2.3 Teknisk målbillede - Driftsplatform

Inspiration til teknisk målbillede for fælles kommunal IT-drift

08.05.2026 I Version 1.3

Indhold

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 Introduktion

Dette dokument angiver rammerne for det tekniske målbillede for den fælleskommunale datacenterkonsolidering. I dokumentet benyttes betegnelsen driftsplatform, som dækker over 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.

Anbefalingerne for driftsplatformen tager udgangspunkt i behovet for at levere stabil og sikker drift for mange kommuner på en fælles platform. Derfor er fokus på resiliens, automatisering og standardisering, som sikrer høj oppetid, effektiv drift og mulighed for at dokumentere sikkerhed og compliance på tværs af hele platformen.

Konsolideringen omfatter et omfattende og komplekst infrastrukturlandskab, hvor kommunerne i dag opererer med forskellige driftsplatforme, varierende virtualiseringsløsninger, uensartede storage arkitekturer og forskelligartede sikkerhedsmodeller. Kommunerne befinder sig samtidig på forskellige modenhedsniveauer inden for områder som standardisering, automatisering, segmentering, redundans og multi-tenancy, hvilket danner afsæt for det fælles tekniske målbillede og de prioriteringer, der følger heraf.

Målbilledet er struktureret omkring arkitekturprincipper, der tilsammen udgør grundlaget for en sikker, skalerbar og standardiseret fælleskommunal driftsplatform:

1. **Arkitekturprincip: Automatisering:** Infrastructure as Code, konfigurationsstandarder, automatiseret drift, CMDB integration og self-service provisionering.
2. **Arkitekturprincip: Segmentering:** Tenant isolation, applikationsbevidst segmentering, firewall regelforvaltning, monitorering af øst-vest trafik og centraliseret DNS/IPAM.
3. **Arkitekturprincip: Datacentre med multi-tenancy:** Logisk tenant adskillelse, standardiseret onboarding og offboarding, chargeback-modeller, SLA-styring og adgangsstyring i multi-tenant miljø.
4. **Arkitekturprincip: Optimal udnyttelse af ressourcer:** Compute konsolidering og rightsizing, Storage optimering, fælles servicekatalog med VM-skabeloner og proaktiv kapacitetsplanlægning.
5. **Arkitekturprincip: Redundans og resiliens:** Multi site-datacenterdesign, compute-redundans, Storage replikering, immutable backup og automatiseret DR-orkestrering.

Dokumentets overordnede vurdering er, at de fem principper tilsammen etablerer det tekniske og operationelle fundament for en managed driftsplatform leverancemodel, hvor IT-serviceorganisationerne leverer sikker, standardiseret compute, storage og platform som en fuldt managed ydelse til de enkelte kommuner.

I læsevejledningen til denne dokumentpakke findes begrebsforklaringer og kildehenvisninger.

2 Nuværende situation (as-is kortlægning)

2.1 Overordnet landskab

As-is kortlægningen foretaget af KL har afdækket et kommunalt landskab præget af heterogenitet.

Det vurderes, at denne infrastruktur repræsenterer en betydelig variation i både teknologivalg, kompetenceniveau og modenhedsgrad. Kommunale datacentermiljøer er udviklet gradvist over tid, ofte med fokus på løbende behov frem for et samlet arkitekturprincip, hvilket kan medføre begrænset skalerbarhed og varierende grad af dokumentation.

2.2 Forventede variationer og modenhedsforskelle

2.2.1 Standardisering og automatisering

Baseret på arbejdet med opgaven vurderes det, at der er markante forskelle i standardiserings- og automatiseringsgraden på tværs af kommunerne. Nogle opererer med formaliserede konfigurationsstandarder, versionsstyrede skabeloner og automatiseret provisionering, mens andre har miljøer, der er konfigureret manuelt uden en overordnet standard. Infrastructure as Code (IaC) er i de fleste kommuner på et tidligt stadie eller endnu ikke i overvejelserne. Navngivning og tagging kan være inkonsistente eller fraværende, og CMDB er muligvis ikke etableret eller opdateres ad hoc.

2.2.2 Mikrosegmentering og netværkssikkerhed

Segmenteringsniveauet varierer fra avanceret mikrosegmentering med identity-baserede policies til helt flade netværk uden logisk adskillelse. Firewall regler kan være vokset organisk over tid med begrænset oprydning og dokumentation. Øst-vest trafikmonitorering er ikke konsekvent implementeret, og DNS/IPAM-arkitekturen er organisk, hvilket medfører risiko for overlappende adresserum.

2.2.3 Multi-tenancy og governance

Formel tenant adskillelse er undtagelsen snarere end normen. Nogle kommuner deler ressourcer i forskellige konstellationer, hvor governance, isolation eller ressourcebegrænsninger måske ikke er det vigtigste. SLA'er er ikke altid formaliseret, og chargeback-modeller baseret på faktisk forbrug er begrænset.

2.2.4 Ressourceudnyttelse og kapacitet

Workload rightsizing er generelt ikke systematisk proces. VM'er kan være overallokerede, og inaktive ressourcer står til rådighed. Storage optimering med deduplikering, komprimering og tiering er ikke konsekvent implementeret. Kapacitetsplanlægning sker ofte reaktivt uden direkte kobling til forventet vækst.

2.2.5 Redundans og resiliens

Nogle kommuner opererer med standalone datacenter design uden sekundær facilitet. Compute-redundans varierer fra fuldt klyngebaseret failover til enkeltstående servere. Storage replikering mellem sites er begrænset, og backupstrategier kan variere, inkl. test af gendannelse. Disaster recovery planer forefindes, men testes sjældent.

2.2.6 Overordnet modenhedsvurdering

Ud fra arbejdet med opgaven vurderes det, at hovedparten af kommunerne befinder sig i det gule scoringsinterval (53–94 point af 120 mulige), svarende til et funktionelt fundament med identificerede gaps. Et mindre antal vurderes at være i det røde interval (24–52 point), hvor grundlæggende transformationsindsats er påkrævet. Kun et fåtal forventes at have høj modenhed (95–120 point). Denne modenhedsfordeling understreger, at overgangen til en fælles driftsplatform kræver differentierede transitionsplaner.

3 Retningslinjer for driftsplatform arkitektur

De følgende retningslinjer beskriver en mulig målarkitektur for konsolidering af driftsplatformen i en fuldt etableret IT-serviceorganisation. Retningslinjerne udtrykker den tilstand, hvor kommuner og IT-serviceorganisationer er konsolideret omkring fælles standarder, sikkerhedsmodeller og driftsprocesser.

Retningslinjerne skal læses som et fælles pejlemærke for både kommuner og IT-serviceorganisationer. For kommunerne som en arkitektonisk retning, der understøtter strategiske og tekniske valg over tid, og for IT-serviceorganisationerne som et blueprint for den ydelse og de kapabiliteter, der skal kunne leveres i fælles drift.

Retningslinjerne er bevidst formuleret normativt og teknologi- og leverandøruafhængigt for at sikre langsigtet robusthed og skalerbar drift. Afvigelser fra retningslinjerne kan forekomme, men skal være bevidste, dokumenterede og håndterede som led i en planlagt transition mod en fælles målarkitektur.

3.1 Arkitektur princip: Automatisering

3.1.1 Retningslinje 1: Navngivning, labelling og tagging

Alle infrastrukturobjekter navngives efter en dokumenteret og automatisk håndhævet konvention. Tags og metadata markerer konsekvent ejer, kritikalitet, miljøtype, backup-klasse og tenant tilhørsforhold og driver aktivt automatisering, compliance-kontrol og omkostningsallokering.

Stordriftsfordele: Fælles navngivnings- og tagging-standard på tværs af 98 kommuner sikrer ensartet rapportering, automatisering og governance.

3.1.2 Retningslinje 2: Konfigurationsstandarder og compliance

Dokumenterede konfigurationsbaselines eksisterer for alle primære systemtyper og håndhæves automatisk via policy-as-code og kontinuerlig compliance scanning. Konfigurationsdrift detekteres og korrigeres automatisk med en fuld audit trail.

Stordriftsfordele: Central konfigurationsstyring reducerer driftsrisiko og sikrer en ensartet baseline på tværs af tusindvis af systemer.

3.1.3 Retningslinje 3: Infrastructure as Code (IaC)

Al infrastruktur er defineret deklarativt i kode og udrulles via CI/CD-pipelines med automatiseret validering, test og deployment. Infrastrukturen er fuldt reproducerbar fra kode alene, og manuelle ændringer er elimineret. Versionsstyring med fuld historik og mulighed for tilbagerulning er standard.

Stordriftsfordele: Automatiseret provisionering muliggør onboarding af kommuner på få timer i stedet for uger.

3.1.4 Retningslinje 4: CMDB og asset management

CMDB er integreret med driftsplatformen via API og opdateres automatisk i realtid. CMDB driver aktiv automatisering, change management og konsekvensanalyse. Alle infrastrukturkomponenter er registreret med attributter for ejer, kritikalitet, miljø, tenant tilhørsforhold og livscyklusstatus.

Stordriftsfordele: Automatiseret CMDB muliggør præcis konsekvensanalyse og kapacitetsplanlægning på tværs af alle tenants.

3.1.5 Retningslinje 5: Automatiseret drift og self-service

Fuld driftsautomatisering med event-drevet orkestrering, self-healing og omfattende self-service. Driftsorganisationen opererer primært via undtagelseshåndtering. Self-service portaler dækker det fulde spektrum af tenant forespørgsler med automatiseret provisionering, compliance valideringog omkostningsberegning.

Stordriftsfordele: Self-service og automatisering reducerer behovet for driftspersonale markant og giver kommunerne hurtigere adgang til ressourcer.

3.2 Arkitektur princip: Segmentering

3.2.1 Retningslinje 6: Netværkssegmentering og tenant isolation

Mikrosegmentering er implementeret på workload niveau med identity baserede policies. Segmentering er dynamisk og tilpasses automatisk ved deployment af nye workloads. Deny-by-default firewall policies er standard, og lateral bevægelse mellem systemer kræver eksplicit policy-godkendelse.

3.2.2 Retningslinje 7: Applikationsisolation og workload policies

Fuld applikationsbevidst mikrosegmentering med automatisk policy generering baseret på workload identitet. Policies opdateres dynamisk og valideres kontinuerligt mod den tilladte kommunikationsmodel. Anomalidetektion identificerer automatisk uventet applikationskommunikation.

3.2.3 Retningslinje 8: Firewall regelforvaltning

Automatiseret firewall policy management med lifecycle styring, automatisk udløb af midlertidige regler og kontinuerlig analyse af regeleffektivitet. Firewall regler styres via policy-as-code med automatiseret deployment og versionsstyring.

3.2.4 Retningslinje 9: Øst-vest trafikmonitorering

Realtids-analyse af al øst-vest trafik med adfærdsbaseret anomalidetektion og automatiseret respons. Fuld synlighed i alle interne kommunikationsflows på tværs af alle tenants, integreret med SIEM/SOAR-platformen.

3.2.5 Retningslinje 10: DNS, IPAM og adressearkitektur

Fuldt automatiseret IPAM og DNS integreret med provisioneringsworkflows. IP-allokering, DNS-opdatering og adresseplan udvidelse sker automatisk uden manuel intervention. Adresseplanen er designet med forudallokeret kapacitet til det fulde antal forventede tenants.

3.3 Arkitektur princip: Datacentre med multi-tenancy

3.3.1 Retningslinje 11: Logisk tenant adskillelse

Fuld tenant isolation med automatiseret håndhævelse og dynamisk ressourceallokering. Provisionering af komplette tenant miljøer sker via deklarative skabeloner inden for minutter. Governance revideres løbende med tenant deltagelse.

3.3.2 Retningslinje 12: Tenant onboarding og offboarding

Standardiseret onboarding- og offboarding proces med delvis automatisering og self-service elementer. Onboarding tid er forudsigelig og minimeret via automatisering og standardiserede migrationsværktøjer. Offboarding sikrer fuldstændig oprydning af compute, storage, netværk og adgange.

3.3.3 Retningslinje 13: Chargeback og ressourcerapportering

Realtids forbrugsdata med automatiseret chargeback og self-service rapportering. Tenants har fuld transparens i eget forbrug og mulighed for selv at optimere ressourceudnyttelsen. Automatiserede anbefalinger til omkostningsoptimering præsenteres proaktivt.

3.3.4 Retningslinje 14: SLA-styring og governance

Automatiseret SLA-monitorering med realtids dashboards, proaktiv risikostyring og kontinuerlig forbedring. SLA-brud detekteres og eskaleres automatisk. Governance modellen beskriver ansvar, eskalering og beslutningskompetence.

3.3.5 Retningslinje 15: Adgangsstyring i multi-tenant miljø

Zero-trust adgangsmodel med just-in-time adgang, kontinuerlig verifikation og automatiseret lifecycle styring. Fuld audit trail for alle administrative handlinger. MFA er påkrævet for al administrativ adgang, og RBAC med tenant adskillelse er standard.

3.4 Arkitektur princip: Optimal udnyttelse af ressourcer

3.4.1 Retningslinje 16: Compute konsolidering og rightsizing

Automatiseret og kontinuerlig rightsizing med dynamisk ressourceallokering. Overallokering forhindres via policies, og ressourcer recirkuleres automatisk. Inaktive VM'er identificeres og afvikles via automatiseret proces.

3.4.2 Retningslinje 17: Storage optimering og deduplikering

Avanceret storage optimering med automatiseret data lifecycle management, dynamisk tiering og kontinuerlig kapacitetsoptimering. Thin provisioning, komprimering og deduplikering er aktiveret som standard.

3.4.3 Retningslinje 18: Fælles servicekatalog og VM-skabeloner

Fuldt automatiseret servicekatalog med self-service provisionering, automatiseret compliance validering og kontinuerlig opdatering. Kataloget dækker komplette applikationsstacks, og nye VM'er provisioneres udelukkende fra godkendte, hærdede skabeloner.

3.4.4 Retningslinje 19: Kapacitetsplanlægning og forecasting

Proaktiv og automatiseret kapacitetsplanlægning med realtids-trendanalyse og forecasting. Kapacitetsplanlægning er integreret med konsolideringskalenderen, så udvidelsen gennemføres, før nye tenants migreres.

3.5 Arkitektur princip: Redundans & Resiliency

3.5.1 Retningslinje 20: Multi site datacenter design

Fuldt aktiv/aktiv multi site design med automatiseret workload distribution og witness site for quorum. Designet understøtter tab af ethvert enkelt site uden servicepåvirkning. Kapaciteten er dimensioneret, så det tilbageblivende site kan håndtere hele lasten.

3.5.2 Retningslinje 21: Compute-redundans og failover

Fuld compute redundans på tværs af sites med automatiseret cross site failover og proaktiv workload distribution baseret på health-monitorering. Predictive failure analysis migrerer workloads præventivt, inden komponentsvigt opstår.

3.5.3 Retningslinje 22: Storage replikering og data-resiliency

Synkron replikering af højkritiske data med automatiseret failover. Differentierede RPO'er valideres kontinuerligt, og data integritet verificeres automatisk mellem primær og sekundær kopi.

3.5.4 Retningslinje 23: Backup-strategi og immutability

Fuldt automatiseret backup lifecycle med immutable kopier, automatiseret gendannelsesverifikation og ransomware beskyttelse. Immutable backup kopier sikrer, at backup data ikke kan slettes eller manipuleres inden for den definerede retentionsperiode.

3.5.5 Retningslinje 24: DR-planer og operationel resiliens

Automatiseret DR-orkestrering med definerede playbooks, automatiseret failover og kontinuerlig validering. DR er integreret i den daglige drift via regelmæssige, automatiserede failover øvelser uden servicepåvirkning.

4 Modningsrejse (transition og transformation)

Modningsrejsen beskriver den faseopdelte vej fra kommunernes nuværende as-is-tilstand til en konsolideret og standardiseret driftsmodel for driftsplatformen. Formålet er at etablere det tekniske og operationelle grundlag, som gør IT-serviceorganisationerne i stand til at overtage og levere en ensartet, sikker og skalerbar managed driftsplatform på tværs af kommunerne.

4.1 Transitionsperioden (nu til 31. december 2027)

- **As-is kortlægning:** Alle kommuner gennemfører en komplet as-is kortlægning af nuværende driftsplatform, herunder virtualiseringsplatforme, Storage arkitektur, netværkssegmentering og backup-løsninger.
- **Modenhedsvurdering:** Hver kommune scores iht. 24-punktsmodellen i samarbejde med IT-serviceorganisationen. Resultaterne danner grundlag for individuelle transitionsplaner.
- **Konfigurationsbaseline:** Etablering af dokumenterede konfigurationsstandarder for alle primære systemtyper som første skridt mod IaC.
- **Navngivning og tagging:** Implementering af fælles navngivningskonvention og tagging-standard for alle nye systemer.
- **CMDB fundament:** Etablering af CMDB med registrering af alle kritiske assets og relationer. Fælles struktur anbefales at baserer sig på key-value pair ("tagging")
- **Segmenteringsfundament:** Implementering af grundlæggende netværkssegmentering med dedikerede zoner pr. tenant og miljøtype.
- **Backup-standardisering:** dokumenterede backup-politikker med regelmæssige gendannelsestests og offsite-kopiering.

4.2 Transformationsperioden (2028–2030)

- Fuld IaC-baseret drift med CI/CD-pipelines og automatiseret validering. Manuelle ændringer elimineret.
- Mikrosegmentering på workload niveau med identity-baserede policies og automatiseret anomalidetektion.
- Multi site aktiv/aktiv datacenter-design med automatiseret workload distribution og transparent failover.
- Fuldt automatiseret servicekatalog med self-service provisionering og compliance-validering.
- Immutable backup med automatiseret gendannelsesverifikation og ransomware beskyttelse.
- Automatiseret DR-orkestrering integreret i den daglige drift via non disruptive testing.
- Zero-trust adgangsmodel med just-in-time access og automatiseret lifecycle styring.
- Realtids chargeback og self-service rapportering med automatiserede optimeringsanbefalinger.

4.3 Risikofaktorer og afbødning

- **Heterogene platforme som transitionsbarriere:** Forskellige hypervisorer og Storage platforme kan komplicere konsolidering. Standardiserede migrationsprocedurer og platformuafhængige principper afbøder dette.
- **Kompetencegab:** IaC og automatisering kræver kombination af drifts- og softwarekompetencer.

- **Datasikkerhed ved migrering:** Migrering af workloads mellem miljøer kræver robust dataintegritetskontrol og validering.
- **Politisk modstand:** Kommuner kan have forbehold mod konsolidering. Klar kommunikation om tenant isolation, governance og servicefordele er påkrævet.

4.4 Faseopdelt roadmap

Område	2026–2027 (Transition)	2028–2029 (Transformation)	2030 (Managed drift)
Standardisering & Automatisering	As-is kortlægning. Konfigurationsbaselines. Navngivning/tagging. CMDB etableret. IaC-pilot.	IaC-baseret drift. Automatiseret provisionering. Self-service portal. Compliance scanning.	Fuld IaC. Self-healing. Management-by-exception. Niveau 5.
Mikrosegmentering	Grundsegmentering. Firewall regeloprydning. IPAM-valg. DNS-konsolidering.	Mikrosegmentering på workload niveau. Øst-vest monitorering. Automatiseret IPAM/DNS.	Identity-baseret segmentering. Anomalidetektion. Niveau 5.
Multi-tenancy	Tenant adskillelse defineret. Onboarding proces dokumenteret. SLA'er aftalt. RBAC implementeret.	Automatiseret onboarding. Chargeback på faktisk forbrug. Zero-trust adgang. Governance-reviews.	Self-service onboarding. Fuld transparens. Niveau 5.
Ressourceudnyttelse	Monitorering etableret. VM-skabeloner. Rightsizing-reviews. Kapacitetsplanlægning påbegyndt.	Automatiseret rightsizing. Storage optimering. Servicekatalog udvidet. Forecasting.	Dynamisk allokering. Fuldt servicekatalog. Proaktiv kapacitet. Niveau 5.
Redundans & Resiliency	Multi site etableret. Backup-standardisering. Compute-klynger. DR-planer dokumenteret.	Aktiv/aktiv design. Synkron replikering. Immutable backup. DR-orkestrering.	Transparent failover. Automatiseret DR. Non-disruptive testing. Niveau 5.

5 Driftsmodel for driftsplatform

5.1 Overordnet driftsmodel

Driftsmodellen baseres på fem bærende principper, der udgør de kvalitative dimensioner for den leverede managed driftsplatform:

- **Cybersikkerhed:** Ensartet højt sikkerhedsniveau baseret på NIS2, ISO 27001 og Statens Tekniske Minimumskrav. Mikrosegmentering, zero-trust og SIEM/SOC integreret i leverancen.
- **Driftssikkerhed:** strukturerede transitionsplaner med kontrolleret overdragelse. SLA-baseret drift med målbare kvalitetskriterier og automatiseret overvågning.
- **Kundetilfredshed:** Tæt samarbejde med den enkelte kommune. Klar rollefordeling. Self-service og transparens i forbrug og performance.
- **Standardisering:** Kommuner modtager en standardiseret managed driftsplatform fra deres IT-serviceorganisation. Enheden bestemmer, hvordan ydelserne leveres.
- **Stordriftsfordele:** Geninvestering af stordriftsgevinster i fælles løsninger, konsolidering og øget sikkerhed.

5.2 Opgavesnit og ansvarsfordeling

I den fælles driftsmodel varetager IT-serviceorganisationen driftsplatformen som en standardiseret managed ydelse. IT-serviceorganisationen varetager:

Compute- og platformsdrift (managed kerneydelse)

Indkøb, ejerskab, konfiguration og levering af hele datacenterinfrastrukturen. Provisionering og lifecycle management af VM'er, containere og platformservices. Automatiseret patching, kapacitetsstyring og performance-optimering.

Cybersikkerhed (integreret i den managed leverance)

Mikrosegmentering og tenant isolation. Adgangsstyring med RBAC og MFA. Logning med tenant isolation. SIEM/SOC-integration. Sårbarhedsscanning og compliance-rapportering.

Storage og databeskyttelse

Storage provisionering med automatiseret tiering og optimering. Backup med immutable kopier og automatiseret verifikation af gendannelse. Replikering mellem sites med differentierede og dokumenterede RPO'er.

Governance og automatisering

Infrastructure as Code med CI/CD-pipelines. CMDB integreret med automatiseret opdatering. Incident-, problem- og release management. Asset management og servicerapportering.

6 RACI-model: Den fælles kommunale driftsmodel

6.1 Ansvarsfordeling for managed infrastrukturydelser

Nedenstående RACI-model er et eksempel på hvordan en ansvarsfordeling kunne se ud, mellem IT-Serviceorganisationerne, den enkelte kommune og eventuelle eksterne leverandører for de fire kerneområder i den fælles driftsmodel. Den faktiske ansvarfordeling skal aftales på regionalt niveau. Modellen afspejler en managed service-model, hvor IT-Serviceorganisationen ejer og driver den fulde infrastrukturstack, og kommunerne er tenants med definerede konsultations- og informationsrettigheder.

Aktivitet	IT-Serviceorganisation	Kommune (lokalt)	Evt. Leverandør
Compute- og platformsdrift			
Indkøb og ejerskab af datacenter-hardware	**A, R**	**I**	**C**
Konfiguration og idriftsættelse af HCI-noder	**A, R**	**I**	**C**
Provisionering af VM'er og containere fra servicekatalog	**A, R**	**C**	**I**
Lifecycle management: patching, opgradering, udfasning	**A, R**	**I**	**C**
Kapacitetsstyring og performance-optimering	**A, R**	**C**	**I**
Fejlhåndtering: detektion, diagnose, eskalering	**A, R**	**I**	**R**
Cybersikkerhed			
Mikrosegmentering og tenant isolation	**A, R**	**I**	**C**
Adgangsstyring: RBAC-rollemodel og policy-design	**A, R**	**C**	**I**
MFA-håndhævelse for al administrativ adgang	**A, R**	**R**	**I**
Centraliseret logning med tenant specifik filtrering	**A, R**	**I**	**C**
SIEM/SOC-integration og hændelsesrespons	**A, R**	**I**	**R**
Sårbarhedsscanning og compliance-rapportering	**A, R**	**I**	**C**
Storage og databeskyttelse			
Storage provisionering med automatiseret tiering	**A, R**	**C**	**I**
Deduplikering, komprimering og kapacitetsoptimering	**A, R**	**I**	**I**
Backup med immutable kopier og retention-politikker	**A, R**	**C**	**I**
Automatiseret gendannelsesverifikation	**A, R**	**I**	**I**
Replikering mellem sites med differentierede RPO'er	**A, R**	**I**	**C**

Aktivitet	IT-Serviceorganisation	Kommune (lokalt)	Evt. Leverandør
Governance og automatisering			
Infrastructure-as-Code: design og CI/CD-pipelines	**A, R**	**I**	**C**
CMDB med automatiseret opdatering og validering	**A, R**	**I**	**I**
Incident-, problem- og release management	**A, R**	**C**	**R**
Asset management og licens lifecycle	**A, R**	**C**	**I**
Chargeback-rapportering og servicerapportering til tenants	**A, R**	**I**	**I**
SLA-monitorering og tenant service reviews	**A, R**	**C**	**I**

R = Responsible (udfører) **A** = Accountable (ansvarlig) **C** = Consulted (konsulteres) **I** = Informed (orienteres)

6.2 Governancestruktur

Strategisk niveau: Kommunerne bevarer det strategiske ansvar. IT-serviceorganisationerne rapporterer på KPI'er knyttet til de fem bærende principper.

Taktisk niveau: SLA-klassificering af service- og leveranceprofiler med dokumenterede redundans- og sikkerhedskrav. Regelmæssige service reviews med tenant repræsentanter.

Operationelt niveau: standardiserede ITIL baserede processer. Automatiseret SLA-monitorering og eskalering. Self-service for standardydelser.

6.3 NIS2-relevans og compliance

Den managed driftsplatform er designet med eksplicit hensyntagen til NIS2-krav:

- Mikrosegmentering med identity-baserede policies og dokumenterede trafikflows.
- Immutable backup med automatiseret verifikation og ransomware beskyttelse.
- Tenant separeret SIEM med defineret retention-politik og krypteret logtransport.
- Zero-trust adgangsstyring med fuld sporbarhed og audit trail.
- Struktureret incident response med koordineret CERT-kapabilitet.
- Auditspor pr. kommune fremvisningsparat for tilsynsmyndigheder.

7 Use Case

7.1 Operationel transformation: Provisionering af en ny virtuel server

Use casen beskriver et optænkt, men realistisk scenarie, hvor et provisioneringsflow benyttes, ud fra en model omkring service leverancer.

Kontekst: En kommune skal have en ny virtuel server til at hoste en opdateret version af et fagsystem. Serveren skal placeres i den fælles infrastruktur (egen tenant) og overholde gældende krav til sikkerhed, backup og netværksisolation.

7.1.1 Niveau 1 - Fragmenteret / Ad hoc

Driftsafdelingen modtager en e-mail fra kommunens IT-ansvarlige med en uformel anmodning om en ny server. E-mailen indeholder et servernavn, et estimeret ressourcebehov og en kontaktperson. En tekniker logger ind på kommunens eksisterende hypervisor og opretter manuelt en ny VM baseret på sin egen erfaring. Under installationen konfigurerer han netværk, DNS og firewall regler manuelt. Serveren placeres i det samme netværkssegment som kommunens øvrige systemer. Navngivningen følger ingen konvention. Ingen tags eller metadata knyttes til serveren, og CMDB opdateres ikke. Backup konfigureres ikke automatisk. Hele processen tager tre til fem dage, og resultatet afhænger af, hvilken tekniker der udfører opgaven.

7.1.2 Niveau 3 - Standardiseret og driftsegnet

Kommunens IT-ansvarlige opretter en anmodning i det centrale ITSM-system via en standardiseret formular med oplysninger om systemets formål, kritikalitetsklasse, ejer og tenant tilhørsforhold. Efter godkendelse provisionerer en tekniker serveren ud fra en godkendt og hærdet VM-skabelon. Serveren navngives efter en dokumenteret standard, og obligatoriske tags tildeles. Netværket placeres automatisk i kommunens dedikerede segment med deny-by-default firewall policies. CMDB opdateres manuelt, og backup-politikken aktiveres baseret på kritikalitetsklassen. Hele processen tager fire til otte timer fra godkendelse til en driftsklar server.

7.1.3 Niveau 5 - Robust og forbedrende

Kommunens IT-ansvarlige logger ind på self-service portalen og vælger ”Ny applikationsserver” i servicekataloget. Portalen guider ham igennem de nødvendige valg, og baseret på hans tenant profil præsenteres kun de tilladte konfigurationer med estimerede månedlige driftsomkostninger i realtid. Inden for minutter eksekverer provisioneringsplatformen en IaC-pipeline: VM’en oprettes fra en versionsstyret, hærdet skabelon; navngivning og tags tildeles automatisk; netværket placeres i det korrekte mikrosegment; backup-politikken aktiveres; CMDB opdateres automatisk; og monitorering konfigureres med tenant specifikke dashboards. Compliance scanning verificerer automatisk, at serveren overholder alle standarder. Hele processen tager under 15 minutter fra anmodning til en driftsklar server.

Denne use case illustrerer, hvordan rejsen fra niveau 1 (lav) til 5 (høj) ikke blot handler om teknisk automatisering, men om en fundamental ændring i driftsmodellen: fra personafhængigt manuelt udførte opgaver til en standardiseret, skalerbar platform, hvor kvalitet, sikkerhed og sporbarhed er indbygget.

8 Stordriftsfordele ved fælleskommunal driftsplatform

Fælles drift som standardiseret managed leverance muliggør en række stordriftsfordele, som ikke er tilgængelige i det nuværende fragmenterede landskab:

- Central sikkerhedsovervågning og SIEM/SOC-kapabilitet retfærdiggjort ved skala på tværs af 98 kommuner.
- Automatiseret compliance-kontrol og rapportering på tværs af tusinder af systemer.
- Fælles servicekatalog med hærdede VM-skabeloner og automatiseret provisionering.
- Kollektive indkøbsaftaler med bedre priser og vilkår for hardware og licenser.
- Muliggør en mere effektiv anvendelse og deling af specialistkompetencer på tværs af kommuner.
- Forudsigelige omkostninger for kommunerne via standardiserede afregningsmodeller.
- Skaber bedre rammer for, at kommunale IT-ressourcer kan prioriteres i forhold til kerneforretning og digital udvikling
- Multi site redundans og DR-kapabilitet, der ikke er økonomisk realistisk for den enkelte kommune.
- Storage deduplikering og kapacitetsoptimering på tværs af tenants med typisk 40–60% besparelse.

9 Eksempel på faseplan og processer til etablering af en driftsplatform

Overordnet procesguide for etablering af platform I et IT-serviceorganisation.

9.1 Indledning

Dette afsnit beskriver de centrale faser og principper for etablering af den logiske infrastruktur i redundante datacentre med en hyperkonvergent infrastruktur (HCI) som fundament for VM-baserede workloads.

Denne guide er derfor formuleret på et generelt niveau og er bevidst leverandør- og platformuafhængig. Formålet er at sikre, at IT-serviceorganisationerne kan etablere en ensartet, redundant og skalerbar platform, der kan håndtere multi-tenant drift med den driftsstabilitet, sikkerhed og automatiseringsgrad, som i scoringsmodellen er 5 (høj).

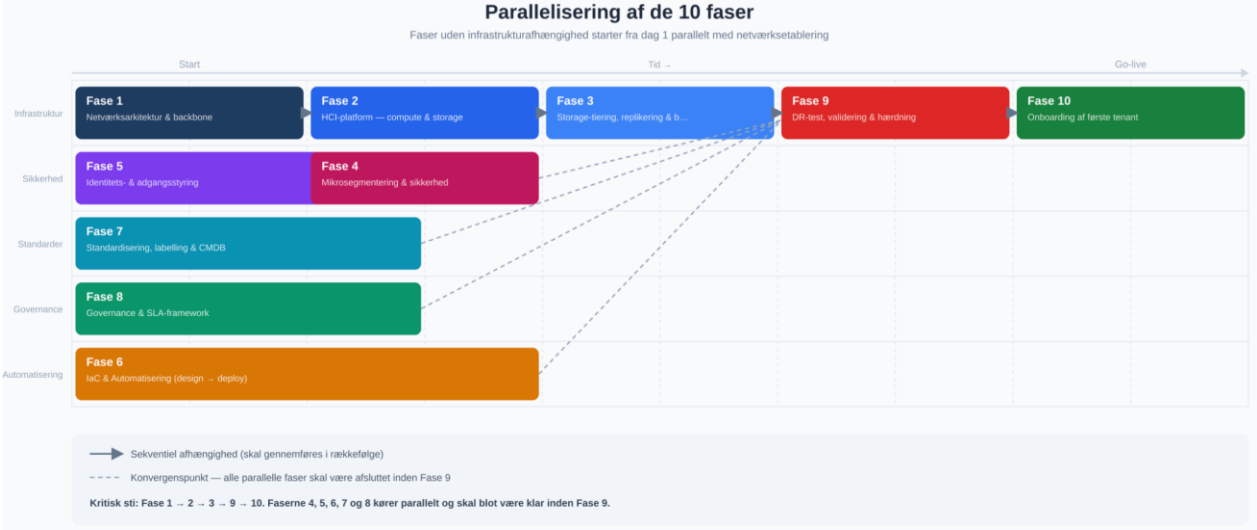
Det forudsættes, at alle fysiske aspekter af etableringen af datacenteret, herunder site-valg, strømforsyning, køling, fysisk sikkerhed og eksterne tilslutninger, er afdækket og på plads. Denne guide fokuserer på den logiske platform: fra netværk og HCI-fundament til idriftsættelse af den første tenant, og er struktureret i 10 faser med tilhørende leverancer og opmærksomhedspunkter.

9.1.1 Målgruppe

Arkitekter med teknisk forståelse for alle komponenter, der indgår i design og opbygning af driftsplatforme.

9.1.2 Parallelle implementeringsfaser

Nedenstående oversigt viser, hvordan de 10 faser kan paralleliseres. Den kritiske sti (Fase 1 → 2 → 3 → 9 → 10) er sekventiel, mens faserne for sikkerhed, standarder, governance og automatisering kan påbegyndes fra dag ét og køre parallelt med etableringen af infrastrukturen.



9.2 Fase 1: Netværksarkitektur & backbone

Det antages, at netværksarkitekturen er rygraden i den fælles platform og skal designes til multi-tenancy, mikrosegmentering og automatisering fra første dag.

Spine-leaf netværkstopologi (eller tilsvarende ikke-blokerende arkitektur) implementeres for at sikre forudsigelig, lav latency og høj båndbredde mellem alle noder i HCI-platformen.

- Dedikerede netværk for storage replikering, vMotion/live migration, management og tenant trafik separeres fysisk eller logisk for at eliminere trafikkonkurrence.
- Redundante forbindelser mellem sites (minimum to uafhængige ruter) dimensioneres til at håndtere fuld replikeringstrafik samt tenant trafik ved failover på site niveau.

- QoS policies implementeres på alle inter site forbindelser for at prioritere replikering og kritisk tenant trafik.
- En skalerbar IP-adresseplan designes med forudallokerede subnets pr. tenant, miljøtype og funktion, understøttet af centraliseret IPAM.

9.3 Fase 2: HCI-platform — compute & storage fundament

Det antages, at en HCI baseret platform udgør det samlede compute- og storage fundament, hvor processorkraft, hukommelse og lagringskapacitet leveres som en integreret, skalerbar enhed. Det forudsættes også, at platformen er i stand til at kunne håndtere tenants.

- HCI-noder deployed i clusters på begge primære sites med identisk eller ækvivalent kapacitet, så hvert site kan håndtere den fulde workload ved failover (N-1 site kapacitet).
- Storage laget konfigureres med den påkrævede redundans (typisk RF2 eller RF3 / erasure coding) for at sikre dataintegritet ved tab af individuelle diske eller noder.
- Compute ressourcer organiseres i ressourcepools med definerede kapacitetsgrænser pr. tenant, håndhævet via policies for at forhindre overforbrug af en ressource.
- Platformen designes til horisontal skalering: tilføjelse af nye noder skal være en standardiseret, ikke-disruptiv operation, der øger både compute og storage proportionelt.
- Hypervisor og HCI management konfigureres med høj tilgængelighed, så tab af management komponenter ikke påvirker den løbende drift af workloads.

9.4 Fase 3: Storage tiering, replikering & backup

Det vurderes, at en differentieret storage strategi er afgørende for at balancere performance, resiliens og omkostningseffektivitet på tværs af kommunernes vidt forskellige workload profiler.

- En tiering model med mindst to niveauer (høj performance og standard) defineres, og placering sker automatisk baseret på workloadens klassificering af kritikalitet.
- Synkron replikering konfigureres for Tier 1 data (RPO = 0) mellem de to primære sites; asynkron replikering for Tier 2-3 data med differentierede RPO'er.
- Deduplikering og komprimering aktiveres som standard på alle storage lag for at maksimere kapacitetsudnyttelsen.
- Backup strategi implementeres med differentierede politikker pr. kritikalitetsklasse, immutable kopier og opbevaring på mindst to geografisk adskilte lokationer.
- Automatiseret gendannelsesverifikation konfigureres, så backup integriteten valideres løbende uden manuel intervention.

9.5 Fase 4: Mikrosegmentering & sikkerhedsarkitektur

Det antages, at sikkerhedsarkitekturen implementeres som en integreret del af platformdesignet. Mikrosegmentering er et af fundamenterne for isolatering af en tenant i en multi-tenant platform (VPC-delen).

- Dedikerede netværkszoner pr. tenant med deny-by-default firewall policies implementeres som standard; al trafik mellem tenants nægtes medmindre eksplicit godkendt.
- Mikrosegmentering på workload niveau konfigureres, så lateral bevægelse mellem systemer, selv inden for samme tenant, kræver eksplicit policy-godkendelse.
- Hærdningsstandarder baseret på anerkendte frameworks (f.eks. CIS Benchmarks) defineres for alle systemtyper og håndhæves via automatiseret compliance scanning.
- Centraliseret logning og overvågning med korrelering på tværs af alle infrastrukturlag konfigureres med tenant specifik filtrering og adgangskontrol.
- Hændelsesresponsplan med specifikke procedurer for multi-tenant scenarier dokumenteres og testes før første tenant onboardes.

9.6 Fase 5: Identitets- & adgangsstyring

Det vurderes, at en robust adgangsstyringsmodel er en forudsætning for sikker multi-tenant drift, hvor driftspersonale fra IT-serviceorganisationen og de individuelle kommuner skal operere på den samme platform med klart afgrænsede rettigheder.

- Rollebaseret adgangskontrol (RBAC) med afgrænsede roller på tenant niveau implementeres, så administratorer kun har adgang til de tenants, de er autoriseret til; cross-tenant adgang kræver separat godkendelse.
- MFA påkræves for al administrativ adgang til alle infrastrukturkomponenter, uanset adgangsmetode.
- Just-in-time-adgang implementeres for privilegerede operationer, så rettigheder tildeles midlertidigt og automatisk tilbagekaldes.
- Kvartalsvise reviews planlægges for alle privilegerede konti med dokumenterede resultater og korrigerende handlinger.

9.7 Fase 6: Automatisering & Infrastructure-as-Code

Det antages, at automatisering er tænkt ind fra dag ét. Al infrastruktur skal være reproducerbar fra kode, og manuelle ændringer skal være undtagelsen.

- Al infrastrukturkonfiguration (compute, netværk, storage, sikkerhed) defineres som kode i et versionsstyringssystem og udrulles via automatiserede CI/CD pipelines.
- Standardiserede, hærdede VM skabeloner etableres i et fælles servicekatalog med defineret livscyklus, versionsstyring og automatiseret opdatering.
- Automatiseret provisioneringsworkflow implementeres, så oprettelse af et komplet tenant miljø (compute, netværk, segmentering, monitorering, backup) kan ske på få minutter.
- Konfigurationsdriftsdetektion etableres, så platformen automatisk kan identificere og korrigere afvigelser fra den godkendte konfiguration.
- Self-service portalen konfigureres for standardiserede tenant forespørgsler med automatiseret godkendelses flow, compliance validering og provisionering.

9.8 Fase 7: Standardisering, labelling & CMDB

Det vurderes, at standardisering af navngivning, tagging og asset management er en forudsætning for både automatisering, rapportering og chargeback i en kommende multi-tenant platform.

- Navngivningskonvention og taggingstrategi defineres og håndhæves automatisk via policies ved provisionering; afvigelser afvises automatisk.
- Obligatoriske metadata pr. objekt inkluderer: tenant, miljøtype, kritikalitetsklasse, ejer, backup-klasse og livscyklusstatus.
- CMDB etableres med automatiseret opdatering via integration med provisionerings- og monitoreringsplatforme; manuelle opdateringer elimineres.
- Chargeback-model baseret på tags implementeres, så ressourceforbrug automatisk allokeres til den korrekte tenant for økonomisk rapportering.

9.9 Fase 8: Multi-tenancy governance & SLA framework

Det anbefales, at governance-modellen for multi-tenant drift er dokumenteret og aftalt med alle parter før den første kommune onboardes. Modellen skal sikre gennemsigtighed, ligebehandling og klar ansvarsfordeling. Forskellige driftsmodeller kan sagtens være en mulighed.

- SLA'er defineres pr. tenant og kritikalitetsklasse med målbare KPI'er for oppetid, performance, responstid og genopretning.
- Governance-modellen dokumenterer ansvar, eskalering, beslutningskompetence og kommunikationskanaler for den fælles driftsorganisation og de individuelle tenants.
- Automatiseret SLA-monitorering med realtids-dashboards og proaktiv alarmering ved potentielle SLA-brud etableres.
- Regelmæssige service reviews med repræsentanter for en kommune planlægges for gennemgang af SLA-performance, hændelser og forbedringsinitiativer.
- Standardiseret onboarding- og offboardingproces dokumenteres med definerede faser, kvalitetskriterier og ansvarsfordeling.

9.10 Fase 9: Disaster recovery test, validering & hærdning

Det vurderes, at den samlede platform skal gennemgå en systematisk validering af alle resiliens mekanismer før den første tenant onboardes. Denne fase er kritisk for at sikre, at designbeslutningerne også fungerer i praksis.

- Komplet site failover-test ved kontrolleret nedlukning af et primært site, med dokumentation af faktisk RPO, RTO og servicekapacitet på det tilbageværende site.
- Witness sitefunktionalitet valideres ved simulering af split-brain scenarier med verifikation af den automatiserede quorum beslutning.
- Compute failover testes ved kontrolleret tab af individuelle noder og verifikation af automatisk workload redistribution uden servicepåvirkning.

- Backup- og gendannelsestests gennemføres for alle kritikalitetsklasser med dokumenterede RTO'er og verifikation af dataintegritet.
- Penetration test og compliance scanning gennemføres mod alle sikkerhedskomponenter, og resultaterne dokumenteres med korrigerende handlingsplaner.

9.11 Fase 10: Onboarding af første tenant & operationel parathed

Det anbefales, at onboarding af den første kommune gennemføres som en kontrolleret pilotfase, der validerer alle processer, automatiseringer og governance-modeller under reelle driftsforhold. Det behøver ikke at være compute-baserede workloads; connectivityelementet (VPC, Virtual Private Cloud) kan også efterprøves i en pilotfase.

- En pilotkommune onboardes med fuld gennemførelse af den standardiserede onboarding proces, inkl. assessment, planlægning, migrering, validering og overlevering.
- Driftsorganisationen bemandes og trænes i alle automatiserede workflows, hændelsesrespons procedurer og multi-tenant governance processer.
- Monitorering, alarmering og rapportering valideres under reel drift med verifikation af tenant specifik filtrering og SLA-rapportering.
- Lessons learned fra pilotfasen dokumenteres og indarbejdes i processer, automatisering og dokumentation, før den næste bølge af kommuner onboardes.
- En skalerings- og kapacitetsplan for de næste 12-24 måneders onboarding udarbejdes baseret på erfaringerne fra pilotfasen.

10 Perspektiv: Agentisk AI for infrastrukturdrift

Det vurderes, at de 10 faser beskrevet i procesguiden repræsenterer den nuværende bedste praksis for etablering af en konsolideret, multi-tenant driftsplatform. Det forventes imidlertid, at fremkomsten af agentisk AI, hvor specialiserede AI-agenter selvstændigt udfører infrastrukturopgaver inden for definerede rammer, vil transformere den operationelle virkelighed for de 5 driftsenheder markant i de kommende år.

Platforme som StackGen illustrerer denne udvikling. Hvor Fase 6 (Automatisering & IaC) i dag forudsætter, at driftsteams manuelt udarbejder deklarative skabeloner (IaC) og CI/CD-pipelines, muliggør en agentisk tilgang, hvor infrastruktur genereres direkte fra beskrivelser, i naturligt sprog, arkitekturdiagrammer eller applikationskode og automatisk oversættes til produktionsklar IaC, der overholder organisationens navngivningskonventioner, tagging policies og sikkerhedsstandarder. Infrastrukturen skrives ikke længere af mennesker; den genereres af AI-agenter, der forstår den specifikke kontekst.

For en multi-tenant platform vil dette potentielt betyde, at tenant onboarding (Fase 10) kan reduceres fra timer til minutter, at konfigurationsdrift (Fase 7) detekteres og korrigeres autonomt, og at sikkerhedshændelser (Fase 4) remedieres automatisk via AI-drevne SRE-agenter, der isolerer kompromitterede workloads og identificerer root cause uden menneskelig intervention. Governance og

compliance kan håndhæves kontinuerligt af en AI-kontrolplan, der sikrer, at ingen ændring bryder de vedtagne regler.

Det anbefales, at de 5 IT-serviceorganisationer allerede i designfasen tager højde for denne udvikling ved at sikre, at den valgte platform eksponerer åbne API'er og understøtter integration med agentbaserede værktøjer. Den investering, der foretages i standardisering, labelling og governance-modeller (Fase 5, 7 og 8), vil udgøre det kritiske fundament, som AI-agenter har brug for: kontekstuel viden om organisationens regler, mønstre og beslutningsprocesser. Uden dette fundament har agentisk AI intet at navigere efter, og med det på plads bliver platformen i stand til at drive sig selv.

10.1 Markedsperspektiv: Gartners forudsigelser for agentisk AI i infrastrukturdrift

Denne udvikling understøttes af markedets førende analysehuse. Gartner forudsiger i rapporten "Predicts 2026: AI Agents Will Transform IT Infrastructure and Operations" (december 2025), at 70% af alle virksomheder i 2029 vil anvende agentisk AI som en integreret del af deres IT-infrastrukturdrift, en stigning fra under 5% i 2025. Gartner fremhæver samtidig, at graden af menneskelig involvering (human-in-the-loop) forventes at falde fra 95% i 2025 til 40% i 2028, og at op mod 50% af I&O-organisationer vil blive omstruktureret inden 2030, i takt med at AI-agenter overtager planlægning og eksekvering af komplekse infrastrukturopgaver.

For de 5 IT-serviceorganisationer understreger dette, at den investering, der foretages i governance, standardisering og automatiseringsfundament i dag, ikke blot tjener den aktuelle konsolidering. Den bygger det fundament, som agentisk AI kræver for at kunne operere sikkert, sporbart og inden for de vedtagne rammer.

Kilde: Gartner, "Predicts 2026: AI Agents Will Transform IT Infrastructure and Operations", Cameron Haight, Ashish Banerjee, Joe Antelmi, Jonathan Forest, Chandra Mukhyala, 4. december 2025.