

Regeringen
Infrastrukturdepartementet

Yttrande över SOU 2021:97 – Slutbetänkande av ”Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift”.

Dnr I2021/03265

Sammanfattning

Statens Skolverk (Skolverket) yttrar sig härmed över It-driftsutredningens slutbetänkande. Synpunkterna som lämnas har avgränsats med hänsyn till Skolverkets kompetens och uppdrag.

Skolverkets synpunkter

Inledning

Skolverket tillstyrker generellt slutbetänkandet i sin nuvarande form. Så som kundmyndighet identifierar Skolverket ett antal utmaningar som kommer belysas i våra kommentarer och synpunkter. Skolverket önskar förtydliganden och ändringar gällande dessa kommentarer och synpunkter.

Generella kommentarer

Skolverket hänvisar till vårt remissyttrande i tidigare betänkande av detta uppdrag SOU 2121:1. Dessa remissvar är fortfarande aktuella.

Alla av Skolverkets yttranden, samt tillstyrkande, baseras på att anslutningen till den samordnade statliga IT-driften ska vara frivillig, nu och i framtiden.

Slutbetänkandet beskriver omfattande om VAD man vill åstadkomma, men väldigt lite HUR det samordnade statliga tjänsteutbudet ska hanteras. Skolverket har därför svårt att ha en tydlig uppfattning om förslagen är bra eller inte. Ett

exempel är att det inte framgår hur infrastrukturmiljön ska separeras för de olika kundmyndigheterna hos leverantörsmyndigheterna. Enligt detta förslag är det svårt för Skolverket att ge förslag på förbättringar av lösningarna, eftersom inga lösningar är beskrivna i förslaget.

Ett exempel är beskrivningen i kapitel 11 som ger slutsatsen att den samordnande statliga IT-driften ska organiseras på ett sådant sätt att den erbjuder myndigheter en "en-väg-in"-lösning. Vår uppfattning är att utredningen har avgränsat sig i sitt förslag till att endast hantera detta i anslutningsförfarandet. Men det är troligtvis den minsta och tidsmässigt kortaste fasen i samarbetet mellan kundmyndighet och leverantörsmyndighet. Den stora och långa utmaningen består i det långa samarbete och partnerskap som myndigheterna ingår i samband med en överenskommelse. Här blir det sannolikt inte en "en-väg-in"-lösning, utan kundmyndigheten måste samarbeta med flera myndigheter, beroende på vem som levererar tjänsten, dvs en "flera-vägar-in"-lösning.

Hur överenskommelserna/IT-förvaltningen ska hanteras och regleras i förlängningen framgår inte av slutbetänkandet och Skolverket uppmanar till ett förtydligande av detta.

Kapitel " Förslag till varaktiga former för samordnad statlig it-drift"

Det finns generell en risk förenad med att samordna it-drift. Det finns alltför många exempel där en störning i anläggningar där it-drift samordnats som medfört att ett stort antal samhällsfunktioner slagits ut genom samma störning. Utredningen lyfter denna risk, men den ska inte underskattas. Den föreslagna lösningen kommer vara än mer riskfylld, då de störningar som kan uppstå har potential att påverka och störa hela statsförvaltningen. Den mitigerande åtgärden att låta olika myndigheter leverera behöver riskbedömas, och den centrala frågan är vilken instans som ska ta ansvar för den aggregerade risken? Ska sammanfattningens skrivning "Försvarsmakten ska få i uppgift att samråda med den samordnande myndigheten i frågor om Sveriges säkerhet kopplade till den samordnade statliga it-driften." tolkas som att det är FM och inte SÄPO som ska svara för detta? FM är inte uppräknad som en av de stöd- och expertmyndigheter som ska stödja.

Kapitel "Utgångspunkter och principer för varaktiga former för samordnad statlig it-drift"

Säkerhet

Att hantera säkerhetsskyddsklassade uppgifter utanför tjänsteutbudet kan innebära att kundmyndigheten trots allt måste ha en egen infrastruktur, med ett stort eget utbud av tjänster. Detta leder till att den effektivitet som eftersträvas kan gå åt motsatt håll, dvs vi betalar för en dubbel infrastrukturell uppsättning, vår egen

infra för säkerhetsskyddsklassade data samt avgift till leverantörsmyndighet för resterande del.

Kapitel 1.1

12 §

"Anslutning till det samordnande statliga tjänsteutbudet ska ske via överenskommelse". Skolverket anser att en sådan överenskommelse ska fastställas i ett leveransavtal mellan leveransmyndighet och kundmyndighet samt med inrättande av SLA (Service Level Agreement) för den levererande tjänsten. Anledningen är att det ska finnas en säkerhet för kundmyndigheten att kunna garantera it-leveranserna mot sin interna verksamhet. Risk finns att små kundmyndigheter annars prioriteras ner till förmån för större myndigheter i händelse av att tjänsten inte fungerar som det ska, t ex i incidentsituationer.

18 §

Även de anslutande kundmyndigheterna bör lämna underlag till lägesbeskrivningen, eftersom det är hos kundmyndigheten upplevelsen och leveransen kan verifieras.

Kapitel 2.3.2

Utredningen nämner i ett antal avsnitt arbete med riskanalyser. På samma sätt som med informationsklassificering vore det en stor fördel om myndigheter som önskar vara kundmyndigheter kunde genomföra och redovisa en riskanalys enligt en utarbetad metod inklusive metodstöd. Erfarenheten av hur riskanalyser genomförs visar att kvalitén och djupet i analyserna skiftar kraftigt. Det vore därför av stort värde för leverantörsmyndigheter att få ett enhetligt underlag när nya kunder önskar ansluta.

Skolverket anser att MSB mest lämpad att ta fram nämnda metodbeskrivningar och stödmaterial kopplade till dessa.

Kapitel 3.3.3

I kapitlet identifieras de tillkommande beredskapsområdena där skola och förskola ingår. Detta är Skolverkets ansvarsområden och innebär att den finns en möjlighet att myndigheten inom kort blir en beredskapsmyndighet med allt vad det innebär. Beredskapsområdena föreslås ingå i den sammanhängande planering som MSB och Försvarmakten ska hålla samman, och det kommer innebära tillkommande särskilda utmaningar för myndighetens informationshantering och infrastruktur som vi inte vidare utreder i detta yttrande.

Kapitel 3.3.4

Utredningens skriver att det är viktigt att statliga myndigheters deltagande i en samordnad statlig it-drift inte påverkar skyddet av aktörers förmåga att planera inför samt utföra sina uppgifter under höjd beredskap och då ytterst krig. I ljuset av den ökade satsningen på totalförsvaret kommer detta omfatta allt fler myndigheter. Hur ska kravet om förfogande tillgodoses? En sådan skrivning kan komma att diskvalificera utländska leverantörer och skulle med stor sannolikhet kunna medföra ett krav på att informationen behandlas inom landets gränser för att garantera tillgänglighet.

Kapitel 6.7

Ett centralt syfte med en samordnad statlig it-drift är att bidra till ökad informationssäkerhet i den statliga förvaltningen. Samtidigt slår utredningen fast att det är oklart i vilken utsträckning Försäkringskassan har bidragit till att öka myndigheternas informationssäkerhet. Detta pekar på att ett annat angreppssätt behövs för att nå det uppsatta målet. De brister i transparens och insyn som lyfts vid FK:s drift behöver hanteras bättre i en större lösning.

Kapitel 9

Skolverket instämmer i att det finns stöd för antagandet att uppdraget inte måste följa av en överenskommelse mellan parterna för att 2 kap. 13 § första stycket TF ska vara tillämplig, utan att det även kan grundas på en författningsreglering. Skolverket finner att det finns behov att som kundmyndighet kunna försäkra sig om att undantaget i 2 kap 13 § TF är tillämpligt och inte endast lita sig mot överenskommelser.

En myndighet har ett ansvar att hantera sina allmänna handlingar, arbetsmaterial eller upptagningar på ett korrekt sätt. Myndigheten kan inte undkomma detta ansvar genom att utkontraktera driften av de IT-system där myndigheten hanterar dessa informationstillgångar.

Försäkringskassan har bedömt att undantaget är tillämpligt på ett övergripande plan avseende de uppgifter som hanteras för kundmyndigheternas räkning. Försäkringskassan har dock inte inom det existerande uppdraget utrett i vilken omfattning undantaget är tillämpligt i förhållande till de enskilda tjänster som ingår i leveransen till respektive kundmyndighet.

Att försäkra sig om att ett uppdrag faller in under 2 kap 13 § TF kan sannolikt bli en utmaning för en kundmyndighet som endast har att förlita sig på en överenskommelse med leverantör. Skolverket hade gärna sett att det låg inom leverantörmyndighets uppdrag att vidta sådana åtgärder att undantaget blir tillämpligt. Utöver ansvaret för myndigheter att hantera sina allmänna handlingar ligger även ansvaret för hanteringen av personuppgifter vilket också kan påverkas av om undantaget i 2 kap 13 § TF är tillämpligt.

En förutsättning för att kunna agera som personuppgiftsbiträde är att man i sin biträdesroll kan ta emot instruktioner från den personuppgiftsansvarige. Rollen som personuppgiftsbiträde innebär att handlingsutrymmet för vilka behandlingar som är tillåtna är begränsade till vad som anges i personuppgiftsbiträdesavtalet. En leverantörsmyndighet kan knappast vilja agera som personuppgiftsbiträde om det inte är fastställt att behandlingen endast innebär teknisk bearbetning eller teknisk lagring för annans räkning.

Om så är fallet är inte beroende av vad de två myndigheterna har överenskommit sinsemellan utan vilka tekniska och administrativa begränsningar för åtkomst som har vidtagits. Vid en eventuell begäran om att få del av till exempel de personuppgifter som behandlats, är respektive part skyldig att göra en självständig sekretessprövning av uppgifterna, 2 kap 17 § TF. Ansvar att genomföra en sekretessprövning kan inte överlåtas på en annan part och kräver en självständig kontroll över uppgifterna.

Oaktat vad som överenskommit mellan de två myndigheterna är leverantörsmyndigheten skyldig att lämna ut uppgifter om de är att anses som handlingar i enlighet med 2 kap 4 § tryckfrihetsförordningen (1949:105), TF. Detta omfattar även överlämnade personuppgifter. Om leverantörsmyndigheten inte endast innehar uppgifterna för teknisk bearbetning och lagring är de vidare skyldiga att följa arkivbestämmelser och regelverk om diarieföring. De utgör också den myndighet som anses förvara inkomna uppgifter enligt 2 kap 6 § TF. Det kan, under sådana förutsättningar, ifrågasättas om leverantörsmyndigheten verkligen är att betrakta som ett personuppgiftsbiträde i den allmänna dataskyddsförordningens bemärkelse. Leverantörsmyndigheten kan i en sådan situation inte försäkra att personuppgifterna endast kommer att behandlas för det ursprungligt angivna ändamålet, som bestäms av personuppgiftsansvarige.

Kapitel 10

Generellt anser Skolverket att en överenskommelse utan tydliga och rättsliga krav, förväntningar och konsekvenser inte är tillräckligt starkt för att kunna säkerställa en rättvis och stabil planering och prioritering av tjänsteleveranser i en gemensam samverkan av IT-drift i staten.

Kapitel 10.2

Det finns många intressenter (kundmyndigheter) med olika behov och olika förutsättningar, som troligtvis erbjuds lösningar som ska vara standardiserade och passa alla. Att lösningarna är flexibla utifrån de olika behoven av säkerhet, tillgänglighet och snabbhet är av stor vikt och Skolverket uppmanar till att utredningen föreslår detta i sitt slutbetänkande.

Tjänsteutbudet och arbetsformerna bör vara utformade för att stödja moderna utvecklingsmetoder och t ex DevSecOps i syfte att främja snabbhet/agilitet/säkerhet i systemutvecklingsprocessen för myndigheten.

10.2.1

Risk att det blir en "IT-avdelning inom IT-avdelningen" som levererar tjänsterna till andra myndigheter, vilket medför en mindre effektivisering än vad som eftersträvas.

Förslagsvis bör instruktionen till leverantörsmyndigheten fastställa att leveransen till kundmyndigheten ska prioriteras. T ex "Myndigheten ska inom ramen för sin IT-infrastrukturverksamhet utföra uppdrag åt andra myndigheter. Myndigheten ska prioritera dessa uppdrag för andra myndigheter"

10.4.1

Med flera levererande parter av infrastruktur, samtidigt som kundmyndigheten avvecklat sin egen organisation för infrastruktur och drift, så finns det en utmaning i supportfrågor. Andra- och tredje linjens support kommer att hanteras av multipla leverantörer (olika leveransmyndigheter och privata aktörer) vilket skapar en risk att det inte finns någon part med kundmyndighetens helhetssyn och helhetsförståelse för verksamhetsprocess, tekniska beroenden inom infrastrukturen, supportprocess, samarbetsformer, etc. Detta kan leda till stora problem med problemlösning. Skolverket uppmanar utredningen att beskriva dessa typer av scenarios, processer och organisationsformer tydligare.

10.4.3

Informationsteknik är i ständigt utvecklande fas. Att utgå endast från "befintlig förmåga" kan medföra att teknisk skuld med ålderstigna lösningar levereras. Skolverket föreslår att det ska tydliggöras att leveransmyndigheterna ska säkerställa framdrift i teknikutvecklingen och erbjuda framtidssäkrade tjänstenivåer till kundmyndigheterna.

10.5.1

Skolverket anser att en sådan överenskommelse ska fastställas i ett tydligt leveransavtal mellan leveransmyndighet och kundmyndighet samt med inrättande av SLA (Service Level Agreement) för den levererande tjänsten. Anledningen är att det ska finnas en säkerhet för kundmyndigheten att kunna garantera it-leveranserna internt.

En anslutning till statens tjänsteutbud är ett mycket omfattande beslut för många myndigheter, vilket påverkar personal, organisation, budget, kompetenser, processer, etc. Om det inte finns en stark förpliktelse för leveransmyndigheten att

fullfölja överenskommelsen så är risken att få myndigheter vågar ansluta sig till tjänsteutbudet.

Kundmyndigheterna måste även ha en möjlighet att säga upp överenskommelsen/avtalet med leveransmyndigheten och träda ur anslutningen om kvaliteten av tjänsten inte lever upp till de servicenivåer som överenskommit. I annat fall riskerar kundmyndigheternas verksamhet och uppdrag att misslyckas. Vid avslutande av överenskommelsen måste kundmyndighetens information och data hålla samma kvalitet som vid ingången i överenskommelsen.

Kapitel 10.6

Utredningen lyfter perspektiv kring ett stärkt civilt försvar och den samordnade it-driftens roll i detta. Detta kan komma att ställa specifika krav enligt Skolverkets kommentarer för kapitel 3. Om statliga aktörer måste ha rådigheten över det samordnade statliga tjänsteutbudet innebär även det särskilda krav på leverantörerna.

Notera även att det är FM som ska vara rådgivande myndighet och inte Säkerhetspolisen trots att den samordnade it-driften inte ska hantera säkerhetsskyddsklassificerad information.

10.6.4

Viktigt att det finns ett tydligt samarbete mellan alla levererande myndigheter då flera tjänster kan ha påverkan på varandra. Det måste då säkerställas en gemensam CAB (Change Advisory Board) där man synkroniserar förändringar i infrastrukturen och tar upp beroenden och risker med dessa förändringar.

Kapitel 11

För tydlighetens skull bör målformuleringen separera benämningen "säkerhet" till "driftsäkerhet" (dvs tillgänglighet av tjänster) och "IT-säkerhet" (dvs skydda myndighetens IT-tillgångar) samt "Informationssäkerhet" (dvs skydda och hantera myndighetens information och data (tillgänglighet, riktighet, sekretess)).

För att organisera en samordnad statlig it-drift föreslås inblandning av en stor mängd statliga aktörer enligt följande:

Den samordnande myndigheten föreslås bli DIGG.

Leverantörsmyndigheter föreslås bli Försäkringskassan, Lantmäteriet, Skatteverket och Trafikverket.

Stöd- och expertmyndigheter föreslås bli Integritetsskyddsmyndigheten, Myndigheten för samhällsskydd och beredskap, Säkerhetspolisen och de länsstyrelser som är tillsynsmyndigheter enligt säkerhetsskyddslagen samt Upphandlingsmyndigheten.

Kammarkollegiet ska få i uppgift att samverka med den samordnande myndigheten om upphandling av ramavtal.

Försvarsmakten ska få i uppgift att samråda med den samordnande myndigheten i frågor om Sveriges säkerhet.

Det finns en uppenbar risk att man i och med den föreslagna organisationen bygger in en tröghet och skapar svårigheter att över tid kunna erbjuda en effektiv och säker samordnad drift. Myndighetssamverkan har till exempel inom informationssäkerhetsområdet inte alltid uppnått ställda förväntningar, något som också framskymtar i utredningen.

Kapitel 11.2

Utredningens förslag på organisering bygger på samverkan. En utmaning med denna form för organisering är att tydliggöra roller, ansvar och beslutsmandat. Det är en utmaning om ansvaret för informationen samtidigt ligger kvar hos kundmyndigheten, men denna inte kan påverka leverantörsmyndigheternas utbud. Den samordnande myndigheten behöver besitta mycket kompetens för att kunna fungera som stöd åt hela statsförvaltningen vad gäller it-drift. Om stödet ska vara som omfattande som det beskrivs i 11.3 och innefatta informationskartläggning och informationsklassning behövs resurser. Idag svarar MSB för metodstöd i dessa frågor, och det är olyckligt om en ny myndighet ska överta MSBs inarbetade roll i detta.

Kapitel 11.10.1

Rätt säkerhet för informationen i samordnad drift

Utredningen lyfter på flera ställen problemet med bristande arbete med informationsklassificering. Utredningen föreslår också att DIGG ska stödja

myndigheterna i deras arbete med informationskartläggning och informationsklassificering.

Det finns en risk att lägga ansvaret för informationsklassningen på DIGG. Myndigheten för samhällsskydd och beredskap (MSB) har sedan länge utfärdat föreskrifter om informationssäkerhet för statliga myndigheter (senaste gången genom MSBFS 2020:6). I dessa föreskrifter ingår avsnitt om informationsklassificering. Det vore därför mest ändamålsenligt att låta MSB fortsättningsvis förskriva om detta och inte splittra det på flera myndigheter. I kapitel 1.5 föreslås en förändring i MSBs instruktion så att MSB ska samverka med DIGG avseende stöd till statliga myndigheter i frågor om informationssäkerhet. Detta kan innebära att avståndet mellan MSB och myndigheter ökar inom ett område där snarare närhet och gemensam utveckling är att föredra.

För att få en samordnad, nationell bedömningsgrund bör MSB även åläggas att komplettera sina föreskrifter med en bedömningsskala. Med en sådan skala som grund ges förutsättningar för att de olika myndigheternas bedömning när det gäller klassning kan ensas och den information som tas in i samordnad it-drift därmed ges rätt skydd. Rätt skydd för informationshanteringen innebär också att samhället i den samordnade it-driften inte onödigtvis överinvesterar i säkerhet för information som klassats i nedre delen av bedömningsskalan.

Kapitel 12.2.1

Berörda företag, branscher m.m anges att ”Kammarkollegiets nuvarande ramavtal för it-drift omfattar 13 tjänsteleverantörer” men för den programvara som Skolverket avropar används ofta ramavtalen för Programvaror och tjänster samt ramavtalet för Kommunikationslösningar. I dessa avtal kan även drift kan avropas. Till dessa ramavtal finns en stor mängd underleverantörer knutna. Det finns alltså ett brett och livskraftigt nät av leverantörer och underleverantörer som har upparbetats under en längre tid. Leverantörerna har anpassat sin affärsverksamhet specifikt till upphandlande myndigheters krav och behov. Vår bedömning är att leverantörers intresse för att upprätthålla en marknad med specifikt fokus på statliga myndigheter kommer att minska avsevärt om en samordnad statlig it-drift genomförs och att det finns en uppenbar risk att detta kommer att utarma och på sikt eliminera denna marknad. I förlängning kommer det att innebära att möjligheterna att upphandla dessa tjänster i konkurrens kommer att begränsas

Kapitel 12.4.3

Utredningen skriver: ”Om en myndighet som har drift i egen regi väljer att ansluta sig skulle det kunna bli aktuellt med avveckling av den interna it-driftsorganisationen.” Detta är bara möjligt i de fallen till exempel säkerhetsskyddsklassificerad information inte förväntas hanteras i tekniska

miljöer på myndigheten. Det kan också innebära en försämrad beställarkompetens på den enskilda myndigheten.

På Skolverkets vägnar

Enhetschef Infrastruktur och plattform Eric Markström

Handlingen är beslutad i Skolverkets
elektroniska ärende- och
dokumenthanteringssystem av:
Claes-Håkan Johansson
(Avdelningschef) den 2022-03-10.

I ärendets slutliga handläggning har även verksjuristen Nina Isaksson, CISSP Eva Hyenstrand, upphandlare Nils-Erik Sandberg, samt enhetschefen Eric Markström (föredragande) deltagit.