

A wide-angle photograph of a modern urban street at dusk. The street is lined with multi-story apartment buildings featuring large windows and balconies. The sky is a deep blue, and the buildings' interior lights are glowing, creating a warm contrast with the cool exterior. The street is paved with light-colored tiles and has a few small, dark, cylindrical bollards in the foreground. The overall atmosphere is calm and contemporary.

Rapport GGW

IT-infrastruktur - Organisation och drift

Gislaved, Gnosjö, Värnamo, Vaggeryd
2026-05-04, v 5.0

Stefan Simicic / Gustav Nilsson

ATERA

Agenda

- **Bakgrund och syfte**
- **Nulägesanalys**
 - IT-infrastruktur i de fyra kommunerna
 - Nyligen genomförda och kommande investeringar
 - Identifierade utmaningar och möjligheter
- **Vägen framåt - Alternativa vägval**
 - Nytt eller befintligt datacenter
 - Business case och förväntade effekter
 - Risk- och sårbarhetsanalys, Pros/Cons
 - Analys kommunernas befintliga datacenter
 - Sammanfattande bedömning
- **Faser och genomförandeplan**
 - Transition och faser
 - Kritiska framgångsfaktorer
- **Föreslagen organisation och roller**
 - Organisationsträd, bemanning, kompetens och samverkan



ATEA



Bakgrund

Kommuner står inför växande utmaningar inom IT med ökade krav på säkerhet, regelefterlevnad, kostnadseffektivitet och kompetensförsörjning.

För att möta dessa utmaningar behöver kommunerna skapa en mer effektiv, säker och hållbar IT-verksamhet.

ATERA

Uppdrag

- Genomföra en kartläggning och ta fram ett inventeringsunderlag tillsammans med respektive kommun för att kunna presentera både muntligt och skriftligt en lämplig arkitektur för datacenter, nät, plattformar och klienter, administrationsverktyg och arbetsmodeller, hallplanering och SLA-nivåer för samverkan inom IT-drift mellan kommunerna Gislaved, Gnosjö, Värnamo, Vaggeryd.
- Ta fram en övergripande genomförandestrategi och logik inkl. organisation, resursbehov.
- Delta på plats som expert vid 4-5 strategimöten inom IT-samverkan.
- Presentation av rapport ska ingå i uppdraget för arbetsgruppen på plats i regionen.





Ingångsvärde

Idag arbetar varje kommun med sin egen IT-infrastruktur, med olika system, processer och resurser. Det innebär utmaningar kring säkerhet, kompetensförsörjning och effektivitet.

Men tänk er att i framtiden kunna:

- Leverera digitala tjänster snabbt och säkert till medborgare och verksamheter, oavsett kommungräns
- Dra nytta av gemensam kompetens och moderna plattformar för att möta nya krav på cybersäkerhet, AI och automatisering
- Skapa en robust, flexibel och kostnadseffektiv IT-organisation som stärker både samhällsnytta och affärsnytta
- Vara en attraktiv arbetsgivare för IT-specialister och driva innovation tillsammans



Nuläge

IT-infrastruktur

ATEA

Fokus på IT-drift

IT-Drift

Loggning och övervakning

Patchning

Backup och restore

Incidenthantering

Säkerhet

Integration

Autentisering

Identitet

Federering

Plattformer

Datorer

Mobiler och plattor

OS

Standardapplikationer

Digital arbetsplats

Datacenter

Servrar

Nätverk

Lagring

IT-infrastruktur

Livscykelhantering hårdvara och licenser

Teknisk support och servicedesk

Verksamhet

Behov 1

Behov ..n

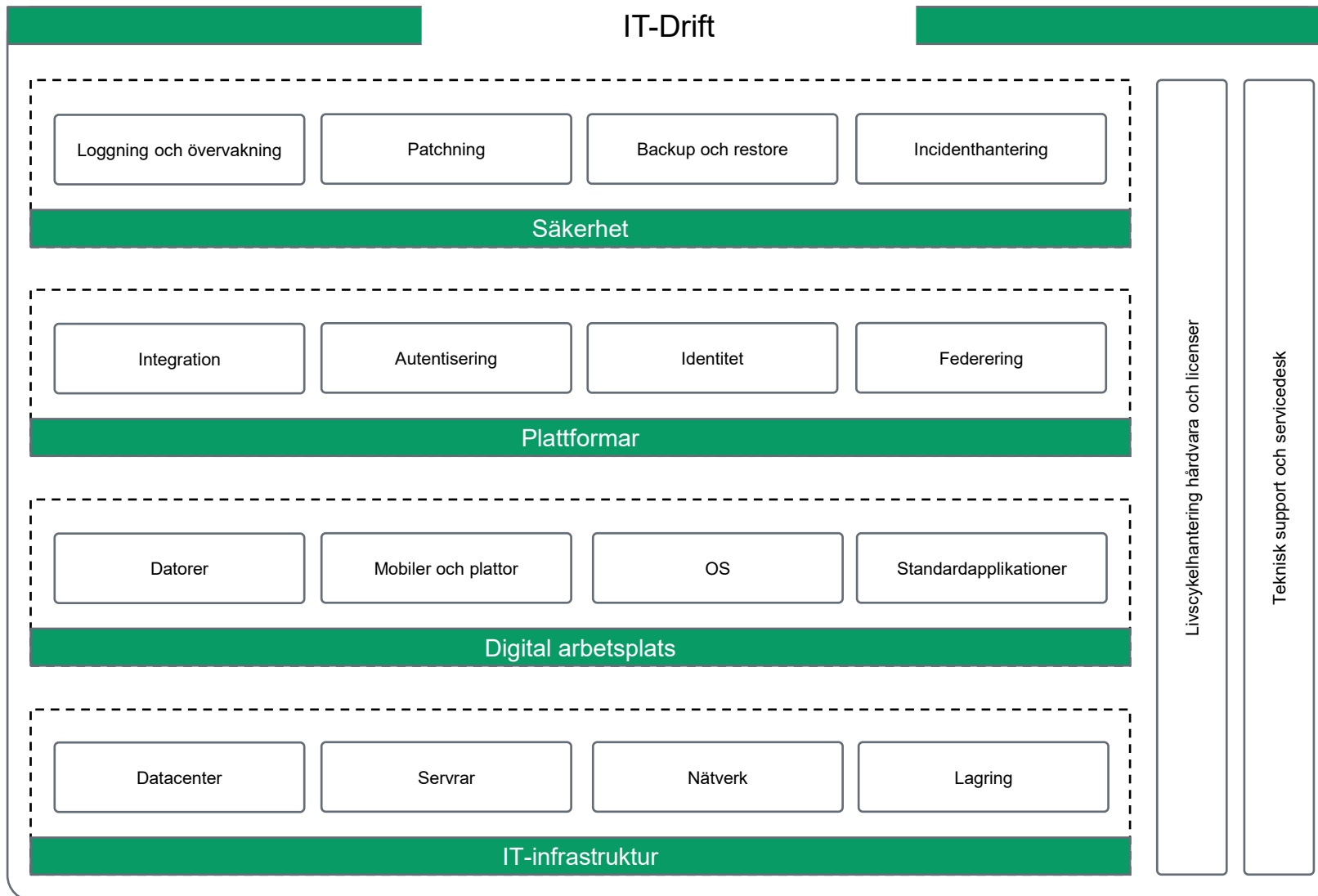
Verksamhetsbehov / utv.

System 1

System ..n

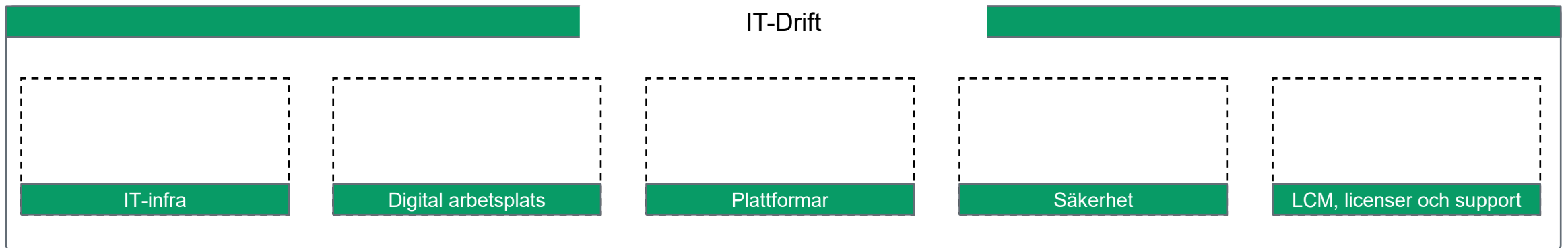
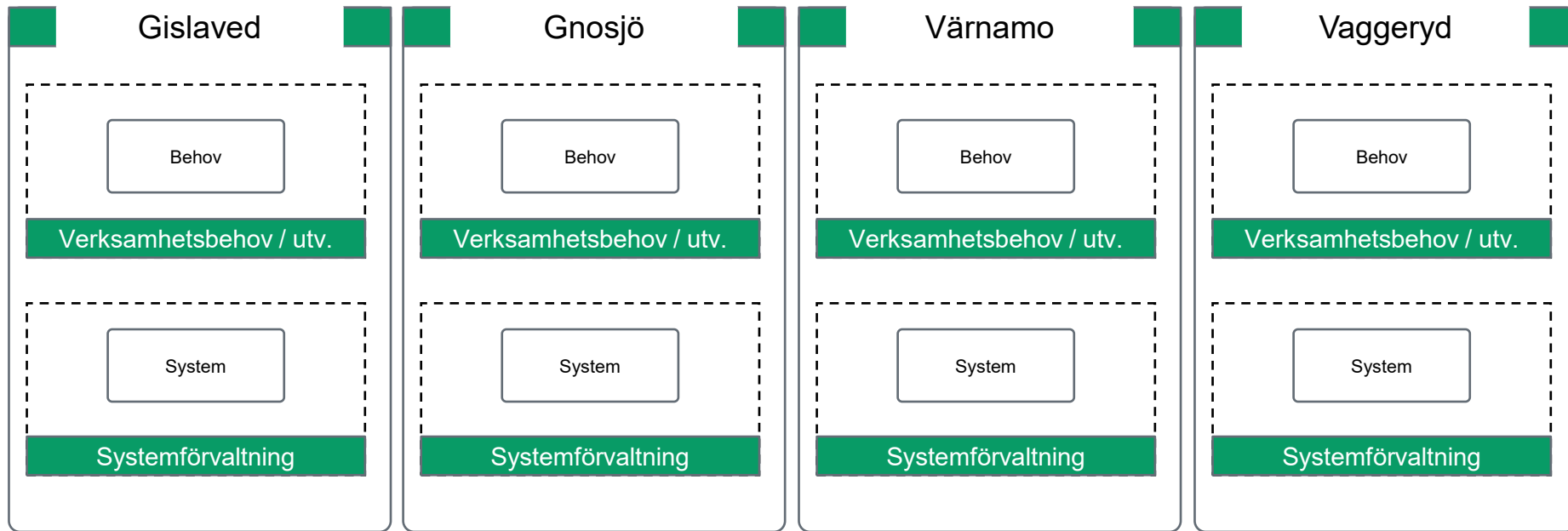
Systemförvaltning

Definition IT-drift

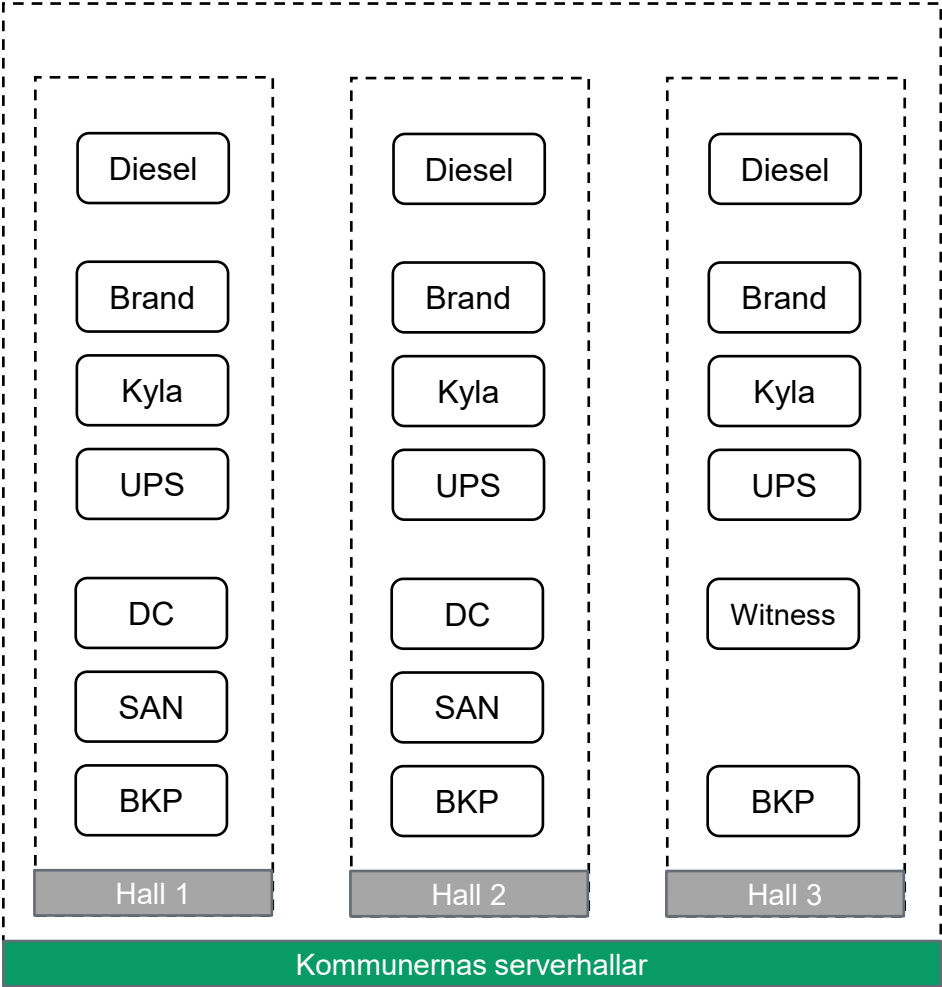


IT-drift omfattar de tekniska och operativa funktioner som krävs för att säkerställa kommunens IT-infrastruktur, plattformar och grundläggande tjänster fungerar stabilt, säkert och effektivt.

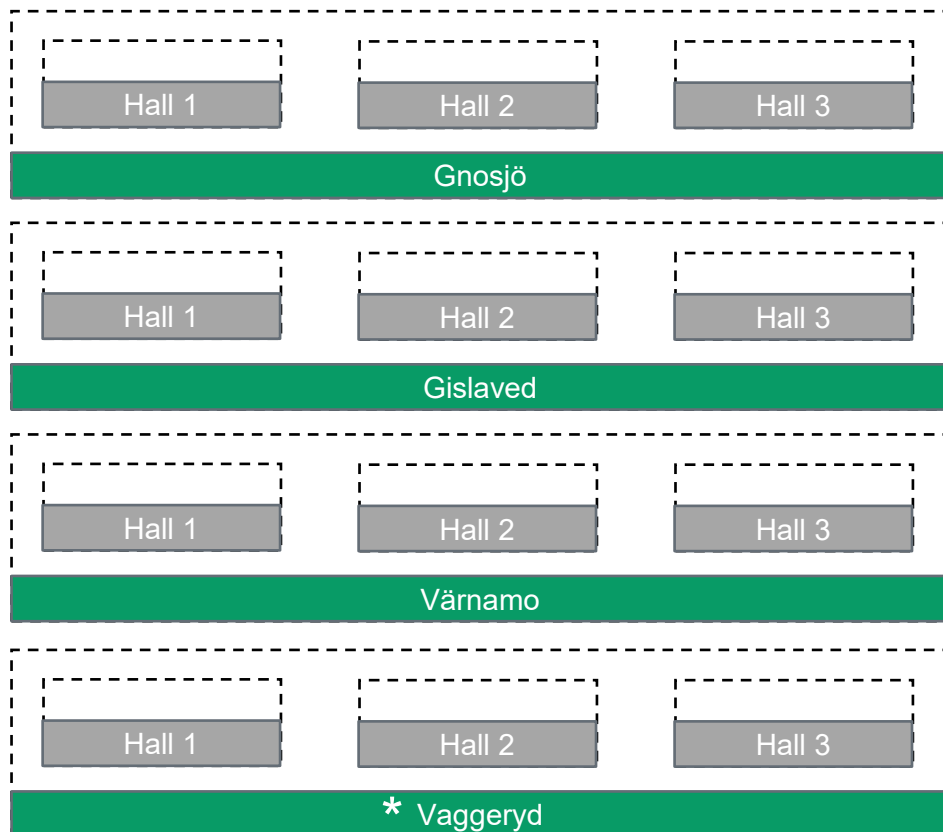
ANSVARSFÖRDELNING



Serverhallar - principbild



SERVERHALLAR - NULÄGE



NULÄGE

Teknisk standard

Varje kommun har tre serverrum med modern och välfungerande infrastruktur för drift av lokala IT-system. Rummen är utrustade med effektiv kylning, UPS-system och dieseldrivna reservkraftsaggregat som säkerställer hög tillgänglighet även vid elavbrott. Den tekniska miljön håller en god standard med stabila racklösningar, korrekt kablagehantering och tillfredsställande fysisk säkerhet.

Drift och redundans

Driften av serverrummen hanteras av respektive kommuns egen IT-organisation. Varje kommun har utformat sina egna rutiner för drift, övervakning och larmhantering. Redundanslösningar finns mellan varje kommuns respektive serverrum. Backup sker lokalt och återställningsprocesser är anpassade efter den egna verksamhetens behov.

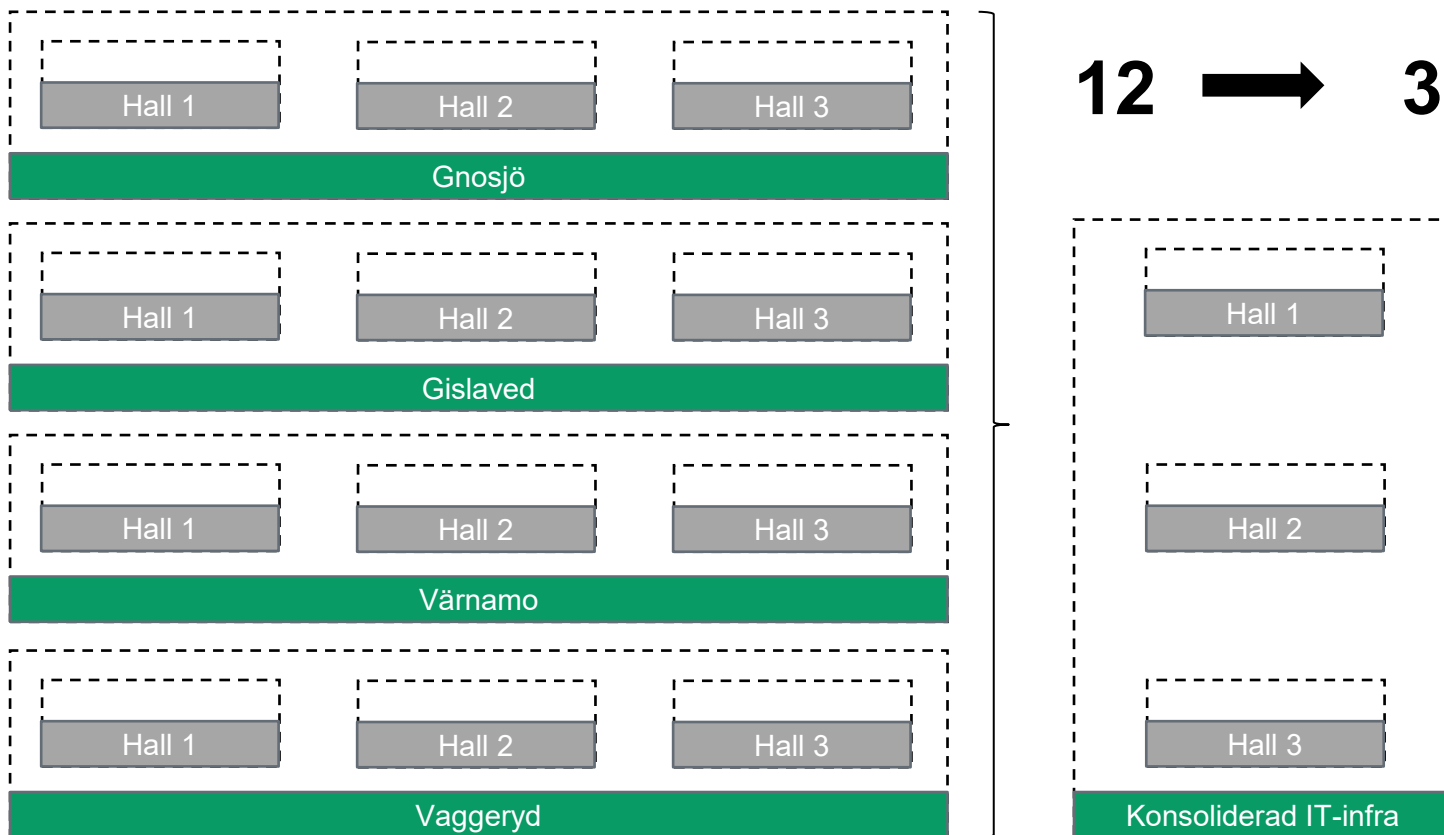
Förvaltning och användning

Varje kommun ansvarar idag självständigt för drift och underhåll av sina egna serverrum.

Säkerhet och åtkomst

Varje kommun ansvarar självständigt för den fysiska säkerheten kring sina serverrum. Säkerhetsnivån är generellt god med låsta utrymmen och passersystem. Åtkomst och behörigheter ges till ett fåtal tekniker eller driftansvariga

Serverhallar - konsolidering



Att gå från 12 till 3 serverrum innebär en betydande effektivisering både driftmässigt och ekonomiskt. Konsolidering minskar behovet av underhåll, el, kylning och övervakning. Färre serverrum och konsoliderad IT-infrastruktur förenklar hantering av backup, patchning och övervakning. Dessutom frigörs lokala resurser och ytor i kommunerna som tidigare använts för serverdrift.



ATEA

ÖVERBLICK

Gislaved	Gnosjö	Värnamo	Vaggeryd
2.700	850	3.100	1.200
Antal anställda			
19	10	25	8
Personal IT-organisation			
2.600	1.300	5.000	2.200
Antal PC (Admin och Skola)			
175	110	280	60
Antal servrar			
1.500	555	1.950	750
Antal nätverksenheter			

Summering

Totalt

7.600

Anställda

62

Personal IT-org.

11.100

Antal PC

620

Antal servrar

4.700

Antal nätverksenh

Trots att varje kommun är relativt liten var för sig, visar den samlade IT-miljön på en betydande organisation.

Med över 11 000 PC, 600 servrar, 4700 nätverksenheter och 62 medarbetare inom IT är det tydligt att **tillsammans förvaltar GGVV-kommunerna en komplex och omfattande digital infrastruktur**, med krav på professionell styrning, hög tillgänglighet och framtidssäkring.



Identifierade *utmaningar* utifrån intervjuerna

Kommunerna står inför flera gemensamma utmaningar, bland annat kompetensförsörjning, tekniska och organisatoriska skillnader samt ökade krav på säkerhet och regelefterlevnad.

Kompetensförsörjning och rekrytering

Svårigheter att rekrytera och behålla rätt IT-kompetens, särskilt spetskompetens inom nätverk, säkerhet och utveckling. Risk för beroende av enskilda personer och intern konkurrens vid rekrytering.

Tekniska och organisatoriska skillnader

Olika tekniska plattformar, fabrikat och lösningar mellan kommunerna kräver omfattande harmonisering och planering. Skillnader i storlek och kultur skapar komplexitet och risk för att mindre enheter tappar inflytande.

Avtal, juridik och ansvarsfördelning

Brist på gemensamma avtal och processer för t.ex. datalagring, personuppgiftsansvar och åtkomst. Risk att en kommun blir ansvarig för en annan utan rätt organisatoriska och juridiska förutsättningar.

Centralisering och lokal förankring

Oro för att centralisering leder till förlorad bredd i arbetsuppgifter och minskat lokalt inflytande. Risk för att personal tappar engagemang och att kompetens försvinner vid bristande kommunikation.

Ekonomi och investeringar

Båda huvudalternativen (bygga nytt eller stärka befintligt) kräver betydande investeringar och resurser. Risk att övergångskostnader underskattas och att ekonomiska konsekvenser inte är tillräckligt analyserade.

Säkerhet och efterlevnad

Ökade krav på cybersäkerhet, NIS2 och GDPR kräver att varje kommun tar stort ansvar, oavsett organisationsform. Bristande backup och struktur för vissa system, t.ex. Office 365.

Kommunikation och förändringsledning

Bristande förståelse för IT-säkerhet och teknikdrivna krav i verksamheten. Oro och osäkerhet kring framtida roller, arbetsuppgifter och jobbsäkerhet. Behov av kontinuerlig och tydlig kommunikation.



ATEA

Identifierade *möjligheter* utifrån intervjuerna

En gemensam IT-organisation öppnar för effektivisering, kompetensutveckling och modernisering. Genom samarbete kan kommunerna dra nytta av skalfördelar, stärkt säkerhet och ökad innovationskraft.

Gemensam organisation och infrastruktur

Möjlighet att bygga en helt ny IT-organisation från grunden, med objektiv rekrytering och rätt kompetens. Skapa en enhetlig och modern infrastruktur som stödjer likvärdig användarupplevelse över kommungränserna.

Effektivisering och kostnadsbesparingar

Gemensamma upphandlingar och arbetssätt kan ge stora besparingar. Samarbete kring support och enklare IT-tjänster är möjligt utan att tappa lokal förankring.

Kompetensutveckling och specialisering

Sammanslagning förväntas ge bättre struktur, möjlighet till specialisering och en modernare, säkrare IT-miljö. Attraktionskraften för IT-specialister ökar och möjligheten till individuell utveckling förbättras.

Standardisering och centralisering

Standardiserade lösningar och centraliserad hantering av programvaror och säkerhet minskar sårbarhet och effektiviserar drift. Möjlighet att införa gemensamma principer och policys kring styrning och teknologi.

Förbättrad säkerhet och compliance

Gemensam backupstrategi, mikrosegmentering och dubbel autentisering stärker säkerheten. Möjlighet att möta ökade krav på informationssäkerhet och lagstiftning.

Flexibilitet och framtidssäkring

Möjlighet att arbeta distribuerat och ändå ha gemensamt ansvar. Framtida organisation kan utformas för att möta både drift- och utvecklingsbehov, inklusive projektledning, arkitekter och verksamhetsnära utveckling.

Lärdomar från andra kommuner

Erfarenheter från Höglandsförbundet och Svenljunga visar att långsiktigt arbete och robusta nätverk ger goda resultat. Inspiration kan hämtas från andra samarbetsmodeller.



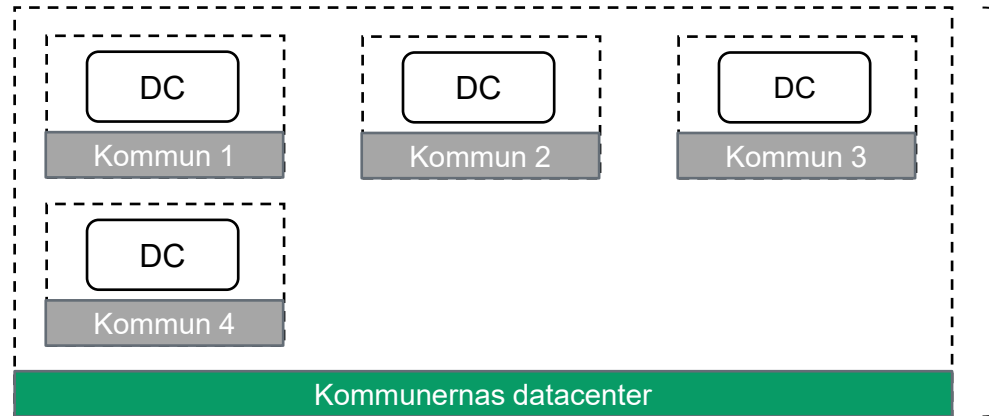
Vägen framåt

Alternativa vägval

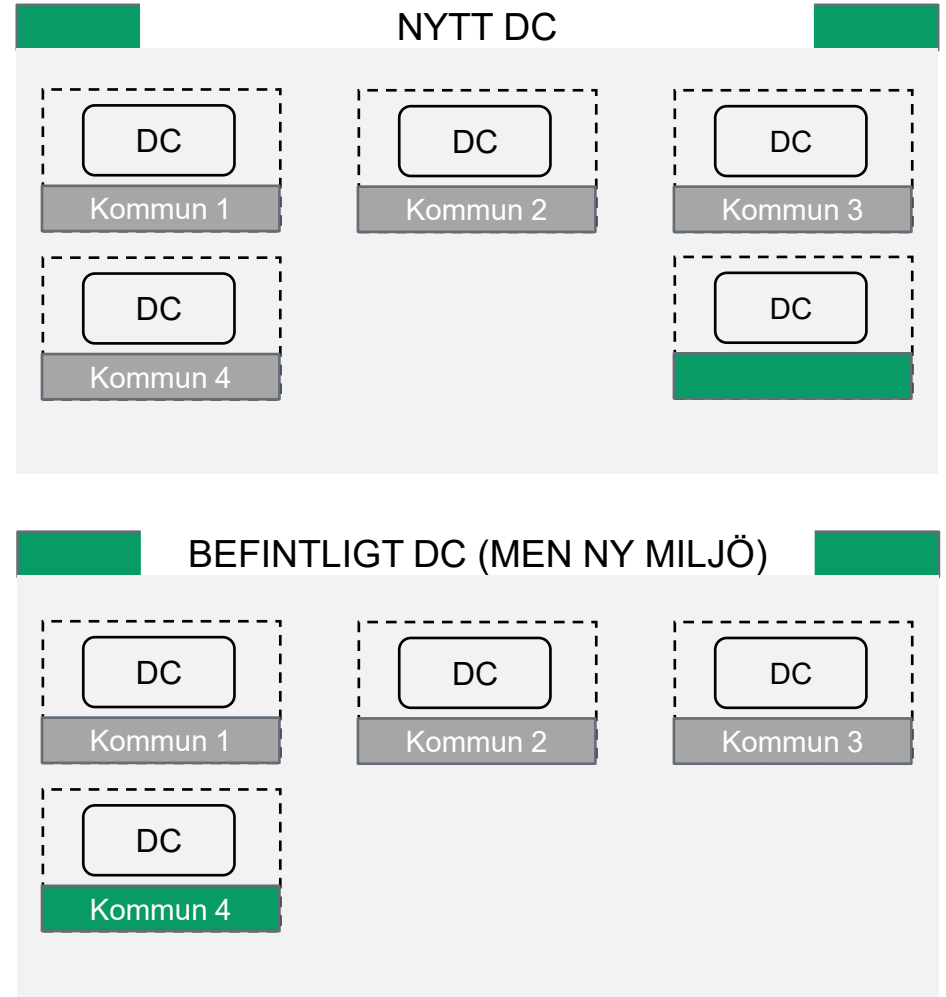
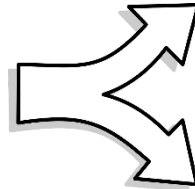


ATEA

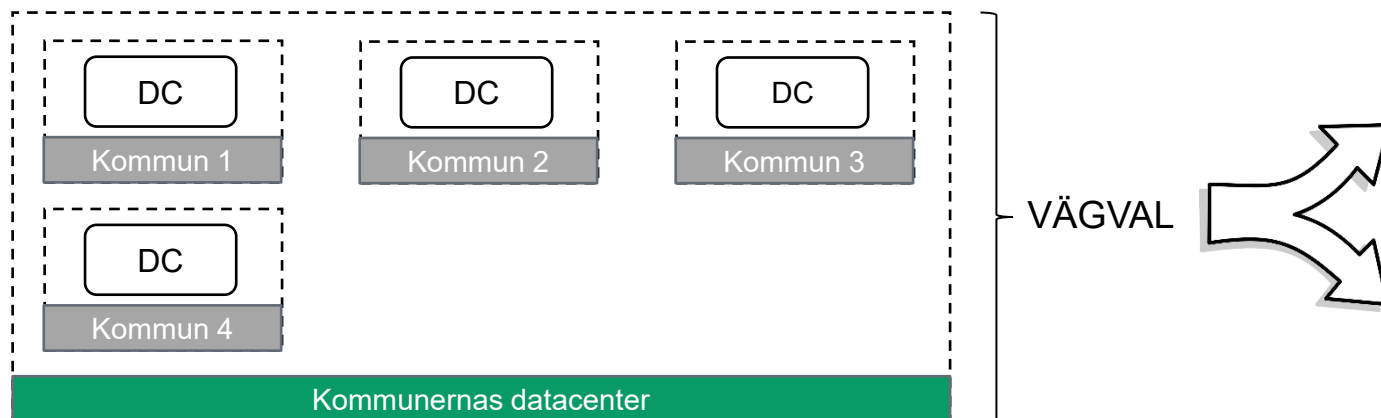
VÄGVAL IT-INFRASTRUKTUR



VÄGVAL



VÄGVAL IT-INFRASTRUKTUR



NYTT DC

IT-organisationen får möjlighet att designa en modern, skalbar och säker infrastruktur från grunden. All hårdvara, datacenternätverk och säkerhetslösningar kan dimensioneras optimalt för den nya gemensamma miljön, utan att behöva ta hänsyn till historiska begränsningar eller tekniska skulder. Detta ger högsta möjliga tillgänglighet, redundans och framtidssäkring, men kräver större initial investering och längre implementationstid.

BEFINTLIGT DC

Återanvända och eventuellt skala upp en kommuns nuvarande datacenter. Här etableras ett nytt logiskt lager (nytt AD, filsystem, nätverk etc.) ovanpå befintlig fysisk infrastruktur. Detta ger betydande besparingar på investeringar och snabbare driftsättning, men innebär att den mottagande kommunen får en central roll och potentiellt större risk för störningar vid migrering och drift. Det kan också finnas tekniska begränsningar i den befintliga miljön som påverkar framtida flexibilitet och säkerhet.

BUSINESS CASE (Tekniskt perspektiv)

	Nytt DC	Befintligt DC
Infrastruktur	Helt ny, optimerad och framtidssäkrad. Möjlighet till maximal redundans och säkerhet.	Återanvändning av befintlig infrastruktur, ev. uppskalning. Risk för tekniska kompromisser.
Investering	Hög initial CAPEX, men lägre OPEX över tid tack vare effektivisering och automation.	Låg initial CAPEX, men risk för ökade OPEX om äldre teknik eller arv kräver mer underhåll.
Implementationstid	Längre ledtid, men färre tekniska kompromisser.	Snabbare driftsättning, men risk för driftstörningar i mottagande DC.
Skalbarhet	Full kontroll över design och framtida expansion.	Begränsad av befintlig DC:s kapacitet och utformning.
Säkerhet	Kan byggas enligt senaste standard (Zero Trust, segmentering, immutable backup).	Risk för kvarvarande sårbarheter om äldre teknik eller processer behålls.

RISK- OCH SÅRBARHETSANALYS

	Nytt DC	Befintligt DC	Kommentar och hantering
Styrning och beslutsfattande	Kräver tydlig styrmodell och gemensam governance från start. Risk för otydliga mandat i övergångsfasen.	Risk för otydligt ansvar mellan parter, särskilt om drift och investeringar fördelas ojämnt.	Etablera styrande forum, beslutsvägar och gemensam roadmap. Dokumentera ansvarsfördelning och mandat tydligt.
Kompetensförsörjning	Möjlighet till specialisering och robust bemanning, men risk för kompetensförlust vid omställning.	Risk för beroende av nyckelpersoner i mottagande DC och ojämn belastning på driftteamet.	Skapa bemanningsplan, kommunicera karriärvägar och säkerställ kompetensöverföring.
Ekonomi och investeringar	Hög initial CAPEX, men lägre OPEX över tid. Risk för politisk känslighet kring investeringsnivå	Lägre initial CAPEX, men risk för dolda kostnader vid uppskalning och framtida reinvesteringar	Tydliggör business case, öronmärk medel och följ upp investeringar och besparingar löpande.
Drift och tillgänglighet	Minimal påverkan på befintlig drift under migrering. Hög tillgänglighet och redundans byggs in från start	Risk för driftstörningar i mottagande DC vid migrering och uppskalning. Begränsad redundans om DC:t inte uppgaderas.	Planera migrering stegvis, upprätta SLA och fallback-planer. Testa kapacitet och redundans innan produktionssättning.
IT-säkerhet	Kan designas enligt senaste standard (Zero Trust, segmentering, immutable backup).	Risk för kvarvarande sårbarheter om äldre teknik eller processer behålls.	Enhetliga säkerhetsprinciper, gemensam SOC och rutiner för incidenthantering. Säkerställ compliance från start.
Regelefterlevnad	Lättare att införa gemensamma processer och roller för GDPR, NIS2 m.m	Risk för varierande nivå på compliance om gamla rutiner lever kvar i befintligt DC.	Utse gemensam compliancefunktion och harmonisera processer innan migrering.
Kulturella skillnader	Kräver aktiv förändringsledning för att skapa gemensam kultur och arbetssätt.	Risk för "vi och dem" känsla om en kommun får för mycket inflytande över DC:t.	Förändringsledning, delaktighet och gemensamma värderingar. Kommunicera syfte och vinster med konsolideringen.
Tekniska standarder	Full kontroll över arkitektur, standarder och versioner.	Risk för teknisk skuld och komplexitet om gamla plattformar och versioner behålls.	Ta fram gemensam referensarkitektur och standarder innan implementation. Planera för gradvis avveckling av äldre teknik
Förändringstakt	Längre implementationstid, men robustare resultat. Risk för stress om tempot blir för högt.	Snabbare start, men risk för långsiktiga kompromisser och behov av framtida omtag.	Kommunicera mål och tidsplan tydligt. Dela upp genomförandet i faser och följ upp kontinuerligt.

PROS OCH CONS - TEKNIKFOKUS

NYTT DC

Ett nytt gemensamt datacenter etableras

PROS

- Helt ny och optimerad infrastruktur, inga tekniska arv eller begränsningar från tidigare miljöer
- Maximal möjlighet till redundans, hög tillgänglighet och modern säkerhetsarkitektur (t.ex. Zero Trust, segmentering)
- Full kontroll över design, kapacitet och framtida skalbarhet
- Möjlighet att införa automatisering och standardisering från grunden (Infrastructure as Code, DevOps)
- Lättare att bygga in stöd för hybrid- och molnlösningar samt framtida teknikutveckling

CONS

- Hög initial investering i hårdvara, datacenternätverk och säkerhetslösningar
- Längre implementationstid innan miljön är produktionssatt
- Risk för tekniska barnsjukdomar i en helt ny miljö utan historik
- Kräver omfattande migrering av data och system från befintliga miljöer
- Större komplexitet i projektledning och teknisk koordinering vid uppstart

BEFINTLIGT DC

En kommuns befintliga lösning används

PROS

- Snabbare driftsättning genom återanvändning av befintlig infrastruktur
- Lägre initial investering där redan existerande hårdvara och nätverk nyttjas
- Möjlighet att stegvis skala upp och modernisera miljön
- Kan dra nytta av beprövade processer och rutiner i det befintliga datacentret

CONS

- Risk för flaskhalsar och begränsad kapacitet om befintlig infrastruktur inte räcker till
- Svårare att uppnå full teknisk standardisering och modernisering
- Kvarvarande teknisk skuld och äldre teknik kan begränsa framtida utveckling
- Ökad risk för driftstörningar i mottagande DC vid uppskalning och migrering
- Begränsad flexibilitet för framtida expansion och integration av nya teknologier

Jämförande analys befintligt DC

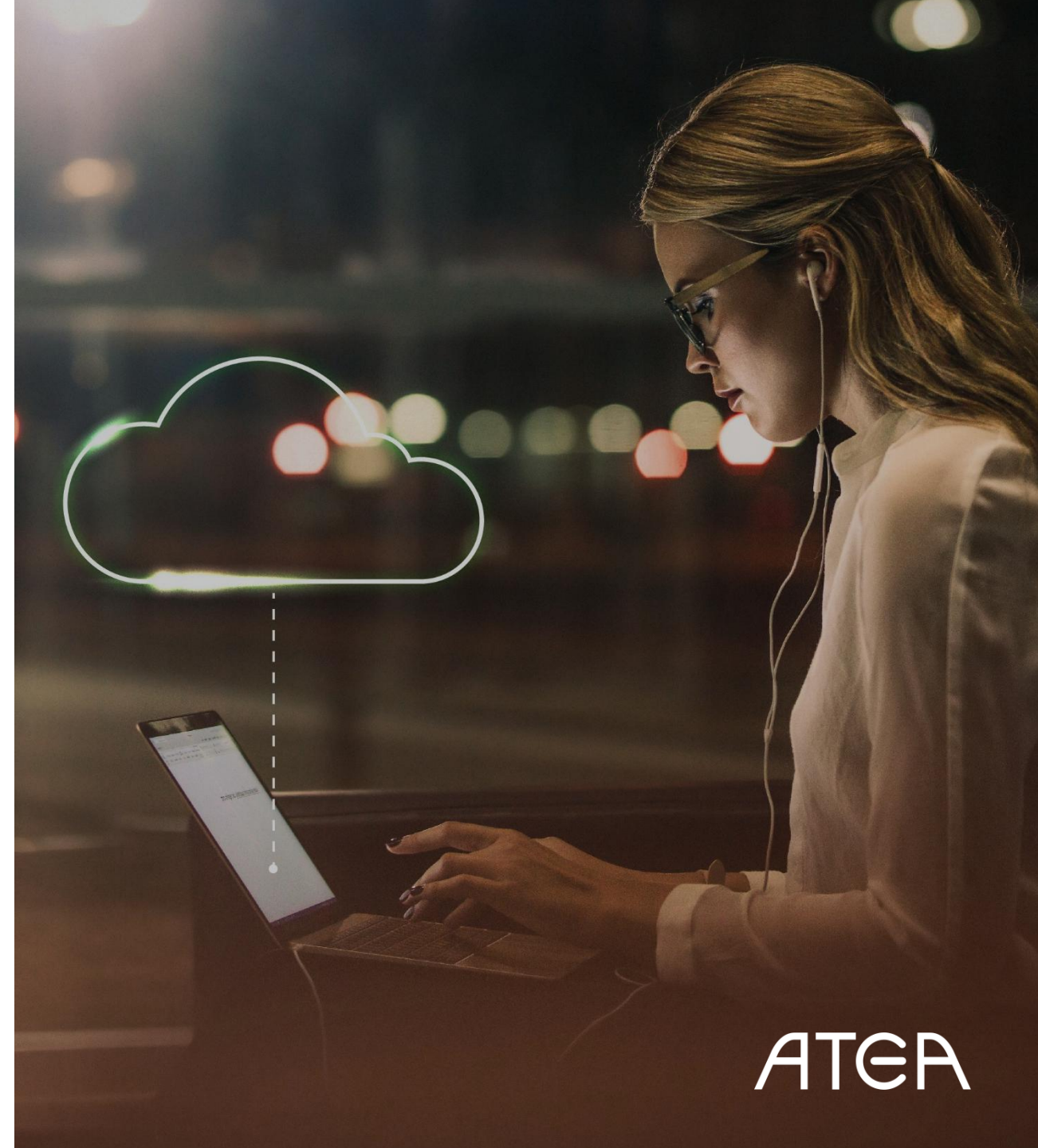
- **Skalbarhet & expansionsmöjligheter** – Kan miljön enkelt byggas ut (ex. fler noder, mer lagring) för att hantera samtliga fem kommuners samlade behov?
- **Parallell drift** – Klarar den att köra både befintlig last och den nya gemensamma plattformens last sida vid sida utan ömsesidig påverkan?
- **Nätverksstruktur & anslutning** – Hur väl ansluten och flersajts-redundant är miljön idag? Hur lätt är det att koppla in övriga kommuner över WAN/fiber?
- **Logisk separation** – Går det att isolera olika arbetslaster (t.ex. olika kommuners system) med virtuella medel (hypervisor, VLAN, storage pools) inom miljön för säker migrering?
- **Risker & begränsningar** – Finns teknikskuld, kapacitetsbrister eller komplexitet som kan utgöra hinder om denna miljö blir den gemensamma plattformens bas?



Sammanfattande bedömning

Förstaval: Befintligt DC - Ett befintligt DC är ett ekonomiskt attraktivt alternativ, men kan innebära tekniska kompromisser och risk för driftstörningar i den mottagande kommunen. Det bör väljas om investeringsutrymmet är begränsat. Situationen med nyinköpt och icke driftsatt DC i Gislaved är det som avgör varför detta alternativ ses som förstaval.

Andraval: Nytt DC - Ur ett tekniskt perspektiv är ett nytt datacenter det mest robusta och framtidssäkra valet. Det möjliggör en optimal design, maximal säkerhet och skalbarhet utan att påverka befintlig drift. Detta alternativ stödjer även kulturell och organisatorisk utveckling i den nya gemensamma IT-organisationen.



ATERA



Besparade investeringar

Genom att nyttja befintlig DC-infrastruktur

Gislaved	Gnosjö	Värnamo	Vaggeryd
	2026 Nytt DC och lagring	2028 SAN Backup VM-Servrar	2025 DC och Lagring - Upphandling pågår

Genom att samordna kommunernas IT-infrastruktur kan betydande investeringar undvikas. Bilagan visar att flera kommuner står inför kostsamma uppgraderingar av lagring, backup och servermiljöer inom 1–2 år. En gemensam plattform eliminerar behovet av parallella investeringar i liknande teknik på flera håll. Istället kan resurser samlas och nyttjas effektivt, vilket ger både ekonomiska och driftmässiga fördelar. Sammanslagningen skapar dessutom bättre förutsättningar för framtida utveckling och gemensam förvaltning.



Faser och genomförande

ATERA

TRANSITION

NULÄGE

Kommunerna har sina respektive IT-organisationer



*Återanvänder befintliga avtal och
reinvesterar i IT-infrastruktur*

TRANSITION

En ny gemensam IT-organisation och IT-miljö etableras



*Skapa gemensam styrning och
organisation samt hantera
befintliga miljöer till nästa steg
är klart*



*Skapa framtidens
gemensamma plattform och
arbetssätt*



*Flytta verksamhetsdata och tjänster
till den nya miljön och stäng ned det
gamla.*

FASER OCH GENOMFÖRANDEPLAN



Etablera och hantera

1

SYFTE: Skapa gemensam styrning och organisation samt hantera befintliga miljöer till nästa steg är klart

FOKUS: styrning, organisation och förändringsledning



Designa och bygg

2

SYFTE: Skapa framtidens gemensamma plattform och arbetssätt

FOKUS: arkitektur, plattformar, säkerhet



Migrera och avveckla

3

SYFTE: Flytta verksamhetsdata och tjänster till den nya miljön och stäng ned det gamla.

FOKUS: tekniskt genomförande, användarstöd, ekonomisk uppföljning

FASER OCH GENOMFÖRANDEPLAN



Målet är att sätta den gemensamma organisationen, etablera styrning och ta ansvar för befintliga miljöer utan att ändra dem i grunden.

Etablera (organisation, styrning) och hantera (befintliga IT-miljöer)

1

SYFTE: *Skapa gemensam styrning och organisation samt hantera befintliga miljöer till nästa steg är klart*

Aktiviteter som omfattas är bla:

- Bilda gemensam IT-ledning och -organisation, arkitekturråd och styrmodell (governance).
- Kartlägga och dokumentera alla befintliga miljöer (servrar, nät, applikationer, licenser, personal).
- Ta över driftansvar och supportprocesser ("as is").
- Harmonisering av basrutiner (incident, backup, behörighetshantering, rapportering).
- Riskanalys för drift under övergångsperioden.

Vad uppnås?

- *Enhetlig styrning och beslutsvägar*
- *Kännedom om alla miljöer och deras risker*
- *Stabil drift utan avbrott*
- *Förberedd organisation inför kommande designarbete*

FASER OCH GENOMFÖRANDEPLAN



Målet är att ta fram målarkitektur, plattformar och processer för en ny gemensam IT-infrastruktur och driftsmodell.

Designa och bygg

2

SYFTE: Skapa framtidens gemensamma plattform och arbetssätt

Aktiviteter som omfattas är bla:

- Fastställa målarkitektur och arkitekturella principer.
- Dimensionera ny miljö (datacenter, moln, nät, arbetsplats).
- Etablera säkerhetsarkitektur (Zero Trust, identitet, backup/DR).
- Välja standardplattformar (ex. M365, SD-WAN).
- Planera livscykel för applikationer (vilka ska moderniseras, avvecklas, flyttas).
- Bygga kärnkomponenter: identitet, nät, basplattform, loggning, automation.
- Ta fram detaljerad migrerings- och avvecklingsplan.

Vad uppnås?

- Färdig målarkitektur och design för alla huvuddomäner.
- Ny miljö klar för pilotdrift.
- Styrmodell för förändringar etablerad.
- Säkerhet, skalbarhet och ekonomi inbyggt från start.

FASER OCH GENOMFÖRANDEPLAN



Målet är att migrera data och tjänster till den nya miljön, stäng ned och avveckla gamla plattformar.

Migrera och avveckla

3

SYFTE: Flytta verksamhetsdata och tjänster till den nya miljön och stäng ned det gamla.

Aktiviteter som omfattas är bla:

- Prioritera system/tjänster och fastställ migreringsordning.
- Testa migreringsverktyg och etablera fallback-processer.
- Flytta identitet, servrar, databaser, integrationer, klienter stegvis.
- Genomföra parallell drift vid behov.
- Avveckla gamla datacenter, serverrum och licenser.
- Utvärdera och optimera efter varje etapp.

Vad uppnås?

- All drift körs i den nya miljön enligt SLA.
- Avvecklade gamla system och frigjord kapacitet.
- Dokumenterad erfarenhet (lessons learned) och etablerad förbättringscykel.

INVESTERINGSKARTA

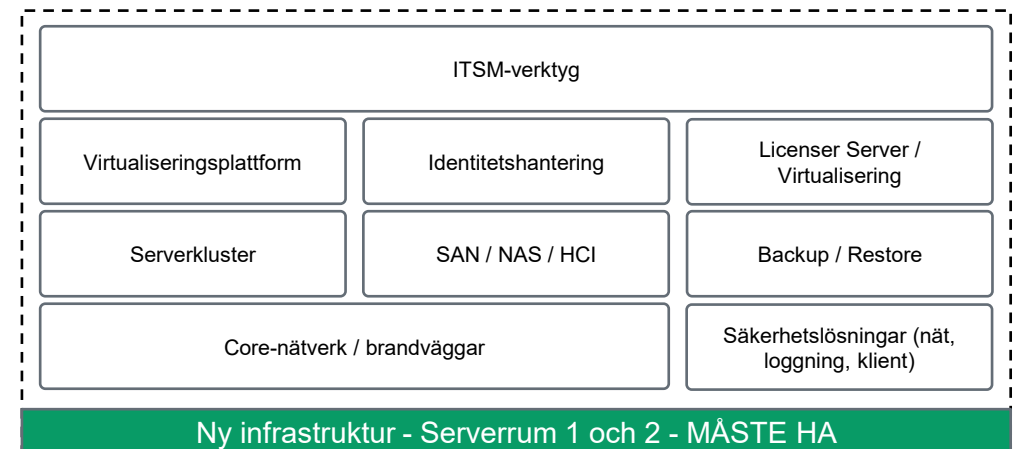


Designa och bygg

Måste ha

- Serverkluster (nya fysiska noder) och virtualiseringsplattform för att drifva den gemensamma miljön.
- Central lagringslösning (SAN/NAS eller hyperkonvergerad) med hög redundans.
- Backup & restore-lösning för hela miljön.
- Två datacenter (befintliga) + en tredje för långtidsbackup och witness
- Kärnnätverk och brandväggar mellan datacentren för redundans och säkerhet.
- Identitetshantering (gemensamt AD/Azure AD, federering, MFA/SSO).
- Grundläggande säkerhetslösningar (antivirus/EDR, segmentering, SIEM/logghantering).
- Server- och virtualiseringslicenser (Windows/Linux, VMware/Hyper-V/KVM).
- ITSM-verktyg (för incident, problem, change)

DC1 och DC2	Primära aktiva zoner och huserar applikationer och data. Separerade geografiskt för redundans.
DR- och Långtids-DC (DC3)	Passiv/Tertiär zon och används för Witness (klusterarbitrering) och Långtidsbackup. <i>Kan användas för offsite replikering för DR.</i>
Core Network och Firewalls	Sammanbinder alla tre DC och styr trafik mellan dem. Brandväggar implementerade både vid in-/utgång (perimetern) och mellan zoner/segment internt (Zero Trust).
Central lagring SAN/NAS/HCI	Högredundant lagring i DC1 och DC2, synkroniserad vid behov. Hyperkonvergerad infrastruktur (HCI) kan användas för enkelhet och skalbarhet.
Backup och restore	Korttidsbackup lagras lokalt i DC1/DC2. Långtidsbackup skickas till DC3. Immutable storage (låst backup) i DC3 för skydd mot ransomware.
Identitetshantering (IDM)	Gemensamt Azure AD/AD som källa för identiteter. Hanterar Federation, MFA, SSO, Conditional Access (villkorlig åtkomst) för att säkra åtkomst baserat på enhetens status.
ITSM-verktyg	Central plattform för Incident, Problem, Asset-, och Change Management.



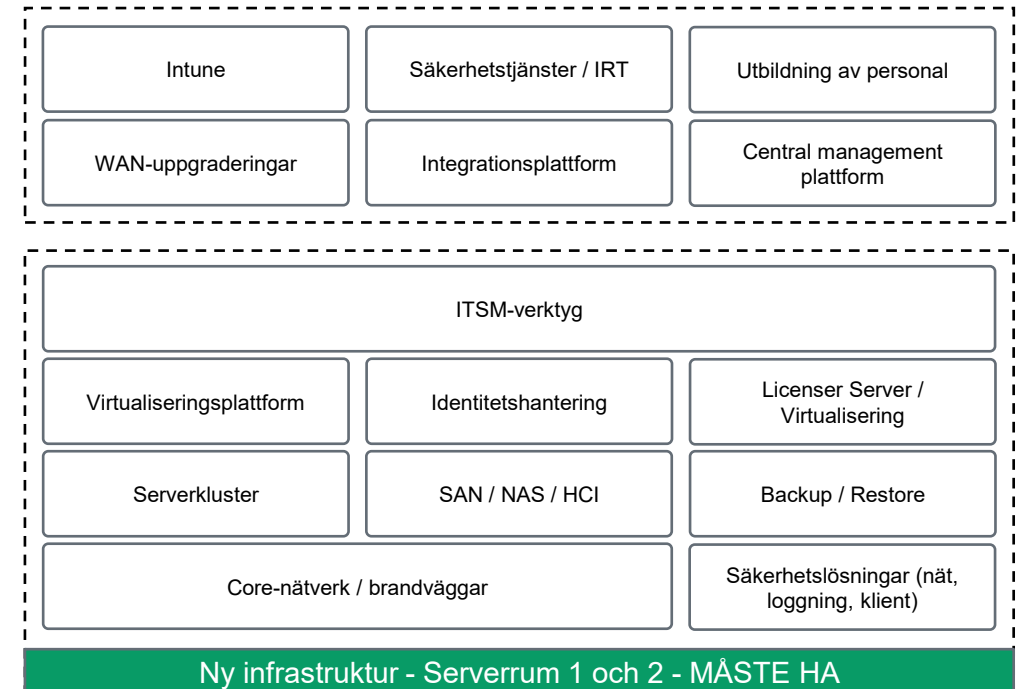
INVESTERINGSKARTA



Designa och bygg

Bör ha (nästa prio)

- WAN-uppgraderingar för att optimera kommunikation mellan kommuner och nya miljöer.
- Integrationstjänster för gemensamma verksamhetssystem.
- Central management-plattform för drift, patchning och övervakning.
- Gemensam klienthantering (SCCM/Intune) för digital arbetsplats.
- Säkerhetstjänster på högre nivå (Zero Trust, DLP, avancerad incidentrespons).
- Utbildning av driftpersonal i nya plattformar.



INVESTERINGSKARTA



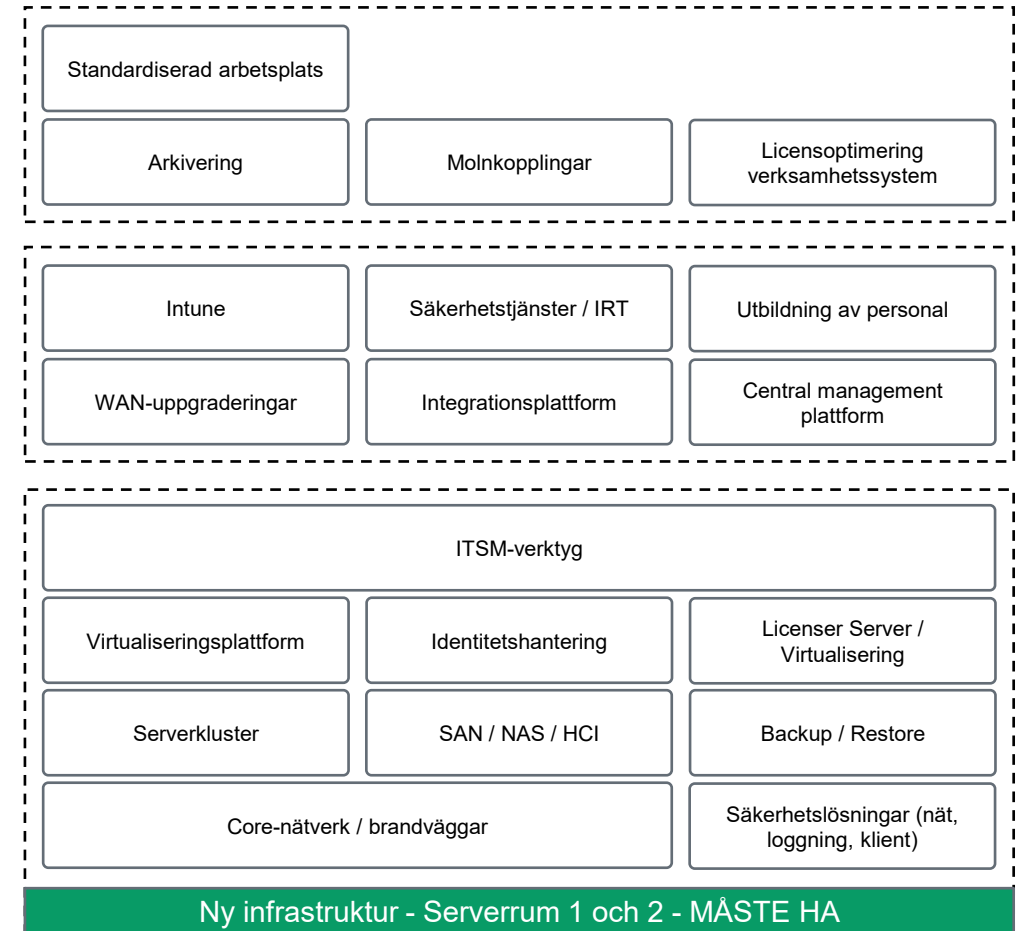
Designa och bygg

Kan vänta (optimering)

- Arkiveringslösning för långtidslagring (separat från backup).
- Molnkopplingar för hybridlösningar (t.ex. Azure Stack, AWS Outposts).
- Samlad licensoptimering för verksamhetssystem (kan göras successivt).
- Optimerade arbetsplatsinvesteringar (standardisering av datorer, plattor, mobiler).



Migrera och avveckla



FASER OCH ROLLER



Etablera och hantera

1

Roller

Förändringsledare, projektledare, jurist,
HR, IT-governance, kommunikatör



Designa och bygg

2

Roller

IT-arkitekt (infra, applikation, data,
integration), nätverks- och
serverspecialist, plattform, testledare,
verksamhet



Migrera och avveckla

3

Roller

Projektledare, migreringsexperter
(klienter, applikationer, databaser),
infosäk, support och servicedesk,
verksamhet

FASER OCH TIDSUPPSKATTNING



Etablera och hantera

1

Timmar
3.000

Interna Externa
2.400 600

4-6 mån →



Designa och bygg

2

Timmar
9.000

Interna Externa
7.200 1.800

10-12 mån →



Migrera och avveckla

3

Timmar
8.000

Interna Externa
6.400 1.600

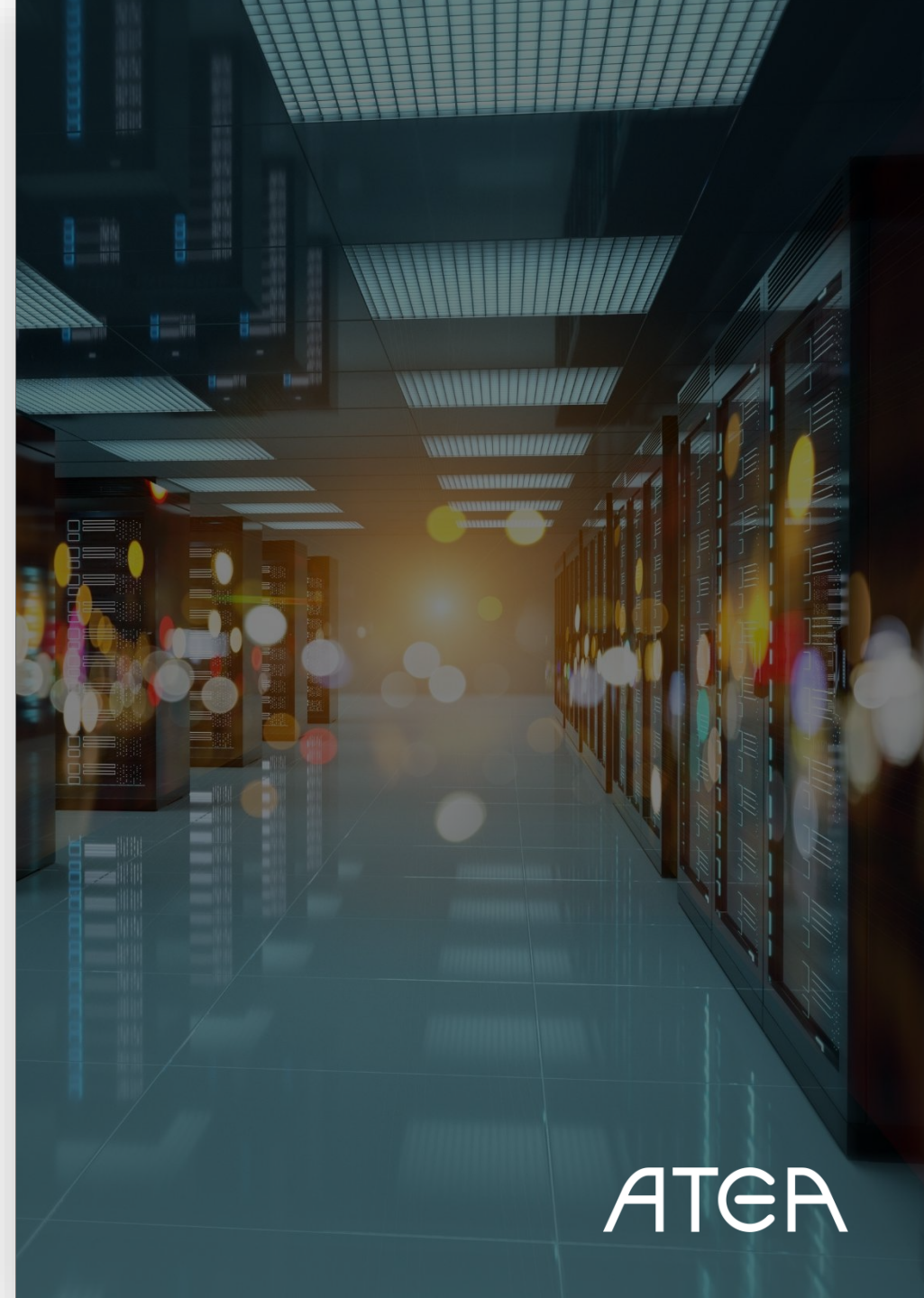
12-24 mån →

ATEA

Kritiska framgångsfaktorer

För att lyckas med en fullständig sammanslagning av kommunernas IT-organisationer krävs tydliga prioriteringar och väl förberedda förutsättningar

Politisk förankring	Tidigt och tydligt stöd från kommunledning och politiska beslutsfattare är avgörande för legitimitet och resurstilldelning. Förankringen bör ske i alla berörda kommuner för att undvika olika ambitionsnivåer.
Gemensam målbild	Alla parter behöver en tydligt definierad vision för hur den nya IT-organisationen ska fungera. En gemensam målbild minskar risken för missförstånd och skapar samsyn kring prioriteringar.
Governance	En styrmodell med klara beslutsvägar, roller och ansvar måste etableras innan projektet startar. Detta ger förutsättningar för effektiva beslut och ett strukturerat genomförande.
Ledarskap	En tydlig ledningsstruktur med engagerade chefer och projektledare behövs för att driva förändringen. Ledarskapet ska inspirera, ge trygghet och kommunicera vinsterna med sammanslagningen.
Kommunikation	Öppen och kontinuerlig dialog med medarbetare, fackliga organisationer och andra intressenter skapar förtroende. Kommunikation ska förklara syftet, hantera oro och lyfta fram framsteg.
Kompetenssäkring	Identifiera nyckelroller och säkerställ att kritisk kompetens finns kvar under hela omställningen. Planera för kompetensöverföring, utbildning och eventuellt nyrekrytering.
Processharmonisering	Kartlägg och jämför befintliga arbetssätt för drift, support och förvaltning. Utifrån analysen etableras gemensamma processer och standarder som alla kan följa.
Teknisk plattform	Beslut om målarkitektur, säkerhetsnivåer och plattformar bör tas tidigt för att styra design och investeringar. Den tekniska lösningen ska möjliggöra effektiv drift och enkel migrering.
Migreringsplan	En realistisk plan för att flytta data, system och tjänster stegvis är central för att undvika driftstörningar. Planen bör inkludera fallback-strategier och tydliga milstolpar.
Budget och finansiering	Projektet kräver en tydligt öronmärkt budget som täcker organisationsförändring, teknik, utbildning och migrering. Tillräckliga medel och en transparent ekonomimodell ger trygghet och förhindrar avbrott i genomförandet.



ATERA

Organisation

ATERA

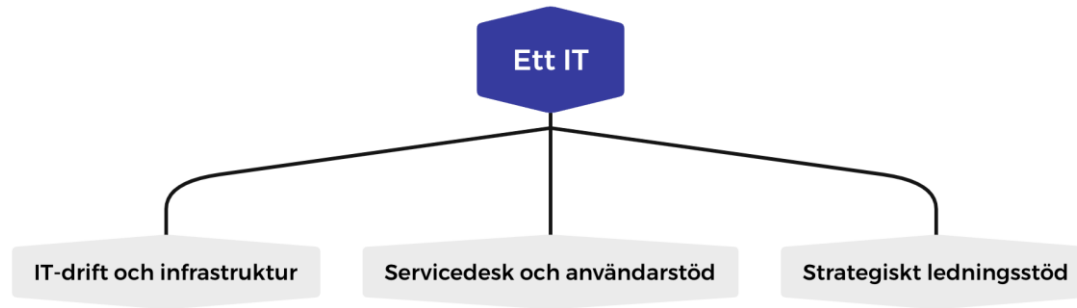
Bemanningsmodell

Roll	Ratio
First line support + LCM	1 per 300-500 användare
Second line support	1 per 800-1200 användare
Servertekniker drift	1 per 100-200 servrar
Nätverkstekniker	1 per 1.000-2.000 användare
Systemtekniker klient	1 per 1.000-1.500 klienter

Totalt idag		
50	62	11.100
IT-drift och support	Personal IT-organisation tot	Antal PC (Admin och Skola)
7.600	620	4.700
Anställda	Antal servrar	Antal nätverksenheter



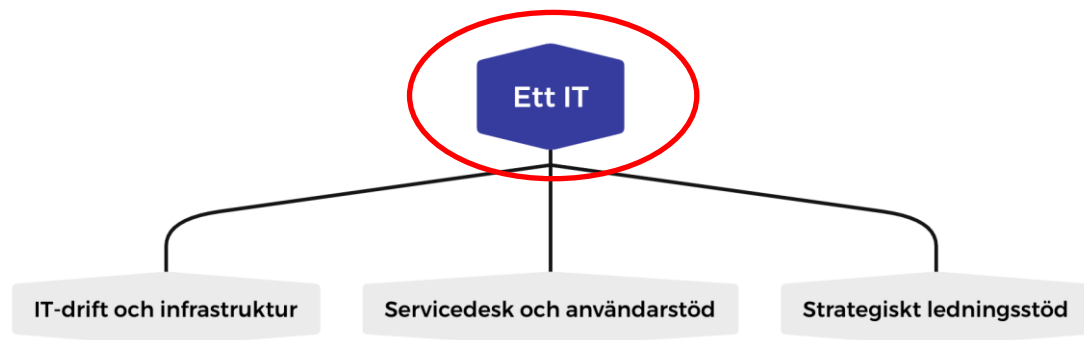
Organisationsträd



Totalt idag		
50	62	11.100
IT-drift och support	Personal IT-organisation tot	Antal PC (Admin och Skola)
7.600	620	4.700
Anställda	Antal servrar	Antal nätverksenheter



Organisationsträd



VD / IT-chef

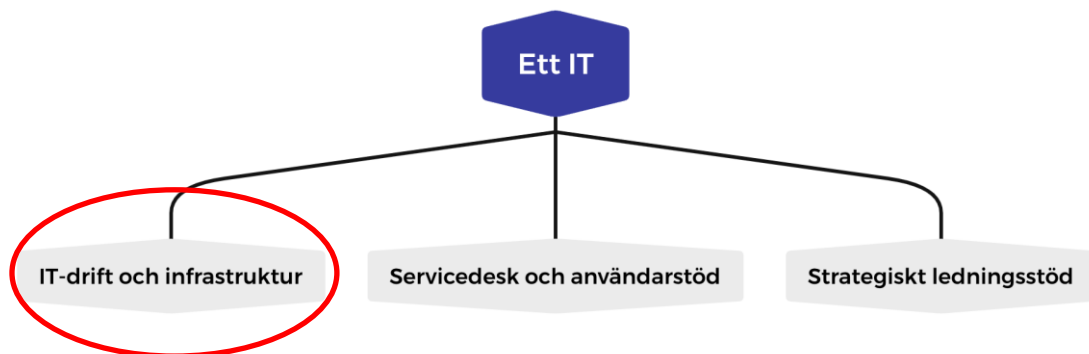
Ansvar: Övergripande ledning av IT-organisationen, strategiskt ansvar för IT-infrastruktur, IT-utveckling och servicedesk, budget och resurshantering.

Rapporterar till: Kommunernas gemensamma politiska / styrande organ (eller styrelse om IT drivs som bolag).

Nyckeluppgifter: Strategi, styrning, uppföljning, risk & säkerhet, rapportering.



Organisationsträd



Enhetschef - IT-drift och infrastruktur

Ansvar: Drift av servrar, lagring, nätverk, datacenter och säkerhet

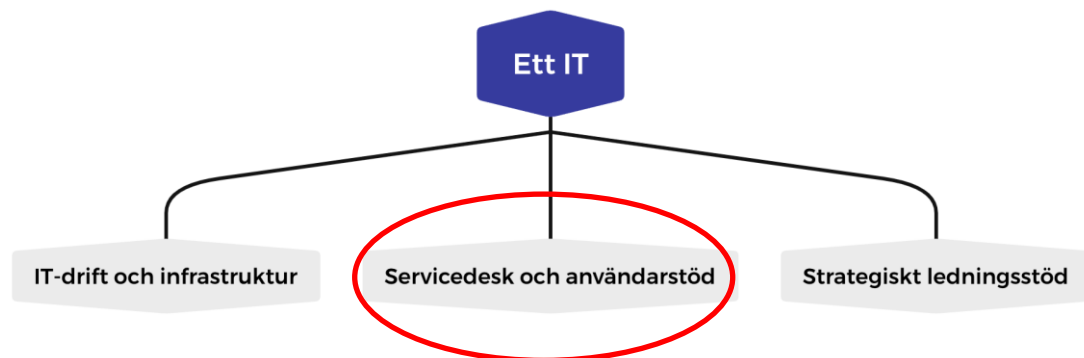
Personal och roller:

- Nätverkstekniker
- Servertekniker drift (Windows/Linux)
- Systemtekniker klient
- Säkerhetsspecialister (inkl. SOC/övervakning)
- DC, Hårdvara, Lagring & backup-ansvariga

Nyckeluppgifter: Operativ drift, SLA-uppföljning, patchning, tillgänglighet, säkerhet, dokumentation



Organisationsträd



Enhetschef - Servicedesk och användarstöd

Ansvar: Hantera alla användarfrågor och incidenter, support, och onboarding av användare.

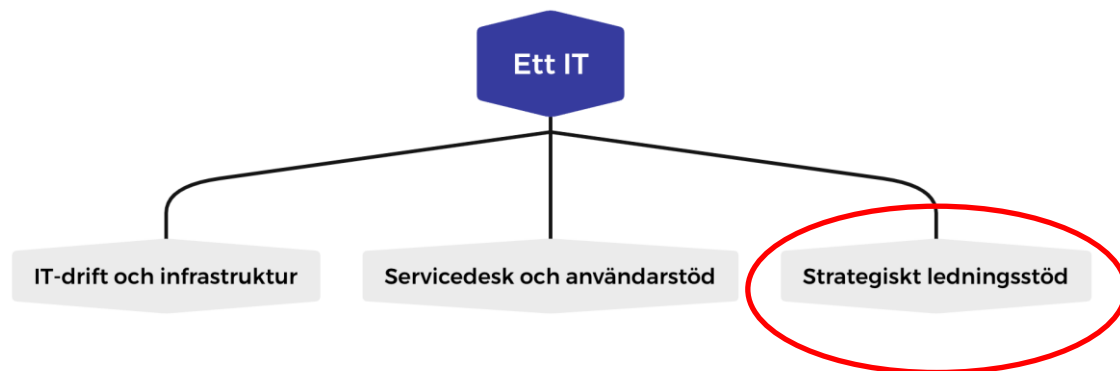
Personal och roller:

- Servicedesktekniker (First line)
- IT-supportspecialister (Second line, klient/os/applikationer)
- IT-tekniker (LCM och på platsen-support)
- Dokumentationsansvarig för instruktioner och processer

Nyckeluppgifter: Incidenthantering, problemhantering, utbildning av användare, dokumentation, supportrapporter.



Organisationsträd



VD / IT-chef är Enhetschef - Strategiskt ledningsstöd

Ansvar: Budget, uppföljning, avtal, licenser, administration, projektstöd och governance.

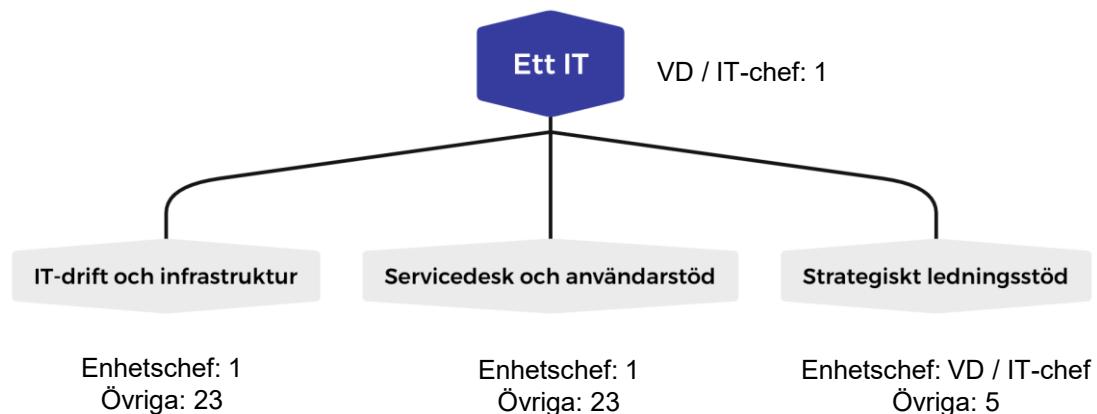
Personal och roller:

- Ekonom/Controller
- Avtals- och licensansvarig
- Administrativt stöd
- Projektcontroller / PMO (stöd till projekt och förändringsinitiativ)
- Säkerhet, arkitektur och IT-verksamhetsutvecklare

Nyckeluppgifter: Budgetuppföljning, ekonomiska analyser, licenshantering, avtal, rapportering till styrelse/ledning.



Organisationsträd (minimalt)



Fördelningslogik

IT-drift & infrastruktur (23) - stort behov p.g.a. 600 servrar + 4.700 nätverksenheter som ska konsolideras och hanteras

Servicedesk (23) - många användare (ca 11.000 PC) kräver stark supportorganisation

Strategiskt ledningsstöd (5) - behövs för att driva organisationen som bolag och hantera licenser, projekt och uppföljning

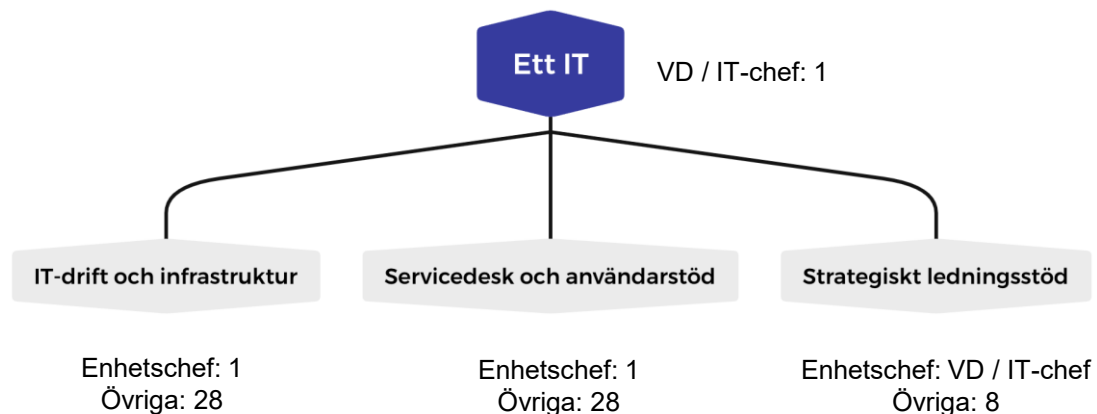
Personal

Chefer : 3

Övriga: 51



Organisationsträd (önskat)



Fördelningslogik

IT-drift & infrastruktur (28) - stort behov p.g.a. 600 servrar + 4.700 nätverksenheter som ska konsolideras och hanteras

Servicedesk (28) - många användare (ca 11.000 PC) kräver stark supportorganisation

Strategiskt ledningsstöd (8) - behövs för att driva organisationen som bolag och hantera licenser, projekt och uppföljning

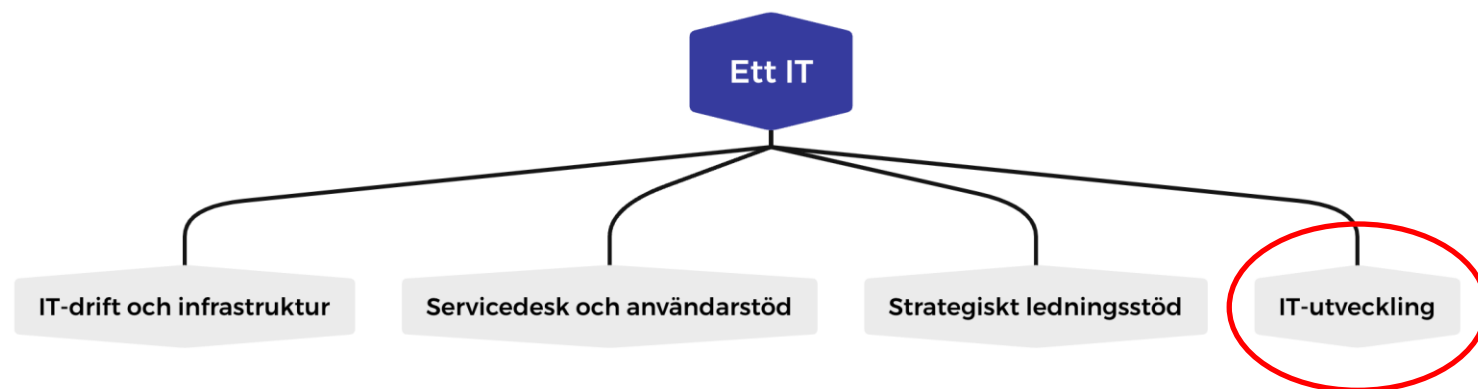
Personal

Chefer : 3

Övriga: 64



Organisationsträd



IT-utveckling

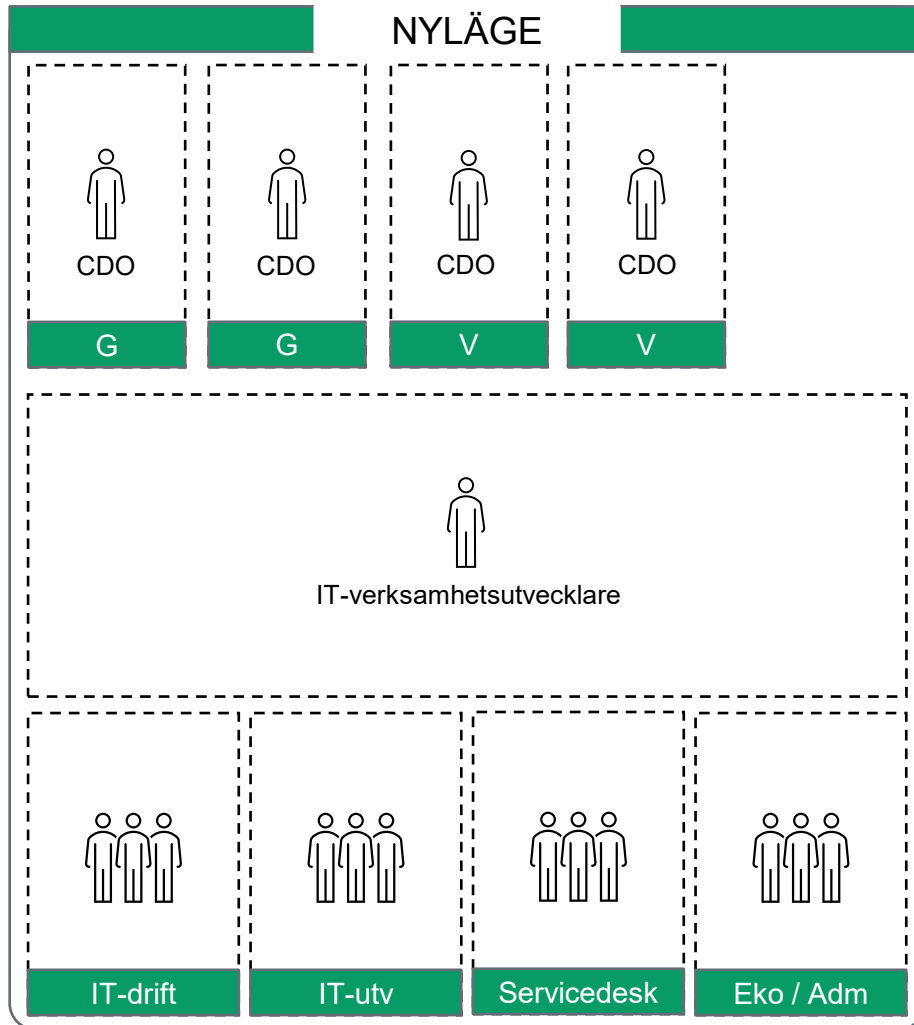
Organisationsbenet IT-utveckling är planerat att etableras i ett senare skede, uppskattningsvis inom 3 - 5 år eller tidigare om verksamhetens behov förändras. Syftet är att säkerställa att organisationen kan växa och anpassas i takt med ökade krav på digitalisering och utveckling.

Detta möjliggör en flexibel och framtidssäkrad struktur där resurser och kompetens kan tillföras när behov uppstår.

På så sätt kan organisationen successivt stärka sitt fokus på innovation och verksamhetsutveckling när tiden är mogen.



SAMVERKAN



BESKRIVNING

IT-verksamhetsutvecklaren fungerar som kommunens länk mellan IT-organisationen och respektive CDO, med fokus på att omsätta digitaliseringsbehov till genomförbara IT-lösningar. CDO ansvarar för att driva kommunens övergripande digitala agenda och behovsbild, medan IT-verksamhetsutvecklaren ansvarar för att konkretisera och prioritera dessa behov i relation till IT-arkitektur, resurser och drift. Modellen bygger på en nära dialog, gemensam prioritering och ett partnerskap där båda rollerna kompletterar varandra.

Behovsinsamling och prioritering

CDO samlar in och strukturerar verksamhetens digitaliseringsbehov. IT-verksamhetsutvecklaren analyserar dessa i relation till IT-miljön och tillgängliga resurser. Tillsammans säkerställer de att rätt initiativ prioriteras och att behov som överlappar mellan kommunerna kan samordnas.

Strategi och arkitektur

CDO driver utvecklingen mot de långsiktiga digitala målen, medan IT-verksamhetsutvecklaren ser till att dessa mål är förenliga med den tekniska arkitekturen och IT-organisationens förmåga. Genom regelbundna dialoger säkerställs att strategiska satsningar kan realiseras utan att skapa fragmentering eller teknisk skuld.

Uppföljning och värdeskapande

CDO ansvarar för att mäta nyttan ur ett verksamhetsperspektiv, exempelvis förbättrad service eller ökad effektivitet. IT-verksamhetsutvecklaren följer upp genomförandet ur ett IT-perspektiv, såsom systemstabilitet, kostnadskontroll och förmågan att stödja framtida behov. Tillsammans skapar de en helhetsbild av värdet och effekten av digitaliseringsarbetet.

Tillsammans mot en robust och framtidssäkrad IT-organisation

Sammanfattning och rekommendation

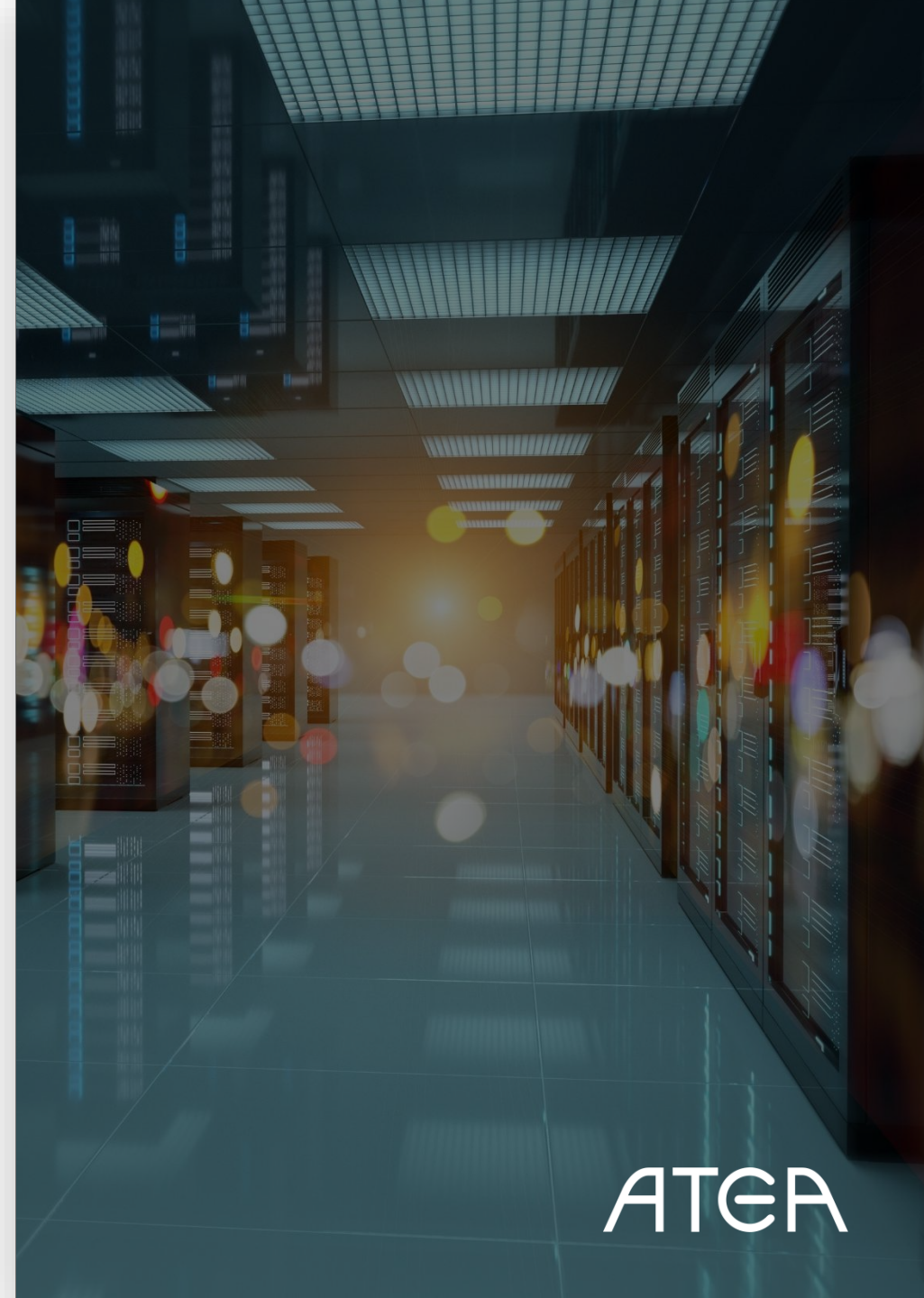
- Fullständig sammanslagning ger långsiktig stabilitet och ökad innovationskraft
- En gemensam organisation stärker styrning, kompetens och säkerhet
- Stor ekonomisk vinst i att minska antalet serverrum
- Använd Gislaved kommuns nyinköpta datacenter för att bygga den nya plattformen på (viss utbyggnad behövs)

Kritiska framgångsfaktorer

- Politisk förankring
- Gemensam styrning och ledarskap
- Kompetenssäkring och processharmonisering
- Ny modern teknisk plattform

Nästa steg

- Beslutsfattande och förankring i alla fyra kommuner
- Etablering av styrgrupp och projektorganisation
- Start av förändringsledning och kommunikationsinsatser



ATERA



Vi svarar gärna på
kompletterande frågor
kring genomlysningen:

Kontaktuppgifter:

Stefan Simicic

Strategisk rådgivare

stefan.simicic@atea.se

Gustav Nilsson

Strategisk rådgivare

gustav.nilsson@atea.se

ATEA