I skärningspunkten mellan

datastyrning, molntjänster och cybersäkerhet

KPMG Sverige

Juni 2026

Förord

Den digitala utvecklingen inom offentlig sektor erbjuder många möjligheter, men även komplexa avvägningar. Krav på effektivisering, samverkan och utveckling sammanfaller med ett växande behov av säkerhet, integritetsskydd och robusthet.

Vi genomförde denna studie med bakgrund i de problem som våra kunder inom offentlig sektor möter idag. Ambitionen med studien är att bidra till ökad förståelse för hur offentlig sektor kan navigera i gränslandet mellan datastyrning, molntjänster och cybersäkerhet. Vi tar utgångspunkt i offentlig sektors tvetydiga behov att dela, modernisera samtidigt som data behöver skyddas.

Genom intervjuer och enkätundersökning med myndigheter belyser studien gemensamma mönster, utmaningar och mognadsgrader. Syftet är att synliggöra hur dessa tre områden hänger samman och dess påverkan på varandra, istället för att peka ut enskilda lösningar.

Vår förhoppning är att detta underlag ska fungera som ett stöd i fortsatt dialog, reflektion och utveckling kring hur offentlig sektor kan stärka sin förmåga att fatta informerade, säkra och långsiktiga beslut i en tid av förändring.

Per Wennström
Director, Management
Consulting Public Sector
KPMG Sweden

Sammanfattning

Studien visar att offentlig sektor befinner sig i en komplex styrningssituation där kraven på att dela, modernisera och skydda data behöver hanteras samtidigt. Analysen av datastyrning, molntjänster och cybersäkerhet visar att områdena är sammanlänkade med varandra. Hur väl offentlig sektor fungerar inom ett område påverkar förutsättningarna inom de andra områdena.

Resultaten pekar på att datastyrning generellt uppvisar en låg mognadsgrad inom offentlig sektor. Brister i tydliga roller, processer, datamodeller och strukturer för datakvalitet leder till fragmenterade systemmiljöer, begränsad spårbarhet och svårigheter att använda data strategiskt. Dessa grundläggande utmaningar får konsekvenser för både molninförande och cybersäkerhetsarbete.

Molntjänster framstår som en nödvändig komponent för framtida modernisering, interoperabilitet och effektivisering, men studien visar att mognadsgraden varierar i offentlig sektor. Skillnaderna kan i mindre utsträckning förklaras av teknik och i större utsträckning av organisatoriska förutsättningar, kultur, informationskänslighet och juridiska tolkningar. Utan en sammanhållen datastyrning riskerar molninitiativ att bli fragmenterade, kostnadsdrivande och förenade med osäkerhet kring hur data får hanteras.

Studien visar att cybersäkerhetsarbetet inom offentlig sektor lider av brist på kompetens och resurser vilket begränsar möjligheten att arbeta långsiktigt, proaktivt och i takt med en snabbt föränderlig hotbild och nya regulatoriska krav. Samtidigt visar studien att de flesta myndigheter har implementerat en strategi, definierat roller och ansvarsområden. Cybersäkerhetsarbetets effektivitet är därmed nära kopplad till hur strategi och roller underbyggs av resurser och kompetensförsörjning.

Sammantaget illustrerar studien en tydlig styrningsparadox: offentlig sektor behöver öka transparens, datadelning och effektivitet, samtidigt som kraven på säkerhet, integritet och kontroll skärps. För att kunna navigera denna paradox krävs ett helhetsperspektiv där datastyrning utgör den stabila grunden som möjliggör både säker användning av molntjänster och en långsiktigt robust cybersäkerhetsförmåga. Studien pekar därmed på behovet av ökad samordning, tydligt ägarskap och strategiskt ledarskap för att stödja en hållbar digital utveckling inom offentlig sektor.

Innehåll

Dela, modernisera och skydda data samtidigt – en växande styrningsutmaning

Utmaningen att hålla känsliga data och kritiska system skyddade i offentlig sektor har aldrig varit större.

En cyberattack inom offentlig sektor betyder inte enbart ekonomiska konsekvenser, utan riskerar även invånarnas välbefinnande samt allmänhetens och den nationella säkerheten. Offentlig sektor befinner sig även i en komplex verklighet där geopolitiska förändringar och ökad spänning i världen har ökat hotet mot kritisk infrastruktur.

Samtidigt utvecklas det regulatoriska landskapet i Europa och Sverige. Nya EU-regelverk och nationell lagstiftning, såsom NIS2-direktivet, den svenska cybersäkerhetslagen (som genomför NIS2), DORA och AI-förordningen ställer ökade krav på informationssäkerhet, operativ motståndskraft, kontinuitet och incidenthantering.

Parallellt sker en snabb teknisk utveckling, inte minst inom molntjänster och AI.

Detta innebär nya möjligheter till effektivisering och innovation, men medför även nya risker och ökade krav på offentlig sektors förmåga att anpassa sig till de nya förutsättningarna.

Förutom externa förutsättningar påverkas offentlig sektor även av interna omständigheter. Organisationer ställer generellt höga krav på säkerhet, och i kombination med specifik lagstiftning och regulatoriska ramar bidrar detta ofta till ökad komplexitet vid investering och implementation av nya IT- och säkerhetslösningar, vilket i sin tur kan påverka organisationers beslutsprocesser.

Många offentliga organisationer brottas även med fragmenterad styrning, där initiativ inom exempelvis molnfrågor, cybersäkerhet och datahantering bedrivs isolerat från varandra. Detta försvårar samordning, kunskapsdelning och ett effektivt riskarbete. Samtidigt finns ofta brist på kritisk kompetens och resurser, särskilt i mindre kommuner och myndigheter, vilket begränsar möjligheten att ta fram och implementera robusta strategier och handlingsplaner för cybersäkerhet och operativ resiliens.

Därtill utgör teknisk skuld en betydande utmaning. Utdaterade system, historiska kortsiktiga IT-lösningar och komplexa systemlandskap ökar både kostnader och risker, samtidigt som de försvårar införandet av moderna säkerhets- och styrningslösningar.

Mot denna bakgrund står offentlig sektor inför behovet av att dela, modernisera och skydda sin data på samma gång. En växande styrningsutmaning har uppstått, där ökade krav på transparens och effektivitet behöver balanseras mot behovet av säkerhet och integritetsskydd. Det skapar en komplex situation där olika intressen och mål måste vägas mot varandra.

Studien tar sin utgångpunkt i denna komplexa verklighet och syftar till att undersöka hur offentlig sektor kan navigera denna paradox.

Centrala strategier och policys inom offentlig sektor idag

Inom offentlig sektor pågår initiativ som syftar till en mer sammanhållen digital transformation.

Dessa utgår från behovet av att stärka styrning, samordning och långsiktig förmåga inom områden som digitalisering, datahantering och cybersäkerhet.

Initiativen tar sig uttryck i gemensamma strategier och policys, samt i etableringen av samverkansstrukturer och organiserade samverkansprogram. En gemensam inriktning är att tydliggöra ansvarsfördelning, förbättra informationsutbytet och främja mer enhetliga arbetssätt, samtidigt som kraven på säkerhet, motståndskraft och regelefterlevnad ökar.

För att fullt ut realisera nyttan av dessa initiativ krävs dock att de nationella strategierna och policys omsätts i praktisk handling i hela offentlig sektor.

För att skapa en nulägesbild presenteras nationella strategier och policys inom dessa områden.

Nationell digitaliseringsstrategi 2025-2030

Strategin beskriver utmaningar kopplade till den svenska decentraliserade förvaltningsmodellen, såsom splittrade och parallella lösningar, ineffektivt nyttjande av resurser, bristande informationsutbyte och fragmenterad samordning. Ansvarsfördelning mellan statliga myndigheter, kommuner och regioner är otydlig. Effektiv och säker datadelning hämmas av fragmenterade system och otydliga regelverk. För att stärka den strategiska styrningen och uppföljningen av digitaliseringen av den offentliga förvaltningen ämnar regeringen fokusera på utveckling, förvaltning och slutligen användning av Ena (en nationell digital infrastruktur).

Nationell strategi för cybersäkerhet 2025-2029

Den nationella strategin för cybersäkerhet tar avstamp i NIS2-direktivet och ett allriskperspektiv, men är samtidigt anpassad utifrån nationella behov. Med detta som utgångspunkt ämnar den nationella strategin att hantera utmaningar som kompetensbrist, komplexa regleringar, leveranskedjor som är sårbara men även brister i systematiskt cybersäkerhetsarbete. Det beskrivs att cybersäkerheten i Sverige påverkas av ett antal sårbarheter inom organisatoriska, tekniska, infrastrukturella och mänskliga faktorer. Strategin anger tre områden för inriktningen för cybersäkerhetsarbete för Sverige: ”Systematiskt och effektivt cybersäkerhetsarbete, ”utvecklad kunskap och kompetensutveckling inom cybersäkerhet” och ”förmåga att förhindra och hantera cybersäkerhetsincidenter”.

Regeringen föreslår en gemensam molnpolicy

Den föreslagna policyn omfattar att stärka offentlig förvaltnings användning av molntjänster, både ur ett säkerhetsperspektiv och ur ett funktions- och innovationsperspektiv. Idag dominerar amerikanska leverantörer marknaden, civilministern pekar på en efterfrågan av svenska eller europeiska leverantörer.

Nationell och EU-lagstiftning – datastyrning, molntjänster och cybersäkerhet

Regelverk	Område	Typ	Beskrivning
NIS2-direktivet, cybersäkerhetslagen	Cybersäkerhet	EU-direktiv, svensk lag	Riskhantering, incident-rapportering, tillsyn
GDPR, Dataskyddslagen	Dataskydd	EU-förordning, svensk lag	Personuppgiftkontroll, intrångsrapportering
Dataförordningen (Data Act)	Dataåtkomst	EU-förordning	Regler för åtkomst och delning av data
EU Cloud Code of Conduct	Molntjänster	Uppförandekod	GDPR-efterlevnad i moln
Förordningen om ett interoperabelt Europa (Interoperable Europe Act)	Interoperabilitet	EU-förordning	Standarder för offentliga datadelade tjänster
AI-förordningen (Articifical intelligence Act)	AI (artificial intelligence)	EU-förordning	Riskklassning av AI, krav på styrning, transparens och mänsklig kontroll

Datastyrning, cybersäkerhet och molnlagring – olika perspektiv på samma informationsresurs

I studien har följande definitioner av områdena använts. Datastyrning, cybersäkerhet och molnlagring handlar alla om att hantera och skydda samma centrala tillgång, organisationens information. De belyser informationsresurser ur olika infallsvinklar. I figuren framgår tre begrepp: flexibilitet, motståndskraft och kultur. Dessa begrepp kan ses som centrala i skärningspunkten mellan områdena. I skärningspunkten mellan dem uppstår en balans där både teknik, säkerhet och kultur samspelar för att organisationens information ska vara både tillgänglig och trygg.

Datastyrning

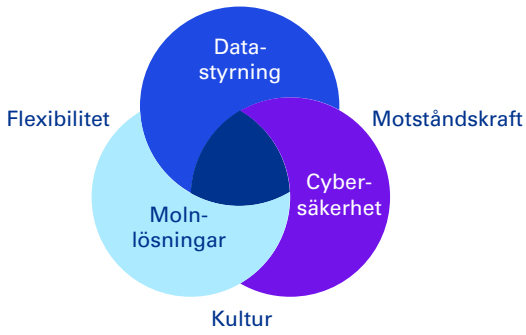
I denna studie används "datastyrning" som en samlingsbeteckning för hur en organisation skapar praktisk kontroll över sin data. Med datastyrning avses här arbete med datakvalitet, masterdata, integration och spårbarhet/härkomst, samt hur data kan nyttjas och delas på ett sätt som stödjer verksamhetens behov.

Cybersäkerhet

Cybersäkerhet avser i denna studie organisationens förmåga att skydda information, IT-system och digitala tjänster mot digitala hot, genom att förebygga, upptäcka och hantera cyberrisker på en nivå som är acceptabel för verksamheten. Det omfattar skydd av nätverk, informationssystem, användare och tjänster mot exempelvis skadlig kod, obehöriga intrång (hackning) och nätfiske.

Molnlagring

Molnlagring avser i denna studie att data lagras på fjärrservrar som nås via internet, i stället för att lagras lokalt i organisationens egna datorer eller fysiska lagringsenheter. Molnlagring kan organiseras på olika sätt beroende på krav på kontroll, säkerhet, efterlevnad och flexibilitet. Det finns olika typer av molnlagring: publik molnlagring, privat molnlagring, hybridmolnlagring och multimolnlagring.



Studiens genomförande

Studien ämnar att skapa ett kunskapsunderlag för myndigheter och andra aktörer inom offentlig sektor. Vi vill understryka de utmaningar offentlig sektor står inför, belysa gemensamma drag men även lyfta blicken framåt. Kunskapsunderlaget är uppdelat i tre delar, ett inledande kapitel, ett kapitel där resultaten analyseras och slutligen presenteras slutsatser och rekommendationer.

Intervjuer

För att skapa detta kunskapsunderlag har både intervjuer och en enkät genomförts. Inom ramen för studien har 11 intervjuer genomförts.

Intervjupersonerna har valts ut genom att de arbetar med dessa områden i organisationen och även har ett övergripande perspektiv på den organisatoriska styrningen inom dessa områden. Intervjuerna var semistrukturerade, vilket gav möjligheten till följdfrågor.

Enkät

Enkäten skickades ut till myndigheter och regioner. Ett enkätverktyg användes för att skicka ut enkäten, men respondenterna gavs även möjligheten att ge sina svar i en PDF.

Myndigheter som har valt att inte delta i studien har i huvudsak angett två anledningar: För det första är det en stor del av myndigheterna som vi skickat ut till som är små myndigheter, ofta med en större värdmyndighet, dessa har därför avstått från att svara. Den andra anledningen som myndigheter har angett är att studien berör ämnesområden som upplevs som känsliga, vilket har gjort att vissa valt att avstå från att delta.

Specifikt cybersäkerhet är ett område som, av förklarliga skäl, ses som känsligt och myndigheter väljer därför att avstå. En ytterligare aspekt som bör uppmärksammas i detta sammanhang är kravet på opartiskhet och likabehandling. För att säkerställa detta väljer vissa myndigheter att vara restriktiva med att delta i studier som initieras av privata aktörer.

Svarsfrekvens för enkätundersökningen:

- Utskick till 247 myndigheter och 20 regioner
- 41 tackat nej
- 30 besvarat enkäten

Begränsningar

Studien har ett antal begränsningar som bör beaktas vid tolkning av resultaten. Det empiriska underlaget är begränsat, vilket innebär att studien inte syftar till att ge en heltäckande bild av samtliga perspektiv inom offentlig sektor. I stället syftar intervjuerna till att ge fördjupad förståelse för centrala frågeställningar och återkommande mönster.

Dessutom bidrar det att känsliga områden, som cybersäkerhet, inte alltid diskuteras öppet. Detta medför att vissa myndigheter väljer att inte delta i studien, vilket påverkar resultatet.

Samtidigt bidrar dessa förutsättningar till att sätta resultaten i ett relevant sammanhang. De utmaningar som rör öppenhet, deltagande och tillgång till information är i sig en del av den verklighet som offentlig sektor har att förhålla sig till.

Vi tror att det är precis av denna anledning som den här studien fyller en funktion för offentlig sektor.

Datastyrning – ett område för utveckling

Datastyrning och "att få ordning på sin data", är något som länge har diskuterats inom offentlig sektor. Trots detta är ämnet högst relevant idag.

I studien framgår att myndigheter idag bedömer sig ha en låg intern mognadsgrad inom datastyrning. I detta avsnitt kommer vi därför gräva djupare i frågorna varför myndigheter upplever en låg mognadsgrad, men även vad det har för konsekvenser för myndigheter.

Trots det långvariga fokuset på datastyrning visar studiens resultat att myndigheter generellt bedömer sin interna mognadsgrad inom datastyrning som låg till måttlig. Endast 5 % uppger att de har en etablerad strategi för datastyrning, och motsvarande andelar anger att de har tydligt definierade roller och ansvar eller etablerade processer för att säkerställa datakvalitet. Samtidigt upplever ingen av de svarande att de har en hög mognadsgrad inom området.

Sammantaget indikerar resultaten att centrala delar av datastyrning ännu inte är fullt utvecklade inom stora delar av offentlig sektor. Detta påverkar förutsättningarna för att använda data strategiskt, säkerställa kvalitet och möjliggöra effektiv datadelning.

I praktiken innebär detta att många myndigheter har begränsade förutsättningar att arbeta datadrivet på ett sammanhållet och långsiktigt sätt. Avsaknad av tydlig styrning, gemensamma processer och tillräckliga resurser leder ofta till fragmenterade arbetssätt.

"Formell policy för datastyrning? Där är vi rudimentära."

IT-direktör på myndighet

Denna aspekt speglas även i intervjuerna. Flera myndigheter beskriver att formella strategier för datastyrning helt saknas, eller att de finns men inte har fått genomslag i det dagliga arbetet.

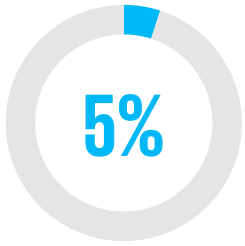
Det beskrivs som frikopplat från den operativa verksamheten. Detta bidrar till att strategin riskerar att förbli en pappersprodukt snarare än ett aktivt stöd i verksamhetsstyrningen.

Respondenterna beskriver att roller kopplade till datastyrning i många fall är formellt definierade i organisationen, men att dessa i likhet med strategin, i begränsad utsträckning omsätts i det praktiska arbetet.

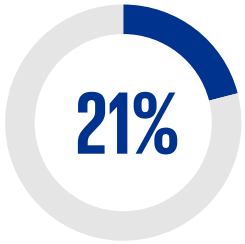
Samtidigt tyder resultaten på att rutiner för datastyrning och för att säkerställa datakvalitet ofta är begränsade eller otydliga. Frågan om vem som i praktiken bär ansvar för data i verksamheten aktualiseras.

Instämmandegrad i enkätundersökning

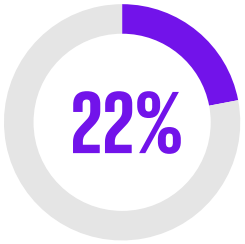
Vi har en etablerad strategi för datastyrning



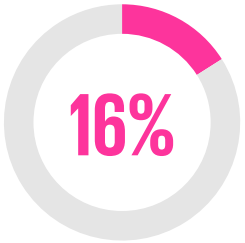
Vi har etablerade processer för att säkerställa datakvalitet



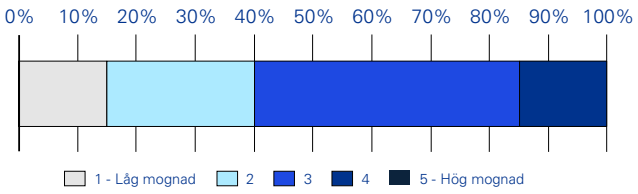
Vi har tydligt definierade roller och ansvar för data



Vi har en god datakvalitet



Hur bedömer ni er mognadsgrad inom datastyrning?



Datastyrning – otillräckliga resurser och otydlig ansvarsfördelning

”Man står fast i arv och lagstiftning som hämmar.”

IT-arkitekt på myndighet

En genomgående låg mognadsgrad inom datastyrning kan förstås som ett resultat av flera samverkande organisatoriska och tekniska faktorer. Datastyrning kräver tydlig styrning, gemensamma arbetssätt och långsiktiga investeringar, men i många myndigheter har området vuxit fram successivt och ofta parallellt med befintliga strukturer. Detta bidrar till att datastyrning inte fullt ut integrerats i verksamhetsstyrningen, utan hanteras fragmenterat och i varierande omfattning.

I intervjuerna beskrivs en återkommande problematik kring datakvalitet, särskilt i större myndigheter eller i verksamheter som hanterar stora datamängder. Utmaningarna rör bland annat osäkerhet kring var data ska lagras, bristande överensstämmelse i masterdata mellan olika system samt avsaknad av tydliga rutiner för rensning och livscykelhantering av data.

Äldre system och historiska lösningar förstärker dessa utmaningar och försvårar ett sammanhållet arbetssätt. I enkätundersökningen framkommer detta även genom att otydliga processer och rutiner lyfts fram som en central.

Vidare framgår att roller kopplade till datastyrning, såsom informationsägare, i varierande grad finns definierade i verksamheterna. Dessa roller används dock inte konsekvent i praktiken, vilket bidrar till otydlighet kring ansvar och ägarskap för data.

Otydlig ansvarsfördelning framstår också som en framträdande utmaning i enkätundersökningen. Myndigheterna beskriver dessutom en avsaknad av sammanhållande datamodeller, vilket leder till fragmenterade och svårintegrerade systemmiljöer.

Äldre system utgör ytterligare en begränsande faktor. Svårigheter att integrera system påverkar effektiviteten i verksamheten och begränsar möjligheten till datadelning, både internt och externt.

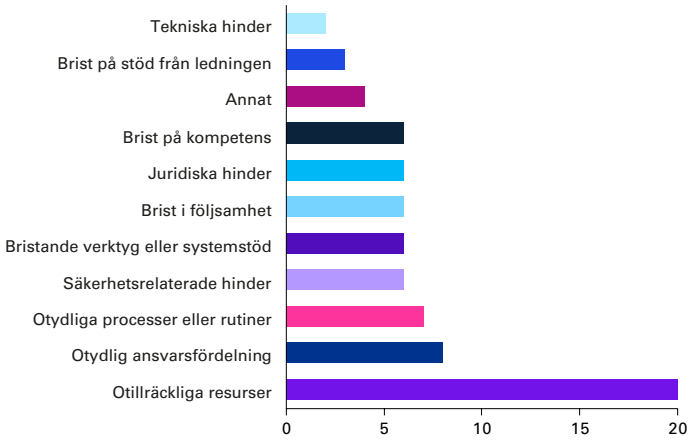
Moderniseringsarbete försvåras av långa systemlivscykler, tekniska beroenden och bristande standardisering, vilket gör att nya lösningar ofta måste anpassas till befintliga strukturer snarare än tvärtom.

Slutligen visar enkätundersökningen att otillräckliga resurser upplevs som den största utmaningen inom datastyrning. Denna bild bekräftas i intervjuerna, där resursbrist beskrivs i termer av begränsade ekonomiska medel, brist på tid, kompetens och tillräcklig bemanning. Sammantaget bidrar detta till att arbetet med datastyrning ofta blir reaktivt.

Ur ett cybersäkerhetsperspektiv innebär detta att åtgärder i många fall vidtas först när risker eller incidenter blivit akuta, snarare än som en del av ett förebyggande och systematiskt arbete.

Sammantaget visar analysen att den låga mognadsgraden inom datastyrning inte kan förklaras av en enskild faktor, utan är resultatet av ett samspel mellan organisatoriska, tekniska och resursmässiga utmaningar.

Hur bedömer ni er mognadsgrad inom datastyrning?



Strategisk datastyrning: Nyckeln till framgångsrika teknik-investeringar och säker AI-implementering

”Med nytt system ska allt bli fantastiskt, men samma problem finns kvar på grund av avsaknad av struktur.”

IT-direktör på myndighet

Citatet fångar en återkommande erfarenhet hos många myndigheter: tekniska investeringar och nya system förväntas lösa långvariga utmaningar, men i praktiken kvarstår problemen när de grundläggande strukturerna för datastyrning saknas. Avsaknad av tydlig styrning, ansvar och gemensamma arbetssätt innebär att ny teknik ofta implementeras ovanpå befintliga brister snarare än att åtgärda dem.

KPMG Global Tech Report 2026: Government and public sector menar att ignorera äldre system kan äventyra framtida teknikinvesteringar. Rapporten beskriver att kvalitetssäkrad, tillförlitlig, integrerad och lättillgänglig data är en förutsättning för teknikinvesteringar ska leda till verksamhets- och tjänsteförbättring. De problem som finns i nuvarande system kommer inte lösas genom ett nytt system eller lösning, utan riskerar istället implementeringen av den nya investeringen.

Det handlar därför om att ta tag i grundproblematiken, sin data. Rapporten menar även att organisationer som regelbundet utvärderar sin data och använder datadrivna arbetssätt får både snabbare och bättre resultat av sina teknikinvesteringar.

Organisationer som har en hög datamognad har även en högre sannolikhet att vara nöjda med värdet som teknikinvesteringen genererar. Denna fråga är något respondenterna reflekterar över i molninförande. En av respondenterna beskriver en lång resa innan samtliga av systemen är ”Cloud-ready”.

Detta bidrar till att låg mognad inom datastyrning får genomgripande konsekvenser, särskilt i takt med att myndigheter i allt större utsträckning inför AI-lösningar, molntjänster och samtidigt möter ett ökande cyberhot.

En låg mognadsnivå inom datastyrning har flera konsekvenser för organisationer. I intervjuerna beskrivs denna problematik ge påföljder vid införandet av AI- och molnlösningar men även gällande det ökade cyberhotet.

Utmaningarna bottnar i att organisationen saknar kontroll över var data finns och om den är korrekt. Detta kan leda till att AI-modeller tränas på felaktig eller känslig information, samtidigt som känslig data riskerar att lagras i system utan tillräcklig säkerhetsklassning.

I det landskap som organisationer befinner sig idag fungerar inte längre den klassiska informationsklassningen där en datamängd klassas för sig. Datamängder kommer idag kombineras på ett sätt, dels genom AI, som kräver strategisk och nytänkande informationsklassning. En myndighet beskriver att de löser detta problem genom att inte koppla sina system till varandra, vilket påverkar effektiviteten i arbetet. Andra respondenter lyfter att de, på grund av den ökade mängden data, inte kommer kunna informationsklassa data manuellt som idag.

Denna aspekt, att respondenterna i huvudsak förhåller sig till frågan om datastyrning utifrån informationsklassning, är framträdande i intervjuerna. Detta fokus riskerar att förlora helheten, där delar som ansvar, kvalitet, livscykel eller användning inte beaktas.

Tre punkter där en bristfällig datastyrning har konsekvenser för myndigheter:

- **Införandet av AI.**
- **Nya teknikinvesteringar, exempelvis molnlösningar.**
- **Cybersäkerhet och informationsklassning.**

*https://kpmg.com/xx/en/our-insights/transformation/kpmg-global-tech-report-2024.html

Molntjänster – styrning och mognad sätter tydliga begränsningar

Moln eller "Cloud" har blivit ordet på mångas läppar. I och med det geopolitiska läget, de ökade cyberhoten, den fortsatta digitala utvecklingen och beroendet av leverantörer står molnfrågan på offentlig sektors agenda. I studien beskriver respondenterna en stor osäkerhet och en upplevelse av att känna sig ensam i frågan. I detta avsnitt kommer vi därför behandla vart myndigheter idag står gällande molntjänster, vilka utmaningar som finns och slutligen vilka fördelar myndigheterna ser med moln.

Resultaten visar att molninförandet i offentlig sektor i stor utsträckning befinner sig i ett delvis etablerat skede. 31 % av myndigheterna uppger att de har en fastställd molnstrategi, men svaren indikerar samtidigt att strategierna ofta är begränsade i omfattning eller ännu inte fullt implementerade i verksamheten.

Molnanvändning sker därmed i många fall utan ett tydligt sammanhållet strategiskt ramverk, vilket bidrar till en ojämn mognadsbild.

När det gäller styrning och ansvar framgår att roller och ansvar för beslut om var och hur data ska lagras endast är tydligt definierade i viss utsträckning.

Detta tyder på att ansvarsfördelningen kring molnfrågor inte alltid är fullt förankrad i organisationen, vilket kan skapa osäkerhet i både strategiska och operativa vägval. Avsaknad av tydliga roller riskerar att leda till försiktighet eller fragmenterade beslut snarare än ett konsekvent införande.

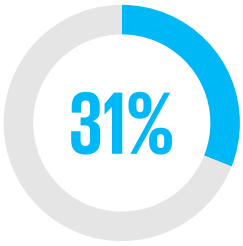
Samtidigt framträder juridiska och säkerhetsrelaterade riskbedömningar som ett relativt mer moget område. En större andel av respondenterna anger att det finns rutiner för att hantera dessa risker i samband med molnanvändning. Detta indikerar att molnfrågan i hög grad hanteras genom ett risk- och regelefterlevnadsperspektiv, snarare än som en del av en bredare strategisk utveckling.

Kompetensfrågan utgör ytterligare en begränsande faktor. 35 % av myndigheterna upplever att de har tillräcklig intern kompetens för att implementera molnlösningar, vilket påverkar förmågan att fatta informerade beslut, genomföra införanden och skala upp användningen av molntjänster över tid.

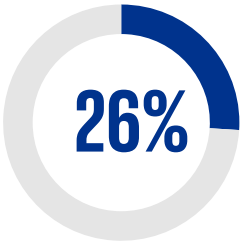
Den samlade bedömningen av mognadsgrad inom molnområdet visar därmed på en relativt låg till måttlig nivå. Analysen pekar på att mognadsgraden i hög grad formas av hur väl strategi, ansvar, kompetens och riskhantering hänger samman. Där dessa komponenter inte är integrerade tenderar molninitiativ att bli försiktiga, isolerade och långsamma, snarare än strategiska och värdeskapande.

Instämmandegrad enkätundersökning

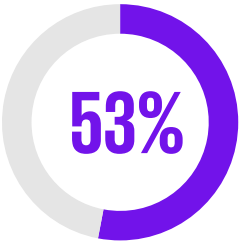
Vi har en etablerad molnstrategi



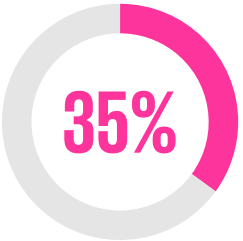
Vi har tydligt definierade roller och ansvar för att bedöma var och hur data ska lagras.



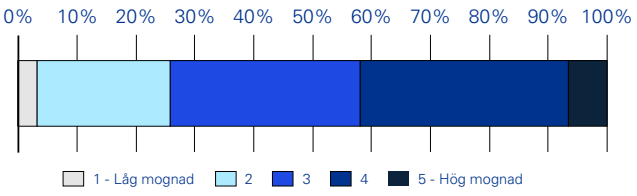
Vi har rutiner för juridiska och säkerhetsrelaterade riskbedömningar kopplade till användning av molntjänster.



Vi har tillräcklig kompetens för att implementera molnlösningar.



Hur bedömer ni er mognadsgrad inom molnstjänster?



Molnstrategier: från restriktivitet till cloud-first

”Folk skrattade när jag för tre år pratade om molnet.”

IT-arkitekt på myndighet

Intervjuerna visar stor skillnad i vart myndigheter befinner sig i sin molnresa. Denna skillnad yttrar sig i myndigheternas molnstrategier. Moln-frågan är komplex och i intervjuerna lyfts många olika perspektiv, från säkerhet, ekonomi, tillgänglighet, juridik till kompetens.

Vissa myndigheter är fortfarande starkt restriktiva till molnlösningar och utgår från lokal drift, medan andra myndigheter har en mer offensiv strategi med Cloud-first som ambition.

Intervjuerna visar att myndigheternas förhållningssätt till molntjänster spänner över ett brett spektrum, från mycket restriktiva till mer offensiva strategier. Gemensamt är dock att valen i hög grad styrs av hur väl organisationerna upplever sig kunna hantera risker kopplade till informationssäkerhet, juridik och kontroll över data. Vissa myndigheter beskriver ett uttalat restriktivt förhållningssätt, där molntjänster endast används i begränsad omfattning eller inte alls.

I dessa fall dominerar egen drift, och molnlösningar betraktas som aktuella först när det saknas alternativa tekniska lösningar. Försiktigheten motiveras framför allt av krav kopplade till dataskydd, personuppgifter och GDPR, och leder till att molntjänster som trots allt används hålls utanför kärnverksamheten.

Andra myndigheter beskriver hur de valt en mer kontrollerad mellanväg genom hybridlösningar. Här kombineras egen kontroll med inslag av molnbaserad infrastruktur, där ansvarsfördelningen är tydlig och informationsklassning fungerar som styrande princip. Endast information med låg skyddsnivå tillåts i molnmiljöer, medan känslig eller sekretessbelagd information fortsatt hanteras i egen regi.

Detta angreppssätt speglar en vilja att dra nytta av molnets fördelar utan att kompromissa med säkerhet och regelefterlevnad.

Samtidigt finns exempel på myndigheter som valt ett mer framåtlutat angreppssätt med en uttalad cloud-first-strategi, där molntjänster ses som förstahandsval när förutsättningarna tillåter. I dessa fall framhålls informationsklassning som en grundläggande möjliggörare, och arbetet beskrivs som en omfattande och långsiktig resa med stark involvering från juridik, informationssäkerhet och verksamhet. Ambitionen är att skapa strukturer som gör det möjligt att både möta regulatoriska krav och successivt öka användningen av molnbaserade lösningar.

Sammantaget handlar skillnaderna i molnanvändning inte i första hand handlar om teknik, utan om styrning, riskhantering och organisatorisk mognad.

Myndigheternas molnstrategier formas av hur väl de upplever sig ha kontroll över sin information och sin förmåga att fatta informerade beslut. Detta bidrar till en fragmenterad mognadsbild, där molnresan drivs i olika takt och med olika angreppssätt beroende på verksamhetens förutsättningar och riskaptit.

Molntjänster – resurser och säkerhetsutmaningar bromsar molninförande

De största utmaningarna inom molnanvändning framgår vara säkerhetsrelaterade hinder, juridiska hinder samt otillräckliga resurser.

Säkerhetsaspekten utgör en central orosfaktor, där rädslan för att tappa kontrollen över data och risken att hamna i rampljuset för nästa stora cyberattack eller läckage gör sig påmind.

Respondenterna tampas alla med frågan gällande hur information hålls säker i organisationen och om molnet är lösning eller problemet i denna fråga. Det är inte endast den tekniska infrastrukturen som ifrågasätts utan de etiska och praktiska konsekvenserna av hantering av känslig information via molnleverantörer bidrar till en känsla av sårbarhet. Gällande de juridiska aspekterna leder den komplexa och ibland svårtydda regleringen till osäkerheter. Myndigheter väljer att avvakta eller arbeta vaksamt med implementeringen av molnlösningar. Spänningen mellan de operativa delarna av verksamheten och jurister speglar det komplexa området.

Utöver säkerhetsrisker- och juridiska utmaningar är resurser en utmaning. Det handlar dels om kompetens, dels om monetära resurser. Bristen på specialiserade kunskaper inom både teknik som juridik förstärker osäkerhet och bidrar till den tvekan som gäller för införandet av molntjänster.

Trots dessa utmaningar visar våra intervjuer att det finns goda exempel på implementeringar av molnlösningar i offentlig sektor. Dessa exempel utgör hybridlösningar med tydlig fördelning och integrerad informationsklassificering. På så sätt säkerställdes att de känsliga uppgifterna hanterades i en kontrollerad och reglerad miljö, samtidigt som myndigheten kunde dra nytta av flexibilitet och verktyg som molntjänsten erbjöd. Även dessa myndigheter lyfter säkerhetsaspekten gällande molntjänster. Myndigheterna betonar vikten av en tydlig exitstrategi men även vetskapen om vilka risker som beslutet att använda molntjänster medför.

I enkätundersökningen framkommer ett antal fördelar som myndigheter ser med molnlösningar i dag och i framtiden. Enligt KPMG Global Tech Report 2024 ser ledare inom offentlig sektor molnlösningar och XaaS (everything as a service) som nyckelfaktorer för att öka effektiviteten och data management. I vår enkätundersökning anger myndigheterna att de största fördelarna är ökad tillgänglighet, enklare underhåll och minskade driftkostnader.

Något intressant är andelen av myndigheter som inte ser fördelar med molntjänster, varken idag eller framtiden. Varför myndigheter ställer sig tveksamma till molntjänster är inte konstigt, tvärtom. Utifrån de utmaningar som myndigheter beskriver upplever vi det svårt att förbise dessa och se möjligheter.

I intervjuerna uttrycks ofta möjligheterna och fördelarna med molntjänster som vad som skulle hända om myndigheten inte väljer att anamma molntjänster. Respondenterna beskriver att de inte tro att det är rätt väg att gå att låsa in sig själv. De beskriver att det försvårar den digitala utvecklingen och interoperabilitet i myndigheten men även mellan myndigheter. Beroende av leverantörer av tjänster eller system lyfts även. Framåt kommer leverantörer i större utsträckning enbart leverera molnlösningar av sina tjänster.

Myndigheter står inför valet att använda sig av molntjänster eller utveckla lösningar själva från grunden. I denna fråga saknar många myndigheter kompetens, resurser och möjlighet att genomföra detta. Respondenterna beskriver att den säkerhet gällande att skydda data från utomstående angrepp som de själva eller mindre leverantörer kan erbjuda inte kan mätas med den säkerhet som större leverantörer erbjuder.

Gällande molntjänster lyfts även aspekten gällande tillgänglighet som en fördel med molntjänster. När myndigheter tidigare har fokuserat på konfidentialitet, har världsläget skiftat fokuset mot tillgänglighet. Respondenterna beskriver att det viktigaste var att låsa in sin data. Informationen behövde tidigare endast skyddas från obehörig åtkomst, data hanterades inom en sluten miljö där hotbilden oftast kom utifrån. Intervjuerna visar att myndigheter nu börjar ifrågasätta dessa gamla sanningar.

Cybersäkerhet – en etablerad grund men med fortsatta utmaningar

Medan många har definierat roller och ansvarsområden, saknar en majoritet tillräcklig kompetens och resurser för att hantera cyberrisker.

Samtidigt står offentlig sektor inför en snabbt föränderlig hotbild, nya digitala arbetssätt och ett förändligt regulatoriskt landskap. Organisationer har en grund, men står inför ett behov av att modernisera både kultur och struktur för att hålla jämna steg med utvecklingen.

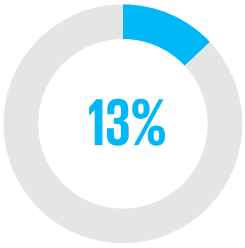
I vår undersökning framgår det att de flesta myndigheter har implementerat en strategi, definierat tydliga roller och ansvarsområden samt etablerat processer för att säkerställa cybersäkerheten.

Däremot visar resultaten att myndigheterna upplever att de inte har i lika stor utsträckning tillräcklig kompetens och resurser för att hantera cyberrisker. Detta beror ofta på att offentlig sektor har svårt att hålla jämna steg gällande lön och förmåner med den privata sektorn.

Det kan begränsa förmågan att arbeta långsiktigt och proaktivt i takt med ökade hot och nya regelverk.

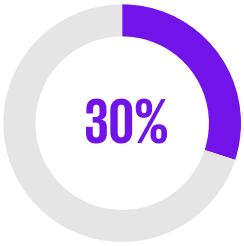
Väl förberedda för implementeringen av den nya cybersäkerhetslagen

En minoritet av myndigheterna upplever sig vara väl förberedda för implementeringen av den nya cybersäkerhetslagen.



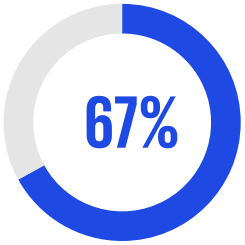
Tillräcklig kompetens för att hantera cyberrisker

En tredjedel av myndigheterna uppger att de har tillräcklig kompetens för att hantera cyberrisker.

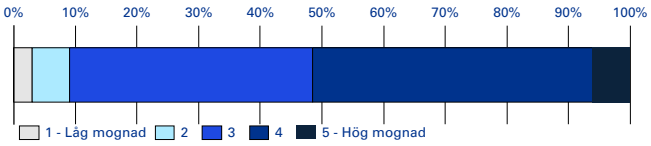


Otillräckliga resurser

En majoritet av myndigheterna lyfter begränsade resurser som en av sina huvudsakliga utmaningar inom cybersäkerhet.



Hur bedömer ni er mognadsgrad inom cybersäkerhet?



Cybersäkerhet – tillräckliga resurser som en av de största utmaningarna

En förutsättning för ett effektivt och långsiktigt cybersäkerhetsarbete är tillgång till tillräckliga resurser och rätt kompetens. I takt med att hotbilden blir mer komplex och kraven på skydd av samhällsviktig verksamhet ökar ställs allt högre krav på offentliga organisationers förmåga att arbeta strukturerat och proaktivt med cybersäkerhet. Samtidigt visar studien att många myndigheter upplever betydande begränsningar i sin kapacitet, vilket påverkar både det förebyggande arbetet och förmågan att möta nya risker.

Utifrån enkätundersökningen framstår otillräckliga resurser som en stor utmaning när det kommer till cybersäkerhet. Dessa tar sig både i uttryck som monetära resurser men även i form av kompetens. Detta speglas även i intervjuerna där myndigheter beskriver svårigheter att rekrytera mer seniora roller inom cybersäkerhet.

I efterfrågan efter kompetens ställs offentlig sektor mot privat, där offentlig sektor har svårt att hålla jämna steg gällande lön och förmåner. KPMG Cybersäkerhet Considerations 2025 menar också att många organisationer som är ansvariga för kritisk infrastruktur inom offentlig sektor saknar expertis eller monetära resurser för heltäckande strategier för resiliens.

Mot denna bakgrund framstår kompetensutveckling som en särskilt viktig faktor för offentlig sektor. Detta omfattar både riktade insatser för att stärka säkerhetsfunktioner och ett fortsatt arbete med att höja den generella medvetenheten i organisationen.

Även om medvetenheten kring cybersäkerhet i viss utsträckning bedöms vara god, visar resultaten att den behöver stärkas ytterligare.

Detta genom kontinuerliga utbildningar, tydliga rutiner, välkända rapporteringsvägar och en organisationskultur där medarbetare känner sig trygga i att rapportera incidenter.

”En digital krigföring som pågår med försök till intrång varje dag. Om folk jämställde det med inbrott, så hade man nog förstått det mer.”

Enhetschef IT-säkerhet

I detta sammanhang framstår den föreslagna nationella satsningen inom cybersäkerhet i budgetpropositionen för 2026 som både efterfrågad och välkommen. Utifrån studiens resultat kan satsningen ses som ett viktigt steg för att adressera de strukturella brister som många myndigheter idag upplever, och som en förutsättning för att stärka den långsiktiga förmågan att möta ett allt mer komplext och krävande cybersäkerhetslandskap.

Analysen pekar på att bristande grundarbete idag skapar strukturella utmaningar inför framtiden. När resurser, kompetens och styrning inte är tillräckligt utvecklade riskerar myndigheter att få svårt att möta både nuvarande och kommande regulatoriska krav.

Cybersäkerhet diskuteras även ur ett beredskaps- och resiliensperspektiv, där behovet av att skydda information ställs mot kravet på tillgänglighet i samhällskritiska funktioner. Respondenterna beskriver en inneboende spänning mellan konfidentialitet och tillgänglighet, särskilt i situationer där verksamheten måste kunna upprätthållas även vid störningar eller kriser.

I detta sammanhang framträder molnfrågan som en central del av beredskapsarbetet. Molntjänster ses både som en potentiell möjliggörare för ökad redundans och skalbarhet, och som en källa till nya risker kopplade till kontroll, beroenden och jurisdiktion. Hur dessa avvägningar hanteras påverkar i hög grad myndigheternas syn på molnanvändning och deras förmåga att bygga långsiktig digital motståndskraft.

Avvägningar mellan effektivitet, transparens och skydd präglar den digitala utvecklingen

Offentlig sektor befinner sig i ett läge där kraven på digital utveckling och effektivisering ökar, samtidigt som behovet av säkerhet, integritetsskydd och kontroll skärps. Myndigheter förväntas i allt högre grad dela och använda data för samverkan, innovation och verksamhetsutveckling, samtidigt som samma data ofta är känslig, skyddsvärd eller strikt reglerad. Detta skapar en grundläggande styrningsparadox, där ambitionen att modernisera och öppna upp behöver balanseras mot kravet på att skydda och begränsa. Denna paradox genomsyrar hur datastyrning, molntjänster och cybersäkerhet hanteras i praktiken.

Val som rör molnanvändning, säkerhetsnivåer och informationshantering handlar sällan om teknik i sig, utan om avvägningar mellan transparens och konfidentialitet, effektivitet och regelefterlevnad samt innovation och risk. När dessa områden utvecklas i olika takt eller utan samordning förstärks spänningarna ytterligare. I det följande sammanförs därför resultaten från studien för att belysa hur brister och styrkor inom datastyrning, molntjänster och cybersäkerhet samverkar, och vad detta innebär för offentlig sektors förmåga att navigera styrningsparadoxen på ett långsiktigt och hållbart sätt.

Sammantaget visar studien att datastyrning, molntjänster och cybersäkerhet är tätt sammanlänkade områden som i praktiken påverkar och förstärker varandra. Myndigheterna beskriver genomgående en låg mognadsnivå inom datastyrning, vilket tar sig uttryck i otydliga roller och processer, avsaknad av enhetliga datamodeller samt bristande strukturer för datakvalitet. Detta leder till fragmenterade systemmiljöer, begränsad spårbarhet och svårigheter att använda data som ett strategiskt underlag i den fortsatta digitala transformationen.

Denna grundproblematik får tydliga konsekvenser även för cybersäkerhet och molninförande. Molnfrågan framstår som ett av de mest polariserande områdena, där vissa myndigheter har valt en mer offensiv cloud-first-strategi medan andra intar ett mycket restriktivt förhållningssätt. Skillnaderna kan i mindre utsträckning förklaras av tekniska möjligheter och i större utsträckning av informationskänslighet, organisationskultur, juridiska tolkningar och historiska arbetssätt.

När datastyrningen är svagt utvecklad riskerar molninitiativ att bygga vidare på befintliga brister, snarare än att lösa dem.

Molntjänster förutsätter konsekvent styrning, homogen informationsklassning och tydlig ansvarsfördelning. När dessa förutsättningar saknas uppstår i stället parallella lösningar, dubbla systemmiljöer och osäkerhet kring hur data får hanteras. Detta driver ökade kostnader, hämmar effektivisering och kan i förlängningen skapa nya säkerhetsrisker. I stället för att fungera som en möjliggörare för modernisering riskerar molninförandet då att förstärka befintlig komplexitet.

I arbetet med cybersäkerhet begränsas utvecklingen av tekniskt arv, fragmenterad data och nya digitala arbetssätt. Kompetensbrist och juridisk komplexitet påverkar förmågan att arbeta långsiktigt och proaktivt.

Frågan om beredskap aktualiserar dessutom en växande spänning mellan konfidentialitet och tillgänglighet, där molninfrastruktur både kan stärka och utmana organisationernas motståndskraft.

Det blir därmed tydligt att de tre områdena inte kan hanteras isolerat. Trots detta präglas många organisationer av bristande samordning mellan datastyrning, molnstrategi och cybersäkerhet. Avsaknaden av ett sammanhållet angreppssätt riskerar att begränsa effekten av enskilda initiativ och försvåra den långsiktiga digitala utvecklingen. Studien pekar därmed på behovet av att se dessa områden som delar av samma styrningsfråga, där helhet, samordning och långsiktighet blir avgörande för att lyckas.

Ledarskap som möjliggörare – eller bromskloss?

I studien framträder även ledarskapet som en viktig aspekt för samtliga tre områden. Ledarskapets roll blir särskilt tydligt i frågor om prioritering, förståelse och ansvar i en kontext präglad av osäkerhet och komplexitet. Det framgår att dessa utmaningar medför att frågorna snarare stannar i ett diskussionsläge, istället för en strategisk plan och väg framåt.

På ledningens agenda

Studien visar att frågor om datastyrning, moln och cybersäkerhet ofta behandlas som operativa eller tekniska, vilket gör att de inte alltid ges utrymme för strategisk diskussion. Respondenterna beskriver hur de arbetar för att få upp dessa frågor på ledningens agenda. När frågorna saknar tydligt ägarskap i ledningen riskerar de att hanteras fragmenterat och reaktivt, snarare än som sammanhållna och långsiktiga styrningsfrågor.

Förståelse är förutsättningen för strategisk dialog

I många organisationer behöver ledningen först förstå frågornas innebörd och samband innan en fördjupad strategisk diskussion kan föras. Studien visar att ledningsdialogen ofta fastnar i förklaringsläge, där fokus ligger på att reda ut begrepp, risker och regelverk, snarare än att diskutera vägval och prioriteringar. När den gemensamma förståelsen saknas blir beslutsfattandet långsamt och försiktigt.

Ansvar, mod och risk-acceptans

Osäkerhet kring juridik, säkerhet och konsekvenser bidrar till att organisationer ofta väljer att avvakta snarare än att agera. Studien visar att rädslan för att göra fel snarare än brist på vilja är en central broms i utvecklingen. Här spelar ledarskapet en avgörande roll genom att tydliggöra ansvar, definiera riskacceptans och legitimera avvägningar. Utan detta riskerar organisationen att fastna i ett status quo där ”att inte besluta” blir ett informellt beslut.

Slutsatser

Studiens övergripande slutsats är att datastyrning utgör den grundläggande förutsättningen för att offentlig sektor ska kunna fatta hållbara och strategiska beslut kring både molntjänster och cybersäkerhet. Utan tydlig styrning av ansvar, dataflöden och användning riskerar initiativ inom moln och säkerhet att bli fragmenterade, reaktiva och svåra att förena med ökade regulatoriska krav.

Studien visar samtidigt att molntjänster är oundvikliga för framtida modernisering och interoperabilitet, men att deras värde endast kan realiseras om de vilar på en genomtänkt datastyrning och integrerad säkerhet.

I detta sammanhang blir det tydligt att cybersäkerhet hänger nära samman med organisationens förmåga att styra, klassificera och skydda sin data på ett enhetligt sätt. Sammantaget pekar studien på behovet av ett helhetsgrepp där datastyrning fungerar som navet som möjliggör både säker användning av molntjänster och en långsiktigt robust cybersäkerhetsförmåga.

Utifrån dessa förutsättningar behöver ledarskapet ta en aktiv och tydlig roll för att bryta den styrningsparadoxen som idag präglar diskussionen kring datastyrning, moln och cybersäkerhet. I en omvärld kännetecknad av ökad osäkerhet, komplexitet och snabba förändringar räcker det inte att hantera frågorna operativt eller tekniskt; de kräver en strategisk dialog på ledningsnivå. Studien visar att utan ett tydligt ägarskap och en gemensam förståelse för hur dessa områden hänger samman riskerar beslut att bli fragmenterade och reaktiva. För att undvika ett status quo där osäkerhet och rädsla för felbeslut leder till passivitet behöver ledningen ta ansvar för att definiera riskacceptans, skapa förutsättningar för välgrundade beslut och säkerställa en långsiktigt integrerad strategi där datastyrning utgör den stabila grunden.

Rekommendationer

1

Bygg en stabil grund i datastyrning för en säker och hållbar digital utveckling

För att uppnå en säker och hållbar digital utveckling krävs ett helhetsgrepp som integrerar en stabil grund i datastyrning. I dag påbörjar många verksamheter moderniseringsinitiativ utan att datastyrningen är tillräckligt etablerad i praktiken. Att bli fångad av trender och ha ett ensidigt fokus på ny teknik riskerar då att skapa nya beroenden, öka osäkerheten kring data och försvåra en skalbar och säker utveckling över tid. En god datastyrning ger organisationen kontroll och riktning i hur data hanteras och används, från kvalitet och spårbarhet till tydliga ansvar och beslut. En central del är att säkerställa att informationsklassning är en integrerad och aktiv del av datastyrningen. Detta innebär att organisationer inte bara skyddar känslig information, utan även kan optimera nyttjandet av data. Frågan blir särskilt relevant vid avvägningar kring användning av molntjänster och AI, där organisationer behöver förstå vilka data de har, hur den får användas och hur risker ska vägas mot verksamhetsnytta. Att bygga en fungerande datastyrning är således en förutsättning för att kunna genomföra digital utveckling på ett säkert och hållbart sätt.

2

Exitstrategi lika viktigt som plan för införande av moln

Leverantörer kommer i allt högre utsträckning erbjuda sina tjänster enbart som molntjänster, vilket ställer krav på myndigheter att anpassa sig och förbereda sig inför dessa nya förutsättningar. Vare sig det är att påbörja sin molnresa eller söka andra lösningar, är detta en fråga som offentlig sektor redan står inför.

3

Förbered för leverantörernas nya förutsättningar

I studien ser vi att framgångsfaktorer för ett fungerande molninförande är informationsklassning och dataseparering samt tydliga exitstrategier och robusta leverantörsavtal.

4

Prioritera kompetens och resurser för att stärka motståndskraft

Det finns ett gap i att säkerställa en tillräcklig cybersäkerhetskultur, de som redan har ordning på sin data och säkerhet ligger före, medan andra riskerar att halka efter. Offentlig sektor måste därför kontinuerligt stärka sin kompetens och anpassa sina strategier, inte minst med tanke på att leva upp till de krav som ställs i ett föränderligt juridiskt landskap.

5

Lyft data, moln och cybersäkerhet till ledningens strategiska agenda för tydligt ägarskap och gemensamma prioriteringar

Studien visar att bristen på strategiskt ägarskap, gemensam förståelse och tydligt ledarskap är centrala hinder för att organisationer ska kunna ta välgrundade och långsiktiga beslut inom datastyrning, moln och cybersäkerhet. För att bryta detta mönster krävs att ledningen tar ett tydligt ansvar, skapar en gemensam begreppsbild och vågar definiera riskacceptans.ster krävs att ledningen tar ett tydligt ansvar, skapar en gemensam begreppsbild och vågar definiera riskacceptans.

Kontaktuppgifter

Du är välkommen att kontakta oss med dina frågor gällande datastyrning, molntjänster och cybersäkerhet inom offentlig sektor.

Per Wennström
Director, Management Consulting Public Sector

+46 73 511 02 35
per.wennstrom@kpmg.se

Visar Lapashtica
Partner, Cyber Security

+46 70 9143675
visar.lapashtica@kpmg.se

KPMG

Visiting address:
Vasagatan 16, Stockholm
Postal address:
P.O. Box 382
SE-101 27 Stockholm

Tel: +46 8 723 91 00
E-mail: info@kpmg.se

kpmg.se