informations- og cybersikkerhed kan arbejde i centrale funktioner på rådhuse, i forvaltninger/centre eller i tilbud eller institutioner. Ud over deres kerneopgave har de en specifik (ambassadør)rolle inden for fx systemforvaltning, risikostyring og brugerstyring.

Koordinering af møder og arrangementer:

- Bidrager til planlægning, organisering og koordinering af møder og arrangementer.

Korrespondance og kommunikation:

- Håndterer indgående og udgående korrespondance på vegne af kommunens ledelse,
- Koordinerer information mellem forskellige afdelinger og interessenter.

Dokumenthåndtering og arkivering:

- Sikrer at vigtige dokumenter, rapporter og referater fra møder bliver korrekt arkiveret og opbevaret.

Støtte til ledelsesbeslutninger:

- Assisterer ledelsen ved at forberede dokumenter, præsentationer og rapporter, der er nødvendige for beslutningstagning.

Opfølgning på opgaver og beslutninger:

- Følger op på igangværende opgaver, projekter og beslutninger, der er prioriteret i kommunen.
- Holder styr på tidsfrister, opdaterer statusrapporter og sikrer, at relevante interessenter bliver informeret om fremdriften.

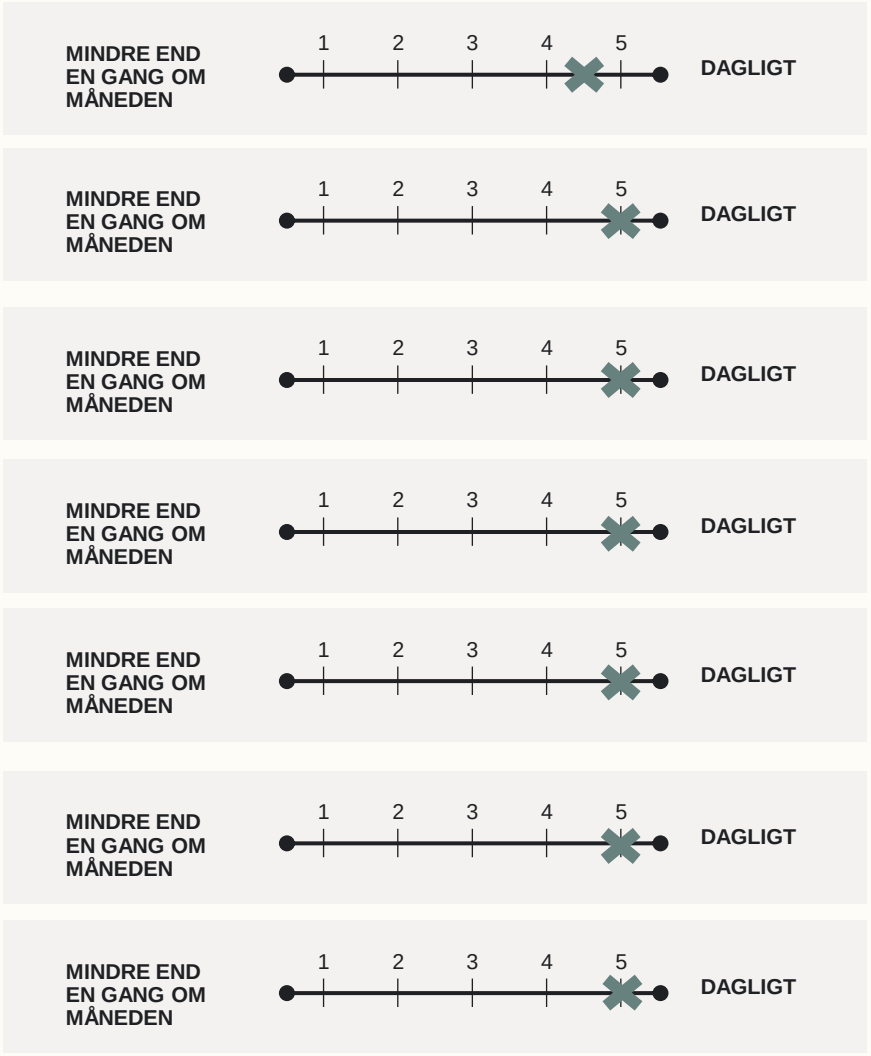
Generel administrativ support:

- Yder generel administrativ support til kommunens ledelse og andre medarbejdere, herunder håndtering af indgående henvendelser, opdatering af kontakter og koordinering af interne ressourcer.

Økonomiopgaver:

- Bidrager til at skabe budgetoverblik og føre tilsyn med overførsler.

Hvor ofte arbejder profilen med arbejdsopgaven?



Kompetenceprofil 2:

Administrativ medarbejder **med specifikke organisatoriske opgaver** inden for informations- og cybersikkerhed

Eksempler på typiske sikkerhedsrelaterede opgaver

Administrative medarbejdere med specifikke organisatoriske opgaver inden for informations- og cybersikkerhed har ud over deres kerneopgave fået tildelt en specifik opgave inden for cyber– og informationssikkerhed. Nogle af disse opgaver inkluderer:

Databeskyttelse og fortrolighed:

- Håndterer følsomme oplysninger, korrespondancer og dokumenter på vegne af kommunen.
- Sikrer at fortrolige oplysninger behandles og opbevares sikkert i overensstemmelse med gældende regler og politikker.

Sikkerhedspolitikker:

- Understøtter implementering af sikkerhedspolitikker på kontoret eller i sekretariatet.
- Bidrager til at der rapporteres til ledelsen/sikkerhedsudvalget omkring implementering af organisatoriske foranstaltninger.

Nødsituationer og krisestyring:

- Hjælper med at implementere krise- og beredskabsplaner samt nødprocedurer, herunder at følge instruktioner fra sikkerhedspersonale, evakuere kontoret, og informere ledelsen og andre medarbejdere om situationen.

Fysisk sikkerhed:

- Bidrager til at opretholde fysisk sikkerhed på kontoret, herunder at rapportere mistænkelig adfærd, sikre at døre og vinduer er låst og at der er adgangskontrol på kontorlokaler og arkiver.

Ledelsesunderstøttelse:

- Understøtter planlægning, organisering, koordinering, dokumentation og opfølgning på møder i ledelsen/sikkerhedsudvalget for at sikre, at der træffes effektive beslutninger.

Hvor ofte arbejder profilen med arbejdsopgaven?

MINDRE END EN GANG OM MÅNEDEN	1 2 3 4 **5**	DAGLIGT
MINDRE END EN GANG OM MÅNEDEN	**1** 2 3 4 5	DAGLIGT
MINDRE END EN GANG OM MÅNEDEN	**1** 2 3 4 5	DAGLIGT
MINDRE END EN GANG OM MÅNEDEN	1 2 **3** 4 5	DAGLIGT
MINDRE END EN GANG OM MÅNEDEN	1 **2** 3 4 5	DAGLIGT

Kompetenceprofil 3:

Administrativ medarbejder **med specifikke tekniske opgaver** inden for informations- og cybersikkerhed

Eksempler på typiske arbejdsopgaver

Administrative medarbejdere med specifikke tekniske opgaver inden for informations- og cybersikkerhed udfører en række opgaver, der understøtter sikker daglige drift og vedligehold af kommunens IT-systemer og -infrastruktur. Her er nogle eksempler på typiske opgaver

Brugerstøtte og helpdesk:

- Leverer brugerstøtte og håndterer helpdesk-anmodninger fra kommunens medarbejdere.
- Besvarer spørgsmål, løser tekniske problemer og yder vejledning til brug af IT-systemer og -software.

Dokumentation og registrering:

- Opretholder dokumentation og registrering af IT-systemer, infrastruktur og brugeroplysninger.
- Opdaterer brugerprofiler, licensoplysninger og systemkonfigurationer.

Systemovervågning og fejlfinding:

- Deltager i overvågning og fejlfinding af IT-systemer og netværk for at identificere og løse potentielle problemer eller nedbrud.
- Analyserer logfiler, udfører systemkontroller og implementerer løsninger for at minimere nedetid og forbedre ydeevnen.

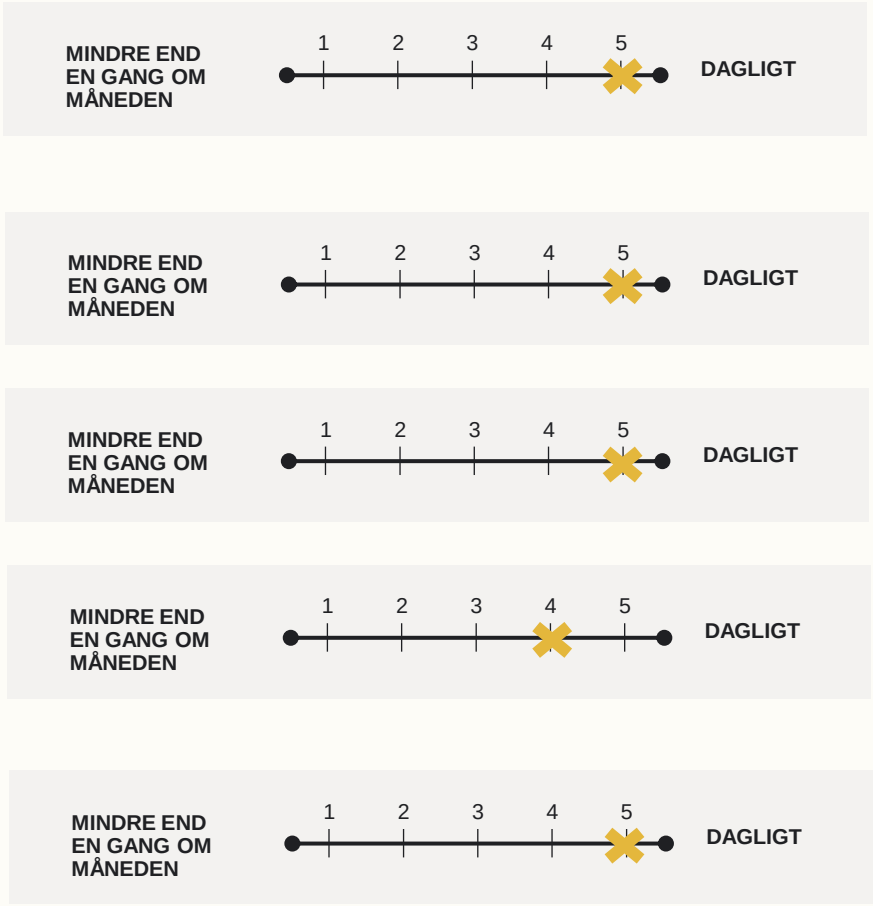
Softwareinstallation og opgradering:

- Installerer, konfigurerer og opgraderer software på kommunens enheder og systemer.
- Understøtter udrulning af sikkerhedsopdateringer, patches og nye applikationer i overensstemmelse med kommunens politikker og procedurer.

Backup og Data Recovery:

- Bidrager til at sikre, at der er effektive backup- og datagendannelsesprocedurer på plads for at beskytte kommunens data mod tab.
- Sikkerhedskopierer regelmæssigt data, tests af gendannelsesprocedurer, og opbevaring af backupmedier i sikre faciliteter.

Hvor ofte arbejder profilen med arbejdsopgaven?



Kompetenceprofil 3:

Administrativ medarbejder **med specifikke tekniske opgaver** inden for informations- og cybersikkerhed

Eksempler på typiske sikkerhedsrelaterede opgaver

Administrative medarbejdere med specifikke tekniske opgaver inden for informations- og cybersikkerhed i kommunerne udfører flere opgaver inden for sikkerhed for at beskytte kommunens IT-systemer, data og netværk mod potentielle trusler og sikkerhedsbrud. Nogle af de opgaver, de typisk udfører, inkluderer:

Databeskyttelse og fortrolighed:

- Sikrer at fortrolige oplysninger behandles og opbevares i overensstemmelse med gældende regler og politikker.
- Sikrer oplysningspligt og samtykke.
- Understøtter overholdelsen af slettepolitikker og bidrager til fortegnelser.

Implementering og vedligeholdelse af sikkerhedspolitikker:

- Hjælper med at implementere og vedligeholde sikkerhedspolitikker og -procedurer for at sikre, at IT-systemer overholder sikkerhedsstandarder og retningslinjer.

Adgangsstyring og brugerrettigheder:

- Administrerer og følger op på brugerkonti og –rettigheder.
- Tildeler og administrerer adgang til brugere til forskellige IT-ressourcer og -systemer.

Netværkssikkerhed:

- Bidrager til at sikre, at kommunens netværk er beskyttet mod eksterne trusler og indtrængende.
- Implementerer firewall- og intrusion detection-systemer, overvåger netværkstrafik og håndterer sikkerhedshændelser.

Sikkerhedspatches og opdateringer:

- Hjælper med at installere og håndtere sikkerhedsopdateringer og patches på kommunens IT-systemer og -applikationer for at lukke kendte sårbarheder.

Sikkerhedskopier og katastrofeberedskab:

- Hjælper med at sikre, at der er effektive backup- og katastrofe-beredskabsplaner på plads for at sikre, at kritiske data og systemer kan gendannes i tilfælde af en katastrofe eller hændelse.

Indkøb af IT og leverandørsamarbejde:

- Understøtter afdækning og udbud ifm. indkøb og understøtter det efterfølgende samarbejde med leverandører, herunder kontraktstyring, revisionserklæringer og databehandleraftaler.

Hvor ofte arbejder profilen med arbejdsopgaven?