# Stärkta förutsättningar för att följa den statliga it-driften

2025:15

STATSKONTORET

STATSKONTORET

**MISSIV**

DATUM
2025-11-28

DIARIENR
2025/74

ERT DATUM
2025-03-13

ER BETECKNING
Fi2025/00643

Regeringen
Finansdepartementet
103 33 Stockholm

## Uppdrag att skapa förutsättningar för en effektiv uppföljning av den statliga it-driften

Regeringen gav den 13 mars 2025 Statskontoret i uppdrag att ta fram indikatorer för att följa upp arbetet med den samordnade statliga it-driften. Uppdraget inkluderade även att kartlägga hur it-driften inom staten är organiserad som helhet samt föreslå vilken myndighet som är lämplig för att följa upp en sådan kartläggning.

Statskontoret överlämnar härmed rapporten *Stärkta förutsättningar för att följa den statliga it-driften* (2025:15). Generaldirektör Annelie Roswall Ljunggren har beslutat i detta ärende. Utredningschef Erik Nyberg, utredare Andreas Pistol, Sanna Rehn och Kajsa Holmberg, föredragande, var närvarande vid den slutliga handläggningen.

Annelie Roswall Ljunggren

Kajsa Holmberg

POSTADRESS: Box 396, 101 27 Stockholm. BESÖKSADRESS: Torsgatan 11. TELEFON VXL 08-454 46 00.
registrator@statskontoret.se www.statskontoret.se

Innehåll

## Bilagor

# Sammanfattning

Statskontoret har haft i uppdrag av regeringen att skapa förutsättningar för att följa upp den statliga it-driften. Uppdraget har inkluderat att föreslå indikatorer som gör det möjligt att följa effekterna av den samordnade statliga it-driften, det vill säga de it-driftstjänster som de tre leverantörsmyndigheterna Försäkringskassan, Skatteverket och Trafikverket tillhandahåller till andra myndigheter enligt it-driftsförordningen (2024:1005). Indikatorerna ska spegla effekterna av den samordnade it-driften när det gäller säkerhet, kostnadseffektivitet och kvalitet, samt gälla för både myndighetsnivån och samhällsnivån. Vi har tolkat det som att det är leverantörsmyndigheterna som ska använda de indikatorer som vi föreslår, när de årligen redovisar effekterna av arbetet med den samordnade it-driften till regeringen. Vi föreslår följande 7 indikatorer:

1. Andelen av de statliga myndigheterna som är anslutna till var och en av de samordnade it-driftstjänsterna
2. Andelen av beredskapsmyndigheterna som är anslutna till var och en av de samordnade it-driftstjänsterna
3. Antalet enheter (till exempel användare eller terabyte) inom var och en av de samordnade it-driftstjänsterna
4. Den genomsnittliga kostnaden per enhet (till exempel användare eller terabyte) inom var och en av de samordnade it-driftstjänsterna
5. Den procentuella skillnaden mellan den debiterade avgiften ett visst år och året efter för var och en av de samordnade it-driftstjänsterna
6. Den genomsnittliga andelen av den överenskomna öppettiden som de samordnade it-driftstjänsternas huvudsakliga funktionalitet är tillgänglig, för var och en av de tjänster som har en överenskommen öppettid
7. De anslutna myndigheternas genomsnittliga kundnöjdhet (NKI) med var och en av de samordnade it-driftstjänsterna.

De två första indikatorerna speglar effekterna av den samordnade it-driften när det gäller säkerhet på myndighetsnivå, och i viss mån på samhällsnivå. Den tredje och fjärde indikatorn speglar effekterna av den samordnade driften när det gäller kostnadseffektivitet på myndighetsnivå, och i viss mån på samhällsnivå. De femte och sjätte indikatorerna speglar i vilken utsträckning som den samordnade it-driften möter de anslutna myndigheternas behov i olika avseenden. De speglar alltså inte effekterna av den samordnade it-driften när det gäller kvalitet vare sig på

myndighets- eller samhällsnivå. Den sista indikatorn speglar hur de anslutna myndigheterna upplever balansen mellan säkerhet, kostnadseffektivitet och kvalitet i den samordnade it-driften.

Sammantaget innebär detta att de indikatorer som vi föreslår inte motsvarar regeringens förväntningar fullt ut. Det beror framför allt på att det inte finns eller går att ta fram några tillförlitliga eller jämförbara data över säkerheten, kostnadseffektiviteten eller kvaliteten i de enskilda myndigheternas it-drift. I stället behöver de indikatorer som vi föreslår bygga på data från leverantörsmyndigheterna. På grund av begränsningarna i dataunderlaget föreslår vi att använda år 2025 som nolläge för indikatorerna, och att leverantörsmyndigheterna redovisar utgångsvärdena för indikatorerna till regeringen i sin återrapportering under 2026.

På grund av begränsningarna i de indikatorer som vi föreslår bedömer vi också att indikatorerna ensamma inte är tillräckliga för att ge regeringen en tydlig bild av effekterna av den samordnade it-driften. Ensamma ger de ger inte heller något användbart beslutsunderlag för att styra och utveckla den samordnade driften. Regeringen och leverantörsmyndigheterna behöver därför komplettera indikatorerna på olika sätt för att det ska gå att bedöma effekterna av den samordnade it-driften när det gäller säkerhet och kostnadseffektivitet.

Regeringen behöver bland annat genomföra årliga gemensamma dialoger med leverantörsmyndigheternas generaldirektörer, myndigheternas huvudmän vid Regeringskansliet och ansvariga statsråd eller statssekreterare. Dialogen bör även inkludera det statsråd eller den statssekreterare som är ansvarig för totalförsvarsfrågorna. Leverantörsmyndigheterna behöver framför allt analysera och förklara värdena på indikatorerna i sin återrapportering till regeringen. För att göra det behöver de ta fram och använda annan information än själva indikatorerna. Det gäller information som visar att den samordnade it-driften är säker i olika avseenden, så att myndigheterna kan fatta välgrundade beslut om att ansluta sig. Det gäller också information som visar hur de samordnade tjänsterna ökar säkerheten i myndigheternas it-drift, samt information som visar vad som driver enhetskostnaderna för de samordnade tjänsterna. Det kan handla om kostnaden per användare, terabyte data eller liknande.

Uppdraget har även inkluderat att kartlägga hur den statliga it-driften är organiserad som helhet och föreslå vilken aktör som bör ansvara för sådana kartläggningar framöver. Vi bedömer att Försäkringskassan är bäst lämpad att kartlägga hur den statliga it-driften är organiserad framöver, om regeringen vill att kartläggningen ska bidra till att utveckla den samordnade it-driften. Men om regeringen i stället vill använda kartläggningen för att öka sin kunskap och utveckla sin politik om förvaltningens digitalisering anser vi att Myndigheten för digital förvaltning (Digg) är bäst lämpad.

Vår kartläggning visar att myndigheterna genomför en majoritet av sin it-drift i egen regi. Det gäller särskilt beredskapsmyndigheter och myndigheter med många årsarbetskrafter. Men vi ser också att de flesta myndigheter kombinerar olika driftsformer och använder it-drift i både privat och samordnad regi, till exempel som komplement till drift i egen regi eller vice versa. Kartläggningen visar även att egen regi är den vanligaste driftsformen för de flesta typerna av it-driftstjänster. Det gäller till exempel datacentertjänster, applikationstjänster samt nätverks- och kommunikationstjänster. Undantaget är molntjänster, där privat regi är den vanligaste driftsformen. Samtidigt visar vår kartläggning att det över tid har blivit mindre vanligt att myndigheterna använder molntjänster i privat regi än 2017 respektive 2021.

# 1 Inledning

Statskontoret har haft i uppdrag av regeringen att skapa förutsättningar för att följa upp den statliga it-driften. Uppdraget har två huvudsakliga delar. Den första delen handlar om den samordnade statliga it-driften, det vill säga de it-driftstjänster som Försäkringskassan, Skatteverket och Trafikverket tillhandahåller till andra myndigheter. I uppdraget ingår att ta fram ett nolläge samt föreslå indikatorer för att följa resultaten och effekterna av arbetet. Indikatorerna ska omfatta faktorerna säkerhet, effektivitet och kvalitet, samt fungera på både aktörs- och samhällsnivå. Den andra delen handlar om att kartlägga hur it-driften i staten är organiserad som helhet, samt föreslå vilken myndighet som är lämplig att fortsätta att kartlägga det framöver.

## 1.1 Den samordnade statliga it-driften i korthet

Arbetet med samordnad statlig it-drift har pågått sedan 2017. Sedan 2025 är det reglerat i förordning. Men arbetets fokus har förändrats över tid.

### 1.1.1 Arbetet med den samordnade statliga it-driften har pågått sedan 2017

År 2017 fick Försäkringskassan i uppdrag av regeringen att erbjuda samordnad och säker it-drift till vissa myndigheter.[1] Två år senare, 2019, tillsatte regeringen en utredning om säker och kostnadseffektiv it-drift för den offentliga förvaltningen (It-driftsutredningen). I slutet av 2021 lämnade utredningen sitt slutbetänkande. Utredningen föreslog att ett antal stora myndigheter skulle få en förordningsstyrd uppgift att leverera it-tjänster åt andra myndigheter, samt att en annan myndighet skulle få i uppdrag att ta fram indikatorer för att följa arbetet. Under 2024 upphörde Försäkringskassans regeringsuppdrag att erbjuda samordnad it-drift, samtidigt som regeringen beslutade om förordning (2024:1005) om samordnad och säker statlig it-drift (it-driftsförordningen). Den 1 januari 2025 trädde förordningen i kraft. Förordningen anger att Försäkringskassan ska samordna arbetet enligt förordningen, och tillsammans med Skatteverket och Trafikverket tillhandahålla it-driftstjänster till andra myndigheter. Senast den 31 mars varje år ska Försäkringskassan redovisa effekterna av arbetet till regeringen. I budgetpropositionen för 2025 aviserade regeringen att även Lantmäteriet ska tillhandahålla it-driftstjänster till andra myndigheter från den 1 januari 2026.[2] Under våren 2025 beslutade regeringen om vårt uppdrag.

---

[1] Regeringsbeslut. *Uppdrag att erbjuda en samordnad och säker statlig it-drift*. 2017-08-24. Fi2017/03257/DF.

[2] Proposition 2024/25:1. *Budgetpropositionen för 2025. Utgiftsområde 18. Samhällsplanering, bostadsförsörjning och byggande samt konsumentpolitik*. s. 36.

### 1.1.2 Den samordnade statliga it-driften ska leda till högre säkerhet och kostnadseffektivitet

Vi tolkar it-driftsförordningen som att syftet med den samordnade statliga it-driften är att höja säkerheten i myndigheternas it-drift på ett kostnadseffektivt sätt. Vi baserar det på att leverantörsmyndigheterna i första hand ska prioritera att ansluta myndigheter vars anslutning leder till högre säkerhet och i andra hand myndigheter vars anslutning leder till ökad kostnadseffektivitet. Leverantörsmyndigheterna ska också beakta totalförsvarets behov när de utformar tjänsterna i det samordnade utbudet. Detta framgår av § 9 respektive 5 it-driftsförordningen.

### 1.1.3 Leverantörsmyndigheternas samverkan går utöver regeringens styrning

Parallellt med arbetet som regeringen har styrt har flera av de berörda myndigheterna samverkat i frågor om säker och samordnad it-drift på eget initiativ. Under 2018 initierade Försäkringskassan och Fortifikationsverket Program 2032 för att samverka om säkra it-utrymmen. Under 2019 initierade Försäkringskassan, Skatteverket, Trafikverket, Lantmäteriet och Transportstyrelsen programmet Säkra it-tjänster i statlig samverkan (SITSSAM).[3] I februari 2024 avvecklade de berörda myndigheterna både Program 2032 och SITSSAM. I stället initierade de berörda myndigheterna i stället det nya programmet Nationell it-drift i samverkan (Nitis) tillsammans med Myndigheten för samhällsskydd och beredskap (MSB). Målet för Nitis är en säker, effektiv och samordnad statlig it-drift som säkerställer att statliga myndigheter kan bedriva sina verksamheter genom hela hotnivåskalan.[4] Det ligger nära hur vi tolkar syftet med den samordnade statliga it-driften. Vi uppfattar också att myndigheterna inom Nitis i praktiken ser att arbetet enligt it-driftsförordningen är en del av det bredare arbetet inom Nitis. Det är till exempel samma kansli på Försäkringskassan som leder arbetet inom Nitis och som samordnar arbetet enligt it-driftsförordningen.

### 1.1.4 Fokus har skiftat från små myndigheter till beredskapsmyndigheter

Under de första åren som Försäkringskassan hade i uppdrag att erbjuda en samordnad statlig it-drift fokuserade myndigheten på små myndigheter. Det berodde på att Försäkringskassans initiala behovsanalys visade att små myndigheter med liten eller ingen it-avdelning hade störst behov av samordnad it-drift. Det följde av att de ofta har svårare än stora myndigheter att upprätthålla en säker och kostnadseffektiv it-drift på egen hand. Det berodde också på att regeringens uppdrag till Försäkringskassan specificerade att myndigheten särskilt skulle beakta

---

[3] SOU 2021:97. *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift*. s. 195f.

[4] Försäkringskassan 2025-03-18. *Nitis-inriktning beslutad den 27 februari 2024 – delar som bedöms mindre känsliga*. FK 2024/006706. s. 4.

små myndigheters förutsättningar.[5] Enligt Försäkringskassans behovsanalys behövde de små myndigheterna i huvudsak någon som kunde sköta deras it-drift som helhet. Därför var helhetstjänsten it-arbetsplats den första tjänsten som Försäkringskassan utvecklade.[6]

Över tid har Försäkringskassan och de övriga leverantörsmyndigheterna skiftat fokus från små myndigheter till beredskapsmyndigheter. Det beror på att världsläget har blivit mer osäkert och att antalet cyberattacker mot myndigheter har ökat, samtidigt som myndigheterna har blivit mer beroende av digitala system för att upprätthålla sin verksamhet.[7] Det beror också på att it-driftsförordningen anger att leverantörsmyndigheterna ska prioritera anslutningar som leder till högre säkerhet (se avsnitt 1.1.2). Däremot nämner förordningen inte små myndigheters förutsättningar, till skillnad från Försäkringskassans tidigare uppdrag.

Enligt företrädare för leverantörsmyndigheterna har beredskapsmyndigheterna generellt större och mer komplicerade behov av it-drift än de små myndigheterna. De efterfrågar i huvudsak enstaka plattforms- och infrastrukturtjänster för att komplettera sin egen it-drift.[8] Därför började Försäkringskassan under de sista åren med sitt regeringsuppdrag att utveckla sådana tjänster, till exempel för att hantera applikationer och för att samarbeta mellan myndigheter. Det senaste året har leverantörsmyndigheterna inom ramen för Nitis fokuserat ännu mer på säkerhet och börjat utveckla tjänster för att säkra data.

### 1.1.5 It-driftsförordningen innebär en nystart för den samordnade statliga it-driften

Enligt it-driftsförordningen är det upp till leverantörsmyndigheterna själva att bestämma vilka tjänster som de ska erbjuda till andra myndigheter. Men de får bara tillhandahålla tjänster som bygger på deras egen it-drift, om inte något annat är föreskrivet. Förordningen anger också att leverantörsmyndigheterna ska finansiera de samordnade tjänsterna genom att ta ut avgifter av de anslutna myndigheterna. Leverantörsmyndigheterna får själva bestämma avgifternas storlek och disponera inkomsterna från avgifterna i verksamheten.

---

[5] Regeringsbeslut. *Uppdrag att erbjuda en samordnad och säker statlig it-drift*. 2017-08-24. Fi2017/03257/DF.

[6] Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift*. s. 7; Försäkringskassan (2023). *Rapport – delredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift*. s. 4.

[7] Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift.* s. 3, 5, 7.

[8] Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift.* s. 7.

I september 2025 fanns det 14 tjänster i det samordnade statliga tjänsteutbudet, enligt den förteckning som Försäkringskassan ska föra enligt § 4 i it-driftsförordningen (bilaga 2). Det handlar om såväl infrastrukturtjänster som plattformstjänster och applikationstjänster av olika slag. Försäkringskassan tillhandahåller de flesta av tjänsterna, men varje leverantörsmyndighet tillhandahåller minst en tjänst.

Flera av leverantörsmyndigheterna tillhandahöll it-drift åt andra myndigheter även före it-driftsförordningen. Skatteverket tillhandahöll och tillhandahåller fortfarande it-drift åt bland annat Kronofogdemyndigheten, Utbetalningsmyndigheten och Valmyndigheten. Det är reglerat i Skatteverkets instruktion. Försäkringskassan tillhandahöll i sin tur totalt nio i-driftstjänster inom ramen för sitt tidigare regeringsuppdrag inom området. Den största var den elektroniska tjänste-legitimationen EFOS med knappt 60 anslutna myndigheter. Därefter kom samarbetstjänsten SAFOS med 35 anslutna myndigheter.[9]

Flera av de nio tjänsterna som Försäkringskassan tog fram och tillhandahöll inom ramen för sitt regeringsuppdrag ingår i dag i någon form i det samordnade statliga tjänsteutbudet som Försäkringskassan och de övriga leverantörsmyndigheterna tillhandahåller enligt it-driftsförordningen. Det gäller bland annat både EFOS och SAFOS. Men förordningen förändrade förutsättningarna för den samordnade it-driften. För det första har uppgiften blivit tydligare och mer långsiktig. För det andra är tjänsteutbudet och beslutet om att ansluta en viss myndighet nu en fråga för gruppen leverantörsmyndigheter i stället för en fråga enbart för Försäkrings-kassan. Därför har Försäkringskassan justerat innehållet i vissa av tjänsterna, enligt företrädare för myndigheten.

### 1.1.6 Efterfrågan på samordnad it-drift överstiger utbudet

Efterfrågan på samordnad it-drift har hittills varit större än vad leverantörs-myndigheterna har kunnat möta. Det beror på att vissa myndigheter har efterfrågat mer komplexa eller verksamhetsanpassade tjänster eller en snabbare anslutnings-process än vad leverantörsmyndigheterna har haft möjlighet att erbjuda. Ju mer komplicerad en intresserad myndighets befintliga it-drift är, och ju mer leverantörs-myndigheterna behöver anpassa en tjänst till den anslutande myndigheten, desto längre tid tar det för leverantörsmyndigheterna att ansluta den. Det uppger företrädare för Försäkringskassan. Under tiden som det var Försäkringskassan som tillhandahöll samordnad it-drift enligt det tidigare regeringsuppdraget hade myndigheten också svårt att planera arbetet med att ansluta nya myndigheter, eftersom de långsiktiga förutsättningarna var osäkra.[10]

---

[9] Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift*. s. 4.

[10] Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift*. s. 5.

En myndighet som vill ansluta sig till en tjänst inom den samordnade it-driften ska vända sig till Försäkringskassan som hanterar förfrågan inom Nitis-kansliet. Kansliet samordnar leverantörsmyndigheternas arbete med att analysera den intresserade myndighetens förutsättningar och behov, samt vilken eller vilka av leverantörsmyndigheterna som har förutsättningar att erbjuda myndigheten tjänsten. Utifrån analysen beslutar Försäkringskassan sedan vilken leverantörsmyndighet som är lämplig, och lämnar över intresseanmälan till dem så att de kan teckna en samverkansöverenskommelse med den anslutande myndigheten om tjänsten. Det innebär att en myndighet kan vara ansluten till tjänster hos flera leverantörsmyndigheter.

## 1.2 Hur vi har genomfört uppdraget

I det här avsnittet beskriver vi hur vi har gått till väga för att genomföra vårt uppdrag. Vi redogör för hur vi tolkar uppdraget, definierar centrala begrepp, och bedömer indikatorer. Vi resonerar också kring hur tillgången på data påverkar våra förslag. Sist men inte minst beskriver vi vilket material vi baserar vår analys och våra förslag på.

### 1.2.1 Hur vi har tolkat vårt uppdrag

Vi tolkar det som att syftet med vårt uppdrag är att skapa förutsättningar för regeringen och leverantörsmyndigheterna att följa behoven och effekterna av den samordnade statliga it-driften. Därmed får regeringen och leverantörsmyndigheterna ett underlag för att styra och utveckla den samordnade it-driften så att den får de önskade effekterna.

Vi tolkar det som att strecksatserna i uppdraget preciserar ett antal förutsättningar som vårt arbete ska skapa. Det handlar om att ta fram en bild av hur myndigheterna organiserar sin it-drift i dag, och föreslå en myndighet som kan följa det framöver. Det handlar också om att ta fram ett nolläge och att föreslå indikatorer som speglar effekterna av den samordnade it-driften när det gäller säkerhet, effektivitet och kvalitet. Vi tolkar det som att det är Försäkringskassan och de övriga leverantörsmyndigheterna som ska använda indikatorerna, för att årligen redovisa effekterna av arbetet med den samordnade it-driften till regeringen i enlighet med it-driftsförordningen. Men vi tolkar även att vi kan föreslå andra åtgärder som förbättrar regeringens och leverantörsmyndigheternas förutsättningar att följa och säkerställa effekterna av den samordnade it-driften, om vår analys visar att de är motiverade.

Sist men inte minst anger uppdraget att vi ska föreslå indikatorer på både aktörs- och samhällsnivå. Vi tolkar det som att aktörsnivå innebär myndighetsnivå, medan samhällsnivå innebär samhället som helhet.

### 1.2.2 Hur vi definierar it-drift, säkerhet, kostnadseffektivitet och kvalitet

Vårt uppdrag innehåller flera centrala begrepp. Ett sådant är begreppet *it-drift*, som inte har någon formell eller förvaltningsgemensam definition.[11] Varken Försäkringskassan, de övriga leverantörsmyndigheterna eller Nitis-myndigheterna har formulerat någon sådan definition. Företrädare för Försäkringskassan förklarar det med att synen på vad som ingår i it-drift rör sig över tid, och att myndigheterna därför behöver kunna röra sig med den. I vår enkätundersökning utgår vi från It-driftsutredningens definition av it-drift, det vill säga det löpande arbetet med att hantera och underhålla hårdvara och mjukvara.[12] Vi använder Kammarkollegiets ramavtal för it-drift för exempel på vad det inkluderar, så som datacentertjänster, molntjänster, nätverks- och kommunikationstjänster, applikationstjänster och supporttjänster samt livscykelhantering av dessa tjänster.[13]

Inte heller när det gäller säkerhet finns det någon entydig definition. Vi utgår i huvudsak från hur It-driftsutredningen definierar säkerhet. Med *säkerhet på aktörsnivå* menar vi därmed i vilken utsträckning som en viss it-driftstjänst möter säkerhetskraven i enskilda myndigheters verksamhet. Det handlar till exempel om att möta krav på säkerhetsskydd, informationssäkerhet, sekretess och skydd för den personliga integriteten. Med *säkerhet på samhällsnivå* menar vi i vilken utsträckning den statliga förvaltningen som helhet har en it-drift som kan stå emot olika störningar och hot i samhället, till följd av såväl yttre som inre påverkan.[14] När det gäller it-drift är kraven på säkerhet inte konstanta över tid. I stället blir kraven kontinuerligt högre, både till följd av den tekniska utvecklingen och att samhället och myndigheternas verksamhet blir alltmer digitaliserad. Det konstaterar både It-driftsutredningen och företrädare för bland annat Digg, MSB och Försvarsmakten.[15] Det innebär att leverantörsmyndigheterna över tid behöver vidareutveckla de samordnade it-driftstjänsterna för att möta myndigheternas krav.

Med *kostnadseffektivitet på aktörsnivå* menar vi kostnaden för att tillhandahålla en viss it-driftstjänst som möter en enskild myndighets krav på säkerhet och kvalitet. Därmed spelar kostnaden för en tjänst ingen roll om den inte möter kraven. Med *kostnadseffektivitet på samhällsnivå* menar vi kostnaden för den statliga förvaltningens it-drift som helhet i relation till regeringens eller de berörda myndigheternas krav på it-driftens säkerhet och kvalitet. En it-drift som möter

---

[11] SOU 2021:1. *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering*. s. 39f.

[12] SOU 2021:1. *Säker och kostnadseffektiv it-drift*. s. 40.

[13] Kammarkollegiet (2025). *Vägledning för avrop från IT-drift Mindre och IT-drift Större*. s. 16–18.

[14] SOU 2021:97. *Säker och kostnadseffektiv it-drift*. s. 55.

[15] SOU 2021:97. *Säker och kostnadseffektiv it-drift*. s. 167, 374f, 396.

kraven till förhållandevis lägre kostnad är mer kostnadseffektiv än en it-drift som möter kraven till en förhållandevis högre kostnad. Men en it-drift som möter kraven behöver se olika ut över tid, eftersom myndigheternas säkerhetskrav ökar kontinuerligt. Det påverkar i sin tur kostnaden för driften, eftersom högre säkerhet generellt innebär högre kostnad.

Därmed går de vanligaste sätten att se på kostnadseffektivitet inte att tillämpa rakt av när det gäller it-drift. Det handlar varken om att tillhandahålla en fast tjänst till lägsta möjliga kostnad eller att tillhandahålla en så bra tjänst som möjligt till en fast kostnad. När det gäller den samordnade it-driften är det nödvändigheten att möta myndigheternas krav som ligger fast, och inte tjänsten eller kostnaden.

Med *kvalitet på aktörsnivå* menar vi i vilken utsträckning som en viss it-driftstjänst möter enskilda myndigheters krav i andra avseenden än säkerhet. Det kan till exempel handla om tillgänglighet och service. Med *kvalitet på samhällsnivå* menar vi hur väl den samordnade statliga it-driften som helhet möter myndigheternas behov. Även när det gäller kvalitet är det sannolikt att myndigheternas krav ökar kontinuerligt, av samma skäl som deras krav på säkerhet ökar.

### 1.2.3 Hur vi har tagit fram våra indikatorer

Vi har analyserat vilka indikatorer för att följa effekterna av den samordnade it-driften som ger regeringen och leverantörsmyndigheterna bäst förutsättningar att styra och utveckla den samordnade driften. Vi har inte analyserat om indikatorer i sig är lämpliga verktyg för att följa effekterna av den samordnade driften, eller om det är just indikatorer som ger regeringen och leverantörsmyndigheterna det mest användbara beslutsunderlaget. Det följer av att vårt uppdrag är att föreslå just indikatorer. Däremot bedömer vi att indikatorer ensamma inte kommer att vara tillräckliga för att följa effekterna av den samordnade it-driften. Därför har vi även analyserat hur regeringen och leverantörsmyndigheterna kan komplettera indikatorerna och göra uppföljningen som helhet mer användbar som beslutsunderlag.

När vi har analyserat möjliga indikatorer har vi utgått från fem kriterier som vi bedömer att indikatorerna behöver uppfylla för att vara användbara. Dessa kriterier säger att indikatorerna måste:

- vara relevanta, det vill säga belysa de egenskaper hos den statliga it-driften som vi vill följa
- vara tillförlitliga, det vill säga mäta det som de avser att mäta, på ett sätt som går att upprepa
- ange en riktning, det vill säga att höga eller låga värden visar på bättre eller sämre resultat

- vara påverkbara, det vill säga att både regeringen och leverantörsmyndigheterna har möjlighet att påverka värdena på indikatorn genom hur de agerar
- vara möjliga att redovisa och analysera årligen, det vill säga vara hållbara och illustrera utvecklingen över tid.

Vi har strävat efter att föreslå indikatorer som bygger på data som leverantörsmyndigheterna redan tar fram, eller som de kan ta fram med en liten arbetsinsats. Det beror på att leverantörsmyndigheterna ska kunna använda indikatorerna i sin redovisning till regeringen under våren 2026, men även på att vi vill hålla nere kostnaden för uppföljningen. Vi föreslår också indikatorer för samtliga enskilda tjänster inom det samordnade utbudet var för sig, i stället för indikatorer som avser ett urval av tjänster eller ett genomsnitt för flera tjänster. Det beror på att leverantörsmyndigheterna kommer att utveckla tjänsteutbudet över tid. Dessutom är indikatorer för enskilda tjänster lättare att tolka än indikatorer som gäller ett genomsnitt för flera tjänster. Det gör indikatorerna mer användbara som beslutsunderlag.

### 1.2.4 Indikatorerna behöver bygga på data från leverantörsmyndigheterna för att vara tillförlitliga

Med grund i kriterierna ovan föreslår vi i huvudsak indikatorer som bygger på data som leverantörsmyndigheterna kan ta fram, och inte på data från de enskilda anslutna myndigheterna. Det beror på att mycket få av de myndigheter vi har varit i kontakt med har tillförlitliga data som visar på säkerheten, kvaliteten eller kostnadseffektiviteten i deras it-drift före respektive efter att de anslöt sig till den samordnade it-driften.

I den mån som enskilda myndigheter har sådana data går de inte heller att lägga samman, eftersom myndigheterna följer upp sin it-drift på olika sätt både sinsemellan och över tid. Ett skäl till det är att det inte finns några förvaltningsgemensamma mått på säkerhet, kostnadseffektivitet eller kvalitet när det gäller it-drift. Ett annat skäl är att den tekniska utvecklingen löpande leder till ny funktionalitet och nya krav på olika it-driftstjänster. Det påverkar både vad myndigheterna definierar som it-drift, säkerheten och kvaliteten i tjänsterna, samt hur mycket tjänsterna kostar. Ytterligare ett skäl är att myndigheternas verksamhet ser olika ut, vilket innebär att de behöver utforma och följa sin it-drift på olika sätt för att möta verksamhetens behov. Det framgår av våra intervjuer med företrädare både för myndigheter som är anslutna och för myndigheter som står utanför den samordnade it-driften, samt med företrädare för leverantörsmyndigheterna och Myndigheten för digital förvaltning (Digg).

#### Inte framkomligt att reglera hur myndigheterna ska redovisa data om it-drift

Vi har övervägt att föreslå regeringen att införa bestämmelser om hur myndigheterna ska redovisa data som rör säkerheten, kostnadseffektiviteten och kvaliteten i sin it-drift. Regeringen skulle i teorin till exempel kunna införa sådana bestämmelser i

förordningen (2000:605) om årsredovisning och budgetunderlag, och ge Ekonomistyrningsverket (ESV) i uppdrag att komplettera dessa bestämmelser med föreskrifter och allmänna råd. Men vi bedömer att det skulle vara mycket svårt att ta fram bestämmelser som är tillräckligt detaljerade för att generera standardiserbara data och samtidigt tillräckligt övergripande för att vara hållbara över tid till följd av den snabba tekniska utvecklingen. Den infrastruktur och mjukvara som är säker i dag kommer till exempel sannolikt inte vara tillräcklig om ett par år. Vi bedömer också att det skulle vara svårt att säkerställa att myndigheterna skulle tillämpa bestämmelserna på ett enhetligt sätt, eftersom it-drift är ett så komplext och snabbrörligt område.

Dessutom är de flesta av myndigheterna som är anslutna till den samordnade it-driften bara anslutna till enstaka tjänster.[16] Det innebär att de har en stor del av sin it-drift i annan regi. Data som visar på säkerheten, kostnadseffektiviteten eller kvaliteten i de anslutna myndigheternas it-drift skulle därmed spegla både de samordnade tjänsterna och myndighetens it-drift i annan regi. Det skulle ge en missvisande bild av effekterna av den samordnade it-driften.

### 1.2.5 Dataunderlaget för indikatorerna styr nolläget

Vårt val att föreslå indikatorer som bygger på data från leverantörsmyndigheterna innebär att 2025 är vårt nolläge. Det betyder i sin tur att leverantörsmyndigheternas återrapportering till regeringen i mars 2026 kommer att innehålla basvärden på våra förslag till indikatorer. Vi har helt enkelt inga tillförlitliga, jämförbara data för tiden före it-driftsförordningen. För vissa av indikatorerna kan data från Försäkringskassan ge en översiktlig bild av utvecklingen under 2017–2024, då myndigheten tillhandahöll it-driftstjänster åt andra myndigheter enligt ett tidigare regeringsuppdrag. Men dessa tjänster hade andra förutsättningar och delvis annat innehåll än de tjänster som Försäkringskassan och de övriga leverantörsmyndigheterna nu tillhandahåller enligt it-driftsförordningen. Därför bedömer vi att data för perioden 2017–2024 inte är fullt jämförbara med data för 2025 och framåt.

### 1.2.6 Dataunderlaget begränsar möjligheterna att ta fram indikatorer för effekter på aktörs- och samhällsnivå

Bristen på tillförlitliga och jämförbara data över säkerheten, kostnadseffektiviteten och kvaliteten i enskilda myndigheters it-drift gör det svårt att ta fram indikatorer som speglar effekterna av den samordnade it-driften i allmänhet, och på myndighets- och samhällsnivå i synnerhet. Därför har vi inte lyckats ta fram indikatorer som möter regeringens förväntningar fullt ut. Våra förslag på indikatorer för att följa effekterna av den samordnade it-driften när det gäller säkerhet och kostnadseffektivitet speglar till exempel bara effekterna på samhällsnivå i viss mån.

---

[16] Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift.* s. 4, 6.

När det gäller kvalitet speglar våra förslag på indikatorer inte effekter av den samordnade it-driften överhuvudtaget, utan hur väl den samordnade driften möter de anslutna myndigheternas behov i en rad avseenden. Vi bedömer att regeringen på så sätt ändå får en bild av kvaliteten i den samordnade it-driften och att regeringen därmed kan följa hur kvaliteten utvecklas över tid. Dessutom bedömer vi att den samordnade it-driftens förmåga att möta myndigheternas säkerhetskrav i praktiken är den enskilt viktigaste kvalitetsfaktorn i den samordnade driften. Vi konstaterar också att it-driftsförordningen inte heller nämner kvalitet.

### 1.2.7 Vilka material vi har baserat vår analys på?

Vi har använt oss av flera olika metoder för att samla in underlag till vår analys. För den del av uppdraget som handlar om att föreslå indikatorer har vi bland annat intervjuat företrädare för expertmyndigheter inom it- respektive säkerhetsområdet, som Digg, Försvarsmakten, Försvarets Radioanstalt (FRA) och Säkerhetspolisen (Säpo). Syftet med intervjuerna har varit att få deras bild av vilka indikatorer som vore lämpliga för att följa effekterna av den samordnade it-driften, samt vad vi i övrigt behöver ta hänsyn till när vi utformar våra förslag.

Vi har även intervjuat företrädare för sex myndigheter som är anslutna till den samordnade it-driften samt tre beredskapsmyndigheter som står utanför. Syftet med intervjuerna har bland annat varit att få myndigheternas bild av hur den samordnade driften fungerar samt vilken information i form av indikatorer, nyckeltal eller annat som de skulle vilja ta del av för att kunna fatta ett välgrundat beslut om att ansluta sig till eller fortsätta att vara ansluten till den samordnade driften. Vi har också inventerat befintliga dataunderlag som vi skulle kunna använda som grund för indikatorer. Bland dessa finns till exempel uppföljningar från Digg, mätningar från MSB samt data från ESV:s statsredovisningssystem Hermes.

Under arbetets gång har vi fört en nära dialog med leverantörsmyndigheterna och de övriga myndigheterna inom Nitis, samt med representanter från Nitis-kansliet som ansvarar för Försäkringskassans samordningsuppdrag enligt it-driftsförordningen. Ett syfte med det har varit att fånga upp deras behov och säkerställa att våra förslag på indikatorer blir användbara för dem i deras fortsatta arbete med den samordnade it-driften. Vi bedömer att om leverantörsmyndigheterna anser att indikatorerna är användbara så bör det också leda till högre kvalitet i deras arbete med att ta fram dataunderlag för indikatorerna och med att analysera vad de visar. Ett annat syfte har varit att dra nytta av deras expertkunskap och erfarenheter av it-drift, och därigenom genomföra uppdraget mer effektivt. Vi har genomfört två workshops med representanter från leverantörsmyndigheterna, de övriga Nitis-myndigheterna och medarbetare vid Nitis-kansliet. Där har vi bland annat diskuterat möjliga förslag på indikatorer och verktyg för att visa att den samordnade it-driften är säker. Samma grupp av myndigheter har också fått läsa ett utkast på de delar av vår rapport som handlar om våra förslag på indikatorer. Både leverantörsmyndigheterna och expertmyndigheterna inom it- och säkerhetsområdet har också fått faktagranska relevanta delar av rapporten.

När det gäller att kartlägga organiseringen av den statliga it-driften som helhet har vi genomfört en enkätundersökning till samtliga 215 myndigheter i den statliga redovisningsorganisationen under perioden juni–augusti 2025. Enkäten är kort och övergripande och syftar till att ge en samlad bild av hur myndigheterna organiserar sin it-drift. Svarsfrekvensen var 93 procent. Bilaga 4 innehåller enkäten i sin helhet.

Vi har även inventerat befintliga dataunderlag för att se om och i så fall hur de går att använda för att kartlägga organiseringen av den statliga it-driften. Som en del i detta arbete har vi talat med företrädare för Kammarkollegiet, Statens servicecenter (SSC), ESV, Digg och MSB. Vi har även begärt ut relevanta data från dessa myndigheter.

# 2 Förslag på indikatorer – säkerhet

I de här kapitlet redogör vi för våra förslag på indikatorer för att följa effekterna av den samordnade statliga it-driften när det gäller säkerhet på aktörs- och samhällsnivå. Vi redogör även för motiven till våra förslag, samt för skälen till att vi har valt bort andra potentiella indikatorer. Vi föreslår följande indikatorer när det gäller säkerhet:

- Andelen av *de statliga myndigheterna* som är anslutna till var och en av tjänsterna inom den samordnade statliga it-driften
- Andelen av *beredskapsmyndigheterna* som är anslutna till var och en av tjänsterna inom den samordnade statliga it-driften.

Med statliga myndigheter menar vi samtliga myndigheter i Statskontorets myndighetsregister som har minst 1 årsarbetskraft och hanterar sin egen administration, det vill säga som inte har någon värdmyndighet. Den 1 januari 2025 var det 223 myndigheter.[17] Vi har valt den populationen eftersom den motsvarar de myndigheter som har långsiktig verksamhet i Sverige och fattar självständiga beslut om hur de organiserar sin it-drift. Därmed bedömer vi att de utgör målgruppen för den samordnade it-driften. Med beredskapsmyndigheter menar vi samtliga myndigheter i bilaga 1 till förordning **(**2022:524**)** om statliga myndigheters beredskap. I september 2025 var det 67 myndigheter. Med tjänsterna inom den samordnade statliga it-driften menar vi de tjänster som ingår i den förteckning som Försäkringskassan ska föra enligt § 4 i it-driftsförordningen.

När det gäller den andra indikatorn föreslår vi att leverantörsmyndigheterna under de närmaste åren fokuserar på att analysera andelen beredskapsmyndigheter som är anslutna till it-driftstjänster för att säkra data. Nitis-myndigheterna kallar dessa tjänster för tjänster för datasäkring. Dessutom föreslår vi att leverantörs-myndigheterna använder nyckeltal och andra typer av information för att visa *att* den samordnade it-driften är säker, samt *hur* den ökar säkerheten hos de anslutna myndigheterna.

[17] Statskontoret (2025). *Statsförvaltningen i korthet*. s. 9.

## 2.1 Andelen anslutna myndigheter speglar den samordnade it-driftens effekter på säkerhet

Vår analys visar att en myndighet bara ansluter sig till en viss samordnad tjänst om de bedömer att den höjer säkerheten i deras it-drift i något avseende. Därför har den samordnade it-driften en positiv effekt på säkerheten på myndighetsnivå varje gång en ny myndighet ansluter sig till en tjänst. På samhällsnivå är effekten större om beredskapsmyndigheter ansluter sig till tjänster med ett uttalat säkerhetssyfte. Men för att myndigheterna ska kunna bedöma hur det påverkar deras säkerhet att ansluta sig till en samordnad tjänst behöver leverantörsmyndigheterna tillhandahålla information som visar hur säker den samordnade driften är i olika avseenden. Leverantörsmyndigheterna behöver också komplettera indikatorerna med information som visar regeringen på vilket sätt säkerheten i en myndighets it-drift ökar när de ansluter sig till en samordnad tjänst.

### 2.1.1 Högre säkerhet är myndigheternas främsta motiv för att ansluta sig till den samordnade it-driften

Utifrån vår analys drar vi slutsatsen att en myndighet bara ansluter sig till en viss samordnad it-driftstjänst om de bedömer att den ökar säkerheten i deras it-drift på något sätt. Det innebär att den samordnade it-driften har en positiv effekt på säkerheten i en myndighets it-drift varje gång en myndighet ansluter sig till en samordnad tjänst. Därmed är andelen myndigheter som är anslutna till var och en av de olika tjänsterna inom den samordnade it-driften relevanta indikatorer på effekten av den samordnade driften när det gäller säkerheten i myndigheternas it-drift på aktörsnivå.

Vår analys visar att myndigheter i huvudsak ansluter sig till den samordnade statliga it-driften för att öka säkerheten i sin it-drift. Kostnaden för och kvaliteten i de samordnade tjänsterna är också väsentliga för de myndigheter som är anslutna eller överväger att ansluta sig till den samordnade it-driften. Men samtliga företrädare för anslutna myndigheter som vi har intervjuat uppger att de har anslutit sig till den samordnade statliga it-driften av just säkerhetsskäl.

På motsvarande sätt uppger företrädare för myndigheter som står utanför den samordnade it-driften att de hittills har valt att stå utanför just för att deras befintliga it-driftslösningar erbjuder en högre säkerhet än de samordnade tjänsterna. Men de skulle överväga att ansluta sig till samordnade tjänster längre fram, om tjänsterna skulle hålla högre säkerhetsnivå eller erbjuda funktioner som de själva inte har tillgång till.

Företrädarna för de anslutna myndigheterna beskriver bland annat att leverantörs-myndigheterna har mer personal med hög kompetens inom it-säkerhet, större möjligheter att investera i säkra it-driftstjänster, samt större vana att hantera säkerhetskänslig information i sin egen verksamhet än vad deras myndigheter har. De beskriver också att de genom att ansluta sig till den samordnade it-driften inte

behöver upphandla egna it-driftstjänster i samma utsträckning som tidigare, eftersom överenskommelserna med leverantörsmyndigheten inte har något slutdatum. De säger att det ökar säkerheten eftersom leverantörsbyten innebär säkerhetsrisker i sig. Det beror på att myndigheterna ofta behöver flytta stora mängder data när de byter leverantörer. Ibland behöver de även byta ut sina system. Dessutom behöver myndigheterna säkerställa att leverantörerna uppfyller deras säkerhetskrav, vilket kräver egen kompetens inom it-säkerhet.

### 2.1.2 Särskilt relevant att analysera andelen beredskapsmyndigheter som är anslutna till tjänster för att säkra data

Vi bedömer att den samordnade it-driften har en positiv effekt på säkerheten i myndigheternas it-drift, även när en liten myndighet utan samhällskritisk verksamhet ansluter sig till en tjänst utan uttalat säkerhetssyfte. Det gäller till exempel tjänsten it-arbetsplats. Men vi bedömer att effekten på säkerheten på samhällsnivå är större om myndigheter med samhällskritisk verksamhet ansluter sig till en tjänst med uttalat säkerhetssyfte, till exempel tjänster för att säkra data. Därför anser vi att andelen beredskapsmyndigheter som är anslutna till den samordnade it-driften i allmänhet, och till tjänster med ett uttalat säkerhetssyfte i synnerhet, är relevanta indikatorer på den samlade effekten av den samordnade it-driften när det gäller säkerheten på samhällsnivå.

Vi bedömer att det kommer att variera över tid vilka tjänster som har störst betydelse för säkerheten på samhällsnivå. Det beror på att det sannolikt kommer nya tjänster i takt med den tekniska utvecklingen och att andelen myndigheter som är anslutna till de befintliga tjänsterna sannolikt kommer att öka. Därför är det inte lämpligt att begränsa indikatorerna så att de enbart omfattar vissa samordnade tjänster. I stället behöver leverantörsmyndigheterna i dialog med regeringen avgöra vilka tjänster som är mest relevanta att analysera i de årliga återrapporteringarna.

Vi föreslår att leverantörsmyndigheterna i de närmaste årens återrapporteringar till regeringen fokuserar på att analysera andelen beredskapsmyndigheter som är anslutna till samordnade tjänster för att säkra data. Vi bedömer att den mest grundläggande aspekten av säker, samordnad statlig it-drift är att de data som leverantörsmyndigheterna behandlar i tjänsterna är säkra, det vill säga konfidentiella, riktiga och tillgängliga.[18]

Företrädare för Nitis-myndigheterna delar den bedömningen. Nitis-myndigheterna har tagit fram en modell för att säkra data på tre nivåer. Varje nivå motsvaras av en specifik it-driftstjänst, som ska ingå i utbudet för den samordnade statliga it-driften. Den första och mest grundläggande nivån och tjänsten handlar om att säkra de data

[18] Swedish Standards Institute (2015). *Terminologi för informationssäkerhet.* SIS-TR 50:2015. Stockholm: SIS.

som en myndighet behöver för att i yttersta fall kunna återuppbygga viktiga samhällsfunktioner efter en stor katastrof eller ett krig. Den andra nivån och tjänsten handlar om att säkra de data som en myndighet behöver för att kunna återuppbygga och återställa hela sin befintliga it-drift. Den tredje nivån och tjänsten handlar om att med hjälp av säkrade data återställa en myndighets it-drift inom 15 dagar, antingen till ursprunglig plats, till alternativ plats i Sverige, eller till molnet.

### 2.1.3 Indikatorerna behöver bygga på hur myndigheterna själva bedömer vilken säkerhet de behöver över tid

Vi bedömer att indikatorer på effekterna av den samordnade it-driften när det gäller säkerhet behöver bygga på hur väl myndigheterna själva bedömer att de samordnade tjänsterna uppfyller deras säkerhetskrav. Annars blir indikatorerna inte hållbara över tid. Det beror på att myndigheterna har olika krav på säkerheten i sin it-drift, eftersom de har olika säkerhetskänslig och samhällskritisk verksamhet. Det beror också på att myndigheternas säkerhetskrav ökar kontinuerligt, oavsett om det är från en låg eller en redan hög nivå.[19] Därför behöver indikatorer på effekterna av den samordnade it-driften när det gäller säkerhet kunna röra sig med myndigheternas säkerhetskrav. Vi åstadkommer det genom att bygga indikatorerna på myndigheternas egen bedömning av om en viss samordnad tjänst höjer säkerheten i deras it-drift.

Vår analys visar att myndigheterna har olika förmåga och förutsättningar att formulera relevanta säkerhetskrav för sin it-drift, och även att bedöma hur väl de samordnade tjänsterna svarar mot de kraven. Därför kan vissa myndigheter ansluta sig till samordnade tjänster utan att veta exakt hur säker it-drift de behöver, och hur väl de samordnade tjänsterna egentligen uppfyller deras behov. Men vi bedömer att det inte försämrar indikatorernas tillförlitlighet på något väsentligt sätt.

Vi bedömer nämligen att de myndigheter som inte har förmåga att formulera relevanta säkerhetskrav sannolikt också har en låg säkerhetsnivå i sina befintliga it-driftslösningar. Dessutom är det arbetskrävande att ansluta sig till den samordnade it-driften, oavsett om det handlar om ett helhetsåtagande eller enstaka tjänster. Det beskriver samtliga företrädare för anslutna myndigheter som vi har talat med. Vi bedömer att det därför är osannolikt att myndigheterna skulle lägga ner det arbetet om de inte bedömer att det skulle öka säkerheten, även om de inte har förmåga att bedöma exakt vilken säkerhet det är som de behöver. Därmed bör det ha en positiv effekt på säkerheten även i dessa myndigheters it-drift att ansluta sig till en samordnad tjänst.

Däremot är det sannolikt att myndigheter som inte har förmåga och förutsättningar att formulera relevanta säkerhetskrav i viss mån överkonsumerar säkerhet när de ansluter sig till en samordnad tjänst. En företrädare för en ansluten myndighet

[19] SOU 2021:97. *Säker och kostnadseffektiv it-drift.* s. 374f, 396.

beskriver till exempel att det är tryggt att vara ansluten till den samordnade it-driften, även om den skulle hålla en högre säkerhetsnivå än vad myndigheten behöver. Även It-driftsutredningen beskriver ett liknande exempel.[20] Sådan överkonsumtion ökar statens totala kostnader för it-drift, eftersom myndigheterna i fråga betalar för en högre säkerhet än vad de faktiskt behöver. Men det tar inte bort inte den samordnade it-driftens positiva effekt på säkerheten i myndigheternas it-drift.

Vi bedömer också att varken vi eller leverantörsmyndigheterna har mandat att överpröva hur enskilda myndigheter bedömer vilken säkerhet som de behöver i sin it-drift. Det beror på att alla myndigheter själva ansvarar för att uppfylla de krav på säkerhetsskydd, informationssäkerhet, it-säkerhet och liknande som gäller deras verksamhet. Det gäller även om de överlåter hela sin it-drift till en leverantörs-myndighet. Däremot har leverantörsmyndigheterna ansvar för att ge myndigheterna förutsättningar att fatta välgrundade beslut om att ansluta sig eller att fortsätta vara anslutna till samordnade it-driftstjänster.

### 2.1.4 Leverantörsmyndigheterna bör visa att den samordnade it-driften är säker

Vårt förslag på indikatorer för säkerhet bygger på slutsatsen att myndigheter bara ansluter sig till en samordnad it-driftstjänst om de bedömer att det ökar deras säkerhet på något sätt. Men för att den slutsatsen och våra indikatorer ska hålla över tid behöver myndigheterna ha möjlighet att bedöma hur det påverkar deras säkerhet att ansluta sig till eller fortsätta att vara anslutna till en samordnad tjänst. Därför behöver leverantörsmyndigheterna tillhandahålla information som visar hur säker den samordnade driften är i olika avseenden. Sådan information är också viktig för att de anslutna myndigheternas ledning ska kunna ta ansvar för att deras interna styrning och kontroll fungerar på ett betryggande sätt. Arbetet med att ta fram informationen bör dessutom vara till hjälp för leverantörsmyndigheterna att identifiera eventuella säkerhetsbrister i den samordnade driften. Dessutom bedömer vi att leverantörsmyndigheterna får starkare incitament att åtgärda bristerna om regeringen och myndigheterna förväntar sig att de ska redovisa denna information.

Vår analys visar att det inte finns något enskilt verktyg som ger en tillräcklig bild av säkerheten i den samordnade it-driften. Därför behöver leverantörsmyndigheterna använda flera av de verktyg som är tillgängliga för att visa hur säker den samordnade it-driften är i olika avseenden. Nedan redogör vi för de verktyg vi anser att leverantörsmyndigheterna bör prioritera: egna säkerhetsregler, extern granskning och FRA:s cybersäkerhetstjänster.

[20] SOU 2021:97. *Säker och kostnadseffektiv it-drift.* s. 167.

### Leverantörsmyndigheterna bör ta fram säkerhetsregler för samtliga samordnade tjänster

Vi bedömer att leverantörsmyndigheterna skyndsamt behöver ta fram och publicera dokument som definierar de säkerhetsregler och säkerhetskrav som var och en av de samordnade tjänsterna ska uppfylla. Sådana dokument är en förutsättning för att intresserade myndigheter ska kunna bedöma hur det skulle påverka deras säkerhet att ansluta sig till olika samordnade tjänster. Det är också en förutsättning för att externa och interna revisorer ska kunna granska tjänsterna i förhållande till fastslagna säkerhetskrav. Men i dag är EFOS den enda av de samordnade it-tjänsterna som har publicerade säkerhetsregler och säkerhetskrav.

När leverantörsmyndigheterna formulerar säkerhetskraven som de olika tjänsterna ska uppfylla bör de så långt det är möjligt utgå från befintliga marknadsstandarder och regelverk, till exempel MSB:s föreskrifter om informationssäkerhet respektive säkerhetsåtgärder i informationssystem för statliga myndigheter. Sådana standarder och regelverk är beprövade och välkända och är därmed legitima. Om det inte finns befintliga standarder eller regelverk att utgå ifrån för en viss tjänst bör leverantörsmyndigheterna ta hjälp av expertmyndigheter som Säpo, FRA och MSB. De behöver också ta hänsyn till befintlig eller kommande lagstiftning för området, som NIS2-direktivet och cybersäkerhetslagen.

### Leverantörsmyndigheterna bör låta externa aktörer granska att de samordnade tjänsterna uppfyller sina säkerhetsregler

Leverantörsmyndigheterna bör ge uppdrag åt lämpliga aktörer att återkommande granska om deras tjänster uppfyller säkerhetsreglerna som de har tagit fram. I vissa fall kan det handla om att en annan statlig myndighet, som till exempel Digg eller PTS, granskar och intygar att tjänsten uppfyller reglerna. I andra fall kan det handla om att en privat aktör gör detta, till exempel en it-revisionsbyrå. Det kan även handla om att en leverantörsmyndighets internrevision granskar att tjänsten uppfyller reglerna. Försäkringskassan har till exempel beslutat att årligen låta sin internrevision granska myndighetens arbete med den samordnade it-driften utifrån myndighetens interna säkerhetsregler.[21]

### Leverantörsmyndigheterna bör använda FRA:s cybersäkerhetstjänster

Vi bedömer vidare att leverantörsmyndigheterna i möjligaste mån bör använda de cybersäkerhetstjänster som FRA erbjuder skyddsvärda verksamheter, samt redovisar om och när de har gjort det. Det kan inkludera it-säkerhetsanalyser, till exempel genom penetrationstester, för att identifiera och motverka sårbarheter i den samordnade it-driften. Det kan också inkludera FRA:s Tekniska Detekterings- och Varningssystem (TDV) för att identifiera intrång i leverantörsmyndigheternas it-system.

[21] Försäkringskassan 2025-02-14. *Internrevisionsplan 2025–2027*. FK 2025/002626. s. 7f.

Vetskap om att leverantörsmyndigheterna har använt FRA:s tjänster är en trygghet i sig för myndigheter som är intresserade av att ansluta sig till en samordnad tjänst. Men det gör det också möjligt för myndigheterna att ha en dialog med leverantörsmyndigheterna om resultaten från FRA:s analyser. På så sätt kan leverantörsmyndigheterna visa att den samordnade driften har god cybersäkerhet. FRA delar bara resultaten av sina it-säkerhetsanalyser med den uppdragsgivare som har begärt analysen. Men företrädare för FRA säger att uppdragsgivaren i sin tur själv kan välja att dela resultatet i en vidare krets om den anser att det är lämpligt.

### 2.1.5 Leverantörsmyndigheterna bör visa hur de samordnade tjänsterna ökar säkerheten

Vi föreslår att leverantörsmyndigheterna systematiskt samlar in information som gör det möjligt att jämföra säkerheten i de samordnade tjänsterna med säkerheten i de anslutande myndigheternas befintliga it-driftslösningar. Därigenom kan leverantörsmyndigheterna ta fram nyckeltal som ger en bild av hur de samordnade tjänsterna ökar säkerheten för de anslutande myndigheterna. Sådana nyckeltal är viktiga för att underbygga våra förslag på indikatorer, eftersom de belägger att det sker en förflyttning från en mindre säker it-driftslösning till en mer säker it-driftslösning när en myndighet ansluter sig till en samordnad tjänst. Nyckeltalen är också viktiga för att ge regeringen en tydlig och utförlig bild av vad effekterna av den samordnade it-driften består i när det gäller säkerhet.

Försäkringskassan och de övriga leverantörsmyndigheterna har under 2025 börjat att undersöka om de kan ta fram ett gemensamt systemstöd för att administrera informationen om och kontakterna med de anslutna myndigheterna. Vi ser flera fördelar med ett sådant systemstöd. Vi bedömer till exempel att leverantörsmyndigheterna skulle kunna utforma systemstödet så att det går att använda även för att jämföra säkerheten i de samordnade tjänsterna och de anslutande myndigheternas befintliga it-driftslösningar. Mer specifikt föreslår vi att leverantörsmyndigheterna för var och en av de samordnade tjänsterna definierar cirka 3–5 konkreta förflyttningar. Dessa ska visa vad det kan innebära ur ett säkerhetsperspektiv för en myndighet att gå från en mindre säker befintlig lösning (A) till en mer säker samordnad lösning (B).

Vi bedömer att leverantörsmyndigheterna själva är bäst lämpade att definiera de exakta förflyttningarna som kan ske i en myndighets säkerhet när den ansluter sig till en viss tjänst. Men vi har några medskick baserat på våra intervjuer med företrädare för ett urval av anslutna myndigheter. Vissa av förflyttningarna kan avse att den anslutande myndigheten får tillgång till ny funktionalitet som höjer deras säkerhet. När det gäller tjänsten EFOS kan det till exempel handla om att den anslutande myndigheten går från inloggning med enfaktorsverifiering som användarnamn och lösenord (A), till inloggning med tvåfaktorsverifiering som utöver användarnamn och lösenord även inkluderar ett personligt tjänstekort (B). Andra av förflyttningarna kan avse att den anslutande myndigheten får tillgång till

samma funktionalitet som tidigare, men med en högre säkerhetsnivå. När det gäller tjänsten SAFOS kan det till exempel handla om att den anslutande myndigheten går från att genomföra videomöten via servrar i länder utanför EU (A) till att genomföra videomöten via servrar i Sverige (B). Förflyttningarna kan också vara unika för en viss tjänst, som i exemplet med EFOS ovan, eller relevanta för flera tjänster, som i exemplet med SAFOS ovan. Det viktigaste är att lägena som motsvarar A och B är tydligt definierade.

Med ovanstående nyckeltal kan leverantörsmyndigheterna visa hur ofta de definierade förflyttningarna uppstår när en myndighet ansluter sig till en samordnad it-driftstjänst. Över tid bör leverantörsmyndigheterna därmed kunna urskilja mönster, till exempel vilka som är de vanligaste förflyttningarna och om det varierar över tid eller mellan olika typer av myndigheter. Det kan leverantörsmyndigheterna göra även om de redovisar informationen på gruppnivå och först när myndigheterna är helt anslutna till tjänsterna i fråga, för att inte röja potentiellt känslig information om myndigheternas nuläge.

Däremot ger nyckeltalen ingen fullständig bild av hur säkerheten ökar när en myndighet ansluter sig till en samordnad tjänst. Det beror bland annat på att det inte går att förutse eller definiera alla tänkbara säkerhetsrelaterade förflyttningar som en myndighet kan göra när den ansluter sig till en tjänst. Därför är det viktigt att leverantörsmyndigheterna definierar de mest väsentliga förflyttningarna.

### 2.1.6 Leverantörsmyndigheterna bör visa på redundansen i de samordnade tjänsterna

Vi föreslår att leverantörsmyndigheterna tar fram en modell som gör det möjligt att följa och visa vilken redundans som de erbjuder i var och en av de samordnade it-driftstjänsterna. Med redundans menar vi förmågan att tillhandahålla tjänsterna från flera olika geografiskt åtskilda platser och på flera olika sätt. Vi bedömer att en sådan modell är ett viktigt verktyg för leverantörsmyndigheterna när det gäller att visa både att den samordnade it-driften är säker i avseendet att den erbjuder en viss redundans, och hur de samordnade tjänsterna kan öka säkerheten i de anslutna myndigheternas it-drift. Dessutom kan en sådan modell förstärka leverantörsmyndigheternas incitament att utveckla och upprätthålla en god redundans.

Vi bedömer att en modell för redundans behöver ta hänsyn till flera aspekter. En aspekt är antalet geografiskt åtskilda datacenter som leverantörsmyndigheterna kan driva de samordnade tjänsterna från. Åtskilda datacenter är det vanligaste sättet att uppnå och mäta redundans.[22] Andra aspekter är antalet olika kommunikationsvägar som leverantörsmyndigheterna kan förmedla tjänsterna via, samt antalet leverantörer som tillhandahåller tjänsterna. Vi anser att varken leverantörsmyndigheterna eller de anslutna myndigheterna har någon nytta av att tjänsterna finns på flera datacenter,

[22] SOU 2021:97. *Säker och kostnadseffektiv it-drift.* s. 295.

om det inte finns kommunikationsvägar att förmedla tjänsterna via eller leverantörer som kan tillhandahålla dem. Därmed blir den lägsta nivån av redundans ett datacenter, en kommunikationsväg och en leverantörsmyndighet. Den högsta nivån bör vara upp till leverantörsmyndigheterna att definiera. Men den skulle kunna innehålla flera geografiskt åtskilda datacenter, flera kommunikationsvägar och flera leverantörsmyndigheter och externa leverantörer både i Sverige och utomlands.

Med hjälp av modellen för redundans bör leverantörsmyndigheterna kunna följa om det sker en förflyttning när det gäller redundans när en myndighet ansluter sig till en viss samordnad tjänst. Därmed kan leverantörsmyndigheterna också följa upp att den totala potentiella redundansen i de anslutna myndigheternas it-drift inte minskar, till exempel till följd av att de avvecklar egna datacenter och avtal med externa leverantörer när de ansluter sig till en samordnad helhetstjänst som it-arbetsplats. Det är viktigt att redundansen inte minskar för att den samordnade it-driften inte ska ha en negativ effekt på säkerheten på samhällsnivå.

Men det kommer fortfarande vara upp till de enskilda anslutna myndigheterna hur de väljer att använda de samordnade tjänsterna. Att en leverantörsmyndighet tillhandahåller en tjänst som erbjuder en viss redundans är ingen garanti för att en ansluten myndighet verkligen utnyttjar den fulla redundansen i fråga. Modellen som vi föreslår fångar inte heller upp skillnader i kvalitet mellan olika datacenter och kommunikationsvägar, till exempel när det gäller kapacitet och säkerhet. Vi bedömer att modellen skulle bli alltför komplex om den även skulle inkludera dessa aspekter.

Vi bedömer att det sannolikt kommer att variera mellan olika tjänster vad som är en lämplig nivå av redundans. Det beror på att en hög redundans är viktigare i vissa tjänster än andra. Det kan till exempel handla om tjänster som ligger till grund för andra delar av en ansluten myndighets it-drift, som datacenter- och plattforms-tjänster. Det beror också på att högre redundans generellt innebär högre kostnad, även om sambandet inte är linjärt.

### 2.1.7 Indikatorerna visar förekomsten av positiva effekter på säkerheten, inte hur stora effekterna är

Våra förslag på indikatorer mäter *effekten* av den samordnade it-driften på säkerheten i myndigheternas it-drift. Mer specifikt mäter de om den samordnade driften har *en positiv effekt* på säkerheten i myndigheternas it-drift. Om en ny myndighet ansluter sig till en samordnad tjänst har den samordnade driften en positiv effekt på myndighetens säkerhet. Om en myndighet konsekvent står utanför den samordnade it-driften har den ingen effekt alls. Om en myndighet lämnar en samordnad tjänst så upphör den samordnade driftens tidigare positiva effekt. Att följa den totala andelen av myndigheterna som är anslutna till varje samordnad tjänst ger därmed en bild av den samordnade it-driftens samlade effekt på säkerheten på myndighetsnivå. Att följa andelen beredskapsmyndigheter som är

anslutna till varje tjänst, särskilt till de tjänster som har ett uttalat säkerhetssyfte, ger i sin tur en bild av den samordnade it-driftens samlade effekt på säkerheten på samhällsnivå.

Indikatorerna mäter inte hur *stor* effekt den samordnade it-driften har på säkerheten i myndigheternas it-drift. De säger alltså inget om hur mycket säkerheten ökar när en myndighet ansluter sig till en viss tjänst. Det gäller både på myndighetsnivå och på samhällsnivå. Indikatorerna mäter inte heller på vilket sätt som säkerheten ökar. Det gör däremot våra förslag till nyckeltal på en övergripande nivå. Sist men inte minst mäter indikatorerna inte hur säker myndigheternas it-drift är i absoluta termer, varken när det gäller de anslutna myndigheterna eller de myndigheter som står utanför den samordnade it-driften. Det beror delvis på att de flesta myndigheter bara har en del av sin it-drift i samordnad regi. Det beror också på att det inte finns några tillförlitliga eller jämförbara data om säkerheten i myndigheternas it-drift som helhet.

## 2.2 Data över säkerheten i myndigheternas it-drift är en ostadig grund för indikatorer

Under vårt arbetes gång har företrädare för Regeringskansliet samt andra myndigheter lyft fram bland annat incidentdata, data från Cybersäkerhetskollen samt våra förslag till nyckeltal som möjliga underlag för indikatorer på effekterna av den samordnade it-driften när det gäller säkerhet. Men vi bedömer att dessa data inte är lämpliga att använda på det sättet. Det beror bland annat på att sådana indikatorer skulle bli svåra att tolka, och på att de inte skulle vara träffsäkra när det gäller att visa på effekter av den samordnade it-driften.

### 2.2.1 Indikatorer som bygger på våra förslag till nyckeltal och verktyg är inte lämpliga

Vi bedömer att våra förslag till nyckeltal och verktyg i huvudsak ger en ögonblicksbild av den samordnade it-driften, och inte en hållbar bild av utvecklingen över tid. Därför är de inte lämpliga som underlag för indikatorer.

Vi bedömer att de nyckeltal vi föreslår för att illustrera *hur* den samordnade it-driften bidrar till öka säkerheten i de anslutna myndigheternas it-drift inte lämpar sig för att ligga till grund för indikatorer. Sådana indikatorer skulle inte vara hållbara över tid. I takt med den tekniska utvecklingen och kontinuerligt högre säkerhetskrav kommer säkerhetsnivån att bli högre, både i den samordnade it-driften och i de anslutande myndigheternas befintliga it-driftslösningar. Därmed kommer de förflyttningar som är relevanta i dag gradvis att bli obsoleta och leverantörsmyndigheterna kommer att behöva ersätta dem med nya. De nya förflyttningarna kommer inte heller att kunna ersätta de tidigare förflyttningarna rakt av, eftersom de kommer att vara olika till sin natur och inte kvantifierbara. En förflyttning från A till B i dag är till exempel inte det samma som en förflyttning från C till D imorgon. Dessutom bedömer vi att många av förflyttningarna kommer att vara unika för en viss tjänst.

Inte heller våra förslag på verktyg som leverantörsmyndigheterna kan använda för att visa hur säker den samordnade it-driften är i olika avseenden lämpar sig för att ligga till grund för indikatorer. Det främsta skälet är sådana indikatorer skulle vara svåra att tolka. Med indikatorer som bygger på resultaten från en extern eller intern revision, andra myndigheters granskningar eller FRA:s penetrationstest skulle vi inte veta om ett bättre resultat visar på att säkerheten har blivit högre eller på att revisionen, granskningen eller testet inte är lika väl utfört som tidigare. Om den som granskar den samordnade it-driften tvärtom hittar fler säkerhetsbrister skulle vi inte veta om det betyder att den samordnade it-driften har blivit mindre säker eller att granskaren hade blivit vassare. Dessutom är det inte säkert att de olika granskningarna kommer att vara tillgängliga eller bli utförda på samma sätt och över tid, vilket gör potentiella indikatorer ännu svårare att tolka.

### 2.2.2 Indikatorer som bygger på incidentdata är alltför svåra att tolka

Alla statliga myndigheter ska rapportera it-incidenter till MSB. Det framgår av 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Myndigheter som hanterar säkerhetsskyddsklassad information ska också rapportera it-incidenter till Säpo, om incidenterna inträffar i informationssystem som har betydelse för säkerhetskänslig verksamhet och incidenten allvarligt kan påverka säkerheten i systemet. Det framgår av 2 kap. 4 § säkerhetsskyddsförordningen. Dessutom har leverantörsmyndigheterna och de flesta andra myndigheter olika interna system för att upptäcka och följa upp it-incidenter.

Vi har övervägt men valt att inte föreslå indikatorer som bygger på incidentdata. Det gäller både sådana incidenter som myndigheterna upptäcker och hanterar internt, och sådana som de rapporterar till MSB eller Säpo. Sådana indikatorer hade till exempel kunnat avse antalet it-incidenter som myndigheterna rapporterar till MSB årligen, före och efter att de har anslutit sig till olika samordnade it-driftstjänster.

Indikatorer som bygger på incidentdata är svåra att tolka. Om myndigheterna upptäcker fler incidenter vet vi inte om det beror på att det faktiskt sker fler incidenter, eller på att myndigheterna har blivit bättre på att upptäcka dem. Om det beror på att det faktiskt sker fler incidenter betyder det att säkerheten har minskat. Men om det beror på att myndigheten har blivit bättre på att upptäcka incidenterna betyder det att säkerheten har ökat. Om myndigheterna rapporterar fler incidenter till MSB eller Säpo vet vi inte heller om det beror på att det faktiskt sker fler incidenter, att myndigheterna upptäcker en större andel av incidenterna, eller att de rapporterar en större andel av de incidenter som de upptäcker. Om det beror på att myndigheterna rapporterar en större andel av de incidenter som de upptäcker säger ett ökat antal rapporterade incidenter ingenting om säkerheten i myndigheternas it-system. Enligt MSB finns det ett stort mörkertal av incidenter som myndigheterna inte rapporterar. MSB baserar det på att många rapporteringspliktiga organisationer

aldrig har rapporterat någon incident, samtidigt som MSB genom andra kanaler återkommande får information om rapporterade incidenter.[23]

### 2.2.3 Indikatorer som bygger på MSB:s mätningar fångar inte upp effekter av den samordnade it-driften

Vi har övervägt men valt att inte föreslå indikatorer som bygger på data från MSB:s mätningar Infosäkkollen respektive It-säkkollen. Sådana indikatorer skulle ha kunnat avse exempelvis enskilda myndigheters resultat före och efter att de har anslutit sig till en samordnad it-driftstjänst.

Infosäkkollen utgår från kraven i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) och It-säkkollen utgår från kraven i MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7). Enligt MSB indikerar ett resultat på minst nivå 3 av 4 i mätningarna att en myndighets interna arbete med informationssäkerhet respektive it-säkerhet uppfyller kraven i föreskrifterna.

Det främsta skälet till att vi har valt bort indikatorer som bygger på data från mätningarna är att de inte fångar upp effekter av den statliga samordnade it-driften. Det är helt enkelt inte tydligt varför enskilda myndigheters interna arbete med informationssäkerhet eller it-säkerhet skulle bli bättre eller sämre till följd av att ansluta sig till en samordnad tjänst. Det gäller särskilt för de myndigheter som bara har en liten del av sin totala it-drift i samordnad regi, eftersom mätningarna gäller myndigheternas verksamhet som helhet.

Dessutom bygger mätningarna på egenrapporterade data, även om myndigheterna ska styrka sina svar genom att bifoga dokumenterade underlag. Att basera indikatorer på myndigheternas resultat riskerar därför att påverka hur myndigheterna besvarar mätningarna. Det skulle underminera både indikatorernas tillförlitlighet och mätningarnas förutsättningar att ge en nationell lägesbild av det systematiska cybersäkerhetsarbetet samt att stödja myndigheternas eget arbete med att utveckla sin cybersäkerhet. MSB använder inte heller myndigheternas svar som underlag för tillsyn av hur myndigheterna följer de berörda föreskrifterna, just för att inte påverka hur myndigheterna besvarar mätningarna. Det uppger företrädare för MSB.

I dag är det dessutom frivilligt för myndigheterna att genomföra mätningarna. 2024 var det bara 120 respektive 114 myndigheter som genomförde Infosäkkollen respektive It-säkkollen och som delade sina svar med MSB.[24] Det ger inte ett tillförlitligt underlag för indikatorer. Men att göra mätningarna obligatoriska skulle riskera att ytterligare påverka hur myndigheterna besvarar dem.

---

[23] Myndigheten för samhällsskydd och beredskap (2025). *Verktyg för ökad motståndskraft och stärkt civilt försvar*. s. 1.

[24] Myndigheten för Samhällsskydd och Beredskap (2025). *Resultatredovisning av Cybersäkerhetskollen 2024*. s. 19f.

### 2.2.4 Indikatorer som bygger på data över redundans eller antalet datacenter

Vi har övervägt men valt att inte föreslå en indikator som bygger på antalet geografiskt åtskilda datacenter som leverantörsmyndigheterna förfogar över. En sådan indikator skulle vara svår att tolka, eftersom datacenter har olika kapacitet och säkerhet. Tre små datacenter i tre vanliga kontorsbyggnader innebär till exempel inte nödvändigtvis en säkrare it-drift än ett stort datacenter i ett atombombssäkert bergrum. Antalet datacenter som leverantörsmyndigheterna förfogar över säger inte heller något om hur myndigheterna använder centren i fråga. Det säger alltså inget om hur stor redundansen faktiskt är när det gäller viss information eller vissa system. Dessutom fångar de indikatorer som vi föreslår ändå upp det övergripande syftet med redundans, det vill säga förmågan att återställa information och upprätthålla verksamheten även vid störningar eller angrepp.

Vårt förslag om en modell för att följa och illustrera redundansen i de samordnade it-driftstjänsterna lämpar sig inte heller för att ligga till grund för indikatorer. Det främsta skälet till det är att modellen innehåller alltför mycket komplex information för att den ska vara möjlig att kondensera till begripliga och relevanta indikatorer. Tvärtom är en av poängerna med modellen just att illustrera att redundans inte bara handlar om antalet datacenter. Det handlar även bland annat om typen av datacenter, var de ligger i förhållande till varandra, kommunikationsvägarna från respektive datacenter, vem som driver dem, samt hur de olika faktorerna är kombinerade. Dessutom är behovet av redundans och nivån på redundansen olika för olika samordnade tjänster, vilket ökar komplexiteten i informationen ytterligare.

# 3 Förslag på indikatorer – kostnadseffektivitet

I det här kapitlet redogör vi för våra förslag på indikatorer för att följa effekterna av den samordnade statliga it-driften när det gäller kostnadseffektivitet på aktörs- och samhällsnivå. Vi redogör även för motiven till våra förslag samt för skälen till att vi har valt bort andra potentiella indikatorer. Vi föreslår följande indikatorer när det gäller kostnadseffektivitet:

- *Antalet enheter* (till exempel användare eller terabyte) inom var och en av de samordnade it-driftstjänsterna
- Den *genomsnittliga kostnaden per enhet* (till exempel användare eller terabyte) inom var och en av de samordnade it-driftstjänsterna.

Med enhet menar vi den enhet som står för den största delen av kostnaderna i en viss tjänst, i de fall som en tjänst är sammansatt av flera olika enheter. Ett sådant exempel är tjänsten it-arbetsplats, som kan inkludera både dator, samarbetsplattform, utskrifter och support. Där står datorn för den största delen av kostnaderna. Med kostnad menar vi fullständig produktionskostnad, inklusive både direkta kostnader och indirekta kostnader. De indirekta kostnaderna inkluderar i sin tur både it-specifika indirekta kostnader, till exempel för chefer inom it-området, samt myndighetsgemensamma indirekta kostnader, till exempel för myndighetsledning och lokaler. Det ligger i linje med den gemensamma ekonomimodell som leverantörsmyndigheterna har kommit överens om att använda för att beräkna sina kostnader för de samordnade it-driftstjänsterna.[25]

## 3.1 Indikatorerna kan visa på realiserade skalfördelar

Vår analys visar att den samordnade it-driften i huvudsak kan bidra till ökad kostnadseffektivitet genom att leverantörsmyndigheterna skapar och tar tillvara skalfördelar. Det innebär den genomsnittliga kostnaden per enhet minskar i takt med att antalet enheter ökar. Leverantörsmyndigheterna kan påverka förekomsten av skalfördelar. Men skalfördelar är inte den enda faktorn som påverkar kostnaden per enhet. Därför behöver leverantörsmyndigheterna så långt det är möjligt förklara hur såväl antalet enheter som andra faktorer påverkar kostnaden per enhet. De andra faktorerna inkluderar både externa faktorer som priset på insatsvaror och interna faktorer som leverantörsmyndigheternas investeringar i att öka säkerheten

[25] Försäkringskassan 2025-06-05. *Ekonomi- och avgiftsmodell för samordnad och säker statlig it-drift.* FK 2024/006706.

eller kvaliteten i de samordnade tjänsterna. Först då kan regeringen använda våra förslag till indikatorer för att följa den samordnade it-driftens effekter när det gäller kostnadseffektivitet.

### 3.1.1 Skalfördelar är den främsta möjligheten att öka kostnadseffektiviteten i myndigheternas it-drift

Vi bedömer att den samordnade it-driftens effekter när det gäller kostnadseffektivitet i huvudsak beror på hur väl leverantörsmyndigheterna skapar och tar tillvara möjligheten till skalfördelar. Vi baserar det på att både företrädare för samtliga leverantörsmyndigheter och It-driftsutredningen lyfter fram att samordnad statlig it-drift kan öka kostnadseffektiviteten just genom möjligheten att ta tillvara skalfördelar.[26] Med skalfördelar menar vi att den genomsnittliga kostnaden per enhet minskar i takt med att antalet enheter ökar. Det gäller exempelvis enheter som användare eller terabyte data. Skalfördelar kan uppstå genom att leverantörs-myndigheterna fördelar sina kostnader för att utveckla en tjänst, eller sina fasta kostnader för till exempel infrastruktur eller personal på fler enheter. Därmed sjunker kostnaden per enhet om allt annat är lika. Antalet enheter beror i sin tur på hur många och hur stora myndigheter som är anslutna till en viss tjänst. Det beror också på i hur stor del av sin verksamhet som myndigheterna använder tjänsten i fråga.

Den samordnade it-driften har därmed en positiv effekt på kostnadseffektiviteten i de anslutna myndigheternas it-drift varje gång leverantörsmyndigheterna tar tillvara en skalfördel. Om skalfördelarna växer så ökar även den positiva effekten, eftersom de anslutna myndigheterna då får tillgång till den säkerhet och kvalitet som tjänsterna erbjuder till en lägre kostnad än tidigare. Därför bedömer vi att både antalet enheter och den genomsnittliga kostnaden per enhet är relevanta indikatorer på den samordnade it-driftens effekter när det gäller kostnadseffektivitet på myndighetsnivå.

Men för att regeringen ska kunna använda dessa indikatorer för att bedöma i vilken utsträckning som leverantörsmyndigheterna tar tillvara möjligheten till skalfördelar behöver leverantörsmyndigheterna redovisa indikatorerna samlat, och relatera dem till varandra. Vi har övervägt att föreslå en indikator som visar kvoten mellan antalet enheter och kostnaden. Men vi har valt att inte göra det, eftersom en sådan indikator är mer komplex och därmed svårare för läsaren att förstå än separata indikatorer för antalet enheter och kostnader per enhet.

Den samordnade it-driftens effekter på kostnadseffektiviteten på samhällsnivå är svårare att mäta. I teorin speglar summan av skalfördelarna som leverantörs-myndigheterna tar tillvara effekterna på samhällsnivå. Men det förutsätter att de anslutna myndigheterna träffsäkert bedömer vilken säkerhet och kvalitet som de behöver i sin it-drift, samt i vilken utsträckning som de samordnade tjänsterna

[26] SOU 2021:97. *Säker och kostnadseffektiv it-drift.* s. 290, 396f.

möter de behoven. Om några av de anslutna myndigheterna överkonsumerar säkerhet eller kvalitet urholkar det den samordnade it-driftens positiva effekter på kostnadseffektivitet på samhällsnivå. Det följer av att en del av pengarna som staten betalar för it-drift skulle ha kunnat göra större nytta någon annanstans.

Samtidigt går det att argumentera för att en eventuell överkonsumtion av säkerhet eller kvalitet subventionerar de samordnade tjänsterna i fråga för de myndigheter som behöver så hög säkerhet och kvalitet som tjänsterna erbjuder. Det följer av att överkonsumtionen då ökar skalfördelarna i tjänsterna så att de blir tillgängliga till ett lägre pris. Det kan också vara kostnadseffektivt på samhällsnivå. Dessutom bör högre säkerhet och kvalitet i de anslutna myndigheternas it-drift innebära färre säkerhetsincidenter, driftstörningar och liknande, vilket också sparar pengar för de anslutna myndigheternas på sikt. Sammantaget bedömer vi därför att indikatorerna ger användbar information om den samordnade it-driftens effekter på kostnads-effektivitet även på samhällsnivå.

### 3.1.2 Leverantörsmyndigheterna kan påverka förekomsten av skalfördelar

Vi bedömer att leverantörsmyndigheterna har stora möjligheter att påverka i vilken utsträckning som de samordnade it-driftstjänsterna är skalbara, eftersom det är de som bygger och tillhandahåller tjänsterna. Leverantörsmyndigheterna kan till exempel göra tjänsterna mer skalbara genom att utforma både dem och sina processer för att ansluta myndigheter på ett standardiserat sätt. Det inkluderar att undvika särlösningar för enskilda myndigheter och att utveckla arbetssätt som drar nytta av de olika spetskompetenser som finns i leverantörsmyndigheternas stora organisationer. Därför anser vi att det är relevant att följa förekomsten av realiserade skalfördelar i samtliga tjänster. På så sätt får leverantörsmyndigheterna också incitament att utforma nya tjänster och vidareutveckla befintliga tjänster så att de i hög utsträckning blir skalbara. Därmed kan indikatorerna över tid bidra till att öka kostnadseffektiviteten i den samordnade it-driften.

Företrädare för leverantörsmyndigheterna beskriver att skalfördelarna i dag är olika stora och lätta att ta tillvara i olika samordnade it-driftstjänster. Helt standardiserade och tydligt avgränsade tjänster som EFOS och SAFOS har till exempel stora skal-fördelar. Det beror på att leverantörsmyndigheterna kan ansluta nya myndigheter till tjänsterna utan någon större arbetsinsats. En bred tjänst med flera fysiska komponenter som it-arbetsplats har däremot jämförelsevis små skalfördelar. Det beror på att leverantörsmyndigheterna behöver kombinera olika tjänster på delvis olika sätt, och förmedla fysiska komponenter till varje ny ansluten myndighet och användare. Det kan till exempel handla om att distribuera fysiska datorer och annan utrustning till nya användare och att tillhandahålla support på plats hos den anslutna myndigheten. De minsta skalfördelarna ser vi när leverantörsmyndigheterna utvecklar kundunika lösningar för enskilda anslutna myndigheter, till exempel för att möta specifika säkerhetskrav eller verksamhetsbehov.

### 3.1.3 Kostnaden per enhet beror på fler faktorer än om det finns skalfördelar

Flera förutsättningar behöver vara uppfyllda för att det negativa sambandet mellan antalet enheter och kostnaden per enhet ska vara linjärt. För det första måste priset på insatsvarorna vara konstant. För det andra behöver innehållet, säkerheten och kvaliteten i enheterna också vara konstant. Vi bedömer att ingen av dessa förutsättningar är helt uppfyllda när det gäller de samordnade it-driftstjänsterna.

Leverantörsmyndigheterna kan inte kan styra kostnaderna på insatsvaror som lokaler, programvarulicenser eller el fullt ut, även om de kan påverka dem genom hur de utformar och löpande ser över sina avtal. Dessutom kan ny lagstiftning eller nya tekniska möjligheter göra det möjligt för leverantörsmyndigheterna att producera och tillhandahålla samordnade tjänster på ett enklare och billigare sätt än tidigare. Men de kan också tvinga leverantörsmyndigheterna till dyra investeringar för att möta nya krav. Vi bedömer till exempel att leverantörsmyndigheterna i praktiken behöver uppdatera och vidareutveckla sina tekniska lösningar och system löpande enbart för att upprätthålla den befintliga säkerhetsnivån i de samordnade it-driftstjänsterna. Det beror på att den tekniska utvecklingen går snabbt. Leverantörsmyndigheterna behöver hålla samma utvecklingstakt som de som kan vilja skada de anslutna myndigheternas verksamhet.

### 3.1.4 Leverantörsmyndigheterna prioriterar högre säkerhet framför lägre kostnader

Leverantörsmyndigheterna har hittills prioriterat högre säkerhet framför lägre kostnader i arbetet med den samordnade it-driften. Det påverkar såväl innehållet och säkerheten som kvaliteten i de samordnade tjänsterna, och därmed kostnaderna per enhet. Högre säkerhet innebär generellt högre kostnad, även om det sambandet inte är linjärt. Det uppger i princip samtliga företrädare för leverantörsmyndigheterna, anslutna myndigheter och expertmyndigheter inom digitaliserings- och säkerhetsområdet som vi har talat med. Ett datacenter i ett bergrum är till exempel dyrare än ett datacenter i en garderob.

Företrädare för leverantörsmyndigheterna uppger att de hittills i huvudsak använder vinsterna från de realiserade skalfördelarna i den samordnade driften till att höja säkerheten i tjänsterna och inte till att sänka enhetskostnaderna. De anser att högre säkerhet är det främsta syftet med den samordnade it-driften. De säger att den samordnade driften syftar till att öka de anslutna myndigheternas säkerhet på ett sätt som är kostnadseffektivt för staten som helhet och inte till att sänka enskilda myndigheters kostnader.

Detta ligger också i linje med hur utredaren i It-driftsutredningen resonerade. Utredaren bedömde att myndigheterna sannolikt skulle öka sina kostnader för it-drift när de ansluter sig till den samordnade it-driften, eftersom de samordnade

tjänsterna erbjuder en högre säkerhet än deras tidigare it-driftslösningar.[27] Ingen av företrädarna för de anslutna myndigheter som vi har intervjuat uppfattar heller att deras kostnader för it-drift har minskat sedan de anslöt sig till den samordnade driften. Men det är också få av dem som har jämfört kostnaderna systematiskt.

### 3.1.5 Leverantörsmyndigheterna behöver visa vad som driver kostnaderna per enhet

Vi bedömer att förändringar i priset på insatsvaror samt i innehållet, säkerheten och kvaliteten i de samordnade it-driftstjänsterna sammantaget innebär att vi inte kan förvänta oss ett linjärt negativt samband mellan den genomsnittliga kostnaden per enhet och antalet enheter även om leverantörsmyndigheterna skulle skapa och ta tillvara skalfördelar i den samordnade it-driften. Kostnaden per enhet bör fortfarande sjunka när antalet enheter ökar. Men den kommer sannolikt inte att sjunka så mycket som den skulle ha gjort om it-driftens insatsvaror, innehåll, säkerhet och kvalitet var konstanta över tid. Detta betyder inte att leverantörsmyndigheterna inte producerar eller tillhandahåller de samordnade tjänsterna på ett kostnadseffektivt sätt. Men det gör det svårare för regeringen att bedöma om den samordnade it-driften är kostnadseffektiv på så sätt att leverantörsmyndigheterna faktiskt realiserar skalfördelar.

Därför behöver leverantörsmyndigheterna förklara vad som ligger bakom förändringar i indikatorvärdena, särskilt när det handlar om relationen mellan antalet enheter och den genomsnittliga kostnaden per enhet. Mer specifikt anser vi att leverantörsmyndigheterna bör förklara i vilken utsträckning som förändringar i den genomsnittliga kostnaden per enheten beror på:

- förändringar i antalet enheter
- förändringar i priset på insatsvaror
- förändringar i tjänsternas innehåll, säkerhet och kvalitet som upprätthåller tjänsternas befintliga säkerhetsnivå
- förändringar i tjänsternas innehåll, säkerhet och kvalitet som höjer tjänsternas säkerhetsnivå.

Om leverantörsmyndigheterna kan förklara detta får regeringen förutsättningar att bedöma i vilken utsträckning som leverantörsmyndigheterna tar tillvara skalfördelar. Regeringen får också förutsättningar att bedöma hur leverantörsmyndigheternas sätt att prioritera påverkar enhetskostnaderna för de samordnade tjänsterna. Det är i sin tur en förutsättning för att regeringen vid behov ska kunna styra leverantörsmyndigheterna att prioritera annorlunda.

---

[27] SOU 2021:97. *Säker och kostnadseffektiv it.* s. 374f, 396.

### 3.1.6 Leverantörsmyndigheterna bör relatera enhetskostnaderna till pris- och löneomräkningen (PLO)

Vi bedömer att leverantörsmyndigheterna har ganska svaga incitament att hålla nere enhetskostnaderna för de samordnade tjänsterna. Det beror på att it-driftsförordningens fokuserar på säkerhet och på att den samordnade it-driftens finansieringsmodell ser ut som den gör. Enligt modellen ska leverantörsmyndigheterna finansiera de samordnade tjänsterna med avgifter som täcker deras egna kostnader. Men det är arbetskrävande för myndigheterna att byta it-leverantör, oavsett om det handlar om en leverantörsmyndighet eller en privat leverantör. Det framgår av våra intervjuer med företrädare för anslutna myndigheter. Företrädare för flera av myndigheterna beskriver att de i praktiken inte har något annat val än att acceptera de avgifter som leverantörsmyndigheterna har bestämt. Därmed riskerar den samordnade it-driften att inte öka kostnadseffektiviteten i myndigheternas it-drift lika mycket som den skulle kunna göra.

För att minska den risken bedömer vi att leverantörsmyndigheterna bör relatera enhetskostnaderna för de samordnade tjänsterna till det pris- och löneomräkningstal (PLO) som regeringen använder för att årligen justera myndigheternas förvaltningsanslag. Mer specifikt bör leverantörsmyndigheterna förklara och motivera varför den långsiktiga relationen mellan enhetskostnaderna och PLO ser ut som den gör. På så sätt får regeringen en tydlig bild av hur leverantörsmyndigheterna väger säkerhet mot kostnad.

PLO bygger på den allmänna pris- och löneutvecklingen i samhället, men inkluderar ett så kallat produktivitetsavdrag som regeringen förväntar sig att myndigheterna ska täcka genom att effektivisera sin verksamhet. Om enhetskostnaderna för de samordnade tjänsterna över tid ökar snabbare än PLO kan det betyda att leverantörsmyndigheterna inte har effektiviserat sitt arbete med den samordnade it-driften i den utsträckning som regeringen förväntar sig. Men det kan också betyda att leverantörsmyndigheterna har använt medlen som de har frigjort genom att effektivisera sitt arbete till att höja säkerheten i den samordnade driften. Vilket av detta som gäller kan leverantörsmyndigheterna visa i sin förklaring.

### 3.1.7 Indikatorerna mäter inte hur kostnadseffektiv den samordnade it-driften är i absoluta termer

Våra förslag på indikatorer mäter *effekten* av den samordnade driften på kostnadseffektiviteten i myndigheternas it-drift. Om leverantörsmyndigheterna realiserar en skalfördel i en samordnad tjänst har den samordnade driften en positiv effekt på kostnadseffektiviteten i myndighetens it-drift. Ju större skalfördelen är, desto större är den positiva effekten. Om en myndighet konsekvent står utanför den samordnade it-driften har den ingen effekt alls. Om en skalfördel upphör eller minskar i en samordnad tjänst upphör eller minskar även den samordnade driftens tidigare positiva effekt i motsvarande grad.

Men för att det ska gå att bedöma förekomsten av skalfördelar och hur stora de är behöver leverantörsmyndigheterna så långt det är möjligt isolera sambandet mellan antalet enheter och den genomsnittliga kostnaden per enhet. Det kan de göra genom att visa att såväl kostnaderna för insatsvaror som innehållet, säkerheten och kvaliteten i tjänsterna är konstant. De kan också göra det genom att visa hur förändringar i dessa faktorer påverkar de genomsnittliga enhetskostnaderna inom var och en av de samordnade tjänsterna.

Indikatorerna mäter inte hur kostnadseffektiv den samordnade it-driften är i absoluta termer. De visar alltså inte om det vore möjligt att producera tjänster med samma innehåll, säkerhetsnivå och kvalitet ännu billigare än vad leverantörsmyndigheterna gör. De säger inte heller något om hur mycket billigare tjänsterna skulle gå att producera, om så vore fallet.

Indikatorerna mäter inte heller om och i så fall i vilken utsträckning som de anslutna myndigheterna överkonsumerar säkerhet. Med överkonsumtion menar vi i vilken utsträckning som de samordnade tjänsterna erbjuder en högre säkerhet än vad de anslutna myndigheterna egentligen behöver.

## 3.2 Inga tillräckliga data för indikatorer på it-kostnader och väntetid

Vår analys visar att det inte finns förutsättningar att ta fram indikatorer som speglar myndigheternas kostnader för it-drift före och efter de har anslutit sig till den samordnade it-driften. Det beror på att det inte finns några tillförlitliga data över myndigheternas kostnader för it-drift. Vi har även övervägt möjligheten att ta fram indikatorer som speglar leverantörsmyndigheternas kapacitet att ansluta nya myndigheter, i form av väntetiden för att få ansluta sig till den samordnade it-driften. Men vi bedömer att sådana indikatorer inte vore träffsäkra, eftersom väntetiden beror på många fler faktorer än leverantörsmyndigheterna kan påverka.

### 3.2.1 Det finns inte några data över it-kostnader före och efter anslutning till samordnad it-drift

Vi har utforskat möjligheten att använda data över myndigheternas it-kostnader före och efter de har anslutit sig till den samordnade it-driften som grund för indikatorer på effekterna av den samordnade it-driften när det gäller kostnads-effektivitet. Men vår kartläggning visar att det inte finns några tillförlitliga sådana data som går att lägga samman.

Det främsta skälet till det är att det inte finns några statliga inrapporteringskoder till statsredovisningssystemet Hermes, så kallade s-koder, som var för sig eller tillsammans gör det möjligt att följa myndigheternas kostnader för it-drift. S-koderna för köpta it-tjänster omfattar till exempel både drift och nyutveckling. Kostnaderna för it-drift i egen regi är fördelade på s-koderna för lön, lokaler, el, avskrivningar och liknande, där själva it-driften inte går att urskilja. Dessutom

tillämpar myndigheterna olika redovisningspraxis och olika definitioner av it-drift. Det innebär att kostnaderna som olika myndigheter redovisar för it-drift i praktiken omfattar olika saker. Vissa myndigheter inkluderar till exempel personalkostnader, medan andra myndigheter inte gör det.[28]

Företrädare för ESV bekräftar att uppgifterna i Hermes inte går att använda för att följa myndigheternas kostnader för it-drift över tid. Det är ett problem som Statskontoret, ESV och Digg lyfter fram i flera tidigare rapporter. Både ESV och Digg har också haft regeringsuppdrag som handlar om att följa och jämföra myndigheternas it-kostnader, utan att komma till rätta med problemen.[29]

Ett annat skäl är att de samordnade it-driftstjänsterna sannolikt skiljer sig från de anslutna myndigheternas tidigare it-driftslösningar. Ett sådant exempel är att de samordnade tjänsterna generellt erbjuder högre säkerhet än myndigheternas tidigare lösningar (se avsnitt 2.1.1 och 3.1.4). Därför skulle det inte vara rättvisande att jämföra myndigheternas it-driftskostnader före och efter att de har anslutit sig till den samordnade it-driften. En sådan indikator skulle i praktiken jämföra äpplen och päron.

### 3.2.2 Indikatorer på väntetid är inte tillräckligt träffsäkra

Vi har övervägt möjligheten att använda den genomsnittliga väntetiden för att ansluta sig till olika tjänster inom den samordnade it-driften som indikatorer på kostnadseffektivitet. Med väntetid menar vi tiden från att en myndighet anmäler intresse för en samordnad tjänst till att de ansluter sig till tjänsten. Syftet med sådana indikatorer skulle vara att spegla leverantörsmyndigheternas kapacitet att ansluta nya myndigheter. Det är relevant att följa eftersom det uppstår skalfördelar när fler myndigheter ansluter sig till den samordnade driften.

Det främsta skälet till att vi ändå har valt bort indikatorer som bygger på väntetid är att väntetiden bara delvis beror på faktorer som leverantörsmyndigheterna kan påverka. Det handlar till exempel om hur snabbt de intresserade myndigheterna kan fatta beslut samt hur komplex deras verksamhet är. Myndigheter med mer komplex verksamhet tar i regel längre tid att ansluta. Dessutom kan de intresserade myndigheternas förutsättningar ändras under tiden de väntar på att bli anslutna. Nya regelverk eller uppgifter kan leda till att en myndighet behöver omvärdera sin

---

[28] Ekonomistyrningsverket (2025:4). *Handledning. Baskontoplan för statliga myndigheter 2025*. s. 3; Ekonomistyrningsverket (2018:28*). Pilotprojekt om ramverk för it-kostnader (TBM)*. s. 19–21.

[29] Se till exempel Statskontoret (2025:2). *Gör jobbet! En mer effektiv användning av Arbetsförmedlingens förvaltningsmedel*. s. 125; Ekonomistyrningsverket (2018). *Pilotprojekt om ramverk för it-kostnader (TBM)*. s. 40; Myndigheten för digital förvaltning (2019*). Myndigheters strategiska it-projekt, it-kostnader och mognad*. s. 42.

intresseanmälan, eller få till en it-driftslösning snabbare än vad leverantörsmyndigheterna kan erbjuda. Därför speglar indikatorerna inte leverantörsmyndigheternas kapacitet särskilt väl.

Indikatorer för väntetid riskerar också att ge leverantörsmyndigheterna incitament att prioritera myndigheter som är enkla och snabba att ansluta framför myndigheter som tar längre tid att ansluta, trots att deras anslutning skulle bidra mer till att höja säkerheten på samhällsnivå. Beredskapsmyndigheterna är ett exempel på denna typ av myndigheter.

# 4 Förslag på indikatorer – kvalitet

I det här kapitlet redogör vi för våra förslag på indikatorer för att följa kvaliteten i den samordnade statliga it-driften och varför vi föreslår just dem. Som indikatorer för att följa kvalitet föreslår vi:

- Den procentuella skillnaden mellan den debiterade avgiften för ett år och året efter för var och en av de samordnade it-driftstjänsterna
- Den genomsnittliga andelen av den överenskomna öppettiden som de samordnade it-driftstjänsternas huvudsakliga funktionalitet är tillgänglig, för var och en av de tjänster som har en överenskommen öppettid.

## 4.1 Indikatorerna på kvalitet visar hur väl tjänsterna uppfyller myndigheternas behov

Vi bedömer att de indikatorerna som vi föreslår för att följa effekterna av den samordnade statliga it-driften när det gäller säkerhet indirekt speglar även kvaliteten i den samordnade driften. Det beror på att högre säkerhet är den huvudsakliga anledningen till att myndigheter ansluter sig till de samordnade tjänsterna. Men för att myndigheter ska ansluta sig till och fortsätta att vara anslutna till de samordnade tjänsterna behöver de också möta andra av myndigheternas behov än säkerhet. Våra förslag till indikatorer på kvalitet syftar till att spegla hur väl den samordnade it-driften möter några av dessa behov. Därmed skiljer sig indikatorerna på kvalitet från våra övriga indikatorer. Det beror på att de övriga indikatorerna syftar till att spegla *effekterna* av den samordnade driften när det gäller säkerheten och kostnads-effektiviteten i myndigheternas it-drift, inte säkerheten och kostnadseffektiviteten i sig. Indikatorerna för kvalitet mäter däremot aspekter av själva kvaliteten i tjänsterna, inte den effekt som de har på kvaliteten i de anslutna myndigheternas it-drift.

## 4.2 De samordnade tjänsternas prisstabilitet är en relevant indikator på kvalitet

Alla myndigheter har ett grundläggande behov av att kunna planera sin ekonomi. Det innebär att de behöver kunna förutse avgifterna för de samordnade tjänsterna, både för att vilja anslutna sig till och fortsätta att vara anslutna till dem. Vi bedömer därför att leverantörsmyndigheternas förmåga att hålla stabila priser för de it-drifts-tjänster som de tillhandahåller är en relevant indikator på kvaliteten i tjänsterna.

Leverantörsmyndigheterna strävar själva efter att enhetspriset för olika tjänster ska fluktuera så lite som möjligt mellan olika år, just för att underlätta för de anslutna myndigheterna att planera sin ekonomi.[30] Det är svårt för de anslutna myndigheterna att hantera stora höjningar av avgifterna från ett år till nästa. Det gäller särskilt små myndigheter. Det framgår av våra intervjuer med företrädare för de anslutna myndigheterna.

It-driftsförordningen anger att leverantörsmyndigheterna ska ta ut avgifter av myndigheterna som är anslutna till det samordnade statliga tjänsteutbudet. Leverantörsmyndigheterna får även bestämma avgifternas storlek och disponera avgiftsinkomsterna. Detta innebär att leverantörsmyndigheterna har fått ett särskilt bemyndigade att ta ut avgifter. Då gäller 5 § avgiftsförordningen (1992:191) och tillhörande föreskrifter (ESVFA 2022:5), som innebär att leverantörsmyndigheterna ska beräkna avgifterna så att de helt täcker verksamhetens kostnader på ett eller några års sikt. Enligt företrädare för ESV handlar det om en tidsperiod på cirka 1–3 år.

## 4.3 It-driftstjänsternas tillgänglighet är också en relevant indikator på kvalitet

Ett av de anslutna myndigheternas grundläggande behov är att komma åt och kunna använda de samordnade it-driftstjänsterna på det sätt och under de tider som de behöver. Vi bedömer därför att tjänsternas tillgänglighet under de tider som leverantörsmyndigheterna och de anslutna myndigheterna har kommit överens om är relevanta indikatorer på tjänsternas kvalitet. Leverantörsmyndigheterna och de anslutna myndigheterna kommer överens om vilka tider en viss tjänsts huvudsakliga funktionalitet ska vara tillgänglig i en så kallad Service Level Agreement (SLA). Leverantörsmyndigheterna följer också upp tillgängligheten för varje tjänst utifrån dessa överenskommelser.

Men alla tjänster i den samordnade it-driften har inte någon överenskommen öppettid som går att följa upp. Det handlar till exempel om tjänster för att återställa data. Sådana tjänsters tillgänglighet blir i praktiken bara testad i skarpt läge när en ansluten myndighet faktiskt behöver återställa sina data. Därför är indikatorn bara relevant för de it-driftstjänster där leverantörsmyndigheterna och de anslutna myndigheterna har kommit överens om öppettider.

Vi bedömer att tjänsternas tillgänglighet sannolikt kommer att vara mycket hög. Vi baserar det på att företrädare för både Försäkringskassan och Skatteverket beskriver att deras tjänster i regel har en tillgänglighet på över 99 procent. Leverantörsmyndigheterna behöver därför beskriva värdena på indikatorerna på ett sätt som är lätt för regeringen och anslutna myndigheter att tolka och följa över tid. En relativt liten minskning i tillgängligheten kan till exempel verka obetydlig, till exempel en

[30] Försäkringskassan 2025-06-05. *Ekonomi- och avgiftsmodell för samordnad och säker statlig it-drift*. FK2024/006706. s. 4.

skillnad på en tiondels procentenhet. Men i praktiken kan det ha stor påverkan på de anslutna myndigheternas verksamhet. Leverantörsmyndigheterna skulle till exempel kunna redovisa värdena på tillgänglighetsindikatorerna i förhållande till referensvärden.

## 4.4 Indikatorerna mäter inte den samordnade it-driftens effekter på kvalitet

Indikatorerna för kvalitet mäter hur väl de samordnade it-driftstjänsterna möter de anslutna myndigheternas behov och förväntningar när det gäller prisstabilitet och tillgänglighet. Ingen av indikatorerna mäter alltså vilka effekter den samordnade it-driften har på kvaliteten i myndigheternas it-drift, det vill säga hur mycket kvaliteten ökar när en myndighet ansluter sig till en viss tjänst. Prisstabilitet och tillgänglighet är dessutom bara två av många kvalitetsaspekter som kan vara viktiga för de anslutna myndigheterna.

Indikatorerna för prisstabilitet respektive tillgänglighet mäter inte heller hur en viss prisstabilitet eller tillgänglighet påverkar de anslutna myndigheternas it-drift eller verksamhet. Myndigheter med stora ekonomiska marginaler kan till exempel ha större möjligheter att hantera tvära kast i priset på de samordnade it-driftstjänsterna än vad myndigheter med en ansträngd ekonomi har. En driftsstörning som inträffar dagen före deadline för ett regeringsuppdrag kan i sin tur vara ett större kvalitetsproblem än en driftstörning som inträffar i mitten av juli när stora delar av statsförvaltningen har semester.

# 5 Förslag på indikatorer – balans mellan säkerhet, kostnadseffektivitet och kvalitet

I det här kapitlet redogör vi för våra förslag på indikatorer för att följa hur väl leverantörsmyndigheterna balanserar de anslutna myndigheternas behov av säkerhet, kostnadseffektivitet och kvalitet i den samordnade it-driften. Vi motiverar också våra förslag. Som indikatorer för att följa balansen mellan säkerhet, kostnadseffektivitet och kvalitet föreslår vi:

- De anslutna myndigheternas genomsnittliga kundnöjdhet (NKI) med var och en av de samordnade it-driftstjänsterna

## 5.1 NKI speglar balansen mellan säkerhet, kostnadseffektivitet och kvalitet

En av leverantörsmyndigheternas viktigaste uppgifter är att balansera säkerhet, kostnad och kvalitet i de samordnade tjänsterna, så att så många myndigheter som möjligt upplever att tjänsterna möter deras behov till ett godtagbart pris. Denna balans är viktig eftersom myndigheterna har olika och rörliga behov när det gäller såväl säkerhet som kvalitet i de olika it-driftstjänsterna. Därmed varierar det också hur mycket säkerhet och kvalitet som myndigheterna är villiga att betala för. Det är viktigt för leverantörsmyndigheterna att hantera detta eftersom den samordnade it-driftens positiva effekter på säkerheten och kostnadseffektiviteten i myndigheternas it-drift ökar ju fler myndigheter som är anslutna.

Vi föreslår att leverantörsmyndigheterna använder ett så kallat NKI (nöjd-kund-index) som indikator på hur nöjda de anslutna myndigheterna är med de olika tjänsterna de är anslutna till. Vi bedömer att sådana indikatorer speglar hur väl de anslutna myndigheterna upplever att leverantörsmyndigheterna balanserar säkerhet, kostnad och kvalitet, även om de har olika bild av vad som är en bra balans. NKI är en standardiserad och internationellt vedertagen metod för att mäta kundnöjdhet. Måttet bygger på kundernas svar på tre standardfrågor, som leverantören därefter väger samman till ett index. Frågorna är:

*Ange på en skala 1–10, där 1=inte alls nöjd och 10=mycket nöjd*

- Hur nöjd är din myndighet totalt sett med it-driftstjänsten ni är ansluten till?
- Hur väl uppfyller it-driftstjänsten som ni är ansluten till er myndighets förväntningar i sin helhet?
- Tänk dig en perfekt it-driftstjänst. Hur nära eller långt ifrån ett sådan ideal upplever du it-driftstjänsten som ni är anslutna till?

Indikatorerna som bygger på NKI speglar därmed de anslutna myndigheternas subjektiva upplevelse av kvaliteten i it-driftstjänsterna. På så sätt hanterar indikatorn både att myndigheterna har olika behov och krav på kvalitet, och att kraven sannolikt ökar över tid. Vi bedömer därför att de anslutna myndigheternas kundnöjdhet är ett relevant mått på hur väl de samordnade it-driftstjänsterna möter deras behov. Vi bedömer också att måttet är hållbart över tid.

Vårt förslag på indikatorer förutsätter att leverantörsmyndigheterna gemensamt genomför årliga kundundersökningar till samtliga myndigheter som är anslutna till en eller flera av de samordnade tjänsterna. Undersökningarna bör inkludera de tre standardfrågorna som ingår i en NKI-undersökning.

Försäkringskassan är i dag den enda av leverantörsmyndigheterna som genomför regelbundna kundundersökningar. Under åren som Försäkringskassan har tillhandahållit samordnade it-driftstjänster enligt det tidigare regeringsuppdraget fokuserade undersökningarna på hur de anslutna myndigheterna upplevde att samverkan med Försäkringskassan fungerade. Under 2025 har Försäkringskassan även börjat följa upp hur nöjda de anslutna myndigheterna är med de enskilda tjänsterna, och bland annat ställt de tre standardfrågorna i NKI. Men hittills har Försäkringskassan bara följt upp en av sina tjänster på det sättet. De övriga leverantörsmyndigheterna har inte genomfört några systematiska kund-undersökningar ännu.

Vi anser att leverantörsmyndigheterna bör genomföra NKI-undersökningarna samlat och gemensamt genom Nitis-kansliet. Ett skäl till det är att leverantörs-myndigheterna då kan ställa frågor om den samordnade it-driften som helhet till de myndigheter som är anslutna till flera olika tjänster. Ett annat skäl är att undersökningarna då blir mer samordnade och lätthanterade för de anslutna myndigheterna. De behöver till exempel bara ta emot undersökningar från en avsändare, vid en tidpunkt.

Företrädare för vissa av leverantörsmyndigheterna lyfter fram att de är tveksamma till den tredje och sista standardfrågan i NKI. De anser att det är svårt att veta vad den anslutna myndigheten lägger i begreppet ”perfekt it-driftstjänst” och vad de därmed jämför den samordnade it-driftstjänsten med. De anser också att de anslutna myndigheterna inte nödvändigtvis skulle vara villiga att betala för sin perfekta it-driftstjänst. Men vi bedömer att leverantörsmyndigheterna ändå bör ställa frågan, delvis just för att den ingår i den etablerade standarden för NKI-undersökningar. Att utesluta eller omformulera frågan skulle göra det svårare att jämföra resultaten från leverantörsmyndigheternas NKI-undersökningar med de från andra myndigheter eller privata aktörer. Ett annat skäl är att indikatorn i fråga enbart är tänkt att spegla kvalitet, inte kvalitet i förhållande till pris. Däremot kan leverantörsmyndigheterna med fördel använda tjänsternas pris för att förklara resultaten från NKI-undersökningarna och sätta dem i ett sammanhang.

Vi bedömer att det är tillräckligt att leverantörsmyndigheterna ställer de tre standardfrågorna. På så sätt styr vi inte leverantörsmyndigheternas kundundersökningar mer än nödvändigt. Vi ger också leverantörsmyndigheterna utrymme att följa upp andra aspekter av hur nöjda de anslutna myndigheterna är. Det kan då vara aspekter som de själva bedömer är relevanta för att utveckla den samordnade it-driften. Det kan till exempel handla om hur nöjda de anslutna myndigheterna är med leverantörsmyndigheternas support, eller lyhördhet för deras behov av ytterligare funktionalitet. De obligatoriska NKI-frågorna vi föreslår kommer därför att komplettera leverantörsmyndigheternas egen uppföljning och inte fungera som en fullständig kundundersökning.

### 5.1.1 NKI visar inte varför myndigheterna är nöjda eller missnöjda

Indikatorerna som bygger på NKI mäter hur de anslutna myndigheterna anser att leverantörsmyndigheterna balanserar säkerhet, kostnadseffektivitet och kvalitet i den samordnade it-driften. Indikatorerna mäter inte balansen mellan säkerhet, kostnadseffektivitet och kvalitet i objektiva eller absoluta termer. Tvärtom är det möjligt att de anslutna myndigheterna över tid blir mindre nöjda med de samordnade tjänsterna trots att tjänsterna blir ”bättre”. Det kan hända, om myndigheternas behov och förväntningar ökar snabbare än tjänsternas säkerhet, kostnadseffektivitet eller kvalitet.

Indikatorerna i fråga visar inte heller vilka aspekter av de samordnade it-driftstjänsterna som de anslutna myndigheterna är mer respektive mindre nöjda med. Därför behöver leverantörsmyndigheterna komplettera indikatorerna med mer detaljerade frågor eller andra underlag för att ta reda på vad som ligger bakom utvecklingen, till exempel om indikatorerna skulle visa en nedåtgående trend för en viss it-driftstjänst. Våra övriga förslag på indikatorer kompletterar NKI-indexet, eftersom de speglar faktorer som sannolikt påverkar de anslutna myndigheternas helhetsupplevelse av it-driftstjänsterna. Därmed kan värdena på de indikatorerna bidra till att förklara varför den generella kundnöjdheten utvecklas som den gör.

# 6 Uppföljningen av den samordnade it-driften kräver mer än indikatorer

I det här kapitlet redogör vi för våra förslag på hur regeringen och leverantörsmyndigheterna kan förstärka arbetet med att följa upp effekterna av den samordnade statliga it-driften för att komplettera indikatorerna och göra dem mer användbara. Vi föreslår att:

- leverantörsmyndigheterna kompletterar indikatorerna med en analys i sin årliga återrapport till regeringen
- regeringen beslutar om ett eller flera mål för leverantörsmyndigheternas arbete med den samordnade statliga it-driften
- regeringen genomför en årlig gemensam dialog med leverantörsmyndigheterna med fokus på den samordnade statliga it-driften, utöver den ordinarie myndighetsdialogen.

## 6.1 Leverantörsmyndigheternas återrapporter behöver fungera som beslutsunderlag

Indikatorerna som vi föreslår ger relevant information om effekterna av den samordnade it-driften, samt hur väl den möter de anslutna myndigheternas behov. Men de ger inte en fullständig bild. Därför bör regeringen använda indikatorerna försiktigt, och leverantörsmyndigheterna komplettera indikatorerna med en analys när de återrapporterar till regeringen. Det är nödvändigt för att regeringen ska kunna dra korrekta slutsatser utifrån och få ett användbart beslutsunderlag.

### 6.1.1 Indikatorer ger inte en fullständig bild av effekterna av den samordnade it-driften

Vi bedömer att våra förslag till indikatorer ger relevant information om effekterna av den samordnade it-driften på myndigheternas it-drift när det gäller säkerhet och kostnadseffektivitet. Indikatorerna ger också relevant information om den samordnade driftens kvalitet ur de anslutna myndigheternas perspektiv. Men indikatorerna ger inte en fullständig bild av effekterna av den samordnade it-driften. Det beror på att en indikator definitionsmässigt är något litet och mätbart som belyser något stort och svårfångat.

Det beror också på att myndigheternas syn på vad som utgör hög säkerhet och kvalitet när det gäller it-drift förändras löpande i takt med den tekniska utvecklingen och samhällets digitalisering. Därmed förändras också vilka tjänster som

leverantörsmyndigheterna ska tillhandahålla på ett kostnadseffektivt sätt. Den samordnade it-driften skjuter därför i praktiken mot ett rörligt mål.

### 6.1.2 Regeringen bör använda indikatorerna försiktigt

Vi bedömer att regeringen inte bör använda indikatorerna som vi föreslår för att jämföra värden för enskilda år rakt av mellan leverantörsmyndigheterna. Det beror bland annat på att leverantörsmyndigheterna tillhandahåller olika tjänster, har olika it-arkitektur och olika sätt att fördela sina kostnader.[31] Tjänsterna har i sin tur olika karaktär, kostnader och anslutna myndigheter. Dessutom ställer de anslutna myndigheterna olika krav, vilket ytterligare påverkar hur komplexa olika tjänster är för leverantörsmyndigheterna att tillhandahålla. Därför kan sådana enkla jämförelser leda till felaktiga slutsatser.

Vi anser att regeringen i stället bör fokusera på att följa utvecklingen över tid inom varje enskild leverantörsmyndighet. Över tid bör regeringen också kunna använda vissa av indikatorerna för att jämföra den långsiktiga utvecklingen mellan leverantörsmyndigheterna, till exempel när det gäller kostnadseffektivitet och kvalitet.

### 6.1.3 Leverantörsmyndigheterna behöver komplettera indikatorerna med en analys

Vi bedömer att leverantörsmyndigheterna behöver komplettera indikatorerna med en analys när de återrapporterar till regeringen. Det är nödvändigt för att regeringen ska kunna förstå vad indikatorerna visar och inte visar, samt för att kunna dra korrekta slutsatser av det. Det är också nödvändigt för att regeringen ska kunna förstå hur värdena på indikatorerna hänger ihop, både med varandra och med hur leverantörsmyndigheterna arbetar och prioriterar. Allt detta är i sin tur nödvändigt för att regeringen ska kunna justera hur de styr den samordnade it-driften om det behövs, samt formulera lämpliga åtgärder för att uppnå andra eller ytterligare effekter än de som leverantörsmyndigheterna återrapporterar.

I analysen behöver leverantörsmyndigheterna förklara värdena på indikatorerna och sätta dem i ett sammanhang. Där är nyckeltal som visar hur den samordnade it-driften ökar säkerheten i de anslutna myndigheternas it-drift ett viktigt verktyg (avsnitt 2.1.5). Detsamma gäller information om vilka faktorer som ligger bakom förändringar av de genomsnittliga kostnaderna per enhet, och jämförelser mellan kostnaderna för den samordnade it-driften och pris- och löneomräkningen (PLO) (avsnitt 3.1.3).

Leverantörsmyndigheterna behöver också redovisa hur de har balanserat säkerhet, kostnadseffektivitet och kvalitet i sitt arbete med den samordnade it-driften. Det handlar till exempel om att visa vilka myndigheter de har prioriterat att ansluta och

---

[31] Försäkringskassan 2025-06-05. *Ekonomi- och avgiftsmodell för samordnad och säker statlig it-drift*. FK2024/006706. s. 3.

vilka tjänster de har prioriterat att utveckla. Det handlar också om att analysera utvecklingen på de olika indikatorerna i relation till varandra. Om tjänsterna håller alltför hög kvalitet eller säkerhetsnivå kommer de att bli så dyra att få myndigheter kan eller vill betala för dem. Men om tjänsterna håller alltför låg kvalitet eller säkerhetsnivå kommer de bara att uppfylla enstaka myndigheters krav, även om de är billiga. Därför behöver leverantörsmyndigheterna hitta en balans mellan säkerhet, kvalitet och kostnad som gör att så många myndigheter som möjligt vill vara anslutna till den samordnade it-driften. Ju fler myndigheter som är anslutna, desto större blir effekterna på säkerhet och kostnadseffektivitet i myndigheternas it-drift (se avsnitt 2.1.1 och 3.1.1).

Sist men inte minst behöver Försäkringskassan och de övriga leverantörsmyndigheterna bedöma vilken information som är säkerhetskänslig. Då ska de också vid behov säkerhetsskyddsklassa den och redovisa de berörda indikatorerna, informationsmängderna och analyserna till regeringen i särskild ordning. Det beror på att viss information sannolikt går att utnyttja för att skada den samordnade it-driften.

## 6.2 Regeringen bör stärka strukturen för att följa upp den samordnade it-driftens effekter

Vi föreslår att regeringen stärker sina strukturer för att följa upp och vid behov styra den samordnade it-driftens effekter. Dels genom att besluta om ett eller flera mål för leverantörsmyndigheternas arbete med den samordnade it-driften, dels genom att föra gemensamma strukturerade dialoger med leverantörsmyndigheterna. Regeringen bör även bevaka att leverantörsmyndigheterna får tillgång till det stöd de behöver från expertmyndigheterna inom säkerhetsområdet, för att tillhandahålla och vidareutveckla den samordnade it-driften.

### 6.2.1 Regeringen bör besluta om ett eller flera mål för leverantörsmyndigheternas arbete

Vi föreslår att regeringen beslutar om ett eller flera mål för leverantörsmyndigheternas arbete med den samordnade statliga it-driften. Vi bedömer att regeringen på det sättet kan underlätta både leverantörsmyndigheternas arbete med att tillhandahålla och vidareutveckla den samordnade statliga it-driften, och deras arbete med att följa upp effekterna av driften. Ett eller ett par sådana mål skulle ge leverantörsmyndigheterna en ännu tydligare inriktning än vad som framgår av it-driftsförordningen. Det bör i sin tur underlätta för leverantörsmyndigheterna att välja vilka tjänster och myndigheter de ska prioritera. Det bör också minska risken för tidsödande låsningar mellan leverantörsmyndigheterna när det gäller sådana vägval. Målen skulle också göra regeringens ambitionsnivå för den samordnade statliga it-driften tydligare för leverantörsmyndigheterna, och därmed hjälpa dem att bedöma och motivera hur mycket resurser arbetet kräver. Sist men inte minst skulle mål för leverantörsmyndigheternas arbete hjälpa regeringen att värdera

effekterna av den samordnade it-driften, eftersom mål skulle ge regeringen något att ställa värdena på indikatorerna mot.

Vi bedömer att det bör vara upp till regeringen att formulera det eller de exakta målen för leverantörsmyndigheternas arbete med den samordnade it-driften. Regeringen bör göra det i dialog med leverantörsmyndigheterna, med utgångspunkt i deras återrapport i mars 2026. Men vi har några medskick, både utifrån vår analys inom ramen för det här uppdraget och Statskontorets samlade erfarenhet. Vi bedömer att målen bör:

- vara konkreta och mätbara, så att det är tydligt för leverantörsmyndigheterna vad de ska uppnå och enkelt för både dem och regeringen att använda målen för att styra verksamheten
- hänga ihop med våra förslag på indikatorer, så att en eller flera av indikatorerna går att använda för att följa progressionen mot målen
- hänga ihop med den samordnade it-driftens syfte så som det framgår av it-driftsförordningen, det vill säga högre säkerhet och kostnadseffektivitet, så att de olika delarna i styrningen hänger ihop och förstärker varandra
- gälla för leverantörsmyndigheterna som kollektiv, så att de även i fortsättningen kan fördela arbetet mellan sig på ett effektivt sätt utifrån sina styrkor och förutsättningar
- vara tidsatt och långsiktigt, så att leverantörsmyndigheterna får tid att utveckla och genomföra sitt arbete för att nå målen.

Vi anser att det är särskilt viktig att målen hänger ihop med den samordnade it-driftens syfte. Ett mål som fokuserar enbart på antalet anslutna myndigheter eller liknande skulle till exempel ge leverantörsmyndigheterna incitament att prioritera att ansluta små myndigheter till standardiserade tjänster. Det följer av att det generellt går fortare än att ansluta stora beredskapsmyndigheter till tjänster för att säkra data. Men att prioritera beredskapsmyndigheterna skulle sannolikt bidra mer till högre säkerhet, även om antalet anslutna myndigheter inte skulle öka lika snabbt.

### 6.2.2 Regeringen bör föra gemensamma strukturerade dialoger med leverantörsmyndigheterna

Vi föreslår vidare att regeringen genomför en årlig gemensam dialog med samtliga leverantörsmyndigheter. Dialogen bör vara skild från de enskilda och ordinarie myndighetsdialogerna, men strukturerad på så sätt att regeringen bör genomföra den årligen enligt ett fast format. Mer specifikt bör dialogen inkludera leverantörs-myndigheternas generaldirektörer, myndigheternas respektive huvudmän vid Regeringskansliet och ansvariga statsråd eller statssekreterare. Dialogen bör även inkludera det statsråd eller den statssekreterare som är ansvarig för totalförsvars-frågorna. Det följer av att it-driftsförordningen anger att leverantörsmyndigheterna

ska ta hänsyn till totalförsvarets behov när de utformar it-driftstjänsterna i det samordnade utbudet. Dialogen bör utgå från leverantörsmyndigheternas årliga återrapport till regeringen enligt it-driftsförordningen.

Vi bedömer att en gemensam dialog är viktig av flera skäl. Det främsta skälet är att den samordnade it-driften är en helhet och inte tre separata delar hos var och en av leverantörsmyndigheterna. Regeringen ställer genom it-driftsförordningen höga krav på leverantörsmyndigheterna att samarbeta och nå konsensusbeslut kring en verksamhet som rör stora och långsiktiga investeringar. Leverantörsmyndigheterna har också börjat agera koordinerat när det gäller den samordnade it-driften, till exempel genom att äska medel för olika delar av driften i sina respektive budgetunderlag.[32] Vi anser att regeringen behöver möta leverantörsmyndigheterna i detta och styra den samordnade it-driften som en helhet även i den löpande myndighetsstyrningen och inte bara i förordningen.

En gemensam dialog är också viktig är för att leverantörsmyndigheterna ligger under olika departement och statsråd. Därför riskerar de att genom informella kontakter få olika signaler om hur de ska prioritera arbetet med den samordnade it-driften i förhållande till sina övriga uppgifter. Historiskt sett har regeringen också styrt leverantörsmyndigheterna på olika sätt. Regeringen har till exempel ofta gett Försäkringskassan många uppdrag i regleringsbrevet, medan Skatteverket sällan har fått sådana uppdrag.[33] Sammantaget riskerar det att försvåra leverantörs-myndigheternas samarbete. Men en gemensam dialog kan överbrygga skillnaderna i hur regeringen styr de olika myndigheterna och minska risken för att de får olika signaler om hur de ska prioritera den samordnade it-driften. Regeringen kan även inkludera företrädare för andra departement, till exempel Justitiedepartementet, vid de gemensamma dialogerna för att ytterligare förstärka helhetsperspektivet i den löpande styrningen av den samordnade it-driften.

Ytterligare ett skäl till en gemensam dialog om den samordnade it-driften är att samtliga leverantörsmyndigheter har en omfattande och samhällsviktig verksamhet utöver den samordnade driften. Därför bedömer vi att den samordnade it-driften sannolikt kommer att få ganska litet utrymme under den ordinarie myndighets-dialogen, om något. Samtidigt är den samordnade driften som helhet alltför samhällsviktig och omsätter alltför mycket pengar för att inte omfattas alls av någon strukturerad dialog.

---

[32] Försäkringskassan (2025). *Budgetunderlag 2026–2028*. s. 9; Skatteverket (2025). *Skatteverkets budgetunderlag 2026–2028*. s. 30f; Trafikverket (2025). *Trafikverkets budgetunderlag 2026–2028*. s, 25f.

[33] Se t.ex. *Regleringsbrev för budgetåret 2023 avseende Försäkringskassan* samt *Regleringsbrev för budgetåret 2023 avseende Skatteverket.*

### 6.2.3 Regeringen bör bevaka leverantörsmyndigheternas tillgång till stöd från expertmyndigheter

Vi anser att regeringen bör bevaka att leverantörsmyndigheterna får tillgång till det stöd de behöver från expertmyndigheterna inom säkerhetsområdet för att tillhandahålla och vidareutveckla den samordnade it-driften. Det handlar i första hand om stöd från Säpo och FRA (se avsnitt 2.1.4). För FRA handlar det både om att stödja leverantörsmyndigheterna med specifika cybersäkerhetstjänster som penetrationstester och att ge råd och stöd genom Nationellt cybersäkerhetscenter (NCSC). Men i framtiden skulle det även kunna handla om stöd från till exempel Försvarets materielverk och Post- och telestyrelsen när det gäller teknisk utrustning och infrastruktur.

Vi bedömer att arbetet med att stödja leverantörsmyndigheterna ryms inom expertmyndigheternas instruktion. För Säpo handlar det om § 6–7 i myndighetens instruktion. Den anger bland annat att myndigheten får ge tekniskt stöd inom säkerhetsskydd. Säpo får också efter medgivande av regeringen bedriva uppdragsverksamhet när det gäller säkerhetsskydd och annat säkerhetsarbete. För FRA handlar det om § 4 i myndighetens instruktion (2007:937). Den anger bland annat att myndigheten får bistå andra myndigheter som hanterar säkerhetskänslig information med cybersäkerhetstjänster. Vi bedömer att den samordnade it-driften bör uppfylla det kriteriet, på grund av att den totala mängden information i de gemensamma systemen. Nationellt cybersäkerhetscenter är en del av FRA, men har en egen instruktion. Enligt § 3 i instruktionen ska centret bland annat lämna råd och stöd till offentliga aktörer i frågor om hot, sårbarheter och risker som rör cybersäkerhet.

Men företrädare för FRA uppger att de behöver prioritera mellan olika förfrågningar om stöd för att deras resurser ska räcka till. De prioriterar då utifrån en samlad bild av hot, skyddsvärde samt eventuella indikationer på allvarliga sårbarheter. Företrädare för Säpo behöver också prioritera sina insatser, och beskriver att de då prioriterar utifrån bland annat skyddsvärde, resultaten från tidigare tillsyn och information om säkerhetshotande händelser inom en viss verksamhet. Därmed finns det inte någon garanti för att vare sig FRA eller Säpo kan eller kommer att prioritera att bistå leverantörsmyndigheterna, enligt företrädare för respektive myndighet.

# 7 Myndigheternas organisering av sin it-drift som helhet

I det här kapitlet redovisar vi vår övergripande kartläggning av hur myndigheterna har organiserat sin it-drift som helhet. Vi föreslår också vilken aktör som är lämplig för att följa upp kartläggningen framöver. Vi anser att Försäkringskassan är den mest lämpliga aktören om regeringen vill använda kartläggningen för att utveckla den samordnade statliga it-driften. Om regeringen däremot vill använda kartläggningen som kunskapsunderlag om förvaltningens digitalisering anser vi att Digg är den mest lämpliga aktören.

## 7.1 Vi har kartlagt hur myndigheterna har organiserat sin it-drift

Vår analys visar att det inte går att använda befintliga data för att följa hur den statliga it-driften är organiserad som helhet. Därför har vi genomfört en egen övergripande enkätundersökning för att kartlägga hur myndigheterna organiserar sin it-drift, och jämfört våra resultat med resultaten från tidigare undersökningar när det har varit möjligt.

### 7.1.1 Befintliga data ger inte en tillräcklig bild av hur myndigheterna har organiserat sin it-drift

Vi har inventerat befintliga datakällor som ger någon form av information om myndigheternas it-drift. Det inkluderar data över avrop från Kammarkollegiets ramavtal för it-drift, ESV:s data över myndigheternas utgifter i statsredovisningssystemet Hermes, Statens servicecenters data över myndigheternas e-handel, samt MSB:s data över myndigheternas digitala leveranskedjor. Men dessa datakällor ger varken en fullständig eller tillförlitlig bild av hur myndigheterna organiserar sin it-drift, särskilt när det gäller drift i egen regi. I bilaga 3 beskriver vi mer ingående vad de olika datakällorna visar och inte visar.

### 7.1.2 Vi har genomfört en enkätundersökning till 215 myndigheter

I brist på befintliga data har vi genomfört en egen enkätundersökning till myndigheterna för att kartlägga hur de har organiserat sin it-drift. Vi har valt att hålla enkäten kort och övergripande för att göra det lättare för myndigheterna att svara. Vi har inte heller haft förutsättningar att samla in mer detaljerad och potentiellt säkerhetskänslig information på ett säkert sätt. Enkäten finns i bilaga 4.

Vi skickade vår enkät till de 215 myndigheterna i den statliga redovisningsorganisationen, för att använda samma population som It-driftsutredningen gjorde och därmed göra våra resultat så jämförbara med deras som möjligt. 199 av de 215 myndigheterna besvarade enkäten i sin helhet, vilket motsvarar en svarsfrekvens på 93 procent. Om vi tar hänsyn till myndigheternas storlek representerar myndigheterna som svarade 95 procent av årsarbetskrafterna i staten som helhet. Vi bedömer därför att våra resultat ger en tillförlitlig bild av hur myndigheterna i redovisningsorganisationen organiserar sin it-drift.

Vi redovisar våra resultat utifrån myndigheternas storlek mätt i antalet årsarbetskrafter, och i de flesta fall även utifrån om myndigheterna var beredskapsmyndigheter eller inte den 1 januari 2025. Vi har däremot gjort ett undantag för små myndigheter med färre än 100 årsarbetskrafter, eftersom det bara finns en beredskapsmyndighet i den kategorin (tabell 1). Om det är färre än fem myndigheter som har besvarat en fråga på ett visst sätt redovisar vi antalet som 2,5 i stället för att redovisa det verkliga antalet mellan 1–4. Vi gör så för att kunna redovisa resultaten för samtliga frågor utifrån samma kategorier, utan att riskera att det går att identifiera enskilda myndigheter.

De myndigheter som inte har svarat på enkäten har olika storlek och status som beredskapsmyndighet, samt tillhör olika sektorer. Men på en övergripande nivå är myndigheter inom säkerhetsområdet samt myndigheter under riksdagen överrepresenterade bland de som inte har svarat på enkäten. Därför är våra resultat inte lika tillförlitliga för dessa typer av myndigheter som för myndigheterna i den statliga redovisningsorganisationen i stort.

**Tabell 1.** **Hur vi kategoriserar myndigheterna och redovisar våra resultat.**

| Myndighetskategori | Antal anställda | Antal svarande | Svarsfrekvens |
|---|---|---|---|
| Små | 0–99 | 58 | 88 % |
| Mellan – Beredskap | 100–999 | 39 | 100 % |
| Mellan – Ej beredskap | 100–999 | 62 | 93 % |
| Stora – Beredskap | 1 000+ | 18 | 95 % |
| Stora – Ej beredskap | 1 000+ | 22 | 92 % |
| **Totalsumma** | - | **199** | **93 %** |

Not: Myndigheter som Försvarsmakten, FRA och Säpo är inte beredskapsmyndigheter enligt förordning 2022:524, även om de är viktiga för Sveriges beredskap. De ingår därför i kategorierna ”Ej beredskap” i tabellen.

### 7.1.3 Vi har jämfört våra resultat med resultaten från tidigare undersökningar

Vi har så långt det har varit möjligt jämfört resultaten från vår enkätundersökning med resultaten från tidigare undersökningar av hur myndigheterna organiserar sin it-drift. De flesta av dessa tidigare undersökningar har fokuserat på specifika aspekter av myndigheternas it-drift. Ett sådant exempel är en enkätundersökning från Statens servicecenter 2017, där myndigheterna under regeringen fick svara på om de sköter sin it-drift i egen regi med egna datacenter, eller om de har utkontrakterad

drift.[34] Ett annat exempel är MSB:s cybersäkerhetskoll från 2024, där de frågade myndigheterna om de hade utkontrakterat lite, en del, en betydande del eller det mesta av sin it-drift. Men MSB konstaterar själva att deras fråga gick att tolka på olika sätt. Dessutom fanns det inga svarsalternativ för myndigheter som antingen inte hade någon utkontrakterad drift alls, eller som hade utkontrakterat hela sin drift.[35] I år kartlägger MSB bland annat myndigheternas it-drift i egen respektive utkontrakterad regi inom ramen för Cybersäkerhetskollen. Men få myndigheter har besvarat de frågorna, vilket gör det svårt för oss att använda resultaten.

Den senaste mer fullständiga undersökningen av hur myndigheterna organiserar sin it-drift är från 2020. Då genomförde It-driftsutredningen en undersökning där myndigheterna i den statliga redovisningsorganisationen bland annat fick svara på om de hade egna datacenter, använde molntjänster och/eller samordnade sin it-drift med en annan myndighet. It-driftsutredningens enkät hade en svarsfrekvens på 88 procent.[36] Vi har försökt att efterlikna It-driftsutredningens undersökning när det gäller vilka som har fått enkäten och vilka frågor som vi ställer. Men vissa av It-driftsutredningens frågor var svåra för myndigheterna att tolka och besvara på ett enhetligt sätt, vilket gör deras resultat mindre tillförlitliga.[37] Därför har vi försökt att förtydliga sådana frågor i vår enkät, även om det gör våra resultat mindre jämförbara med utredningens. Vi bedömer också att vissa av frågorna i tidigare undersökningar inte längre är lämpliga att ställa utifrån det nuvarande säkerhetsläget. Det handlar till exempel om frågor om hur många datacenter som olika myndigheter har och var de ligger. I princip samtliga myndighetsföreträdare som vi har talat med uppger att de inte skulle besvara sådana frågor i dag.

## 7.2 Stora skillnader mellan hur små och stora myndigheter organiserar sin it-drift

Våra enkätresultat visar att myndigheterna genomför en majoritet av sin it-drift i egen regi. Det gäller särskilt beredskapsmyndigheter och myndigheter med många årsarbetskrafter. Samtidigt visar våra resultat att förekomsten av samordnad it-drift har ökat över tid, och att de flesta myndigheter kombinerar åtminstone två olika driftsformer.

---

[34] Statens servicecenter (2017). *En gemensam statlig molntjänst för myndigheternas it-drift*. s. 25f.

[35] Myndigheten för samhällsskydd och beredskap (2025). *Resultatredovisning av Cybersäkerhetskollen 2024*. s. 127f.

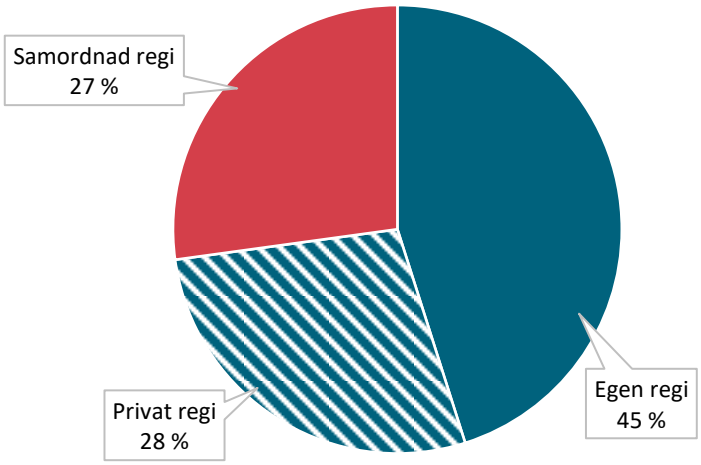
[36] SOU 2021:1. *Säker och kostnadseffektiv it-drift.* s. 82–91.

[37] SOU 2021:1. *Säker och kostnadseffektiv it-drift.* s. 88.

### 7.2.1 Myndigheterna genomför en majoritet av sin it-drift i egen regi

Våra resultat visar att myndigheterna genomför en majoritet av sin it-drift i egen regi. De svarande myndigheterna uppskattade att de lägger knappt hälften av sina kostnader för it-drift på drift i egen regi, en dryg fjärdedel på drift i privat regi och en dryg fjärdedel på samordnad drift (figur 1).

**Figur 1.** **Myndigheternas uppskattade kostnader för it-drift fördelade på egen, privat respektive samordnad regi.**



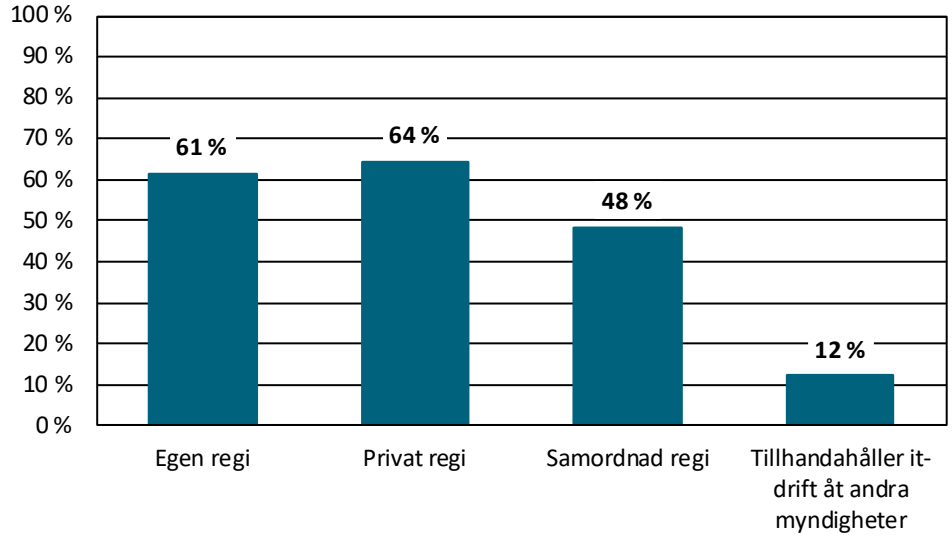

Källa: Statskontorets enkätundersökning 2025.

Egen regi definierar vi som it-drift i egna lokaler där myndigheten äger utrustningen och använder egen anställd personal eller konsulter som de arbetsleder på plats. Privat regi definierar vi som it-drift som myndigheten genom offentlig upphandling eller på något annat sätt uppdrar åt en privat leverantör att hantera. Samordnad regi definierar vi som it-drift som myndigheten låter en annan myndighet hantera åt dem. Det handlar om leverantörsmyndigheterna inom den samordnade statliga it-driften, Men också om myndigheter som tillhandahåller it-driftstjänster åt universitet och högskolor eller länsstyrelser, samt om myndigheter som är samlokaliserade värdmyndighet för nämndmyndigheter och liknande.

### 7.2.2 Förekomsten av samordnad it-drift har ökat över tid

Våra enkätresultat visar att drygt 60 procent av de svarande myndigheterna har it-drift i egen respektive privat regi i någon omfattning. En något mindre andel, 48 procent, uppger att de har samordnad it-drift i någon omfattning (figur 2).

**Figur 2.** **Andel av myndigheterna som har it-drift i egen, privat respektive samordnad regi samt tillhandahåller samordnad it-drift åt andra myndigheter.**




Källa: Statskontorets enkätundersökning 2025.

Våra resultat är inte fullt jämförbara med resultaten från tidigare undersökningar, men de tyder på att det har blivit vanligare med både privat och samordnad regi över tid. I Statens servicecenters undersökning från 2017 uppgav 40 av 166 svarande myndigheter att de har lagt ut sin it-drift på en privat aktör, vilket motsvarar 24 procent. 18 av de svarande myndigheterna uppgav att de har lagt ut driften på andra statliga myndigheter, vilket motsvarar 11 procent. I It-driftsutredningens undersökning svarade 36 av 158 myndigheter att en annan myndighet hanterar deras it-drift, det vill säga drygt 23 procent. Den undersökningen innehåller ingen motsvarande fråga om drift i privat regi.

Det är 24 av de 199 svarande myndigheterna i vår undersökning som uppger att de hanterar hela eller delar av en annan myndighets it-drift, vilket motsvarar 12 procent. I It-driftsutredningens enkät uppgav 14 av 158 svarande myndigheter att de tillhandahåller it-drift till annan myndighet, vilket motsvarade 9 procent.[38] Vår undersökning tyder alltså på att både antalet och andelen myndigheter som tillhandahåller it-drift åt andra myndigheter har ökat något sedan 2020.

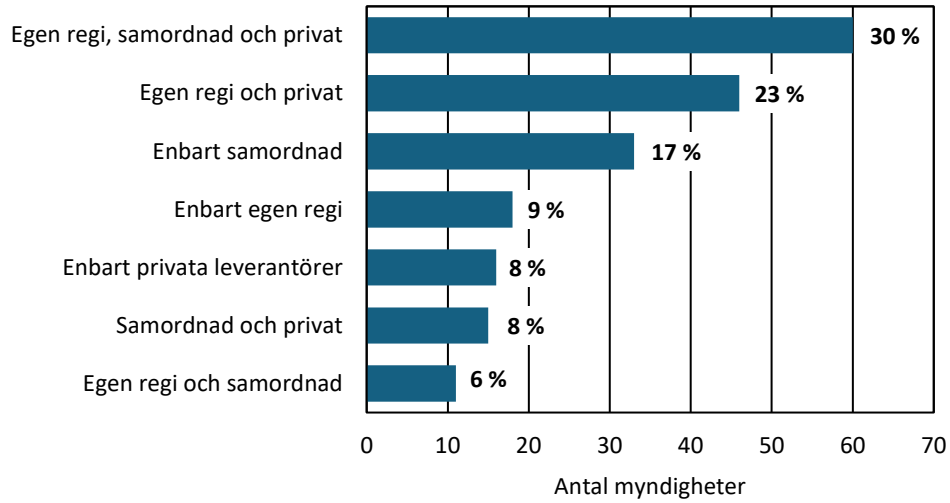
### 7.2.3 De flesta av myndigheterna kombinerar olika driftsformer

Även om myndigheterna genomför en majoritet av sin it-drift i egen regi är det bara nio procent av myndigheterna som har hela sin it-drift i egen regi (figur 3). De flesta av myndigheterna kombinerar minst två driftsformer, men ofta alla tre. 30 procent av de svarande myndigheterna uppger att de har it-drift i såväl egen som

[38] SOU 2021:1. *Säker och kostnadseffektiv it-drift*. s. 89.

privat och samordnad regi, medan 23 procent uppger att de kombinerar it-drift i egen och privat regi. Bland de myndigheter som bara har en driftsform är samordnad it-drift den vanligaste formen. 17 procent av myndigheterna uppger att de enbart har samordnad it-drift. I denna grupp finns de flesta av länsstyrelserna och de små myndigheter som har en värdmyndighet. Figur B2–B4 i bilaga 4 innehåller en mer detaljerad analys av hur myndigheterna kombinerar driftsformer.

**Figur 3.** **Antal och andel av myndigheterna som har it-drift i egen, privat respektive samordnad regi.**




Källa: Statskontorets enkätundersökning 2025.

Not: Figur är baserad på fråga 9.

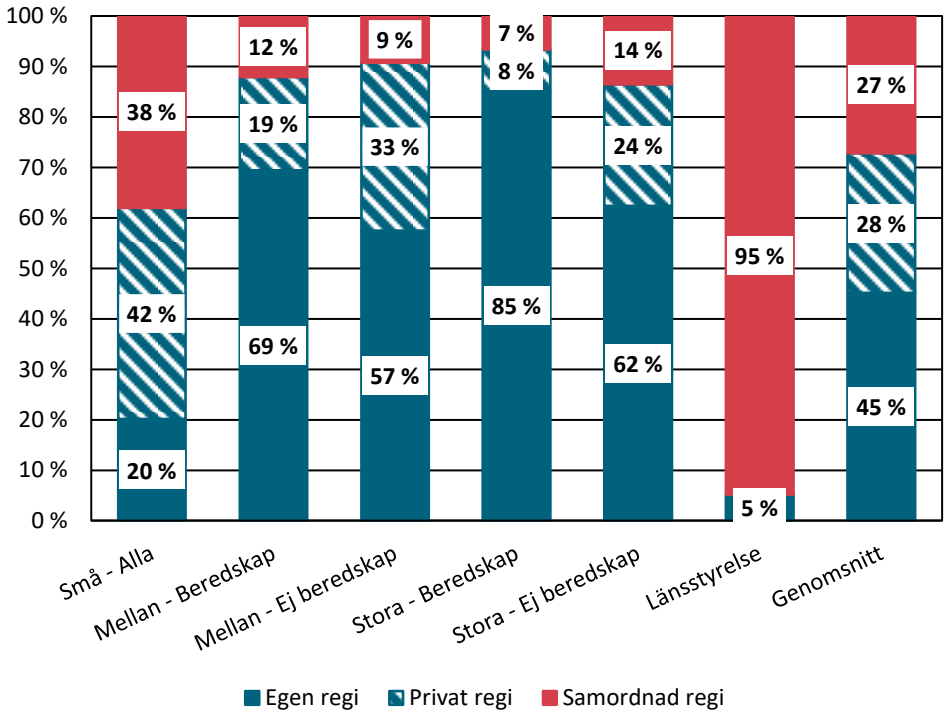
Våra samtal med företrädare för olika myndigheter både utanför och inom den samordnade statliga it-driften visar att myndigheterna har flera och delvis olika skäl för att kombinera olika driftsformer. I vissa fall handlar det om att öka redundansen i myndighetens it-drift, genom att använda flera olika leverantörer. I andra fall handlar det om att få tillgång till en viss funktionalitet, som myndigheten inte har råd att upprätthålla på egen hand eller som bara enstaka leverantörer tillhandahåller. Det kan också handla om andra säkerhetsaspekter än redundans, till exempel möjligheten att ha full rådighet över känsliga system och data.

### 7.2.4 Stora myndigheter och beredskapsmyndigheter har mest it-drift i egen regi

Vår analys visar att myndigheterna organiserar sin it-drift på olika sätt utifrån storlek och status som beredskapsmyndighet. Myndigheter med fler årsarbetskrafter har oftare en större andel av sin it-drift i egen regi. Dessutom har beredskapsmyndigheterna oftare en större andel av sin it-drift i egen regi. Det framkommer när vi gör en enkel regressionsanalys för att undersöka vilka faktorer som påverkar i vilken utsträckning som myndigheterna har it-drift i egen regi.

Analysen visar att både storlek och status som beredskapsmyndighet har ett positivt samband med andelen drift i egen regi, oberoende av varandra (tabell B2 och figur B5 i bilaga 4). Stora beredskapsmyndigheter har i genomsnitt 85 procent av sin it-drift i egen regi medan små myndigheter i genomsnitt har 20 procent av sin drift i egen regi (figur 4). Det motsatta mönstret gäller för it-drift i privat regi. Bilaga 4 innehåller resultaten från regressionsanalysen i sin helhet, samt en analys av myndigheternas driftsformer utifrån verksamhetsområde (cofog).

**Figur 4.** **Myndigheternas uppskattade kostnader för it-drift fördelade på egen, privat respektive samordnad regi.**



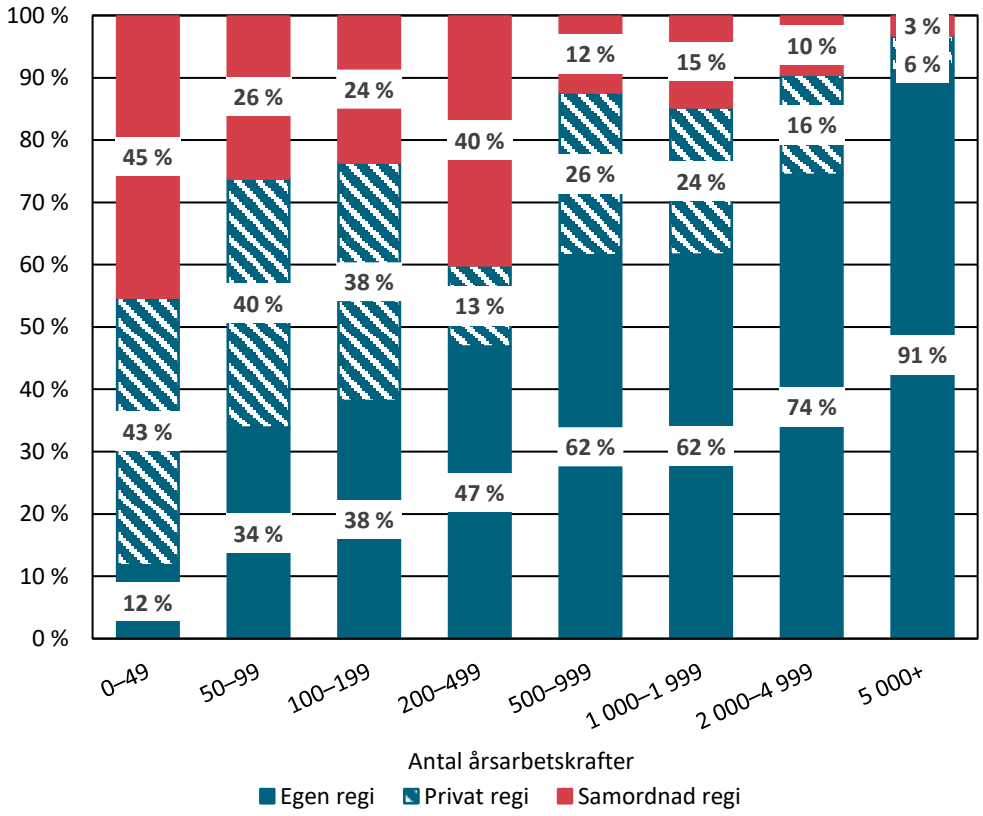

Källa: Statskontorets enkätundersökning 2025.

Not: Vi särredovisar länsstyrelserna eftersom deras svar skiljer sig från övrigas i kategorin Mellan – beredskap, och påverkar resultaten i den kategorin för mycket om vi redovisar dem samlat.

Mönstren blir ännu tydligare när vi bryter ner myndigheterna i mindre storleks-kategorier utifrån antalet årsarbetskrafter. Då framgår att myndigheter med 0–49 års-arbetskrafter i genomsnitt har 12 procent av sin it-drift i egen regi. Motsvarande andel för myndigheter med fler än 5 000 årsarbetskrafter är 91 procent (figur 5). Undersökningarna från Statens servicecenter och It-driftsutredningen visade också att egen regi var vanligare bland stora myndigheter.[39]

[39] SOU 2021:1. *Säker och kostnadseffektiv it-drift*. s. 84; Statens servicecenter (2017). *En gemensam statlig molntjänst för myndigheternas it-drift*. s. 27.

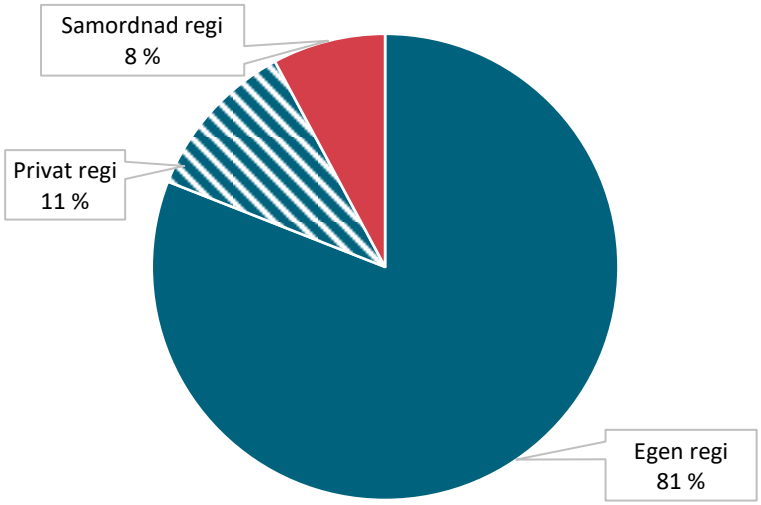
**Figur 5.** **Myndigheternas uppskattade kostnader för it-drift fördelade på egen, privat respektive samordnad regi, utifrån antal årsarbetskrafter.**




Källa: Statskontorets enkätundersökning 2025.

När vi viktar myndigheternas uppskattningar av sina kostnader för it-drift i olika former utifrån antalet årsarbetskrafter blir resultatet att egen regi står för 81 procent av myndigheternas kostnader för it-drift, privat regi för 11 procent och samordnad regi för 8 procent (figur 6, jämför med figur 1). Vi bedömer att resultaten åtminstone delvis speglar att Försäkringskassan initialt fokuserade på att tillhandahålla samordnade it-driftstjänster till små myndigheter. Flera av tjänsterna som de nuvarande leverantörsmyndigheterna har utvecklat med beredskapsmyndigheterna i åtanke är så nya att de inte går att ansluta sig till ännu.

**Figur 6.** **Myndigheternas uppskattade kostnader för it-drift fördelade på egen, privat respektive samordnad regi, viktade utifrån antalet årsarbetskrafter.**




Källa: Statskontorets enkätundersökning 2025.

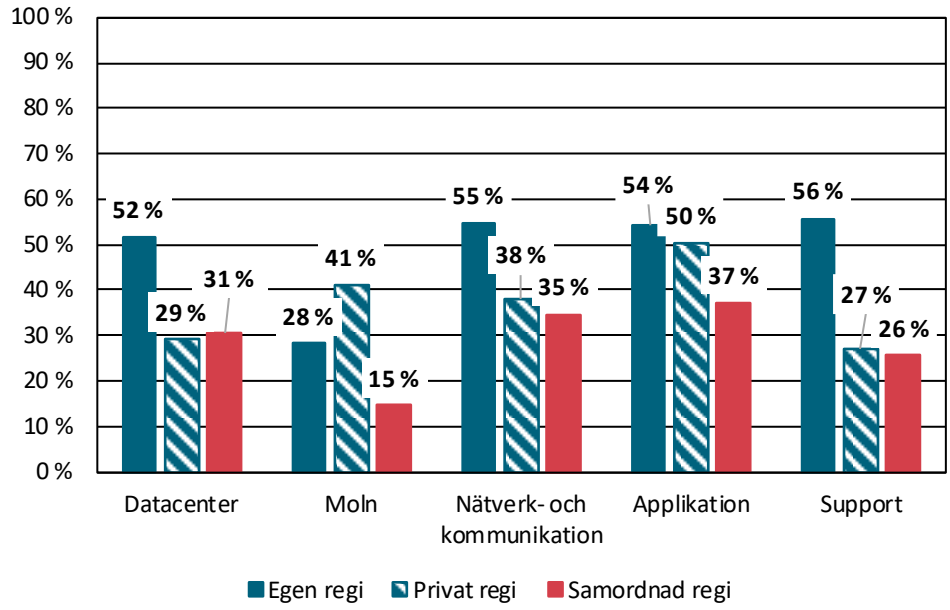
## 7.3 Myndigheterna använder olika driftsformer för olika typer av tjänster

Våra enkätresultat visar att myndigheterna använder olika driftsformer för olika typer av it-driftstjänster. När det gäller datacentertjänster, applikationstjänster, nätverks- och kommunikationstjänster samt supporttjänster är egen regi den vanligaste driftsformen. Men när det gäller molntjänster är privat regi är den vanligaste driftsformen. Samtidigt har andelen av myndigheterna som använder molntjänster i privat regi minskat över tid. Det ser vi när vi jämför våra enkätresultat med resultaten från tidigare undersökningar.

### 7.3.1 Myndigheter med datacenter i egen regi har även andra tjänster i egen regi

Våra enkätresultat visar att egen regi är den vanligaste driftsformen för alla typer av tjänster som vi har frågat myndigheterna om utom molntjänster. Det gäller alltså datacentertjänster, nätverks- och kommunikationstjänster, applikationstjänster samt supporttjänster. Drygt 50 procent av de svarande myndigheterna uppger att de har dessa typer av tjänster i egen regi i någon omfattning (figur 7). Vår analys visar vidare att det i hög utsträckning är samma myndigheter som har samtliga dessa typer av tjänster i egen regi. Myndigheter som har datacenter i egen regi har i cirka 90 procent av fallen även minst någon nätverks- och kommunikationstjänst, applikationstjänst och supporttjänst i egen regi.

**Figur 7.** **Andel av myndigheterna som har olika typer av it-driftstjänster i egen, privat respektive samordnad regi.**




Källa: Statskontorets enkätundersökning 2025.

Våra resultat visar att förekomsten av datacentertjänster i egen regi har minskat över tid. I Statens servicecenters undersökning från 2017 uppgav 111 av 166 myndigheter att de har egna datacenter, vilket motsvarar 67 procent.[40] I It-driftsutredningens undersökning från 2020 var motsvarande siffra 100 av 158 myndigheter, det vill säga 63 procent.[41] I vår undersökning uppger 52 procent av de svarande myndigheterna att de har datacentertjänster i egen regi. Men vi behöver vara försiktiga när vi jämför resultaten, eftersom frågorna är formulerade på olika sätt. SSC och It-driftsutredningen frågade till exempel specifikt om datacenter, medan vi frågade om datacentertjänster. De tidigare undersökningarna fokuserade också på datacenter när det gäller drift i egen regi, medan vi frågade myndigheterna även om andra typer av tjänster.

Vi har formulerat de olika typerna av tjänster utifrån Kammarkollegiets ramavtal för it-drift. Vi bedömer nämligen att de är förhållandevis välkända inom förvaltningen och att Kammarkollegiet har gjort ett stort förarbete med att kategorisera och beskriva olika typer av tjänster.[42] I bilaga 4 framgår i större detalj vad som ingår i de olika typerna av tjänster.

---

[40] Statens servicecenter (2017). *En gemensam statlig molntjänst för myndigheternas it-drift*. s. 25.

[41] SOU 2021:1. *Säker och kostnadseffektiv it-drift drift.* s. 83–84.

[42] Kammarkollegiet (2025). *Vägledning för avrop från IT-drift Mindre och IT-drift Större*. s. 16–18.

### 7.3.2 Molntjänsterna skiljer sig från övriga typer av tjänster när det gäller driftsform

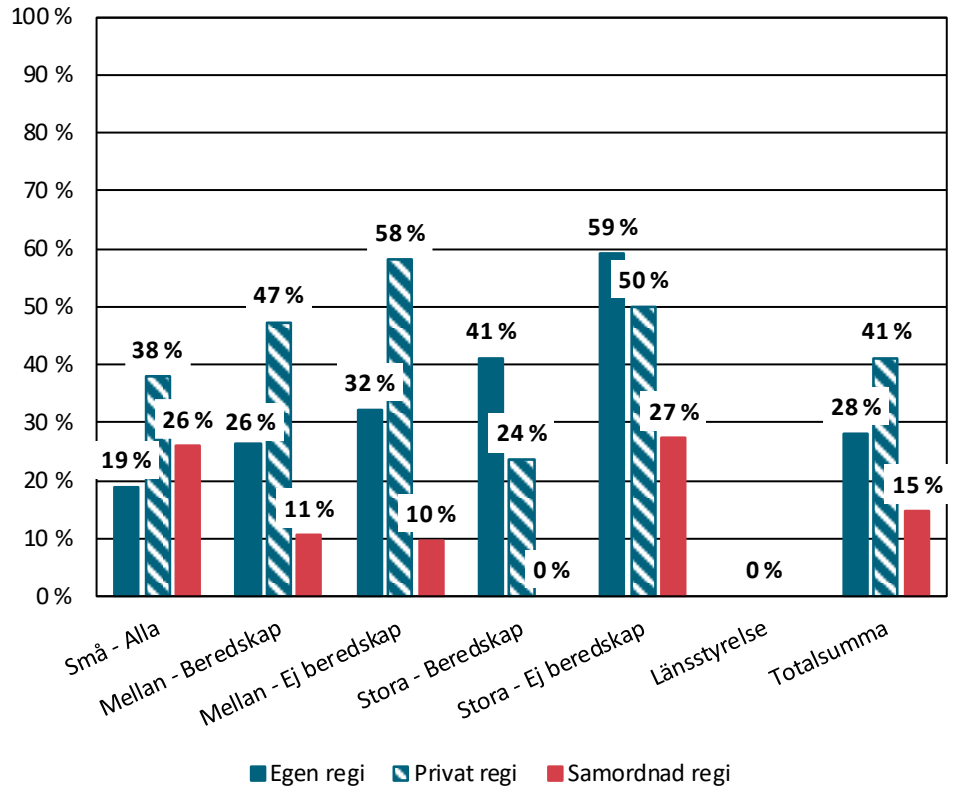
Våra enkätresultat visar vidare att molntjänsterna skiljer sig från de andra typerna av it-driftstjänster när det gäller driftsform. För molntjänsterna är privat regi den vanligaste driftsformen, med 41 procent bland de svarande myndigheterna. Det är också en avsevärt lägre andel av de svarande myndigheterna som uppger att de har molntjänster i egen eller samordnad regi jämfört med de övriga typerna av tjänster, 28 procent respektive 15 procent. Vi bedömer att resultaten speglar tillgången på molntjänster i egen respektive samordnad regi, som är lägre än för de övriga typerna av tjänsterna. Det uppger även företrädare för bland annat Digg, ESV och Försvarsmakten som vi har talat med.

### 7.3.3 Stora skillnader mellan myndigheter i hur de använder molntjänster i privat regi

Vår analys visar att det finns stora skillnader mellan olika kategorier av myndigheter när det gäller hur de använder molntjänster i egen och privat regi (figur 8). Vi ser ett positivt samband mellan att ha molntjänster i egen regi, storlek på myndigheten och myndighetens status som beredskapsmyndighet. Detta ligger i linje med hur vanligt det är med it-drift i egen regi i stort. Det är bara 19 procent av de små myndigheterna som uppger att de har molntjänster i egen regi, jämfört med 59 procent av de stora beredskapsmyndigheterna. Däremot är det bara 24 procent av de stora beredskapsmyndigheterna som uppger att de använder molntjänster i privat regi. Det skiljer sig avsevärt från övriga kategorier av myndigheter. Både bland de stora och mellanstora myndigheterna som inte är beredskapsmyndigheter, samt de mellanstora beredskapsmyndigheterna, är det förhållandevis vanligt med molntjänster i privat regi. Högst är andelen bland de mellanstora myndigheterna som inte är beredskapsmyndigheter, varav 58 procent av de svarande använder molntjänster i privat regi.

En motsvarande analys av hur olika kategorier av myndigheter organiserar driften av datacentertjänster, nätverks- och kommunikationstjänster, applikationstjänster och supporttjänster finns i bilaga 4.

**Figur 8.** **Andel av myndigheterna som har molntjänster i egen, privat respektive samordnad regi.**

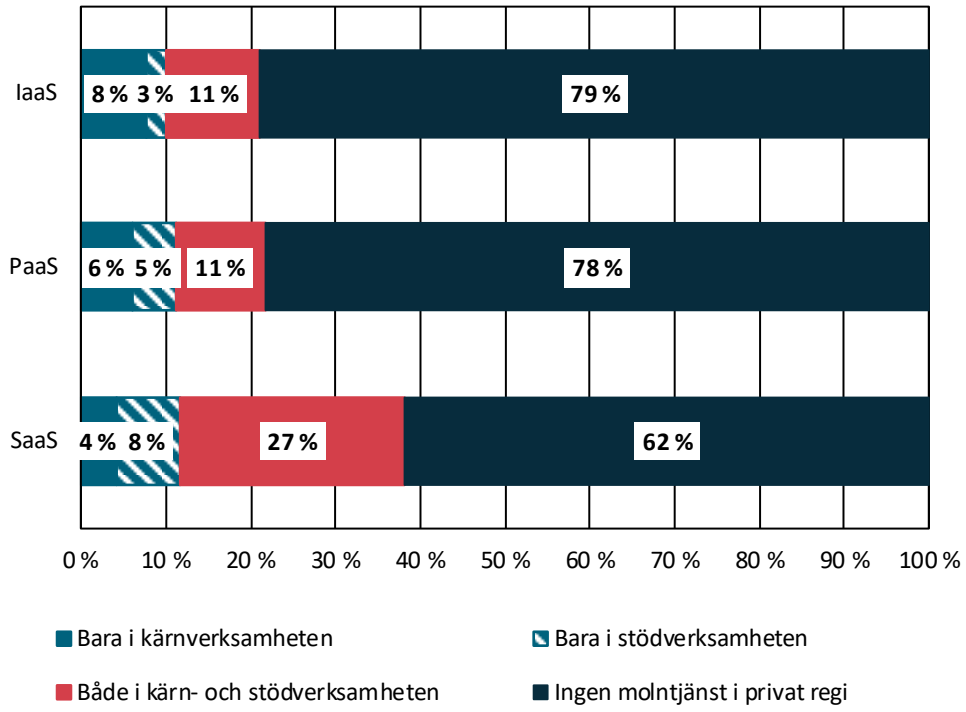



Källa: Statskontorets enkätundersökning 2025.

### 7.3.4 Vanligast med molntjänster i privat regi för tillgång till mjukvara och applikationer i publika moln

Våra resultat visar att det är vanligast att myndigheterna använder molntjänster från privata leverantörer för att få tillgång till olika typer av mjukvara, utan att kontrollera den underliggande infrastrukturen så som servrar eller nätverk. I it-kretsar kallas det för *Software as a service* (SaaS). 38 procent av de svarande myndigheterna använder den typen av molntjänster från privata leverantörer i någon del av verksamheten (figur 9). Det motsvarar 93 procent av de myndigheter som uppger att de använder molntjänster från privata leverantörer. Men det är även förhållandevis vanligt att myndigheterna använder molntjänster som ger dem tillgång till infrastruktur som servrar, nätverk och liknande, eller plattformar för att driva egna mjukvaror och applikationer. Sådana typer av molntjänster kallas i it-kretsar för *Infrastructure as a service* (Iaas) respektive *Platform as a service* (PaaS). Det är 21 respektive 22 procent av de svarande myndigheterna som använder den typen av molntjänster från privata leverantörer i någon del av sin verksamhet. Det motsvarar 51 respektive 52 procent av myndigheterna som uppger att de använder molntjänster från privata leverantörer.

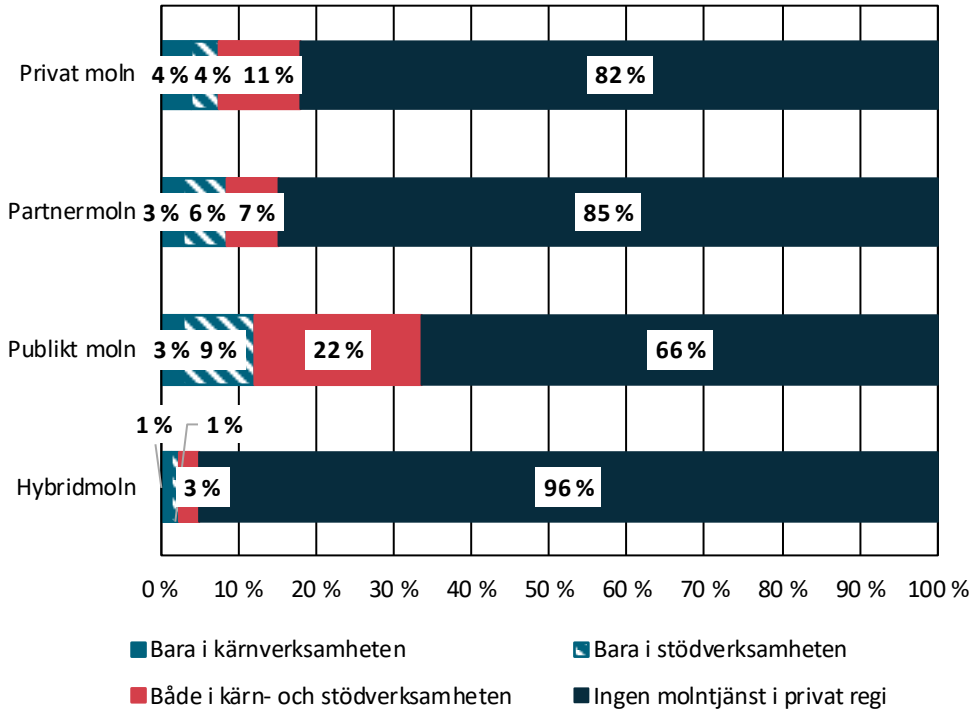
**Figur 9.** **Andel av myndigheterna som har molntjänster i privat regi, utifrån typ av molntjänst och del av verksamheten.**




Källa: Statskontorets enkätundersökning 2025.

När det gäller typen av moln är det vanligast med publika moln, det vill säga moln som potentiellt är tillgängliga för alla organisationer på marknaden (figur 10). 34 procent av de svarande myndigheterna uppger att de använder sådana moln från privata leverantörer. De andra typerna av moln är mer ovanliga. Det är till exempel bara 18 procent av de svarande myndigheterna som använder ett privat moln, det vill säga ett moln som bara de har tillgång till. Andra slags moln är ännu mer ovanliga, som gruppmoln som flera specifika organisationer har tillgång till, samt hybridmoln som är en kombination av två eller fler av de övriga typerna.

**Figur 10.** **Andel av myndigheterna som har molntjänster i privat regi, utifrån typ av moln och del av verksamheten.**



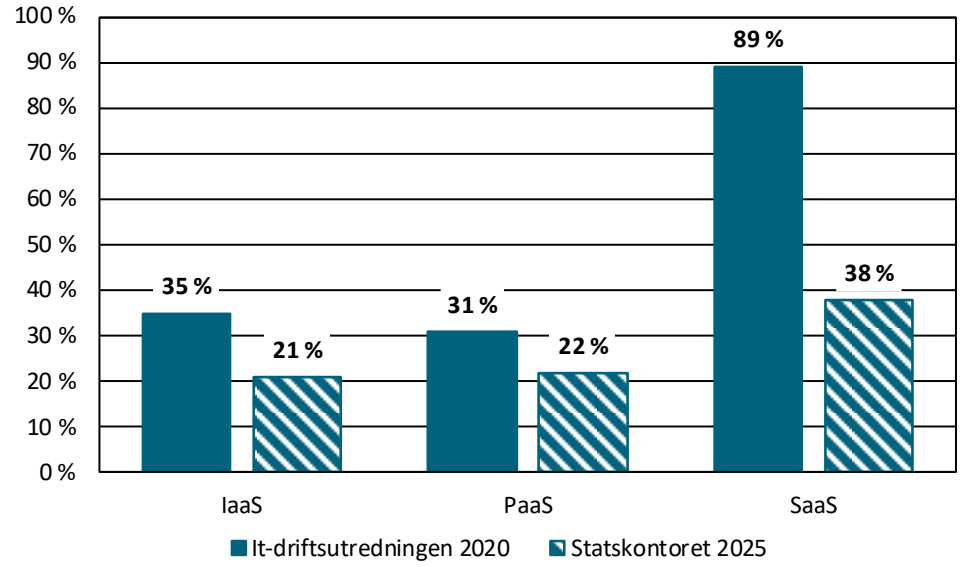

Källa: Statskontorets enkätundersökning 2025.

Våra resultat visar att de svarande myndigheterna använder molntjänster från privata leverantörer i ungefär samma utsträckning i stöd- och kärnverksamheten. Det gäller samtliga typer av molntjänster och moln. De största skillnaderna gäller publika moln och infrastrukturtjänster (IaaS). Publika moln är något vanligare i stödverksamheten. Infrastrukturtjänster är något vanligare i kärnverksamheten. Men skillnaderna är inte större än 5–6 procentenheter (figur 9 och 10).

### 7.3.5 Mindre vanligt att myndigheterna använder molntjänster i privat regi i dag än 2020

Vi har jämfört våra resultat om hur myndigheterna använder molntjänster i privat regi med It-driftsutredningens. En avsevärt lägre andel av de svarande myndigheterna uppger att de använder sådana molntjänster i dag än 2020 (figur 11). Minskningen gäller samtliga typer av molntjänster i privat regi. Men den är mest markant när det gäller SaaS, det vill säga molntjänster som ger tillgång till mjukvara eller applikationer. I It-driftsutredningens enkät uppgav 89 procent av de svarande myndigheterna att de använder sådana molntjänster från privata leverantörer. I vår enkät uppger bara 38 procent av de svarande att de gör det.

**Figur 11.** **Andel av myndigheternas som har molntjänster i privat regi 2020 respektive 2025, utifrån typ av molntjänst.**




Källa: Statskontorets enkätundersökning 2025; SOU 2021:1. s. 86.

Vi bedömer att minskningen inte går att förklara med skillnader i undersökningarnas utformning eller svarsfrekvens, även om dessa faktorer kan ge små skillnader i resultaten. Vi baserar det på att frågan om molntjänster från privata leverantörer samt beskrivningarna av de olika typerna av molntjänster är snarlikt formulerade i vår och utredningens undersökning. Svarsmönstren är också desamma, med Iaas och Paas ungefär lika vanliga och Saas avsevärt vanligare. Dessutom har båda undersökningarna en hög svarsfrekvens. Resultatet ligger också i linje med hur företrädare för leverantörsmyndigheterna och myndigheter både inom och utanför den samordnade it-driften resonerar om olika driftsformer och typer av it-driftstjänster i våra intervjuer. Många av dem beskriver att ”pendeln har svängt” från it-drift i privat regi, inklusive molntjänster, till it-drift i egen regi. Det har skett bland annat till följd av Rysslands fullskaliga invasion av Ukraina. Den har ökat säkerhetsmedvetandet och lett till mer diskussion om riskerna med molntjänster i privat regi både inom förvaltningen och i samhället i stort.

## 7.4 Syftet med att kartlägga myndigheternas it-drift avgör vem som bör fortsätta göra det

Vi har även i uppdrag att föreslå vilken myndighet som är lämplig att fortsätta följa hur myndigheterna organiserar sin it-drift. Vi bedömer att regeringens syfte med att kartlägga förvaltningens it-drift avgör vem som är lämplig att göra det. Om regeringen vill använda resultaten från sådana kartläggningar för att utveckla den samordnade statliga it-driften anser vi att Försäkringskassan är bäst lämpad för uppgiften. Om regeringen i stället vill använda resultaten för att öka sin kunskap och utveckla politik om förvaltningens digitalisering anser vi att Digg är bäst lämpad.

### 7.4.1 En kort och övergripande kartläggning ökar chansen för användbara resultat

När vi har övervägt vilken aktör som är lämplig att fortsätta att följa hur myndigheterna organiserar sin it-drift har vi utgått ifrån att en kort och övergripande enkät ökar sannolikheten att myndigheterna kan och vill besvara den. Det ökar chansen för att uppnå hög svarsfrekvens, vilket i sin tur gör kartläggningen mer relevant och användbar både för regeringen och förvaltningen. Ett stöd för detta är att en stor andel av myndigheterna besvarade vår enkät, och bara någon enstaka myndighet avstod från att besvara någon viss fråga för att de bedömde att svaren skulle kunna vara säkerhetskänsliga. Samtidigt var det en avsevärt lägre andel av myndigheterna som besvarade MSB:s mer omfattande och detaljerade leveranskedjekoll 2025. Båda undersökningarna var regeringsuppdrag.

Vi bedömer vidare att det i dag är svårt att samla in och aggregera omfattande och detaljerad information om hur myndigheterna organiserar sin it-drift. Det beror på att många myndigheter bedömer att informationen är säkerhetskänslig och därför inte vill lämna den ifrån sig. Vi baserar det på våra samtal med företrädare för leverantörsmyndigheterna samt myndigheter inom och utanför den samordnade it-driften. Vi baserar det också på att företrädare för bland annat Säpo, Försvarsmakten och FRA uppger att det generellt är riskabelt och olämpligt att samla in och lägga samma den typen av information.

### 7.4.2 Försäkringskassan är lämplig om kartläggningen ska utveckla den samordnade it-driften

Vi bedömer att Försäkringskassan är den mest lämpliga aktören att fortsätta att följa hur myndigheterna organiserar sin it-drift som helhet, om regeringen anser att kartläggningen ska vara ett verktyg för att utveckla den statliga samordnade it-driften. Det beror på att Försäkringskassan som samordnade myndighet redan ansvarar för övergripande administrativa uppgifter som rör den samordnade it-driften. De inkluderar till exempel att föra en förteckning över vilka it-driftstjänster som ingår i det samordnade statliga utbudet och att förvalta beskrivningarna av tjänsterna i fråga.

Vi anser att en kartläggning av hur myndigheterna organiserar sin it-drift ger en bild av utvecklingspotentialen i den statliga samordnade it-driften. Det gäller både potentiella målgrupper för den samordnade driften och potentiella tjänster. Därmed skulle kartläggningen kunna fungera som ett underlag för regeringen och leverantörsmyndigheterna när de bedömer vilken typ av myndigheter som de vill prioritera att ansluta och vilka tjänster som de vill prioritera att utveckla. Vi bedömer att det syftet går att uppfylla med en övergripande kartläggning som ligger i linje med den som vi har genomfört inom ramen för vårt uppdrag.

Om regeringen väljer att ge Försäkringskassan i uppgift att fortsätta att följa hur myndigheterna organiserar sin it-drift som helhet anser vi att regeringen bör koppla uppgiften till Försäkringskassans roll som samordnande myndighet och reglera det

i it-driftsförordningen. På så sätt kan regeringen både tydliggöra syftet med kartläggningen och ge arbetet långsiktigt stabila förutsättningar.

### 7.4.3 Digg är lämplig om kartläggningen ska vara kunskapsunderlag om förvaltningens digitalisering

Vi bedömer att Digg är den mest lämpliga aktören att fortsätta att följa hur myndigheterna organiserar sin it-drift som helhet, om regeringen anser att kartläggningen ska vara ett verktyg för att utveckla sin kunskap och politik om förvaltningens digitalisering. Vi baserar det på att Digg redan ansvarar för att följa upp, analysera och beskriva utvecklingen av digitaliseringen av den offentliga förvaltningen och samhället i övrigt. Det framgår av § 2 i myndighetens instruktion. Som en del av den uppgiften genomför Digg redan i dag en årlig enkätundersökning för att följa upp myndigheternas digitalisering. Dessutom genomför Digg återkommande en rad andra enkätundersökningar om it- och digitaliseringsfrågor till myndigheter.

Samtidigt är Diggs befintliga enkätundersökningar inte bara till fördel för en sådan kartläggning. Den årliga undersökningen av myndigheternas digitalisering är redan mycket omfattande. Vi bedömer att det finns en betydande risk att ytterligare frågor om hur myndigheterna genomför sin it-drift skulle minska svarsfrekvensen. Ytterligare frågor riskerar också att försämra kvaliteten på myndigheternas svar. Om Digg i stället skulle kartlägga myndigheternas it-drift genom en separat enkätundersökning finns också en risk för en låg svarsfrekvens, till följd av att myndigheterna anser att de redan får och besvarar så många enkäter från Digg.

Om regeringen väljer att ge Digg i uppgift att fortsätta att följa hur myndigheterna organiserar sin it-drift som helhet anser vi att regeringen och Digg behöver hjälpas åt att prioritera bort vissa av de befintliga frågorna i enkäten om myndigheternas digitalisering, så att det totala omfånget inte ökar jämfört med i dag. Vi anser även att regeringen bör reglera uppgiften i Diggs instruktion, för att tydliggöra syftet med kartläggningen och ge arbetet långsiktigt stabila förutsättningar.

I budgetpropositionen för 2026 meddelade regeringen att de avser att slå samman Digg och Post- och telestyrelsen den 1 januari 2027. På sikt bör uppgiften därmed vara reglerad i den nya myndighetens instruktion.

### 7.4.4 MSB lämplig om kartläggningen ska omfatta säkerhetskänslig information

Vi bedömer att det är både svårt och olämpligt att kartlägga hur myndigheterna organiserar sin it-drift i detalj, eftersom sådan information riskerar att vara säkerhetskänslig. Men regeringen kan ändå vilja samla in den typen av information och använda resultaten av kartläggningen för att öka sin kunskap och utveckla politik om förvaltningens it-drift utifrån ett säkerhetsperspektiv. Då bedömer vi att MSB är bäst lämpad för uppgiften. Vi baserar det på att MSB har tillgång till krypterade kanaler för att samla in och hantera information från andra myndigheter. Det är

nödvändigt om kartläggningen ska omfatta säkerhetskänslig information. MSB har dessutom redan i uppdrag att genomföra leveranskedjekollen, vilken inkluderar frågor om myndigheternas it-drift från privata leverantörer.

Leveranskedjekollen innehåller i dag inte några frågor om it-drift i samordnad eller egen regi. Om MSB får i uppdrag eller väljer att fortsätta att genomföra leveranskedjekollen återkommande skulle de kunna lägga till sådana frågor. Samtidigt är undersökningen redan mycket omfattande. Därför riskerar ytterligare frågor att ytterligare försämra undersökningens redan låga svarsfrekvens.

Om regeringen väljer att ge MSB i uppgift att fortsätta följa hur myndigheterna organiserar sin it-drift som helhet anser vi att regeringen bör reglera uppgiften i myndighetens instruktion. Men i praktiken handlar det om att reglera den i FRA:s instruktion. Det beror på att regeringen har beslutat att cybersäkerhetsverksamheten vid MSB ska övergå till FRA under 2026, och att FRA ska överta MSB:s befintliga instruktionsenliga uppgifter på området.

# Referenser


Ekonomistyrningsverket (2018:28). *Pilotprojekt om ramverk för it-kostnader (TBM).*

Ekonomistyrningsverket (2025:4). *Handledning. Baskontoplan för statliga myndigheter 2025.*

Försäkringskassan 2025-02-14. *Internrevisionsplan 2025–2027*. FK 2025/002626.

Försäkringskassan 2025-03-18. *Nitis-inriktning beslutad den 27 februari 2024 – delar som bedöms mindre känsliga*. FK 2024/006706.

Försäkringskassan (2023). *Rapport – delredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift.*

Försäkringskassan (2025). *Rapport – Slutredovisning av uppdraget att erbjuda samordnad och säker statlig it-drift*.

Försäkringskassan (2025). *Budgetunderlag 2026–2028.*

Försäkringskassan 2025-06-05. *Ekonomi- och avgiftsmodell för samordnad och säker statlig it-drift.* FK 2024/006706.

Myndigheten för digital förvaltning (2025). *Enkätrapport om e-fakturering och e-handel i offentlig förvaltning.*

Myndigheten för samhällsskydd och beredskap (2025). *Verktyg för ökad motståndskraft och stärkt civilt försvar.*

Myndigheten för samhällsskydd och beredskap (2025). *Resultatredovisning av Cybersäkerhetskollen 2024.*

Myndigheten för samhällsskydd och beredskap (2025). *Fördjupningsinformation om Cybersäkerhetskollen. Beskrivning och bakgrund till Cybersäkerhetskollen, MSB:s uppföljningsstrukturer för systematiskt cybersäkerhetsarbete.* fordjupningsinformation-csk-2025.pdf.

Myndigheten för samhällsskydd och beredskap (2021). *Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten.*

Regeringsbeslut 2025-02-27. *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra en kartläggning av digitala leveranskedjor och att ta fram en modell för uppföljning av digitala leveranskedjor*. Fö2025/00390.

Regeringsbeslut 2019-09-19. *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.* Ju2019/03058/SSK, Ju2019/02421/SSK.

Regeringsbeslut 2015-01-15. *Uppdrag att fördjupa arbetet med jämförelser av it-kostnader och att kartlägga it-projekt med hög risk*. N2015/738/EF.

Proposition 2024/25:1. *Budgetproposition för 2025. Utgiftsområde 18. Samhällsplanering, bostadsförsörjning och byggande samt konsumentpolitik*.

Proposition 2024/25:34. *Totalförsvaret 2025–2030*.

SOU 2021:1 *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Delbetänkandet av It-driftsutredningen*.

SOU 2021:97. *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift. Slutbetänkandet av It-driftsutredningen.*

Skatteverket (2025). *Skatteverkets budgetunderlag 2026–2028.*

Statens servicecenter (2017). *En gemensam statlig molntjänst för myndigheternas it-drift*.

Statskontoret (2025). *Statsförvaltningen i korthet.*

Swedish Standards Institute (2015). *Terminologi för informationssäkerhet*. SIS-TR 50:2015. Stockholm: SIS.

Trafikverket (2025). *Trafikverkets budgetunderlag 2026–2028.*

Bilaga 1

# Regeringsuppdraget

Regeringen

**Regeringsbeslut** **III:1**

2025-03-13
Fi2025/00643

**Finansdepartementet**

Statskontoret
Box 396
101 27 Stockholm

## Uppdrag till Statskontoret att skapa förutsättningar för en effektiv uppföljning av den statliga it-driften

### Regeringens beslut

Regeringen ger Statskontoret i uppdrag att ta fram indikatorer för uppföljning av arbetet med det samordnade statliga tjänsteutbudet för it-drift.

I uppdraget ingår att

- ta fram ett nolläge för mätning av arbetet,
- föreslå indikatorer på aktörs- och samhällsnivå för säkerhet, effektivitet och kvalitet, och
- i övrigt föreslå de indikatorer som bedöms relevanta för en effektiv uppföljning.

Statskontoret ska även kartlägga organiseringen av it-driftslösningarna inom staten som helhet. Myndigheten ska i denna del lämna förslag på vilken myndighet som är lämplig att följa upp en sådan kartläggning.

Statskontoret ska när uppdraget utförs inhämta synpunkter från Försäkringskassan, Skatteverket, Trafikverket, Myndigheten för digital förvaltning, Myndigheten för samhällsskydd och beredskap, Ekonomistyrningsverket, Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt och övriga aktörer som myndigheten bedömer är relevanta.

Statskontoret ska senast den 30 november 2025 lämna en skriftlig redovisning av uppdraget till Regeringskansliet (Finansdepartementet).

För uppdraget får Statskontoret under 2025 använda högst 1 000 000 kronor som ska redovisas mot det inom utgiftsområde 22 Kommunikationer för

Telefonväxel: 08-405 10 00
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 24
E-post: fi.registraton@regeringskansliet.se

budgetåret 2025 uppförda anslaget 2:4 Informationsteknik och telekommunikation, anslagsposten 4 Informationsteknik – del till Kammarkollegiets disposition. Medlen betalas ut engångsvis efter rekvisition till Kammarkollegiet senast den 1 december 2025.

Medel som inte har använts för avsett ändamål ska återbetalas senast den 31 december 2025 till Kammarkollegiet. Vid samma tidpunkt ska en ekonomisk redovisning av använda medel lämnas till Kammarkollegiet.

Redovisning, rekvisition och återbetalning ska hänvisa till diarienumret för detta beslut.

## Bakgrund

Av förordningen (2024:1005) om samordnad och säker statlig it-drift framgår att Försäkringskassan, Skatteverket och Trafikverket ska tillhandahålla it-driftstjänster inom ramen för det samordnade statliga tjänsteutbudet och stödja myndigheter vid val av it-driftslösning. Försäkringskassan ska årligen redovisa effekterna av arbetet med det samordnade statliga tjänsteutbudet av it-drift till regeringen.

I syfte att skapa goda förutsättningar för en ändamålsenlig redovisning av arbetet enligt förordningen är det viktigt att undersöka hur den samordnande statliga it-driften i nuläget är strukturerad och organiserad för att därefter fastställa ett utgångsläge (nolläge) mot vilket resultat och effekter av arbetet enligt förordningen kan jämföras. Därutöver är det centralt att det tas fram indikatorer för uppföljning av arbetet på såväl aktörs- som samhällsnivå. För detta är indikatorer avseende säkerhet, effektivitet och kvalitet centrala för att säkerställa att de lösningar som erbjuds ger rätt stöd och bidrar med säkra och kostnadseffektiva it-driftstjänster.

Av it-driftsutredningens slutbetänkande Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift (SOU 2021:97) framgår att myndigheterna ofta har en blandning av it-drift de själva hanterar och it-drift de utkontrakterat till privata tjänsteleverantörer eller samordnat med andra statliga myndigheter. Regeringen kan konstatera att det saknas en övergripande lägesbild över hur myndigheterna valt att organisera sin it-drift inom staten som helhet, något som är särskilt angeläget i förhållande till teknikutvecklingen på området med bl.a. molntjänster. Även om faktorerna som påverkar valet av driftsform kan skilja sig åt mellan myndigheterna

skulle en övergripande lägesbild kunna utvisa om det finns möjlighet att ytterligare utveckla arbetet med säkra och kostnadseffektiva it-driftslösningar inom staten. Mot denna bakgrund finns det ett behov av att kartlägga organiseringen av it-driftslösningarna inom staten som helhet och lämna förslag på vilken myndighet som är lämplig att följa upp en sådan kartläggning.

På regeringens vägnar

Erik Slottner

David Källström

Kopia till

Justitiedepartementet/PO
Försvarsdepartementet/CF och MF
Socialdepartementet/SF
Finansdepartementet/BA, DOF, ESA, IEA, SFÖ och SKA
Landsbygds- och infrastrukturdepartementet/SPN och US
Ekonomistyrningsverket
Försvarets radioanstalt
Försvarsmakten
Kammarkollegiet
Myndigheten för digital förvaltning
Myndigheten för samhällsskydd och beredskap
Skatteverket
Säkerhetspolisen
Trafikverket

Bilaga 2

# Det samordnade statliga tjänsteutbudet

**Tabell B1. Det samordnade statliga tjänsteutbudet, oktober 2025.**

| Tjänst | Leverantörs-myndighet | Kort beskrivning |
|---|---|---|
| Virtuell data-centertjänst (vDC) | Försäkrings-kassan Skatteverket | En tjänst som ger en ansluten myndighet tillgång till en egen isolerad virtuell datacentermiljö för servrar, nätverk och lagringsresurser enligt avtalade volymer och viss prestanda. |
| Objektbaserad lagring | Försäkrings-kassan Skatteverket | En tjänst för att lagra stora mängder ostrukturerat data. Den kan till exempel användas vid lagring och back-up av stora mängder data. |
| Samarbets-plattform för offentlig sektor (SAFOS) | Försäkrings-kassan | En plattform för att underlätta samverkan mellan myndigheter. Består tex av en chatt, en mötestjänst och en samarbetstjänst med funktioner för information och planering. Tjänsterna är lämpliga för myndigheter som arbetar med data som inte får lagras i utländska molntjänster. |
| E-identitet för offentlig sektor (EFOS) | Försäkrings-kassan | En elektronisk tjänstelegitimation som ger förutsättningar för säker inloggning för medarbetare och bidrar till säker inpassering, signering av dokument och utskrift samt myndighetsövergripande dialoger. |
| Kapacitetstjänst (CAP) | Försäkrings-kassan | En plattform för att utveckla, distribuera och hantera applikationer på ett modulärt, automatiserat och skalbart sätt. Vidareutveckling av tjänsten pågår i samarbete med anslutna myndigheter. |
| Webbanalys | Försäkrings-kassan | En helhetslösning för att mäta vilken aktivitet som finns på webbplatser (insamling, lagring, kapacitet och analysverktyg). Erbjuds som en dedikerad tjänst utformad utifrån kundens behov. |
| Digitala kontoret | Försäkrings-kassan | En samling standardiserade tjänster där tjänsten Digital arbetsplats är grunden. Tjänsterna innefattar inloggning med säker identifiering, möjligheter till distansarbete och ständigt fokus på förbättring, självbetjäning och automation. Som tillval finns digital mötesutrustning, kontorsskrivare och virtuell digital arbetsplats. |
| Webbplattformar för offentlig sektor (WEFOS) | Försäkrings-kassan | En tjänst där drift, utveckling och förvaltning sker i Försäkringskassans datacenter av säkerhetsklassad personal. En standardtjänst som erbjuder funktioner för säker och skräddarsydd upplevelse för myndigheters kontakt med medborgarna. |
| Utskick | Försäkrings-kassan | En tjänst för utskick av fysiska brev till postoperatör eller utskick av elektroniska dokument till mottagarens digitala brevlåda. För samtliga utskick skapas statistik- och rapporthantering. |

| Tjänst | Leverantörs-myndighet | Kort beskrivning |
|---|---|---|
| DSP BH – säker arbetsplats för nivå begränsat hemlig | Trafikverket | En tjänst som möjliggör säkert tal och meddelanden, videokonferens och dokumentdelning både inom den egna myndigheten samt med andra myndigheter som är anslutna till tjänsten. Tjänsten riktar sig i fösta hand till beredskapsmyndigheter. |
| Extern autentisering Legitimeringstjänst | Skatteverket | Tjänster som ger tillgång till den infrastruktur som krävs för att kunna verifiera användarens e-legitimation på ett korrekt sätt. Tjänsten hanterar olika e-legitimationer. Stommen är de e-legitimationer som Digg tilldelat kvalitetsmärket ”Svensk e-legitimation”. Säker e-legitimering för användare i övriga världen finns också att tillgå. |
| Digitala underskrifter – underskriftstjänst | Skatteverket | Tjänster som ger möjlighet att få dokument digitalt underskrivna med hjälp av alla de e-legitimationer som stöds i legitimeringstjänsten. Förutsätter Extern autentisering – Legitimeringstjänst. |

Källa: Mottaget från Försäkringskassan, oktober 2025.

Bilaga 3

# Befintliga datakällor som rör myndigheternas it-drift

Vi har gått igenom en rad befintliga datakällor som innehåller information som rör myndigheternas it-drift. Vår analys visar att ingen av datakällorna är tillräcklig för att ge en bild av hur it-driften i staten är organiserad som helhet. Datakällorna är förhållandevis mer användbara för att ge en bild av it-driften i privat respektive samordnad regi än it-driften i egen regi. Men inte heller för de förstnämnda driftsformerna ger befintliga data en tillräcklig bild. Nedan redogör vi för de datakällor vi har gått igenom samt vad de visar och inte visar.

## Hermesdata från ESV över myndigheternas kostnader för it-drift

Samtliga myndigheter i den statliga redovisningsorganisationen rapporterar ekonomisk information till statsredovisningssystemet Hermes, som ESV förvaltar. Myndigheterna är skyldiga att rapportera informationen på särskilda statliga inrapporteringskoder, så kallade s-koder. Det framgår av 21 § Förordningen (2000:606) om statliga myndigheters bokföring och ESV:s föreskrifter och allmänna råd (ESVFA 2022:2) Syftet med s-koderna är att myndigheterna ska rapportera sin ekonomiska information på ett enhetligt sätt.

Två av s-koderna omfattar kostnader för it-drift: utomstatliga respektive inomstatliga inköp av it-tjänster. De utomstatliga inköpen motsvarar inköp från privata leverantörer och de inomstatliga inköpen motsvarar inköp från andra myndigheter. Därmed innehåller dessa koder information om hur myndigheterna organiserar sin it-drift i privat respektive samordnad regi. Men kostnaderna som myndigheterna rapporterar in på koderna omfattar även annat än it-driftstjänster. Det gäller till exempel it-konsulter som arbetar med att utveckla ny hårdvara eller mjukvara, och inte med att hantera eller underhålla befintlig dito. Vi bedömer att det urholkar möjligheten att använda data över utomstatliga inköp av it-tjänster för att följa myndigheternas kostnader för it-drift i privat regi, eftersom vi inte vet hur stor del av kostnaderna som avser drift respektive utveckling. Därmed ger myndigheternas kostnader för utomstatliga inköp av it-tjänster ingen tillförlitlig bild av deras kostnader för it-drift i privat regi.

Däremot bedömer vi att data över de inomstatliga inköpen av it-tjänster i huvudsak avser just driftstjänster, eftersom vi uppfattar att det är ovanligt att myndigheter köper kompetens från andra myndigheter för att utveckla sina it-system. Därför bör dessa data ge en ungefärlig bild av myndigheternas kostnader för samordnad statlig it-drift. Data över myndigheternas inomstatliga inköp av it-tjänster överensstämmer också i stort med vad vi vet om vilka myndigheter som är anslutna till en helhets-

tjänst inom den samordnade statliga it-driften, samt när de anslöt sig till den. Men inte heller dessa data är helt tillförlitliga, eftersom vi inte vet säkert i vilken utsträckning som myndigheter köper it-utveckling av varandra. Hermes innehåller inga s-koder som gör det möjligt att följa myndigheternas kostnader för it-drift i egen regi. Därmed går det inte heller att använda data från Hermes för att följa myndigheternas totala kostnader för it-drift över tid. Företrädare för ESV bekräftar det.

Vi har övervägt att föreslå ESV att utöka s-kodsystemet med koder som specifikt avser it-drift. Men vi har valt att inte lämna något sådant förslag. Ett skäl till det är att det inte finns någon formell eller förvaltningsgemensam definition av it-drift. Även om vi, ESV eller någon annan myndighet formulerade en sådan skulle den sannolikt inte heller vara hållbar över tid, eftersom synen på vad som ingår i it-drift förändras med den tekniska utvecklingen. Även med en s-kod för it-drift skulle myndigheterna därmed i praktiken inkludera olika typer av kostnader när de rapporterade i Hermes. Det skulle ge data av låg kvalitet och liten jämförbarhet över tid.

Ett annat skäl är att s-kodsystemet är uppbyggt utifrån kostnadsslag och inte verksamhetsslag. Myndigheterna rapporterar till exempel sina kostnader för personal, lokaler och avskrivningar oavsett var i verksamheten de uppstår, inte sina kostnader för it-drift, ärendehandläggning och tillsyn oavsett om det är personal, lokaler eller avskrivningar som ger upphov till kostnaderna. Det innebär att en eller flera s-koder för it-drift skulle gå på tvärs med kodsystemet i övrigt, och kräva att myndigheterna rapporterade samma kostnader i flera kategorier. Det skulle ge en missvisande bild av myndigheternas totala kostnader. För att undvika det skulle ESV behöva bryta ut kostnaderna för it-drift ur samtliga befintliga kostnadsslag, det vill säga utöka s-kodsystemet med koder för it-driftspersonal, it-driftslokaler och så vidare. Det skulle innebära ett mycket stort antal nya koder, och en haltande logik i kodsystemet som helhet om it-drift var den enda verksamheten som myndigheterna skulle särredovisa.

## E-handelsdata från Statens servicecenter över myndigheternas inköp av it-driftstjänster

E-handelsdata är information om till exempel elektroniska beställningar, leveranskvittenser och fakturor som myndigheter och deras leverantörer utbyter mellan sina respektive systemstöd.[43] Nästan alla myndigheter med fler än 50 anställda är skyldiga att hantera sina inköp av varor och tjänster på det sättet. Det framgår av 3§ i förordning (2003:770) om statliga myndigheters elektroniska informationsutbyte.

[43] Se till exempel Myndigheten för digital förvaltning (2025). *Enkätrapport om e-fakturering och e-handel i offentlig förvaltning*. s. 5f.

SSC tillhandahåller en e-handelstjänst som 124 myndigheter använde vid tidpunkten för vår undersökning. 2024 var det 76 av dessa myndigheter som även använde någon av SSC:s gemensamma kontoplaner, och 66 av dem använde även ekonomisystem och bokföringstjänster från SSC. Det innebär att SSC med förhållandevis enkla medel kan ta fram data över dessa 66 myndigheters totala årliga inköp av it-driftstjänster, hur dessa är fördelade mellan kontona it-konsulter, it-licenser och övriga köpta it-tjänster, samt hur stor del av inköpen som är inomstatliga respektive utomstatliga.

Vi bedömer att dessa data ger både relevant och tillförlitlig information om myndigheternas kostnader för it-drift i privat respektive samordnad regi. Vi ser inget uppenbart skäl till att de 66 myndigheterna för vilka e-handelsdata är tillgängliga inte skulle kunna vara representativa för myndigheterna i redovisningsorganisationen som helhet. Enligt företrädare för SSC är det som främst skiljer dessa myndigheter från andra att de vid något tillfälle har haft en ekonomidirektör som tror på e-handel. Däremot säger data inte något om i vilken omfattning som myndigheterna har it-drift i egen regi. Data är dessutom bara tillgänglig för en knapp tredjedel av myndigheterna i den statliga redovisningsorganisationen. Men antalet myndigheter som använder Statens servicecenters e-handelstjänst, gemensamma kontoplan, ekonomisystem och bokföringstjänster har ökat över tid.

Vi bedömer därför att e-handelsdata är på sikt kan vara användbara för att triangulera resultaten av kartläggningar som bygger på enkätundersökningar. Genom att jämföra de 66 myndigheternas e-handelsdata med deras Hermesdata är det möjligt att verifiera data över de inomstatliga inköpen av it-driftstjänster från båda källorna. Vi kan också få en bild av hur stor andel av de utomstatliga inköpen av it-tjänster som utgörs av konsulter, samt i vilken utsträckning som andelen konsultkostnader varierar mellan myndigheter. Om jämförelsen skulle visa att variationerna är små skulle vi eventuellt kunna extrapolera den genomsnittliga andelen konsultkostnader för de 66 myndigheterna till samtliga myndigheter som rapporterar i Hermes.

## Data från Kammarkollegiet över myndigheternas avrop från de statliga ramavtalen för it-drift

Kammarkollegiet ansvarar för att tillhandahålla och förvalta statliga ramavtal för bland annat it-drift, och kan ta fram data över värdet på de totala avropade tjänsterna per ramavtal och år. Men sådana data ger inte en heltäckande eller tillförlitlig bild av myndigheternas kostnader för utkontrakterad it-drift respektive it-drift i privat regi. Det beror på att myndigheterna kan upphandla tjänster utanför ramavtalen, till exempel om tjänsterna i fråga inte ingår i ramavtalen.

Myndigheter som upphandlar utanför ramavtalen är skyldiga att underrätta Kammarkollegiet om det genom en så kallad avstegsanmälan. Enligt företrädare för Kammarkollegiet har ramavtalsleverantörerna informerat dem om att det är förhållandevis vanligt att myndigheterna köper tjänster utanför ramavtalen. Men

Kammarkollegiet har inte information om hur stora belopp eller vilka myndigheter det handlar om när myndigheterna inte gör någon avstegsanmälan, och det finns sannolikt ett mörkertal av myndigheter som inte underrättar Kammarkollegiet när de går utanför ramavtalen. Sammantaget innebär detta att Kammarkollegiet inte vet hur stor andel av myndigheternas totala utkontrakterade it-drift som de avropar från ramavtalen.

Dessutom gäller ramavtalen bara under fyra år, även om de enskilda kontrakten som myndigheterna avropar från ramavtalen kan vara längre. Nya ramavtal innebär delvis nya villkor och nytt innehåll, vilket gör det svårt att använda avropsdata för att följa myndigheternas it-drift i privat regi över avtalsperioder. Under den nuvarande avtalsperioden finns till exempel ett särskilt ramavtal för myndigheter med färre än 100 anställda, till skillnad från den föregående avtalsperioden. Dessutom har säkerhetskraven på leverantörerna blivit och innehållet i tjänsterna delvis förändrats.

## Data från Myndigheten för samhällsskydd och beredskap över myndigheternas digitala leveranskedjor

MSB fick i februari 2025 ett regeringsuppdrag som bland annat handlade om att kartlägga och identifiera för samhället särskilt skyddsvärda digitala leveranskedjor.[44] MSB har valt att inkludera kartläggningen i sin befintliga mätning Cybersäkerhets-kollen. I kartläggningen frågar MSB myndigheterna om tjänster och infrastruktur som levererar eller gör det möjligt att leverera digitala produkter för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem. Kartläggningen är omfattande med många och detaljerade frågor. Myndigheterna får bland annat ange vilka system de har anlitat externa leverantörer för, vilket land leverantören har sitt huvudsakliga säte i, eventuella namn på underleverantörer och vilken typ av system det gäller (figur B1).[45]

**Figur B1. Utsnitt ur Leveranskedjekollens kartläggningsdel.**

**Kartläggning Leveranskedjekollen**

**Ange vilka av organisationens nätverks- och informationssystem som bedöms vara kritiska för organisationens förmåga att bedriva sin kärnverksamhet**

| ID | Namn | Leverantör | Leverantörens säte | Underleverantörer | Underleverantörernas säte | Typ av system | Driftsform | Avtalstid | Systemets kritikalitet | Systemets redundans | Kommentarer |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Ange namn på produkten/tjänsten.* | *Ange leverantörens namn.* | *Ange det land där leverantören har sitt huvudsakliga säte/huvudkontor.* | *Ange namnen på leverantörens underleverantörer, i de fall och i den utsträckning detta är känt.* | *Ange de länder där underleverantörerna har sitt huvudsakliga säte/huvudkontor, i de fall och i den utsträckning detta är känt.* | *Ange i rullistan vilken typ av system som det rör sig om. Ta hjälp av informationen i MSB:s kommentar.* | *Ange i rullistan vilken driftsform som används för systemet.* | *Ange i rullistorna när (år och månad) som avtalet med leverantören upphör.* År Månad | *Ange i rullistan hur länge som systemet kan vara otillgängligt innan det blir kritiskt för verksamheten. Tänk bort ev. redundans i* | *Ange i rullistan i vilken utsträckning redundans finns om systemet blir otillgängligt.* | *Vid behov, ange kommentarer för att förtydliga era svar.* |

Källa: Myndigheten för samhällsskydd och beredskap (2025). *Leveranskedjekollen*.

[44] Regeringsbeslut 2025-02-27. *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra en kartläggning av digitala leveranskedjor och att ta fram en modell för uppföljning av digitala leveranskedjor*. Fö2025/00390.

[45] MSB (2025). *Fördjupningsinformation om Cybersäkerhetskollen*.

Dessa data skulle kunna ge en bild av förekomsten av it-drift i egen respektive utkontrakterad regi (privat eller samordnad). Men få myndigheter besvarade kartläggningen 2025. Svaren säger inte heller något om hur stor andel av sin totala it-drift som myndigheterna har i olika driftsformer.

Bilaga 4

# Enkätundersökning

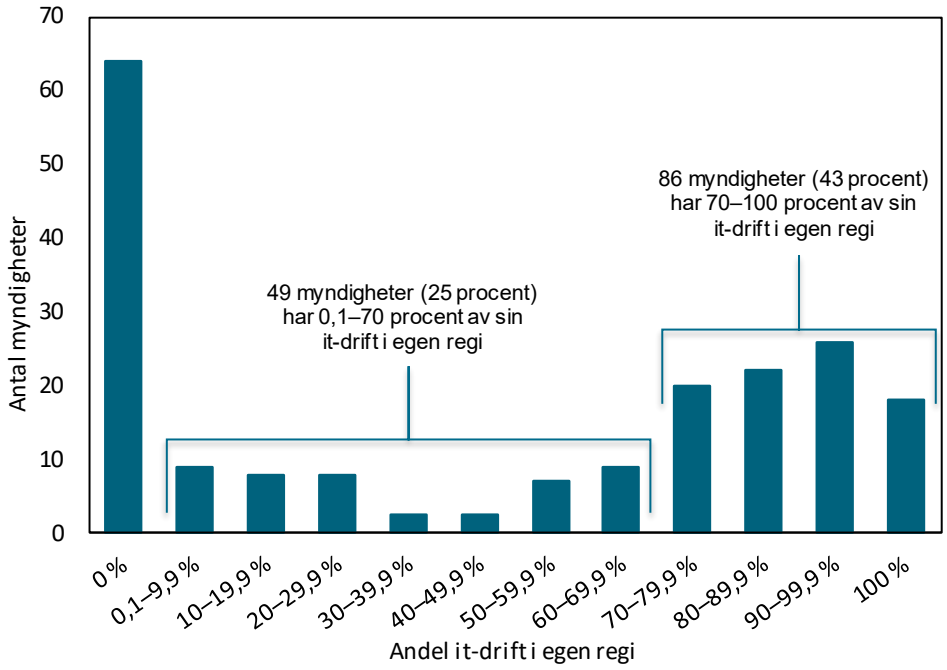
I denna bilaga redovisar vi kompletterande figurer och analyser av våra enkätresultat. Enkäten i sin helhet finns i slutet av bilagan.

## Myndigheternas användning av it-drift i olika regi

I huvudrapporten redovisar vi att myndigheterna har en majoritet av sin it-drift i egen regi. Vi bad myndigheterna att uppskatta hur deras kostnader för it-drift var fördelade mellan driftsformerna egen, samordnad och privat regi. Nedan fortsätter vi att analysera hur myndigheterna använder och kombinerar olika driftsformerna genom att analysera en driftsform i taget.

Myndigheternas användning av it-drift i egen regi går att gruppera i tre kategorier (figur B2). Myndigheter utan it-drift i egen regi (32 procent), de med upp till 70 procent av sin it-drift i egen regi (25 procent) samt de med 70 procent eller mer av sin it-drift i egen regi (43 procent).

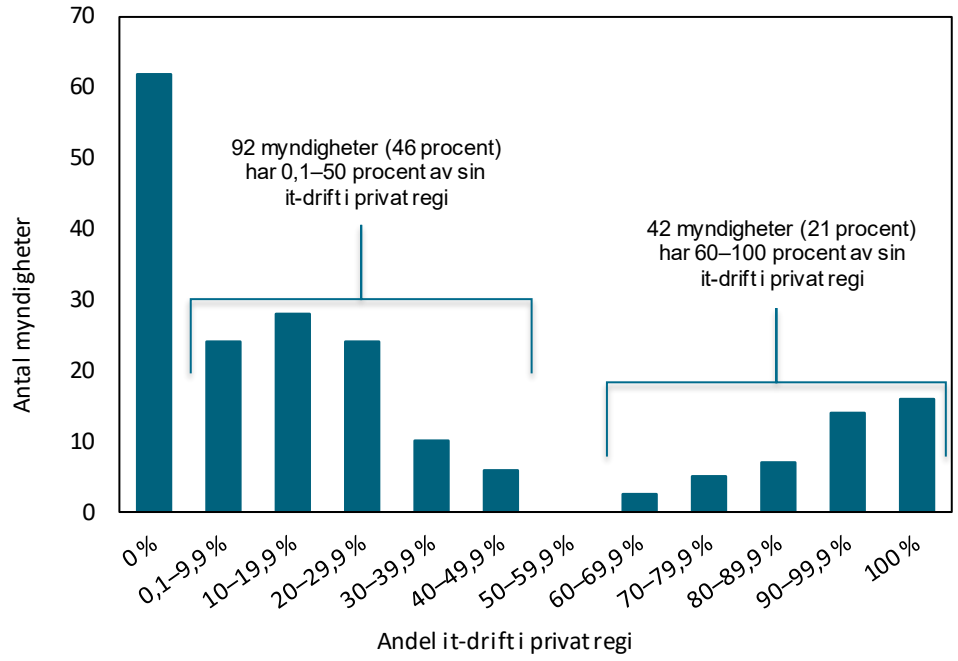
**Figur B2. Myndigheternas användning av it-drift i egen regi, utifrån andel it-drift i egen regi.**




Källa: Statskontorets enkätundersökning 2025.

Tolkning: Åtta myndigheter har 10–19,9 procent av sin it-drift i egen regi.

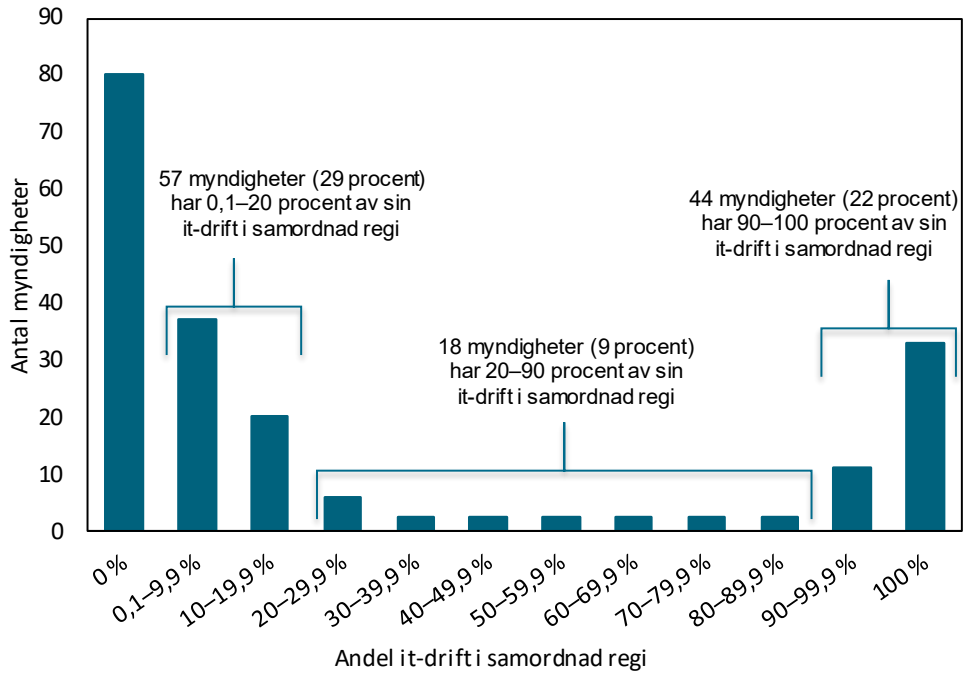
**Figur B3.** **Myndigheternas användning av it-drift i privat regi, utifrån andel it-drift i privat regi.**




Källa: Statskontorets enkätundersökning 2025.

Tolkning: 28 myndigheter har 10–19,9 procent av sin it-drift via privata leverantörer.

**Figur B4.** **Myndigheternas användning av it-drift i samordnad regi, utifrån andel samordnad it-drift.**




Källa: Statskontorets enkätundersökning 2025.

Tolkning: 20 myndigheter har 10–19,9 procent av sin it-drift i samordnad regi.

Myndigheternas användning av it-drift i samordnad regi går att gruppera i fyra kategorier (figur B4). Myndigheter som inte använder samordnad drift (40 procent), de som har samordnad drift i liten utsträckning (29 procent), de som har samordnad drift i relativt stor utsträckning (9 procent), samt myndigheter som nästan bara har samordnad drift i (22 procent).

Myndigheternas användning av it-drift i privat regi går att gruppera i tre kategorier (figur B3). Myndigheter som inte har it-drift i privat regi (31 procent), de som har upp till 50 procent av sin drift i privat regi (46 procent), samt de som har 60 procent eller mer i privat regi (23 procent).

## Regressionsanalys av myndigheters it-drift i egen regi

I huvudrapporten konstaterar vi att ju större myndigheterna är mätt i antalet årsarbetskrafter, desto större andel av sin it-drift genomför de i egen regi. Dessutom har beredskapsmyndigheterna en större andel av sin it-drift i egen regi än övriga myndigheter. Det framgår av de figurer som vi redovisar i huvudrapporten samt på en regressionsanalys som vi redovisar nedan. Metoden är OLS och den beroende variabeln är andelen av myndigheters it-drift som de genomför i egen regi. Analysen visar att:

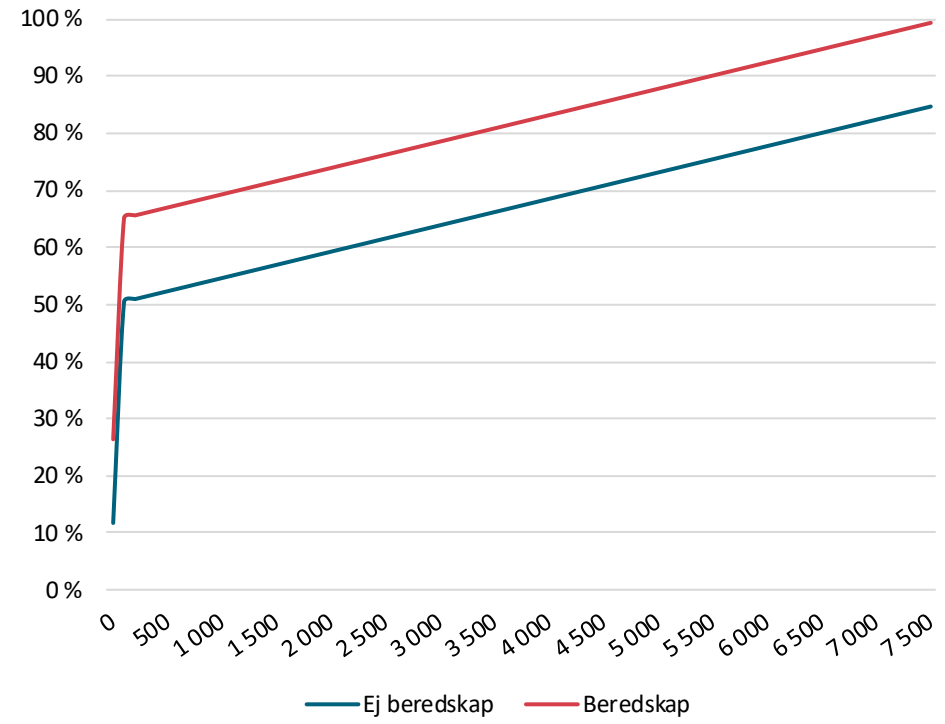
- Det finns ett statistiskt signifikant positivt samband mellan storleken på myndighet och andelen it-drift i egen regi
- Det finns ett statistiskt signifikant positivt samband mellan status som beredskapsmyndighet och andelen it-drift i egen regi
- Det är framför allt mycket små myndigheter har en låg andel it-drift i egen regi.

**Tabell B2. Utfall av regressionsanalys, andel it-drift i egen regi som beroende variabel.**

| | Koefficienter | Standardfel | t-kvot | p-värde |
|---|---|---|---|---|
| Konstant | 49,98 | 3,52 | 14,21 | 0,00 |
| Dummy – Mindre än 50 ÅA | -38,35 | 6,53 | -5,87 | 0,00 |
| ÅA 2025 | <0,01 | 0,00 | 2,87 | 0,00 |
| ÅA 2025^2 | <0,01 | 0,00 | -1,99 | 0,05 |
| Beredskap | 14,63 | 6,49 | 2,26 | 0,03 |

För att illustrera regressionsresultaten visar vi hur den förväntade andelen it-drift i egen regi förändras i relation till antalet årsarbetskrafter vid en myndighet (figur B5). Vi har delat upp resultaten för myndigheter som är beredskapsmyndigheter och myndigheter som inte är det.

**Figur B5.** **Andel egen regi beroende på myndighetens storlek och om det är en beredskapsmyndighet eller ej, förväntat värde baserat på regressionsresultat.**



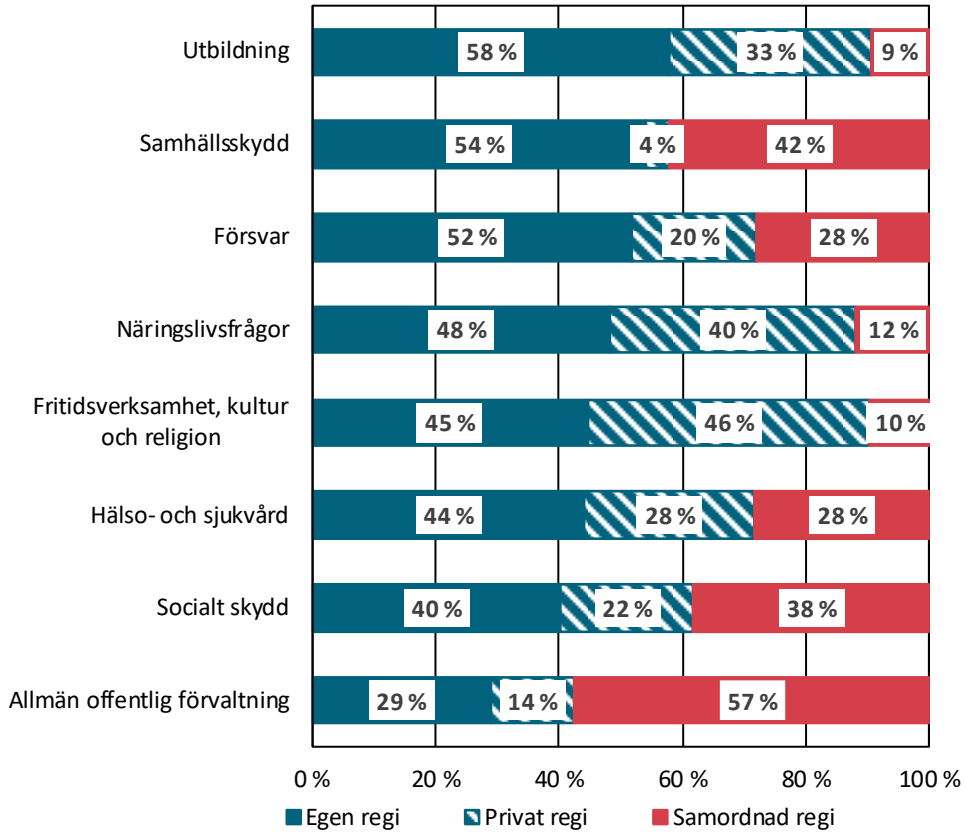

Källa: Statskontorets enkätundersökning 2025.

Tolkning: En myndighet med 500 anställda förväntas ha 52 procent av sin it-drift i egen regi om den inte är beredskapsmyndighet. En beredskapsmyndighet i samma storlek förväntas ha 66 procent i egen regi.

## Fördelning mellan driftsformer utifrån verksamhetsområde

I huvudrapporten framgåratt större myndigheter i genomsnitt har en större andel it-drift i egen regi i jämförelse med små myndigheter, och att beredskaps-myndigheter i genomsnitt har en större andel it-drift i egen regi i jämförelse med övriga myndigheter. Nedan delar vi upp myndigheterna verksamhetsområde (cofog) i stället. Vi kan se att det är utbildningsmyndigheter följt av myndigheter inom samhällsskydd och försvar som har högst andel it-drift i egen regi (figur B6). Vi kan också se att användningen av samordnad it-drift varierar mellan kategorierna – myndigheter inom allmän offentlig förvaltning samt samhällsskydd och socialt skydd använder samordnad drift i högst utsträckning.

**Figur B6.** **Myndigheternas uppskattade kostnader för it-drift fördelade på egen, privat respektive samordnad regi.**




Källa: Statskontorets enkätundersökning 2025.

Tolkning: Myndigheter inom allmän offentlig förvaltning har i genomsnitt 29 procent av sin it-drift i egen regi.

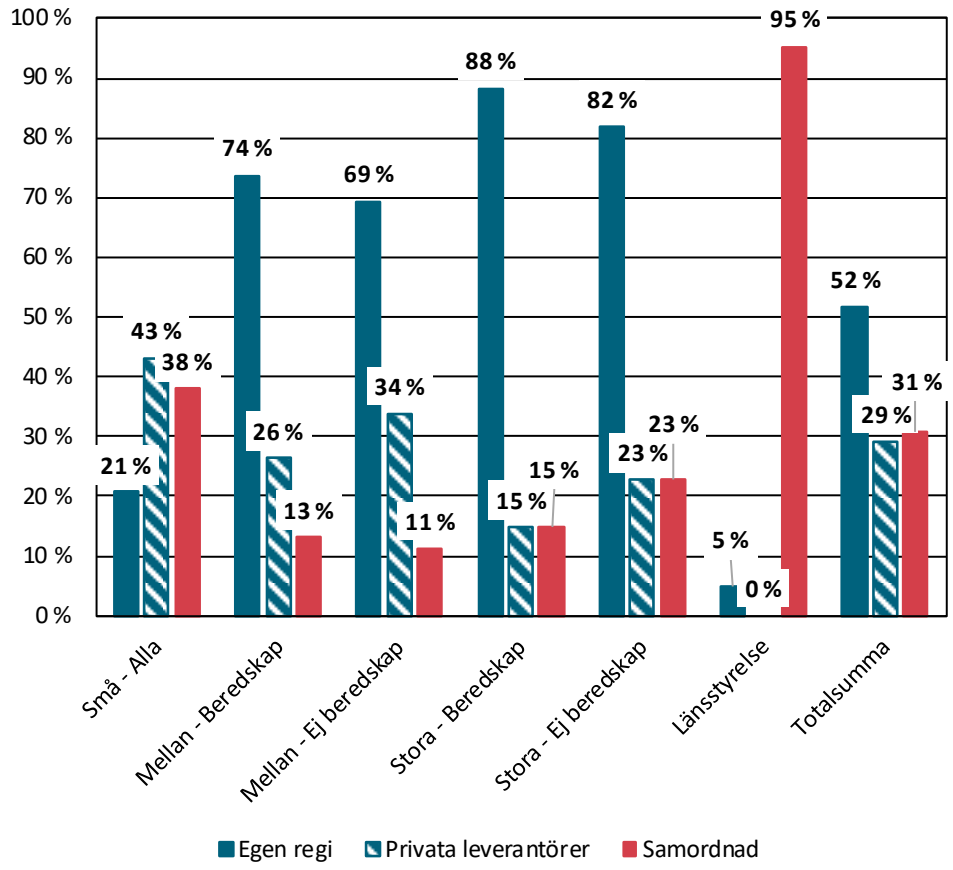
## Detaljerad analys per typ av it-driftstjänst

I huvudrapporten redovisar vi andelen av myndigheterna som har molntjänster i egen, privat respektive samordnad regi, uppdelat på typ av myndigheter. Här redovisar vi motsvarande resultat för datacentertjänster, nätverks- och kommunikationstjänster, applikationstjänster och support.

### Datacentertjänster

De flesta typer av myndigheter har datacentertjänster i egen regi (figur B7). Det är framför allt små myndigheter som har datacenter i privat eller samordnad regi.

**Figur B7.** **Andel av myndigheter som har datacentertjänster i egen, privat respektive samordnad regi, utifrån myndighetstyp.**

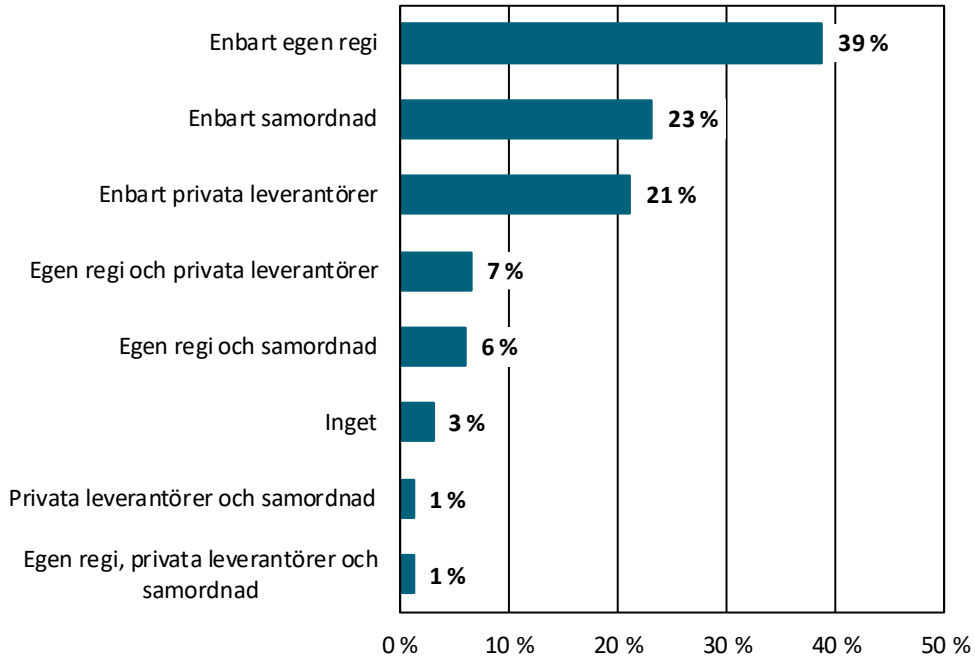



Källa: Statskontorets enkätundersökning 2025.

Tolkning: 21 procent av de små myndigheterna har datacentertjänster i egen regi.

Det är ovanligt att myndigheterna kombinerar driftsformer för datacenter (figur B8). 83 procent av myndigheterna kombinerar inte driftformer för datacenter. De undantag som finns består främst av myndigheter som har datacenter i egen regi *och* från privata leverantörer samt egen regi *och* samordnad regi.

**Figur B8.** **Andel myndigheter som har datacentertjänster i egen, privat respektive samordnad regi.**




Källa: Statskontorets enkätundersökning 2025.

Tolkning: 7 procent av myndigheterna har datacentertjänster både i egen och privat regi.

## Molntjänster

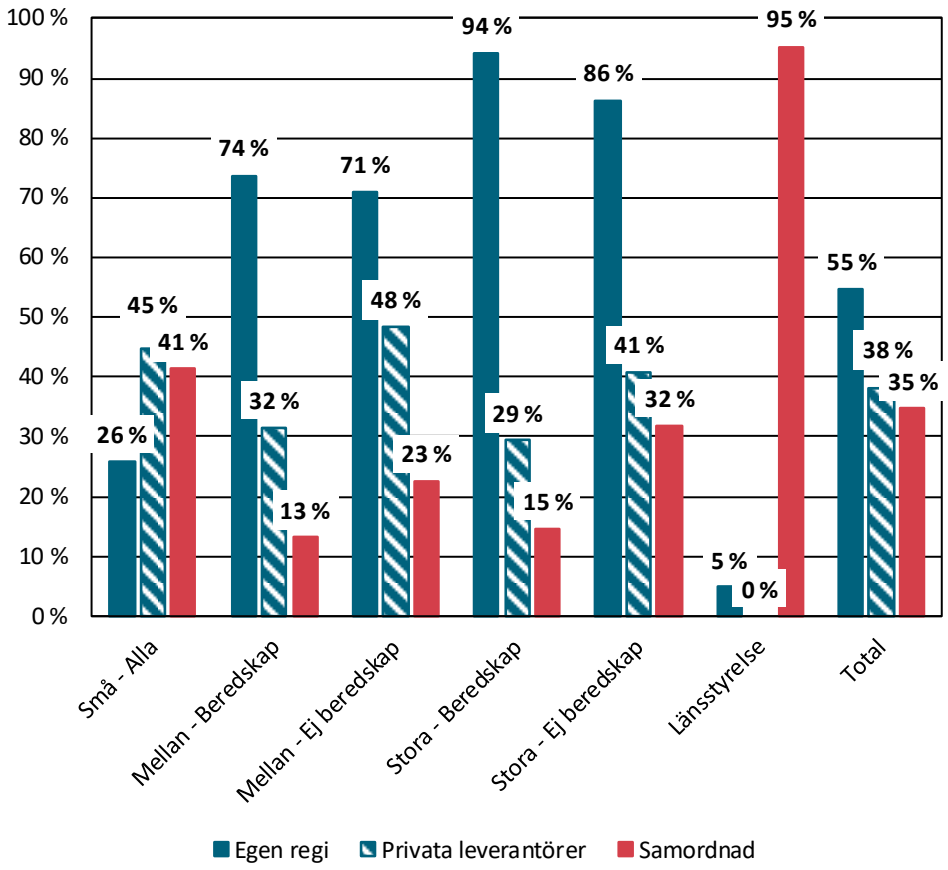
I huvudrapporten analyserade vi myndigheternas användning av olika typer av molntjänster i privat regi. Nedan beskriver vi det i större detalj.

Det finns alla typer av kombinationer när det kommer till hur myndigheterna använder sig av molntjänsttyperna IaaS, PaaS och SaaS från privata leverantörer. Det finns myndigheter som enbart har en av dessa typer av tjänster i stöd-verksamheten, eller i kärnverksamheten, myndigheter som kombinerar två av de olika typerna av tjänster på olika sätt i stöd- eller kärnverksamheten, samt myndigheter som har alla tre typerna av tjänster i både stöd- och kärnverksamheten. Det är vanligt att myndigheter kombinerar privat/partner/publikt/hybrid moln på samma sätt som för IaaS, PaaS och SaaS. Det vanligaste är dock att myndigheterna har en typ av moln (43 myndigheter) följt av två typer av moln (19 myndigheter) följt av tre typer av moln (16 myndigheter).

## Nätverks- och kommunikationstjänster

För de flesta typer av myndigheter är det vanligast att ha nätverks- och kommunikationstjänster i egen regi (figur B9). Det är framför allt små myndigheter och stora myndigheter som inte är beredskapsmyndigheter som använder sådana tjänster i samordnad regi. Det är inte så stora skillnader i användningen av nätverks- och kommunikationstjänster mellan i privat regi mellan myndighetstyperna.

**Figur B9.** **Andel av myndigheter som har nätverks- och kommunikationstjänster i egen, privat respektive samordnad regi, utifrån myndighetstyp.**



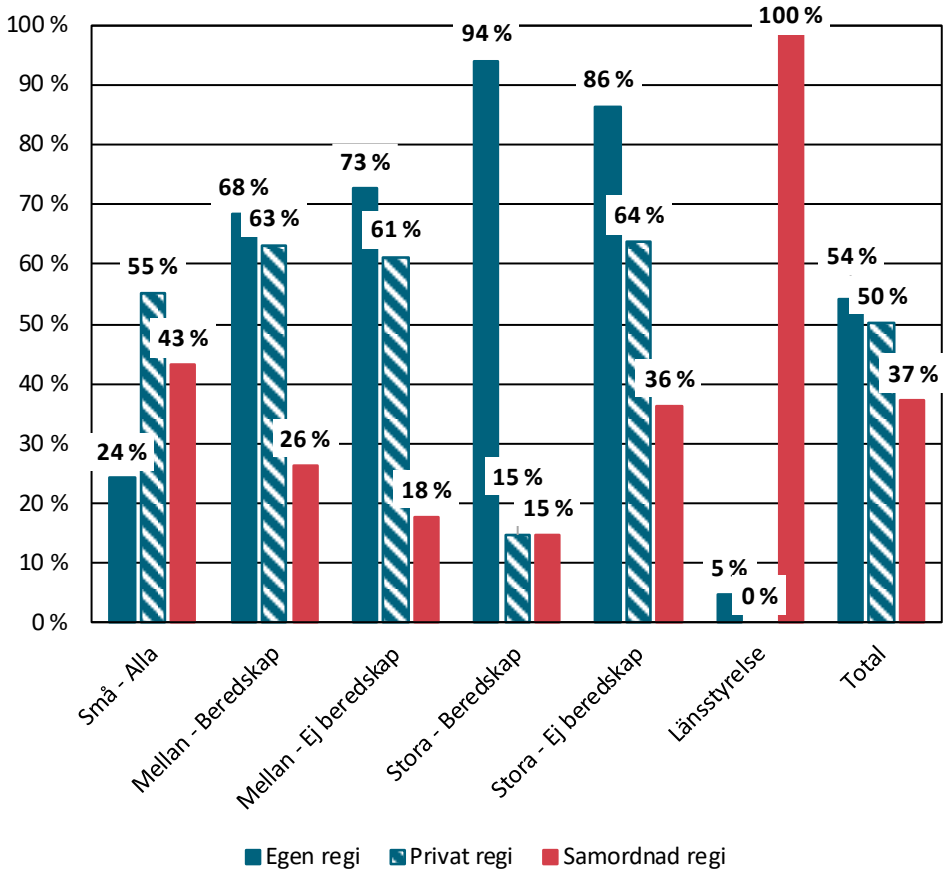

Källa: Statskontorets enkätundersökning 2025.

Tolkning: 26 procent av de små myndigheterna har nätverks- och kommunikationstjänster i egen regi.

## Applikationstjänster

Det finns ett positivt samband mellan storleken på myndigheten och andelen som har applikationstjänster i egen regi (figur B10). Applikationstjänster i samordnad regi är vanligast bland små myndigheter och stora myndigheter som inte är beredskapsmyndigheter.

**Figur B10.** **Andel myndigheter som har applikationstjänster i egen, privat respektive samordnad regi, utifrån myndighetstyp.**



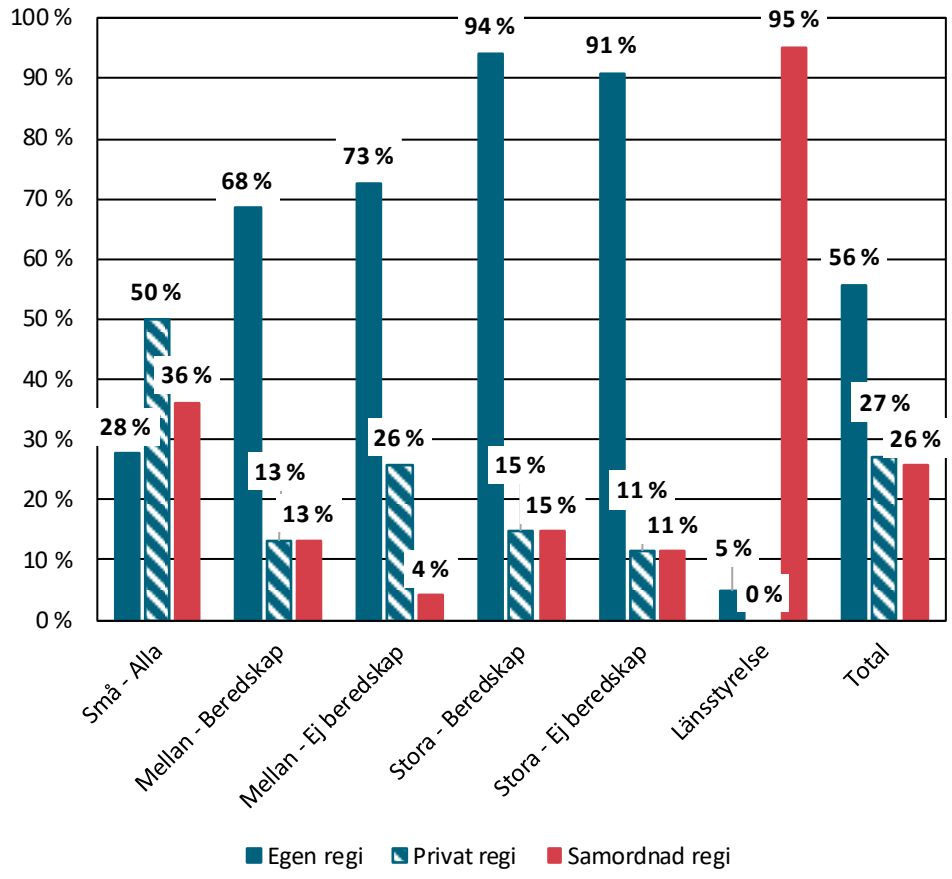

Källa: Statskontorets enkätundersökning 2025.

Tolkning: 24 procent av de små myndigheterna har applikationstjänster i egen regi.

## Supporttjänster

Även när det gäller supporttjänster finns det ett positivt samband mellan storleken på myndigheten och andelen supporttjänster i egen regi (figur B11). Det är vanligast bland små myndigheter att använda supporttjänster från privata leverantörer.

**Figur B11.** **Andel myndigheter som har supporttjänster i egen, privat respektive samordnad regi, utifrån myndighetstyp.**




Källa: Statskontorets enkätundersökning 2025.

Tolkning: 28 procent av de små myndigheterna har supporttjänster i egen regi.

# Metod för enkätundersökningen

## Svarsfrekvensen är hög i enkätundersökningen

Enkätundersökningen skickades ut under juni 2025 och var öppen till september 2025. Enkäten skickades till de 215 myndigheterna i den statliga redovisnings-organisationen varav 199 myndigheter (93 procent) besvarade enkäten i sin helhet. Enkäten skickades till myndigheternas registrator-mejl. Vi skickade under perioden då enkäten var öppen två påminnelser till de myndigheter som inte hade svarat på enkäten. Vi tog telefon- och mejlkontakt med merparten av de myndigheter som inte hade svarat på enkäten när sista svarsdatum började närma sig i syfte att svara på eventuella frågor om enkäten samt be myndigheten att svara på enkäten. Totalt kontaktade vi cirka 30 myndigheter på det sättet, varav de flesta också besvarade enkäten.

Kontakterna visade att det i huvudsak var interna oklarheter kring ansvaret för att besvara enkäten, eller långa interna beredningsprocesser, som var orsaken till att myndigheterna inte hade besvarat enkäten tidigare. Ett par myndigheter uppgav att de inte hade kapacitet eller prioriterade att besvara enkäten. Ingen myndighet uppgav att de avstod från att svara för att de bedömde att deras svar skulle vara säkerhetskänsliga.

### Enkäten var enkel att besvara

När vi ringde runt till myndigheter som inte hade svarat på enkäten passade vi också på att fråga myndigheterna om enkätens innehåll och varför de inte hade svarat ännu. Vi fick i de samtalen inga indikationer på att enkäten skulle vara svår att besvara eller att den är otydlig och så vidare. Vi fick ej heller några indikationer eller kommentarer om att myndigheten inte ämnar svara på enkäten då innehållet i svaren skulle kunna vara säkerhetskänsligt.

### Respondenterna behövde inte svara på alla frågor

Alla myndigheter svarade inte på alla frågor i enkätundersökningen då vi använde oss av aktiveringar av vissa frågor. Exempelvis fick respondenter som på fråga 1 (Har er myndighet någon it-drift i egen regi?) svarade ”Ja” inte besvara fråga 4 (Vilken typ av it-driftstjänster har ni i egen regi?) och så vidare. Alla fick dock besvara fråga 9 (Hur är er myndighets it-drift fördelad mellan olika driftsformer?) oavsett vad man svarat på tidigare frågor i enkäten.

### Resultaten bearbetades i vissa fall

De redovisade andelarna och antalen har bearbetats på ett sätt. Om det är minst en men färre än fem myndigheter som har besvarat en fråga på ett visst sätt redovisar vi antalet som 2,5 i stället för att redovisa det verkliga antalet 1,2,3 eller 4. Andelar följdändrades. Vi gjorde så för att kunna redovisa resultaten för samtliga frågor utifrån samma kategorier, utan att riskera att enskilda myndigheter går att identifiera. Om antalet är noll eller fem gjordes ingen bearbetning.

### Länsstyrelsernas svar hanterades i särskild ordning

Länsstyrelsen i Västra Götaland samordnar it-driften för samtliga länsstyrelser. Alla länsstyrelser förutom Västra Götaland har på grund av denna samordning klassats som användande av samordnad drift. På grund av det avvikande arrangemanget i förhållande till övriga myndigheter valde vi att redovisa länsstyrelserna i en egen kategori när resultat delas upp på myndighetskategorier. Länsstyrelserna hade annars hamnat i myndighetskategorin ”Mellan – Beredskap”. Vi har klassat alla länsstyrelser som svarande på enkäten, med förbehållet att länsstyrelsen i Västra Götaland besvarat på alla länsstyrelsers vägnar.

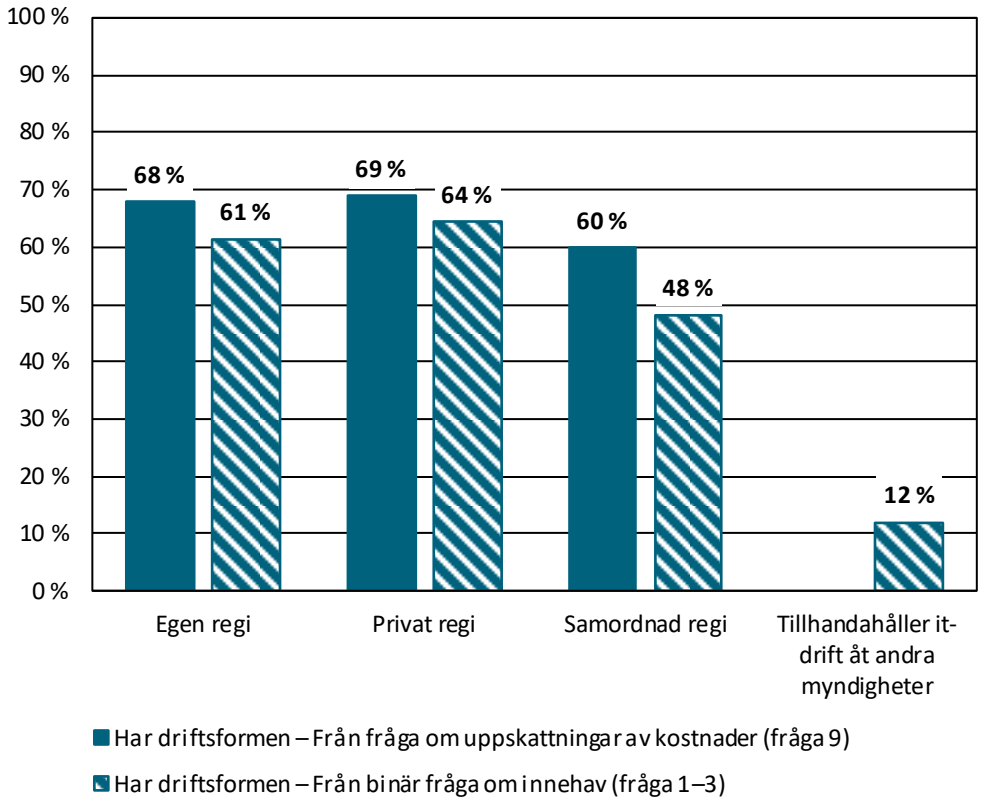
## Potentiellt motstridiga svar i enkäten

Vi ställde frågor huruvida myndigheten har it-drift i egen regi, från privata leverantörer eller om någon annan myndighet hanterar hela eller delar av deras it-drift (frågorna 1–3). Denna redovisas i figur 2 i huvudrapporten. Denna fråga var binär, det vill säga man kunde svara ja eller nej för respektive kategori.

Det finns en liten skillnad mellan utfallet av den frågan och frågan där myndigheterna ombeds uppskatta andelen av deras kostnader som går till de olika driftsformerna (fråga 9). Exempelvis finns det respondenter som svarat att de inte har it-drift i egen regi, men att en andel större än noll av kostnaderna går till it-drift i egen regi. Vi har kontaktat ett antal myndigheter som svarat på ett sådant sätt. En myndighets förklaring till detta är att myndigheten inte driftar något själva men att de har anställda som arbetar med att ställa krav mot leverantörer och liknande och stöd internt. Där angavs att myndigheten inte har drift i egen regi och att en andel större än noll av kostnaderna gick till drift i egen regi. En annan myndighet uppgav att de hade problem med att kategorisera en viss server-lösning. En annan myndighet lät ägandeskapet av hårdvaran vara vägledande när frågan om drift i egen regi skulle besvaras.

Diskrepansen som uppstår i myndigheternas svar framgår i figur B12. Vi kan se att skillnaderna är relativt små. Vi visar denna skillnad för att förklara skillnader mellan figurer som går att identifiera i huvudrapporten.

**Figur B12.** **Skillnad i utfall mellan fråga där andel av kostnader för it-drift skattades och fråga som besvarades ja eller nej.**




Källa: Statskontorets enkätundersökning.

Not: En myndighet har respektive driftsform om den uppskattade kostnaden för driftsformen är större än noll.

# Enkäten i sin helhet

## Missiv i mejl till registrator

Statskontoret har i regeringsuppdrag att kartlägga hur de statliga myndigheterna organiserar sin it-drift. Här kan du läsa mer om uppdraget: Uppdrag till Statskontoret att skapa förutsättningar för en effektiv uppföljning av den statliga it-driften – Regeringen.se.

Den här enkätundersökningen är en del i vår kartläggning. Du som svarar behöver ha god kännedom om hur myndigheten har organiserat sin it-drift. Vi tänker att du till exempel är it-chef eller liknande på myndigheten. Använd gärna PDF-filen nedan för att inhämta nödvändig information från kollegor men låt en person ansvara för att fylla i själva enkäten. Enkäten behöver inte besvaras i ett svep, svar sparas vid varje sidbyte i enkäten. Om du vill få en överblick över enkätfrågorna kan du ladda ner en PDF-kopia av enkäten här.

Vi är mycket tacksamma om ni vill besvara vår enkät. Vi behöver dina svar senast den 29 augusti. Undersökningen består av maximalt 10 frågor.

Myndighetens svar blir allmän handling och utgör underlag till den rapport som vi publicerar senast den 30 november 2025. Vi kommer att sammanställa resultaten och redovisa dem på en övergripande nivå. Det kommer därför inte gå att urskilja enskilda myndigheters svar i rapporten.

## Missiv i enkätverktyget

Statskontoret har i regeringsuppdrag att kartlägga hur de statliga myndigheterna organiserar sin it-drift.

Den här enkätundersökningen är en del i vår kartläggning. Du som svarar behöver ha god kännedom om hur myndigheten har organiserat sin it-drift. Vi tänker att du till exempel är it-chef eller liknande på myndigheten. Använd gärna PDF-filen nedan för att inhämta nödvändig information från kollegor men låt en person ansvara för att fylla i själva enkäten. Enkäten behöver inte besvaras i ett svep, svar sparas vid varje sidbyte i enkäten.

*Med it-drift avser vi den löpande hanteringen och underhållet av hårdvara som servrar och datorer, samt mjukvara som datorprogram och operativsystem. Det inkluderar it-tjänster som t.ex. datacentertjänster, molntjänster, nätverks- och kommunikationstjänster, applikationstjänster, supporttjänster och livscykelhantering av dessa.*

## 1. Har er myndighet någon it-drift i egen regi?

*Med egen regi avser vi verksamhet i egna lokaler där ni äger utrustningen och använder egen anställd personal eller konsulter som ni arbetsleder på plats i egna lokaler.*

- O Ja
- O Nej
- O Vet ej

## 2. Har er myndighet någon it-drift utkontrakterad till privata leverantörer?

*Med utkontraktering avser vi att en myndighet genom offentlig upphandling eller på något annat sätt uppdrar åt en privat leverantör att hantera hela eller delar av sin it-drift.*

- O Ja
- O Nej
- O Vet ej

## 3. Har er myndighet samordnat någon del av er it-drift med en annan/andra myndigheter?

Du kan välja flera svarsalternativ.

- ☐ Ja, en annan myndighet hanterar hela eller delar av vår it-drift
- ☐ Ja, vår myndighet hanterar hela eller delar av en annan/andra myndigheters it-drift
- ○ Nej
- ○ Vet ej

## 4. Vilken typ av it-driftstjänster har ni i egen regi?

Du kan välja flera svarsalternativ.

- ☐ Datacentertjänster
- ☐ Molntjänster
- ☐ Nätverks- och kommunikationstjänster
- ☐ Applikationstjänster
- ☐ Supporttjänster
- ☐ Annan/andra tjänster
- ○ Vet ej

## 5. Vilken typ av it-driftstjänster har ni utkontrakterat till privata leverantörer?

Du kan välja flera svarsalternativ.

- ☐ Datacentertjänster
- ☐ Molntjänster
- ☐ Nätverks- och kommunikationstjänster
- ☐ Applikationstjänster
- ☐ Supporttjänster
- ☐ Annan/andra tjänster
- ○ Vet ej

## 6. Vilken typ av it-driftstjänster har ni samordnat med en annan myndighet?

Du kan välja flera svarsalternativ.

- ☐ Datacentertjänster
- ☐ Molntjänster
- ☐ Nätverks- och kommunikationstjänster
- ☐ Applikationstjänster
- ☐ Supporttjänster
- ☐ Annan/andra tjänster
- ○ Vet ej

## 7. Vilken typ av molntjänster från privata leverantörer använder ni?

*Med **kärnverksamhet** avser vi verksamheten som utgår från myndighetens instruktion, regleringsbrev eller motsvarande.*
*Med **stödverksamhet** avser vi till exempel ekonomi- och löneadministration, bokningssystem, friskvårdssystem och liknande.*

Du kan välja flera svarsalternativ

| | Ja, i kärnverksamheten | Ja, i stödverksamheten | Nej | Vet ej |
|---|---|---|---|---|
| Infrastruktur som en tjänst (IaaS) | ☐ | ☐ | ○ | ○ |
| Plattform som en tjänst (PaaS) | ☐ | ☐ | ○ | ○ |
| Mjukvara som en tjänst (SaaS) | ☐ | ☐ | ○ | ○ |

## 8. Vilken **typ av moln** från privata leverantörer använder ni?

*Med **kärnverksamhet** avser vi verksamheten som utgår från myndighetens instruktion, regleringsbrev eller motsvarande.*
*Med **stödverksamhet** avser vi till exempel ekonomi- och löneadministration, bokningssystem, friskvårdssystem och liknande.*

Du kan välja flera svarsalternativ

| | Ja, i kärnverksamheten | Ja, i stödverksamheten | Nej | Vet ej |
|---|---|---|---|---|
| Privat moln, som bara vår myndighet har tillgång till | ☐ | ☐ | ○ | ○ |
| Partnermoln/gruppmoln, som bara specifika organisationer har tillgång till | ☐ | ☐ | ○ | ○ |
| Publikt moln, som är potentiellt tillgängligt för alla organisationer | ☐ | ☐ | ○ | ○ |
| Hybridmoln, som är en kombination av minst två övriga molntyper | ☐ | ☐ | ○ | ○ |

## 9. Hur är er myndighets it-drift fördelad mellan olika driftsformer?

Uppskatta hur stor andel av kostnaderna för er myndighets it-drift som avser drift i egen regi, drift som är utkontrakterad till privata leverantörer, respektive drift som är samordnad med och hanteras av en annan/andra myndigheter. Vi har förståelse för om ni inte har exakta siffror på detta, men ber er uppskatta så gott ni kan.
**Har ni enbart en driftsform ange 100.**

| Driftsform | Procent av kostnaderna |
|---|---|
| Egen regi | |
| Utkontrakterad till privata leverantörer | |
| Samordnad med en annan/andra myndigheter | |

10. Här kan du lämna andra kommentarer om myndighetens it-drift som du vill skicka med till Statskontoret i arbetet med uppdraget