

1. Hoveddokument

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 | Version 1.3



Conscia
Secure progress

De samlede dokumenter er udarbejdet som et arbejds- og referencegrundlag. Videreformidling, kopiering eller anvendelse i andre sammenhænge bør ske med omtanke og med kendskab til dokumentets formål og kontekst. Eventuelle udskrifter betragtes som ukontrollerede.

Indhold

1	Executive Summary	3
2	Introduktion	5
2.1	Grundlæggende opgave og fælles ambition	5
2.2	De tekniske målbilleder.....	6
2.3	Vision: Det resiliente driftscenter	6
2.3.1	Resiliens som arkitektonisk og organisatorisk disciplin.....	8
3	Teknisk målbillede	9
3.1	Arkitekturprincipper – fælles retning og styrende rammer.....	9
3.2	Sikkerhed – fælles modenhed og tydeligt ansvar	10
3.3	Driftsplatform – robusthed, forudsigelighed og skalerbar drift	11
3.4	LAN/WAN – fælles fundament for decentral virkelighed.....	12
3.5	Compliance – operationaliseret ledelsesansvar	13
3.6	AI i relation til det tekniske målbillede.....	13
4	Transition – kontrolleret overgang til fælles drift.....	15
4.1	Faseopdelt overgang.....	15
4.2	Sammenhæng til det tekniske målbillede	16
4.3	Tværgående styring og governance	16
4.4	Roller og ansvar.....	17
4.4.1	Eksempel på RACI.....	17
4.5	Transition som fundament for videre udvikling.....	18
5	Transformation – kontinuerlig udvikling og modenhed	19
5.1	Fælles standarder og lokal anvendelse	20
5.2	Samspil med transition	20
5.3	Ledelsesmæssig betydning.....	20
6	Næste skridt – hvordan kommer vi videre?.....	21

Dette dokument bygger på de arkitekturprincipper, der er fastlagt i hoveddokumentet, og som er kvalificeret gennem en analyse- og workshopfase med deltagelse fra relevante kommunale aktører. Principperne afspejler dermed både et fagligt perspektiv og de erfaringer og behov, der er identificeret på tværs af kommunerne.

Dokumentet består af udvalgte arkitekturprincipper og tilhørende anbefalinger baseret på erfaringer, analyser, best practice og standarder, som vurderes at være centrale for at understøtte en stabil, sikker og robust fælleskommunal IT-drift.

Dokumentet er et fagligt udgangspunkt for det videre arbejde med at etablere en konkret arkitektur og implementeringsplan i den enkelte IT-serviceorganisation. Dette arbejde forudsætter lokal tilpasning og skal gennemføres i samspil med ejerkommunerne samt med inddragelse af eksisterende producenter og leverandører, hvor det er relevant.

Det endelige ambitionsniveau for sikkerhed, drift og servicemodel fastlægges af den enkelte IT-serviceorganisation på baggrund af ejerkommuners behov, prioriteringer og risikovurderinger.

1 Executive Summary

Cybersikkerhed skal hæves i kommunerne. Det ønske blev formuleret som et mål i økonomiaftalen for 2026 mellem regeringen og KL. Det centrale organisatoriske greb i aftalen er, at IT-driften i de 98 kommuner skal konsolideres i 4-5 IT-serviceorganisationer. Aftalen indeholder 2 centrale milepæle. Pr. 1/1 2027 skal IT-serviceorganisationerne være dannet. Pr. 31/12 2027 skal IT-serviceorganisationerne have overtaget driften.

Materialet er udarbejdet af Conscia Danmark A/S på opdrag fra KL. KL er opdragsgiver og programansvarlig, mens Conscia er faglig afsender på de beskrevne vurderinger, sigtelinjer og arkitekturprincipper.

Etableringen af fælles IT-serviceorganisationer er en væsentlig ledelses-, styrings- og sikkerhedsopgave, hvor fælles drift kan skabe bedre forudsætninger for højere cybersikkerhed og mere effektiv ressourceudnyttelse, men også stiller større krav til arkitektur, governance og klare ansvarsforhold.

I august 2025 etablerede KL et nationalt program for at understøtte opstart og overblik af opgaven. En opgave var en as-is-analyse, der viste et komplekst og fragmenteret IT-landskab, særligt inden for netværk og sikkerhed, præget af variation i arkitektur, sikkerhedsniveau og driftspraksis.

På den baggrund har KL efter en markedsafsøgning indhentet ekspertbistand fra Conscia Danmark A/S med fokus på netværk og sikkerhed. Conscia er blevet bedt om at opstille inspiration til sigtelinjer og konkrete arkitekturgreb, inspireret af best practice og den lovgivning, som kommunerne er underlagt, med henblik på at etablere et bæredygtigt og fremtidssikret fundament for fælles IT-drift.

Det tekniske målbillede er derfor ikke udtømmende, men består af udvalgte arkitekturprincipper, som Conscia vurderer at være centrale for at understøtte en stabil og robust drift. Leverancen er udarbejdet som en ramme og et fagligt udgangspunkt for det videre arbejde med en færdig arkitektur- og implementeringsplan i hver IT-serviceorganisation. Dette arbejde skal udføres i samspil med ejerkommunerne og med inddragelse af eksisterende producenter og leverandører, hvor relevant.

Leverancen består overordnet af 3 hovedleverancer:

- 1) Et teknisk målbillede som inspiration til, hvor IT-serviceorganisationerne kan være om 5-8 år.
- 2) Et transitionsdokument, der beskriver tiltag, sekvens og nødvendige investeringer fra nu frem til 31/12 2027
- 3) Et transformationsdokument, der overordnet beskriver, hvordan vejen kan se ud fra etableringen af en fælles IT-driftsplatform til realiseringen af det tekniske målbillede.

Det tekniske målbillede har 4 overordnede emner: sikkerhed, LAN/WAN (netværk), driftsplatform og compliance. De udgør tilsammen det faglige fundament for IT-serviceorganisationerne i fremtiden. Målbilledet giver et samlet overblik over centrale tekniske retninger og principper, der understøtter konsistente valg og styring af samspillet mellem drift, sikkerhed og compliance. Det er Conscias anbefaling at indføre teknisk ensartethed, hvor det er hensigtsmæssigt, for at skabe bedre forudsætninger for sikkerhed, compliance og hændelseshåndtering.

I tilknytning til de tekniske dokumenter er der udarbejdet et detaljeret rammeværk til vurdering af modenhed, der kan anvendes til at fastlægge ambitionsniveauet for IT-serviceorganisationerne og assistere den enkelte kommune i vurderingen af den aktuelle modenhed i forhold til det foreslåede målbillede, via strukturerede evalueringer. Samlet giver dette et direkte anvendeligt grundlag for en konstruktiv dialog om teknologi, samt fundament for planlægning af gennemførelsen af transition i henhold til fastsatte milepæle og deadlines.

Transition og transformation beskrives som to sammenhængende, men adskilte spor, der tilsammen understøtter udviklingen af en fælleskommunal IT-drift.

Transition med udgangspunkt i det tekniske målbillede omfatter de aktiviteter og organisatoriske greb, der er nødvendige for at etablere fælles drift og samarbejde inden for de politisk fastsatte tidsrammer. Transitionen indeholder udvalgte elementer af det tekniske målbillede, men udgør ikke en samlet teknisk realiseringsplan.

Transformation omfatter den efterfølgende og langsigtede videreudvikling og modning af både teknik, drift og samarbejdsformer. Transformationen tager ligeledes afsæt i dele af det tekniske målbillede, men forudsætter, at dette videreudvikles og konkretiseres over tid.

Tillige beskrives overordnede principper og rammer, der understøtter lokal og regional afklaring af opgavesnit mellem kommuner og IT-serviceorganisation, som i det videre forløb kan fastlægge en detaljeret organisations- eller ansvarsmodel. Materialet indeholder et eksempel på en proces for at onboarder en kommune til en IT-serviceorganisation for at illustrere nogle af de afklaringer og valg, der skal foretages.

Det forudsættes, at konkrete ansvarsforhold og prioriteringer løbende fastlægges gennem dialog og beslutninger i de relevante styringsfora. Det tværregionale samarbejde forudsættes forankret i eksisterende governance strukturer, herunder faste koordineringsfora mellem de regionale styregrupper.

Fraregnet dette executive summary, er målgruppen for leverancen IT-chefer i ejerkommunerne, ledere af transitionsenhederne, it-arkitekter og teknikere. Den samlede leverance kan anvendes som:

- en fælles teknisk reference og rammesætning
- et grundlag for videre konkretisering og modning af det tekniske målbillede
- en støtte til planlægning, dialog og prioritering i kommuner, transitions- og IT-serviceorganisationer
- inspiration til næste skridt i implementering

Det er Conscias ambition, at der med udgangspunkt i materialet kan skabes et realistisk fundament for fælles IT-drift i hver IT-serviceorganisation.

Det tekniske målbillede er udarbejdet med inddragelse af relevante faglige og ledelsesmæssige aktører. Arbejdet har involveret ca. 25 personer fra kommunerne, transitionsorganisationerne og KL, via de af KL faciliterede tekniske og strategiske grupper for det tekniske målbillede.

2 Introduktion

Dette afsnit sætter en fælles og ambitiøs ramme for det tekniske målbillede, herunder transition og den efterfølgende transformation, for etablering af IT-serviceorganisationerne.

Målbilledet er leverandør- og producentagnostisk og skal understøtte lokale beslutninger, prioriteringer og forskellighed i udgangspunkt og tempo. Den primære målgruppe er den tekniske organisation, herunder IT-chefer, arkitekter, driftsledere og programledere.

Formålet er at skabe et klart pejlemærke med strategisk betydning og med afsæt i eksisterende standarder og lovgivning, som kan guide arkitekturbeslutninger, reducere risiko og sikre sammenhæng mellem tekniske valg, governance og drift, uden at foreskrive en fast implementeringsmodel.

2.1 Grundlæggende opgave og fælles ambition

Den fælleskommunale IT-serviceorganisation har til opgave at etablere et professionelt, robust og skalerbart fundament for driften af kommunal IT-infrastruktur på tværs af selvstændige organisationer. Opgaven omfatter fastlæggelse af fælles principper, ensartede kvalitetsniveauer og klare styringsmekanismer, der understøtter fleksible teknologiske valg og kan bære både nuværende og fremtidige behov på tværs af løsninger, produkter og leverandører.

IT-serviceorganisationen fungerer som et samlet teknisk og driftsmæssigt omdrejningspunkt, der muliggør ensartet drift, høj sikkerhed og dokumenterbar compliance, samtidig med at kommunerne bevarer ejerskab, ansvar og prioriteringsret for deres egne systemer og forretningskritiske services. Det tekniske målbillede udgør den fælles reference for dette samarbejde ved at tydeliggøre forventninger, minimumsniveauer og snitflader mellem parterne.

For ledelsen i IT-serviceorganisationen er opgaven at etablere en fælles og professionel platform, hvor drift, sikkerhed og compliance er forankret i strukturer og principper frem for i enkeltpersoner eller lokale praksisser. Dette kræver:

- Standardiserede arkitekturprincipper
- Klare ansvars- og snitlademodeller mellem kunde og leverandør
- Dokumenterede processer for drift, ændringer og hændelseshåndtering
- Gennemsigtighed i risici, afvigelser og teknisk gæld

IT-serviceorganisationen skal kunne rumme forskelle i kommunernes udgangspunkt, men samtidig håndhæve et fælles minimumsniveau for sikkerhed, dokumentation og styring. Det tekniske målbillede anvendes her som et ledelsesværktøj, der gør prioriteringer eksplicite og understøtter dialogen med kommunerne om modenhed, kvalitet og udvikling.

For kommunernes ledelse ændrer samarbejdet med IT-serviceorganisationen karakteren af IT-opgaven, uden at ansvaret reduceres. Fokus flyttes fra daglig teknisk drift til aktivt ejerskab og styring gennem:

- Tydeligt system- og dataejerskab
- Klassifikation af forretningskritikalitet og afhængigheder
- Prioritering af risici og investeringer
- Dialog om servicekvalitet, modenhed og krav

Kommunen bevarer ejerskab til sine data, fagsystemer og forretningskrav og træffer fortsat de forretningsmæssige beslutninger på et oplyst grundlag. IT-serviceorganisationen bidrager med et forudsigeligt, professionelt og dokumenterbart teknisk fundament, som understøtter kommunens beslutningsrum. Det tekniske målbillede tydeliggør forventninger, roller og gensidige forpligtelser og danner grundlag for et kunde-/leverandørforhold præget af fælles ansvar, transparens og klar ansvarsfordeling.

2.2 De tekniske målbilleder

De fire tekniske målbilledokumenter: Sikkerhed, Driftsplatform, LAN/WAN og Compliance, giver et samlet overblik over centrale tekniske retninger og principper, som understøtter konsistente valg og en styring af samspillet mellem drift, sikkerhed og compliance. Hvert dokument beskriver udvalgte dele af det tekniske målbillede inden for sit område og fungerer som en fælles reference for dialog og videre konkretisering i det efterfølgende arbejde.

I tilknytning til de tekniske dokumenter er der udarbejdet et detaljeret rammeværk til vurdering af modenhed, der kan anvendes til at fastlægge ambitionsniveauet for IT-serviceorganisationerne og assistere den enkelte kommune i vurderingen af den aktuelle modenhed i forhold til ambitionen, via strukturerede scorecards. Samlet giver dette et direkte anvendeligt grundlag for konstruktiv dialog samt planlægning og gennemførelse af transition i henhold til fastsatte milepæle og deadlines.

2.3 Vision: Det resiliente driftscenter

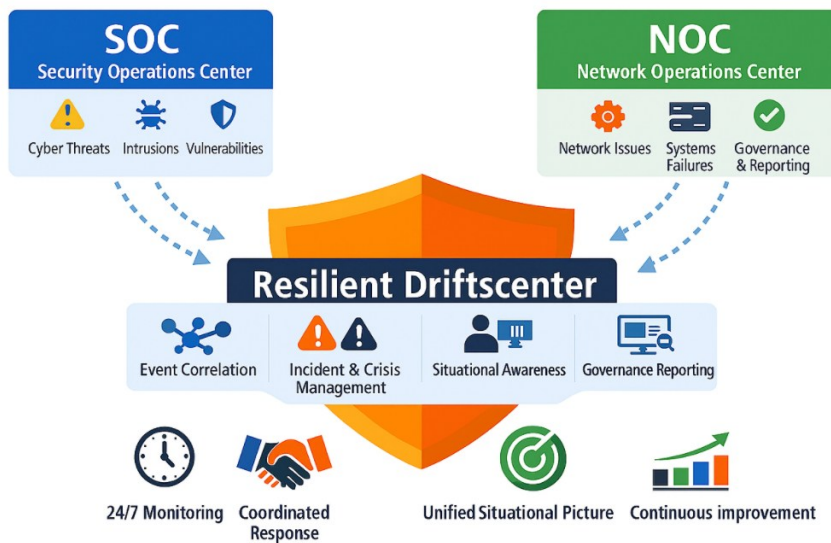
Visionen har det lange lys på, og anbefalingerne i det tekniske målbillede er generelt af langt mere jordnær karakter. Dog har det været vigtigt for opgaven at have en fælles referenceramme at sigte imod, og det anbefales, at IT-serviceorganisationerne skaber egne pejlemærker for fremtiden.

Resiliens handler i denne sammenhæng om evnen til at forebygge, modstå og hurtigt genetablere normal drift efter tekniske, sikkerhedsmæssige eller organisatoriske hændelser.

Arbejdet med det tekniske målbillede tager afsæt i en samlet vision for det resiliente driftscenter. Når kommunernes digitale tjenester samles i fælles drift, får stabilitet, kontinuitet og sikkerhed stadig større betydning for både borgernes hverdag og forvaltningens funktionsevne. IT-serviceorganisationen skal derfor betragtes som en samfundskritisk produktionsenhed, hvor høj tilgængelighed, robust sikkerhed og driftsmæssig kontinuitet er centrale forudsætninger for kommunernes digitale robusthed og handlekraft.

Det resiliente driftscenter er en arkitektonisk og ledelsesmæssig ambition om robust og vedvarende levering af kritiske kommunale services under varierende belastninger og hændelser.

Ambitionen omfatter håndtering af tekniske fejl, menneskelige fejl og eksterne påvirkninger såsom cyberangreb eller forsyningssvigt.



Illustrationen viser et resilient driftscenter, hvor drift, sikkerhed og overvågning er samlet i én sammenhængende funktionsmodel. Driftscenteret udgør det operationelle knudepunkt mellem SOC (Security Operations Center) og NOC (Network Operations Center). Det skaber en fælles situationsforståelse på tværs af sikkerheds- og netværksdrift og sikrer, at specialiseret viden koordineret anvendes til hurtig og effektiv håndtering af hændelser.

SOC bidrager med overvågning af cybertrusler, indtrængningsforsøg og sårbarheder, mens NOC overvåger netværk, systemer, kapacitet, fejl og ydeevne. I det resiliente driftscenter samles disse strømme af data og hændelser, hvor de korreleres på tværs af drift og sikkerhed. Det muliggør hurtigere og mere præcis hændeshåndtering, styrket situationsbevidsthed og et fælles beslutningsgrundlag.

Illustrationen understreger, at resiliens opnås gennem konvergens mellem overvågning, hændeshåndtering og ledelsesrapporte ring. Driftscenteret understøtter døgnbemandet overvågning, koordineret respons, et fælles overblik over risici og driftstilstand samt løbende forbedring baseret på erfaringer og målinger.

Samlet set illustrerer billedet, hvordan det resiliente driftscenter skaber et professionelt grundlag for stabil drift, effektiv krisehåndtering og ledelsesmæssig styring, hvor både drift og sikkerhed indgår som integrerede og gensidigt afhængige elementer.

Målet er, at hver kommune bevarer den nødvendige kontrol, samtidig med at den får adgang til et professionelt driftsmiljø. Et miljø hvor konsekvenserne af nedbrud er analyseret og accepteret på ledelsesniveau, hvor genopretningstider og datatab er fastlagt og forudsigelige, og hvor beredskab er integreret i den daglige drift frem for at være et dokumentationsprodukt.

Det resiliente driftscenter muliggør, at kommunale IT-chefer kan føre en mere kvalificeret dialog med sin direktion og sine fagområder om risici, prioriteringer og investeringer, baseret på faktiske kapabiliteter frem for individuelle antagelser.

For ledelsen i IT-serviceorganisationen repræsenterer det resiliente driftscenter et skifte væk fra traditionelle driftsmodeller, hvor stabilitet i en vis grad har været baseret på lokalkendskab, manuelle procedurer og implicit viden.

Visionen baserer sig på teknisk arkitektur, som prioriterer indbygget redundans, kontrollerede fejlscenarier og dokumenteret, testet genopretning, hvilket reducerer risikoen for driftsafbrydelser og styrker den samlede robusthed og sikkerhed.

Et konsolideret driftscenter, der håndterer mange kommuner, skal kunne dokumentere et højere resiliensniveau end enkeltstående lokale løsninger. Det skyldes, at et fælles driftsmiljø får en bredere samfundsmæssig og organisatorisk betydning: hændelser kan potentielt påvirke flere kommuner samtidig, og cyberangreb eller fejl kan få større konsekvens, hvis de ikke effektivt isoleres. Derfor skal robusthed, segmentering, beredskab, overvågning og gendannelsesevne dokumenteres og efterprøves som en integreret del af driftsmodellen.

For ledelsen i kommunerne handler visionen om det resiliente driftscenter først og fremmest om tillid og forudsigelighed. Når kommunernes systemer samles i fælles drift, skal løsningen skabe tydelig værdi gennem professionel drift, bedre ressourceudnyttelse og høj operationel kvalitet, samtidig med at sikkerhed og robusthed som minimum matcher det niveau, kommunerne selv kan etablere lokalt.

I dialogen med kommunerne fremhæves ønsket om fortsat at kunne levere et højt serviceniveau til både medarbejdere og borgere som et centralt hensyn. Dette ønske præger forventningerne til overgangen til en fælles driftsplatform, hvor kontrol, ansvar og beslutningsrum i højere grad deles eller koordineres mellem flere aktører. Med afsæt i denne ambition understøtter visionen ledelsen ved at skabe et fælles grundlag for tillid, forudsigelighed og klare snitflader for ansvar, styring og rapportering.

2.3.1 Resiliens som arkitektonisk og organisatorisk disciplin

Et centralt element i visionen er, at resiliens ikke alene betragtes som et teknisk anliggende, men opnås gennem et samspil mellem arkitektur, processer og organisation. Det indebærer en tæt konvergens mellem drift, sikkerhed, overvågning og compliance-procedurer, understøttet af et fælles datagrundlag for beslutningstagning, hændeshåndtering og dokumenteret efterlevelse. Samtidig etableres kortere og tydeligere beslutningsveje i forbindelse med afvigelser og kriser. Visionen peger på en samlet funktionsmodel, hvor overvågning, sikkerhed og compliance arbejder integreret på tværs, og hvor ledelsen har ét konsolideret overblik over både driftstilstand, risikoeksponering og efterlevelse af gældende krav.

I den følgende introduktion beskrives elementerne i det tekniske målbillede i overordnede træk.

3 Teknisk målbillede

Det tekniske målbillede er struktureret omkring fire centrale discipliner: Sikkerhed, Driftsplatform, LAN/WAN (lokale og eksterne netværk) og Compliance. Tilsammen dækker de væsentligste tekniske forudsætninger for en stabil, sikker og sammenhængende fælleskommunal IT-drift. De fire discipliner beskriver tekniske principper og skal ses som indbyrdes afhængige elementer, der tilsammen understøtter robusthed, skalerbarhed og styring.

I det følgende introduceres hver disciplin med fokus på rolle, anvendelse og samspil med den samlede tekniske helhed.

3.1 Arkitekturprincipper – fælles retning og styrende rammer

For at beramme opgaven omkring det tekniske målbillede i hver IT-serviceorganisation er omdrejningspunktet et sæt arkitekturprincipper, der er udvalgt i forbindelse med opstart af opgaven. Principperne er efterfølgende præsenteret og afstemt med interessenter fra kommuner og kommende IT-serviceorganisationer i workshops om det tekniske målbillede.

De 15 arkitekturprincipper udgør et fælles afsæt for de tekniske målbilledokumenter og anvendes som et gennemgående styrings- og vurderingsgrundlag på tværs af Sikkerhed, driftsplatform, LAN/WAN og Compliance. Principperne fungerer som et fælles sprog og en fælles referenceramme, der knytter de enkelte tekniske discipliner sammen og sikrer konsistens i de beskrevne tekniske retninger og løsninger.

Principperne fungerer som pejlemærker, der omsætter overordnede ambitioner til konkrete design- og beslutningskriterier. De udgør en fælles reference for drift, sikkerhed, transition og den efterfølgende transformation.

ARKITEKTURPRINCIPPER			
Sikkerhed	Standardisering	Konsolidering	Segmentering
Security by design	Adressetildeling	Datacentre med multi-tenancy	Makro-segmentering og large-scale netværk
Kategorisering af systemer	Zonemodeller	Redundans og resiliens	Mikro-segmentering for kategoriserede systemer
Overvågning og auditing	Logiske netværksstrukturer	Ensartede og skalerbare topologier	
Zero Trust	Redundansprincipper	Optimal udnyttelse af ressourcer	
		Automatisering	

I dokumenterne anvendes arkitekturprincipperne til at underbygge valg af tekniske retninger og prioriteringer, tydeliggøre sammenhænge og afhængigheder mellem de enkelte discipliner og skabe en rød tråd mellem tekniske løsninger, drift, sikkerhed og styring.

For IT-serviceorganisationerne kan arkitekturprincipperne anvendes som et praktisk værktøj i det videre arbejde, herunder ved:

- vurdering af konkrete tekniske løsninger, ændringer og investeringer
- prioritering mellem lokale tilpasninger og fælles standardisering
- dialog med kommuner om konsekvenser, valg og fravalg

- løbende modenhedsvurdering og videreudvikling af den fælles drift

3.2 Sikkerhed – fælles modenhed og tydeligt ansvar

Sikkerhed i en fælleskommunal IT-serviceorganisation skal forstås som en fælles disciplin, hvor tekniske kontroller, organisatoriske snitflader og ledelsesmæssigt ansvar hænger uløseligt sammen. Det tekniske målbillede tager udgangspunkt i, at ingen kommune er stærkere end det samlede svageste led, og at sikkerhed derfor må etableres og drives efter fælles principper og fælles minimumsniveauer.

Udgangspunktet er Security by Design: sikkerhed og risikovurdering indtænkes systematisk i design og videreudvikling af infrastruktur og services. Målet er at arbejde med et dokumenteret og ledelsesmæssigt accepteret risikoniveau, hvor både konsekvens og sandsynlighed håndteres gennem proportionelle tekniske og organisatoriske kontroller.

Der lægges vægt på:

- Klare ansvarsforhold mellem IT-serviceorganisationen og kommunerne, baseret på en fælles ansvarsmodel.
- Ensartet minimumsniveau for sikkerhed på tværs af kommuner, uanset lokalt udgangspunkt.
- Robusthed, resiliens og evnen til hurtigt at opdage, håndtere og genoprette driften efter hændelser.

Sikkerhed bliver dermed et aktiv, der understøtter stabil drift, opbygger tillid og styrker beslutningskraften som en integreret del af den samlede udvikling.

For IT-serviceorganisationens ledelse betyder det, at sikkerhed etableres som et grundlæggende designelement i arkitektur, driftsmodeller og governancestruktur fra starten. Sikkerheden forankres gennem ensartede principper for segmentering, adgangskontrol, overvågning og hændelseshåndtering, samtidig med at der er rum for fleksible valg af teknologier, produkter og leverandører inden for de fælles rammer.

For kommunernes ledelse indebærer overgangen til fælles drift en tydelig og bevidst rollefordeling, hvor kommunen fastholder ansvaret for systemejerskab, dataklassifikation og vurdering af forretningskritikalitet.

Sikkerhedsmæssigt skaber målbilledet dermed et fælles sprog for risiko, modenhed og prioritering. Det gør det muligt for ledelsen, både centralt og lokalt, at føre en kvalificeret dialog om, hvor der bevidst accepteres risiko, og hvor der investeres i øget beskyttelse.

3.3 Driftsplatform – robusthed, forudsigelighed og skalerbar drift

Driftsplatformen i målbilledet er defineret med fokus på driftsrobusthed. I denne sammenhæng omfatter driftsplatformen compute, storage, virtualisering og containerplatforme, backup og recovery samt automation. Målbilledet for driftsplatformen afgrænser sig til de tekniske og operationelle elementer, der understøtter den fælles drift, dvs. det fysiske datacenter, herunder bygninger, racks, kabling, køl og nødstrøm, forudsættes at være til stede.

I et setup med mange selvstændige juridiske entiteter er det afgørende, at driftsplatformsarkitekturen er baseret på veldefinerede principper for tilgængelighed, redundans og forandring, som understøtter stabil drift og konsistente arbejdsgange.

Det tekniske målbillede for driftsplatformen beskriver en bevægelse mod en standardiseret, sikker og skalerbar platform, der kan rumme kommuner med forskellige behov og modenhedsniveauer.

Investeringen i en standardiseret og robust driftsplatform er afgørende, fordi den reducerer de samlede risici og omkostninger ved kommunal IT-drift over tid. En sådan platform begrænser konsekvenserne af driftsfejl og hændelser, så serviceafbrydelser bliver kortere, mere forudsigelige og lettere at håndtere. Samtidig sænker standardisering og skalerbarhed den samlede livscyklusomkostning, idet variation, manuel håndtering og teknisk gæld reduceres, og nye behov kan håndteres inden for den fælles struktur. Endelig skaber driftsplatformen et grundlag for styring og prioritering, IT-serviceorganisationen får transparens i risiko, kvalitet og investeringer og dermed mulighed for at træffe ansvarlige, datadrevne beslutninger på tværs af kommuner og modenhedsniveauer.

Målbilledet er kendetegnet ved:

- Multi-tenant arkitektur med klar logisk adskillelse, så data og drift holdes klart adskilt mellem kommunerne.
- Høj grad af standardisering og automatisering for at sikre forudsigelighed og effektiv drift.
- Indbygget resiliens og redundans, så kritiske tjenester kan opretholdes under fejl og hændelser.
- Transparent ressourcestyring, der muliggør ansvarlig kapacitetsplanlægning og økonomisk styring.

Målbilledet for driftsplatformen fungerer som et fælles teknisk fundament, der både understøtter stabil drift i transitionsfasen og muliggør løbende transformation mod mere konsoliderede og automatiserede løsninger.

For IT-serviceorganisationens ledelse handler det om at kunne levere en stabil og forudsigelig platform, hvor kapacitet, vedligeholdelse og fejlscenarier planlægges og håndteres på en struktureret måde. Det tekniske målbillede understøtter en arkitektur, der muliggør løbende videreudvikling og konsolidering af platforme og samtidig skaber grundlag for at realisere skalafordele inden for både sikkerhed og økonomi til gavn for ejerkommunerne.

For kommunernes ledelse betyder det, at de kan basere deres systemporteføljer på en driftsplatform med kendte egenskaber: klart definerede SLA forventninger, dokumenterede failover mekanismer og en tydelig adskillelse mellem kritiske og ikke-kritiske services. Det skaber tryghed både i den daglige drift og i dialogen med forretningen.

Driftsplatformen fungerer dermed som en fælles produktionsplatform, der understøtter professionalisering af driften, samtidig med at kommunernes forretningsmæssige valg kan træffes fleksibelt inden for en stabil, sikker og skalerbar ramme.

3.4 LAN/WAN – fælles fundament for decentral virkelighed

Netværket er den mest tværgående del af den fælles infrastruktur og er ofte det område, hvor forskelle mellem kommuner er mest synlige. Målbilledet for LAN/WAN tager derfor udgangspunkt i behovet for ensartet driftsegnethed, ikke ensartet topologi.

Når dokumentet her går i dybden med tekniske netværksprincipper, skyldes det, at de har direkte implikationer for sikkerheden: segmentering (logisk adskillelse) begrænser spredning ved hændelser, og logging/overvågning understøtter hurtig detektion, afklaring og genopretning. Netværket er rygraden i det fælles driftsetup og skal understøtte både sikkerhed, skalerbarhed og fleksibilitet.

Det tekniske målbillede for netværk bygger på:

- Modulær og hierarkisk arkitektur, der kan udvides uden grundlæggende redesign.
- Standardiserede designprincipper for adressering, routing, segmentering og redundans.
- Klar adskillelse mellem kommuner og systemkategorier gennem makro- og mikrosegmentering.
- Indbygget kapacitet til overvågning, logging, og governance.

Målbilledet for LAN/WAN skal sikre, at kommunerne kan indgå som ligeværdige parter i en fælles driftsmodel, hvor trafik, data og ansvar holdes entydigt adskilt, og hvor sikkerhed og compliance er indlejrede forudsætninger for samarbejde, styring og tillid på tværs af organisationen.

For IT-serviceorganisationen betyder det, at netværksdrift skal kunne ske efter fælles principper for segmentering, overvågning, fejlretning og håndtering af ændringer. Et netværk, der er designet forskelligt i hver kommune, er vanskeligere at overvåge og støtte samlet – og kan øge den samlede drifts- og sikkerhedsrisiko.

For kommunerne betyder det, at lokale behov fortsat kan imødekommes, men inden for en fælles arkitektonisk ramme. Det kan f.eks. være forskelle i lokationsstruktur, forbindelsestyper eller anvendelse, men baseret på fælles standarder for sikkerhedszoner, adgang og logging.

LAN/WAN-målbilledet skaber en balanceret sammenhæng mellem central styring og lokal fleksibilitet. Netværket udgør et fælles driftsfundament frem for en samling lokale særhensyn og etablerer dermed en klar forudsætning for en skalerbar og effektiv fælles drift.

3.5 Compliance – operationaliseret ledelsesansvar

I målbilledet er compliance indarbejdet som en integreret disciplin, der forankres i den daglige drift. Dette er et bevidst valg, der understøtter, at efterlevelse af blandt andet de tekniske minimumskrav og NIS2 håndteres systematisk og løbende frem for særskilt i forbindelse med en audit.

Centralt er forståelsen af, at sikkerhed opnås gennem et tæt samspil mellem tekniske løsninger, kontrolmekanismer og de processer, der omgiver dem. Overholdelse af krav og etablering af teknologiske kontroller udgør et nødvendigt fundament, men den reelle beskyttelse understøttes af, at kontroller løbende testes, følges op på og indgår i klare procedurer og arbejdsgange. Gennem dette samspil sikres det, at tekniske sikkerhedsforanstaltninger fortsat er effektive, og at afvigelser opdages og håndteres rettidigt som en integreret del af den daglige drift.

Der fokuseres derfor på:

- Klare governance strukturer og dokumenteret ansvarsfordeling.
- Teknisk mapping af kontroller, der forbinder krav med konkrete arkitektur- og driftsvalg.
- Revisions- og rapporteringsparathed som en naturlig del af den daglige drift.

I materialet indgår 2.4.1 Compliance kortlægning i forhold til arkitekturprincipperne, i forhold til NIS2, ISO27001, CIS kontroller og Tekniske minimumskrav.

Compliance bliver dermed et styringsværktøj, der understøtter ledelsesbeslutninger og risikobaseret prioritering.

For IT-serviceorganisationernes ledelse er compliance et styringsværktøj. Når krav er oversat til tekniske og organisatoriske kontroller, og disse er dokumenteret og løbende overvåget, bliver compliance en del af den normale driftsdialog, på linje med opetid og performance.

For kommunerne giver dette gennemsigtighed. De får indsigt i, hvilke kontroller der er implementeret centralt, hvad der forventes lokalt, og hvor der eventuelt er afvigelser, der kræver en stillingtagen. Det skaber et fælles faktuel grundlag for ledelsesbeslutninger og prioriteringer.

Compliance-målbilledet understøtter dermed både myndighedskrav og intern governance og bidrager til at professionalisere relationen mellem driftscenteret og kommunerne. Det gør det muligt at stå samlet over for tilsyn, revision og offentlighed – med dokumentation, der er konsistent og troværdig.

3.6 AI i relation til det tekniske målbillede

AI udvikler sig hurtigt og skaber løbende nye muligheder for analyse, automatisering og beslutningsstøtte i drift af infrastruktur. For det tekniske målbillede forstås anvendelse af kunstig intelligens som en funktionalitet, der realiseres oven på den fælles driftsplatform. AI betragtes som en mulighed for videreudvikling og optimering og indgår dermed som en naturlig forlængelse af et modent teknisk og organisatorisk fundament.

Det tekniske målbillede skaber rammerne for anvendelse af AI ved blandt andet at understøtte:

- skalerbar compute kapacitet og containerplatforme
- automatiserede driftsprocesser og standardiserede arbejdsgange
- central overvågning, logning og dataindsamling
- identitetsbaseret adgangsstyring og segmentering
- klare ansvarsmodeller og styring på tværs af kommuner

På dette fundament kan AI anvendes i forskellige sammenhænge, f.eks. til analyse, beslutningsstøtte, optimering af drift og kapacitetsudnyttelse samt videreudvikling af automatisering. Den konkrete anvendelse afhænger af kommunernes forretningsmæssige behov, modenhed og prioriteringer og kan udvikles gradvist over tid.

AI anbefales anvendt som en fleksibel og fremadskuende kapabilitet, der kan indarbejdes løbende i takt med udviklingen i behov, regulering og organisatorisk parathed. Denne tilgang skaber mulighed for at udnytte nye teknologiske muligheder, samtidig med at anvendelsen sker inden for en stabil ramme, der understøtter sikkerhed, compliance og governance. AI bliver dermed en naturlig forlængelse af den eksisterende platform og bidrager til løbende innovation og effektivisering af driften.

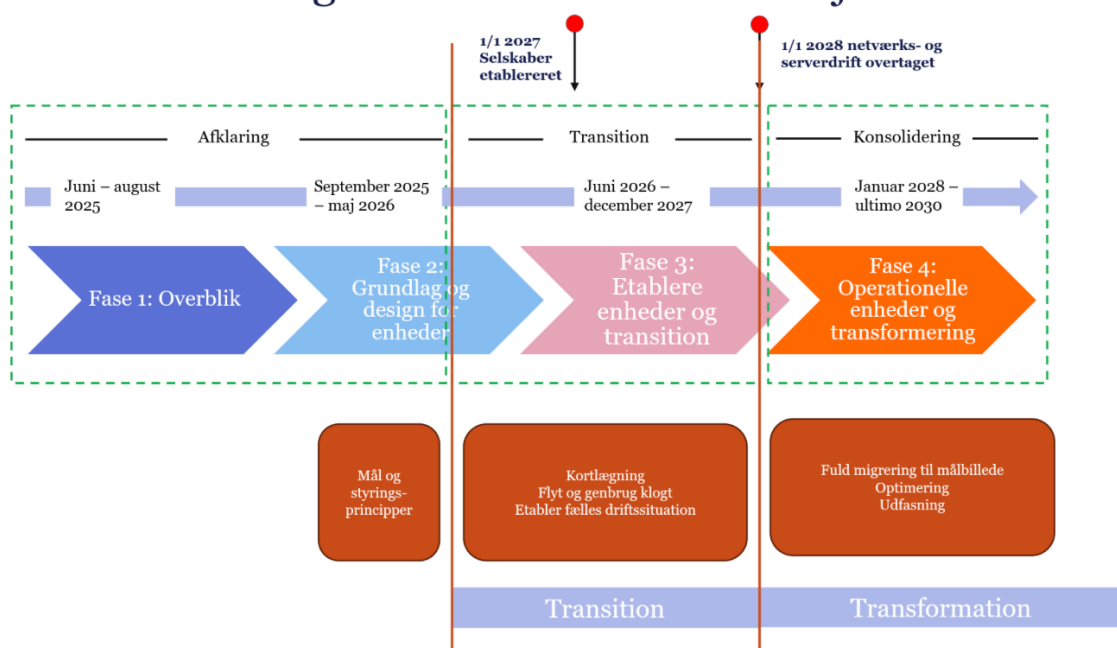
4 Transition – kontrolleret overgang til fælles drift

Transitionen beskriver den kontrollerede overgang fra kommunal drift til fælles IT-serviceorganisationer og udgør den strukturelle ramme for overdragelse af ansvar, opbygning af ensartede niveauer og reduktion af driftsrisici. Transitionen fokuserer på etablering, stabilisering og klargøring og skaber de tekniske og organisatoriske forudsætninger for en fælles drift.

KL angiver perioderne for transition og transformation som illustreret i denne tidslinje:

Transitions- og transformations- tidslinje

KL



Tids- og faseplane april 2026

Transitionsforløbet er i forhold til det tekniske målbillede tilrettelagt som en faseopdelt model, der understøtter ledelsesmæssige beslutninger om governance, prioritering, investeringer, risikohåndtering og overdragelse. Faserne og de beskrevne aktiviteter skal ses som et fælles afsæt og inspirationsgrundlag, hvor den konkrete planlægning og gennemførelse sker regionalt i tæt samspil mellem kommuner og IT-serviceorganisationer.

Transitionen gennemføres med hensyntagen til, at kommunerne har forskellige tekniske og organisatoriske udgangspunkter. Arbejdet er baseret på målsætninger, modenhedsvurdering, og bevidste prioriteringer, under hensyntagen til den kommunes ønskede implementeringstempo.

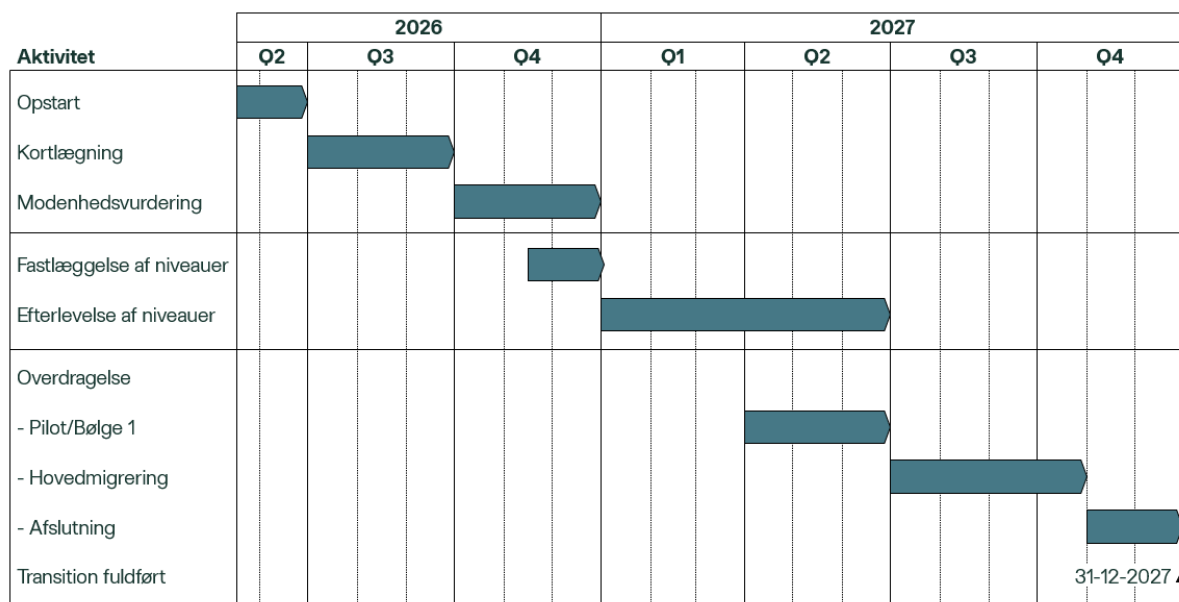
4.1 Faseopdelt overgang

Transitionsmodellen er bygget op omkring fem sammenhængende faser, som tilsammen sikrer progression fra overblik til stabil overdragelse:

- **Kortlægning**, hvor det eksisterende tekniske og organisatoriske landskab dokumenteres og fælles overblik etableres.

- **Modenhedsvurdering**, hvor kommunernes parathed vurderes i forhold til teknik, dokumentation, drift og sikkerhed.
- **Fastlæggelse af niveauer**, hvor fælles minimumsniveauer for drift, netværk og sikkerhed fastsættes som styringsgrundlag.
- **Efterlevelse af niveauer**, hvor tekniske og organisatoriske gaps lukkes, og drift stabiliseres.
- **Overdragelse**, hvor ansvar og drift formelt overgår til den fælles IT-serviceorganisation med efterfølgende stabiliseringsperiode.

Under hensyntagen til Økonomiaftalen, kunne afviklingen af faserne inspirationsmæssigt se ud som herunder; den konkrete planlægning skal ske i regionerne:



Faserne skaber et tydeligt beslutningsgrundlag og muliggør løbende prioritering og justering af tempo og rækkefølge uden at kompromittere kvalitet og sikkerhed.

4.2 Sammenhæng til det tekniske målbillede

Transitionen anvender udvalgte elementer af det tekniske målbillede som reference og pejlemærke, herunder fælles standarder, definerede minimumsniveauer og centrale arkitekturprincipper inden for drift, netværk og sikkerhed. Transitionen etablerer dermed de overordnede rammer, der gør det muligt at omsætte det tekniske målbillede til drift på et ensartet, kontrolleret og gradvist implementerbart grundlag.

Det forudsættes, at videre konkretisering, videreudvikling og optimering af det tekniske målbillede fortsætter i transformationssporet.

4.3 Tværgående styring og governance

For at sikre fremdrift og sammenhæng forudsætter transitionen en klar governance struktur med fælles styringsfora, faste beslutningspunkter og ensartet rapportering. Tværgående styring

anvendes til at skabe overblik over risici, afhængigheder og parathed på tværs af kommuner og IT-serviceorganisation.

Transitionen foreslås opdelt i bølger, et praktisk værktøj til at håndtere variation i kompleksitet og modenhed. Hver bølge følger samme grundstruktur, hvilket understøtter læring, genbrug af erfaringer og ensartet kvalitet i overdragelsen.

4.4 Roller og ansvar

Transitionen bygger på et tydeligt samarbejde mellem kommuner og IT-serviceorganisation. Roller og ansvar er fordelt, så fremdrift, kvalitet og sikkerhed understøttes parallelt. Af praktiske hensyn kan enkelte roller varetages af samme personer på tværs af organisationer, særligt i opstartsfasen, så længe ansvar og beslutningskompetence er tydeligt afgrænset.

4.4.1 Eksempel på RACI.

Tabellen er illustrativ og udgør inspiration til udvalgte opgaver og roller. Endelige ansvarsfordelinger og snitflader fastlægges regionalt og kan tilpasses lokale forhold og aftaler, f.eks. i forbindelse med udarbejdelse af lokale driftshåndbøger.

Opgave / ansvar	IT-serviceorg.	Kommune	Leverandør	Kommentar
Driftsplatform (servere, storage, virtualisering, backup etc.)				
Design af fælles driftsplatform (arkitekturprincipper, standarder)	R	C	C	Platformen designes centralt inden for fælles målbillede
Etablering og konfiguration (compute, storage, virtualisering)	R	I	C	ITSO udfører på baggrund af fælles standarder
Drift og overvågning (kapacitet, performance, tilgængelighed)	R	I	C	Løbende drift forankres hos ITSO
Backup, restore og gendannelsestest	R	C	C	Kommune inddrages ift. forretningskrav (RPO/RTO)
Patching og teknisk vedligehold	R	I	C	Indgår som del af professionel drift
Klassifikation af systemkritikalitet	C	R	I	Forbliver et kommunalt ansvar
Risikoaccept (fx planned downtime, workaround)	C	A	I	Kommune bærer fortsat forretningsansvar
Overholdelse af NIS2 (samlet)	C	A	I	Kan ikke uddelegeres

Opgave / ansvar	IT-serviceorg.	Kommune	Leverandør	Kommentar
LAN/WAN og netværksinfrastruktur				
Overordnet netværksarkitektur (zonestruktur, Zero Trust-principper)	R	C	C	Fælles arkitekturprincipper

Opgave / ansvar	IT-serviceorg.	Kommune	Leverandør	Kommentar
WAN-design og central netværksdrift	R	I	C	Drift konsolideres i ITSO
Netværksovervågning (NOC, alarmer, hændelser)	R	I	C	Én fælles driftsfunktion
Segmentering og isolation (kommuner/systemklasser)	R	C	C	Kommune inddrages via klassifikation
Lokal adgang (bygninger, udstyr, brugere)	C	R	I	Afhænger af lokal organisering
Prioritering af netværksrelaterede ændringer	C	A	I	Kommune beslutter ud fra behov
Hændelsesrapportering (NIS2 §12/13)	C	A	I	ITSO leverer input, kommune indberetter
Dokumentation af afhængigheder og kritiske flows	C	R	C	Forretningsviden er kommunal

4.5 Transition som fundament for videre udvikling

Transitionen markerer etableringen af fælles drift og danner grundlaget for det videre arbejde med modenhed, standardisering og kontinuerlig forbedring. Gennem kontrolleret overgang, fælles niveauer og tydelig styring skabes et solidt fundament, som transformationssporet kan videreudvikle over tid.

5 Transformation – kontinuerlig udvikling og modenhed

Transformation beskriver den langsigtede udvikling af fælleskommunal IT-drift og sætter rammen for, hvordan drift, sikkerhed og samarbejde modnes og forbedres over tid. Hvor transition fokuserer på etablering og stabilisering af fælles drift, understøtter transformationen en systematisk videreudvikling af tekniske kapabiliteter, arbejdsgange og styringsformer.

Transformationssporet er et flerårigt udviklingsforløb, hvor IT-serviceorganisationer og kommuner i fællesskab opbygger højere teknisk og organisatorisk modenhed. Udviklingen tager afsæt i erfaringer fra driften, ændrede krav fra omverdenen og et stigende behov for stabilitet, sikkerhed og forudsigelighed i leverancen af digitale services.

De beskrevne faser, tiltag og aktiviteter i transformationssporet fungerer som et inspirations- og planlægningsgrundlag. De giver en fælles struktur for dialog, prioritering og beslutning, hvor tempo og rækkefølge kan tilpasses lokale forudsætninger og politiske rammer.

I transformationssporet arbejdes der videre med det tekniske målbillede. Arkitekturprincipper, standarder og kontrolkrav konkretiseres, afprøves i drift og justeres løbende, så de fortsat kan anvendes som et praktisk styringsredskab og omsættes til konkrete designvalg, målinger og investeringer.

For ledelsen i IT-serviceorganisationen er transformation det spor, der sikrer, at den fælles drift udvikler sig i takt med nye krav til sikkerhed, compliance og driftskvalitet. Transformationen understøtter overgangen til mere ensartet, datadrevet og systematisk styring og bidrager til en løbende professionalisering af samarbejdet med kommunerne.

Transformationen understøtter blandt andet:

- En gradvis bevægelse mod en mere proces- og datadrevet driftsmodel, hvor beslutninger baseres på fælles, valide data frem for individuelle vurderinger og manuelle processer.
- Øget standardisering af processer, arkitektur og arbejdsgange dér, hvor det bidrager til højere driftsstabilitet, bedre sikkerhed og lettere styring.
- Opbygning af fælles værktøjer, målemetoder og styringsmekanismer, som understøtter ensartet overvågning, rapportering og ledelsesmæssig opfølgning på tværs af funktioner.
- En styrket og operationaliseret sammenhæng mellem drift, sikkerhed og compliance, hvor krav til efterlevelse er indarbejdet i de daglige processer og styringsmodeller.

Det tekniske målbillede fungerer som et strategisk pejlemærke for den videre udvikling og understøtter prioritering af kapabiliteter, uden at fastlægge konkrete teknologivalg eller implementeringsrækkefølger.

For ledelsen i kommunerne repræsenterer transformationen et fælles udgangspunkt for, hvordan kommunal IT-drift kan understøtte stabile og sikre services over tid. Transformationen giver øget

transparens i drifts- og sikkerhedsniveauet og styrker kommunernes mulighed for at prioritere investeringer og risici på et fælles og oplyst grundlag.

Over tid bidrager transformationen til:

- mere systematisk arbejde med systemejerskab, klassifikation og risikovurdering
- bedre overblik over drifts- og sikkerhedsniveau på tværs
- fælles pejlemærker for teknisk modenhed og kvalitet
- et tydeligere ledelsesfokus på forretningens behov og prioriteringer

Kommunernes råderum til at vælge løsninger bevarer, samtidig med at fælles rammer giver et stabilt fundament for samarbejde og drift.

5.1 Fælles standarder og lokal anvendelse

Transformationen understøtter en balanceret udvikling, hvor fælles standarder anvendes som løftestang for kvalitet og effektivitet, samtidig med at der er plads til lokale tilpasninger. Rammerne bidrager til tydelige minimumsniveauer, mens lokale variationer kan håndteres hensigtsmæssigt og dokumenteret.

Denne tilgang gør transformationen til et centralt redskab i arbejdet med teknisk kompleksitet, historiske løsninger og fremtidige krav og understøtter fælles prioritering og gennemsigtighed i beslutningsgrundlaget.

5.2 Samspil med transition

Transition og transformation udgør to sammenhængende udviklingsspor med forskellige formål. Transition skaber det nødvendige organisatoriske og tekniske fundament for fælles drift, mens transformationen anvender dette fundament til løbende at øge modenhed, kvalitet og robusthed.

Aktiviteter, der ikke kan gennemføres i transitionen, kan indgå i transformationssporet, hvor de videreudvikles og prioriteres over tid.

5.3 Ledelsesmæssig betydning

Etableringen af fælleskommunal IT-drift markerer begyndelsen på en ny måde at servicere brugere på. Det forudsætter vedvarende ledelsesmæssig opmærksomhed, tydelige prioriteringer og løbende dialog om modenhed, risiko og investering.

Transformationen giver kommuner og IT-serviceorganisationer et fælles grundlag for at håndtere fremtidige tekniske, regulatoriske og samfundsmæssige krav gennem koordineret udvikling og fælles styring.

6 Næste skridt – hvordan kommer vi videre?

Det tekniske målbillede med tilhørende modenhedsvurderinger, transition- og transformationsdokumenterne er i vid udstrækning dokumenter som fungerer som opslagsværk til inspiration for det videre arbejde.

På den korte bane, kan de væsentligste aktiviteter opsummeres følgende:

I transitionsorganisationen:

- Etabler transitionsenheder med beslutningskompetence og ressourcer til at bemande en projektorganisation
- Skab et koordinationsudvalg på tværs af enhederne, som kan fastlægge eventuelle 'fælles-fælles' standarder, f.eks. omkring logning
- Etabler de kommunerettede standarder først f.eks. kortlægning og dokumentation af konfigurationerne (gerne i et CMDB)
- Understøt kortlægning af eksisterende infrastruktur i ejerkommunerne
- Skab et overblik over aktiviteter på den kritiske vej ift. overdragelsestidspunktet (31/12-2027), f.eks. fysiske omgivelser, nødvendige services og klogt genbrug af eksisterende infrastruktur med respekt for det ønskede målbillede
- Etabler et overblik over kommunernes modenhed, vha. kommunernes selvevaluering
- Definér første udkast til et servicekatalog, baseret på kommunernes ønsker og målsætninger
- Start etableringen af en onboarding proces, se onboarding eksemplet
- Udarbejd detaljerede arbejdsplaner, herunder overdragelsesplan.

I kommunen:

- Etabler en projektorganisation og bemand alle roller efter den foreslåede transitionsmodel
- Definér de ønskede services med tilhørende niveau for enheden, f.eks. ved brug af den leverede scoringsmodel
- Start modenhedsvurdering, opdel evt. ift. fagområder som skole, hjemmepleje og kontor
- Start kortlægning af eksisterende infrastruktur - Hardware såvel som software, licenser, og aftaler med leverandører og registrer dette i et konfigurationsstyringssystem (CMDB)
- Indsaml og opdater relevant applikations dokumentation på servere som ønskes flyttet
- Definér målsætning for transitionen ved overdragelse til enheden, baseret på modenhedsvurdering og kortlægning
- Udarbejd en Gap analyse mellem nuværende situation og ønsket målsætning ved overdragelse
- Udarbejd detaljerede arbejdsplaner, herunder overdragelsesplan.