Digital suveränitet i praktiken

En strategisk guide för svenska organisationer som vill behålla kontroll över data, identitet, drift och framtida handlingsfrihet.

Whitepaper · Molnkontoret · Version 1.0, publiceringsversion · 2026-07-08

> Detta whitepaper är ett strategiskt beslutsunderlag och ersätter inte juridisk rådgivning, DPIA, informationssäkerhetsanalys eller upphandlingsjuridisk granskning.

En strategisk guide för svenska organisationer som vill behålla kontroll över data, identitet, drift och framtida handlingsfrihet

Whitepaper Molnkontoret Version: 1.0 – publiceringsversion **Datum:** 2026-07-08

Redaktionell not

Detta whitepaper är framtaget som ett strategiskt beslutsunderlag för svenska organisationer som vill förstå och stärka sin digitala suveränitet (*digital sovereignty*). Det är inte juridisk rådgivning och ersätter inte en formell rättslig bedömning, DPIA, informationssäkerhetsanalys eller upphandlingsjuridisk granskning.

Molnkontoret använder begreppet digital suveränitet som ett praktiskt samlingsbegrepp för organisationens faktiska kontroll över data, identiteter, åtkomst, drift, integrationer, leverantörsberoenden och exitmöjligheter. Fokus ligger inte på teknik som ideologi, utan på handlingsfrihet, affärsrisk och långsiktig styrbarhet.

Executive summary

Digitaliseringens första fas handlade om att göra information och arbetsflöden digitala. Den andra fasen handlade om molnet. Den tredje fasen handlar om kontroll.

Svenska organisationer har under lång tid flyttat dokument, kommunikation, möten, identiteter och verksamhetskritiska processer till externa molntjänster (*cloud services*). Det har gett högre tillgänglighet, snabbare införande och starkare funktionalitet. Samtidigt har nya beroenden byggts in i organisationernas kärnprocesser.

Frågor som tidigare kunde hanteras som tekniska eller juridiska bilagor har blivit strategiska ledningsfrågor:

- Vem kontrollerar vår data?
- Vem kontrollerar våra identiteter?
- Vilka jurisdiktioner påverkar leverantören?

- Kan vi begränsa AI-funktioner och nya dataflöden?
- Kan vi exportera data, metadata, behörigheter och arbetsflöden?
- Kan vi byta leverantör, driftmodell eller plattform utan orimlig verksamhetspåverkan?

Digital suveränitet handlar inte om att all teknik måste ägas internt. Det handlar inte heller om att alla globala plattformar är olämpliga. Det handlar om att förstå vilka beroenden organisationen accepterar, vilka den bör minska och vilka den inte bör bygga in i verksamhetskritiska processer.

En organisation med låg digital suveränitet kan vara effektiv i dag men sakna handlingsfrihet i morgon. En organisation med högre digital suveränitet har bättre förmåga att hantera regulatoriska förändringar, minska leverantörsinlåsning (*vendor lock-in*), styra informationsflöden, använda AI mer ansvarsfullt och byta väg när förutsättningarna förändras.

Molnkontorets modell bygger på fem dimensioner:

1 Data

2 Identitet

3 Drift

4 Integrationer

5 Exit

Modellen är tänkt att användas i ledningsdiskussioner, upphandling, riskanalys, informationsklassning, molnstrategi, AI-strategi och förvaltningsplanering.

Huvudtesen är enkel:

Digital suveränitet är inte en teknisk detalj. Det är en ledningsfråga för att hantera risk, kostnad och framtida handlingsfrihet.

---

1. Varför digital suveränitet har blivit en ledningsfråga

1.1 Digitaliseringens blinda punkt

Digitalisering beskrivs ofta som en rörelse från analogt till digitalt, från lokalt till molnbaserat och från manuellt till automatiserat. Den beskrivningen är korrekt, men ofullständig.

När dokument, möten, chatt, identitet och samarbetsytor flyttas till externa plattformar flyttas inte bara teknik. Även kontrollpunkter flyttas.

Organisationen får nya möjligheter, men också nya beroenden. Det kan handla om beroenden till en leverantör, ett format, en identitetslösning, en licensmodell, en driftmodell, en integration eller ett juridiskt ekosystem.

Dessa beroenden är ofta osynliga så länge allt fungerar. De blir tydliga först när något förändras: en leverantör höjer priset, ett avtal ändras, en ny regulatorisk tolkning påverkar datahantering, AI-funktioner börjar behandla verksamhetsdata på nya sätt eller organisationen vill migrera till en annan lösning.

Digital suveränitet handlar om att identifiera dessa beroenden innan de blir verksamhetskritiska begränsningar.

1.2 Molnet löste många problem men skapade nya styrningsfrågor

Molntjänster har gjort det möjligt att snabbt få tillgång till skalbar infrastruktur, moderna samarbetsverktyg och löpande uppdaterade tjänster. Det är en stor styrka. Men samma egenskaper som gör molnet effektivt skapar också styrningsfrågor.

Organisationen behöver förstå:

- vem som styr driftmiljön,
- vem som har privilegierad åtkomst,
- vilka underleverantörer som används,
- hur support och fjärradministration fungerar,
- hur data kan exporteras,
- hur behörigheter kan återskapas,
- och vilka praktiska möjligheter som finns att lämna tjänsten.

När molnet var nytt sågs dessa frågor ofta som tekniska detaljer. I dag är de strategiska, särskilt för organisationer som hanterar personuppgifter, sekretessbelagd information, samhällsviktiga processer, kunddata, forskningsdata, teknisk dokumentation eller ledningsinformation.

1.3 Regelverken pekar mot mer kontroll

Flera regelverk och europeiska initiativ pekar i samma riktning: mer dokumenterad kontroll, tydligare ansvar och bättre förmåga att hantera digitala beroenden.

GDPR kräver att personuppgifter behandlas lagligt, säkert och ansvarsfullt. Det räcker inte att köpa en molntjänst. Organisationen behöver veta vem som har ansvaret, var data lagras, vilka underleverantörer som används och hur supportflödena ser ut. Om personuppgifter kan nås eller behandlas utanför EU/EES behöver det vara analyserat och dokumenterat.

Cybersäkerhetslagen, som genomför NIS2-direktivet i Sverige, gäller från den 15 januari 2026. Den ställer tydligare krav på riskanalyser, säkerhetsåtgärder, incidenthantering och ledningens ansvar för berörda

verksamheter. MSB beskriver cybersäkerhet som en ledningsfråga: ledningen ska förstå organisationens cybersäkerhetsrisker och övervaka det systematiska säkerhetsarbetet.

Det gör digital suveränitet direkt relevant för ledning och styrelse. För att kunna ta ansvar behöver ledningen veta vilka digitala beroenden som finns, vilka som är accepterade och vilka som kan påverka kontinuitet, dataskydd, säkerhet eller framtida handlingsfrihet.

EU:s Data Act stärker reglerna kring tillgång till och användning av data. En central del är att underlätta byte mellan leverantörer av databehandlingstjänster och stärka interoperabilitet (*interoperability*) och portabilitet (*portability*) på molnmarknaden.

AI Act och GDPR:s tillämpning på AI för in ytterligare en dimension. När AI används i verksamhetsprocesser behöver organisationen förstå vilken data som behandlas, var den behandlas, om frågor och svar sparas, vilka underleverantörer som används och hur mänsklig kontroll, loggning och ansvarsfördelning fungerar. Ur suveränitetsperspektiv är AI inte bara en funktion. Det är ett nytt lager av dataanvändning.

EU:s arbete med *sovereign cloud*, gemensamma dataområden (*data spaces*), Cloud and AI Development Act och teknologisk suveränitet visar samma riktning: digitalisering ska kunna kombineras med kontroll, säkerhet, interoperabilitet och europeisk handlingsfrihet.

1.4 Digital suveränitet ersätter inte dataskydd, informationssäkerhet eller cybersäkerhet

Digital suveränitet överlappar dataskydd, informationssäkerhet och cybersäkerhet, men är inte samma sak.

Dataskydd frågar: behandlas personuppgifter lagligt och ansvarsfullt?

Informationssäkerhet frågar: skyddas informationens konfidentialitet, riktighet och tillgänglighet?

Cybersäkerhet frågar: skyddas system och digitala tjänster mot hot, angrepp och incidenter?

Digital suveränitet frågar: kan organisationen kontrollera, påverka och förändra sin digitala miljö över tid?

En lösning kan vara GDPR-kompatibel men svår att lämna. Den kan vara tekniskt säker men skapa strategisk inlåsning. Den kan lagra data inom EU men ändå ha svag portabilitet, otydlig supportkedja eller beroenden till proprietära format.

Digital suveränitet binder därför samman juridik, säkerhet, arkitektur, upphandling, drift, verksamhet och ledning.

1.5 Vanliga felbedömningar

Det finns fyra vanliga förenklingar som bör undvikas.

För det första är EU-lagring inte samma sak som suveränitet. Geografisk placering är viktig, men organisationen behöver även förstå juridisk åtkomst, underbiträden, support, fjärradministration,

krypteringsnycklar och exportmöjligheter.

För det andra är svensk drift inte automatiskt digital suveränitet. En tjänst kan drivas i Sverige men ändå vara proprietär, svår att exportera från eller starkt leverantörskontrollerad.

För det tredje är öppen källkod (*open source*) inte automatiskt frihet. Öppen källkod kan ge transparens, portabilitet och möjlighet till oberoende drift, men utan dokumentation, förvaltning, säkerhetsprocesser och kompetens kan även en öppen lösning bli svår att kontrollera.

För det fjärde är digital suveränitet inte anti-amerikansk teknikpolitik. Många globala plattformar är tekniskt starka och kan vara rätt val i många sammanhang. Frågan är inte om en leverantör är “bra” eller “dålig”. Frågan är vilka beroenden organisationen accepterar.

---

2. Vad digital suveränitet betyder i praktiken

Digital suveränitet är organisationens förmåga att självständigt kontrollera, påverka och förändra sin digitala miljö över tid.

Det handlar inte om total självförsörjning. Det handlar inte om att all teknik måste vara egenutvecklad. Det handlar inte om att alla leverantörer måste vara svenska.

Det handlar om faktisk handlingsfrihet.

För en organisation innebär digital suveränitet att kunna fatta informerade beslut om:

- var data lagras,
- hur data behandlas,
- vem som har åtkomst,
- vem som kontrollerar identiteter,
- hur drift sker,
- vilka integrationer som används,
- vilka leverantörer som är kritiska,
- hur en tjänst kan lämnas,
- och hur organisationen kan byta väg när förutsättningarna förändras.

Digital suveränitet är inte ett ja-eller-nej-värde. En organisation kan ha stark kontroll över identitet men svag exitförmåga, god datalokalisering men låg portabilitet, eller hög cybersäkerhet men stark leverantörsinlåsning.

Därför behöver suveränitet bedömas dimension för dimension.

2.1 Ett mer användbart sätt att ställa frågan

Den vanliga frågan är:

> **Är lösningen säker?**

Den frågan är nödvändig, men inte tillräcklig.

En mer komplett fråga är:

> **Är lösningen säker, styrbar och möjlig att lämna?**

Säkerhet handlar om att skydda. Styrbarhet handlar om att kunna påverka. Exit handlar om att kunna förändra.

Alla tre behövs. Utan säkerhet blir lösningen riskfylld. Utan styrbarhet blir organisationen beroende av beslut den inte kontrollerar. Utan exit blir valfriheten teoretisk.

Ett enkelt exempel:

En organisation kan använda en säker samarbetsplattform med stark kryptering, hög tillgänglighet och avancerad hotdetektion. Den kan ändå ha låg digital suveränitet om metadata inte kan exporteras, behörigheter inte kan återskapas, externa användare inte granskas regelbundet eller nya AI-dataflöden inte kan begränsas per informationsklass.

Det betyder inte att plattformen är dålig. Det betyder att organisationen behöver veta var kontrollen slutar.

2.2 Kontroll ska följa informationens värde

Alla digitala arbetsytor behöver inte samma kontrollnivå. En organisation kan rimligen acceptera lägre suveränitet för lågkänsligt, kortlivat eller publikt material. Samma organisation kan behöva betydligt högre kontroll för styrelsehandlingar, upphandlingsmaterial, ledningsdokument, beredskapsinformation, kunddata eller känsliga projekt.

Digital suveränitet handlar därför inte om att göra allt maximalt kontrollerat. Det handlar om att placera rätt information i rätt miljö med rätt kontrollnivå.

En praktisk princip är:

> **Ju större konsekvens vid datatapp, otillåten åtkomst, förändrade leverantörsvillkor eller svår migration, desto högre krav på digital suveränitet.**

3. Molnkontorets femdimensionella modell

Molnkontorets modell gör digital suveränitet praktisk genom fem kontrollområden: data, identitet, drift, integrationer och exit.

Dimension	Huvudfråga	Typisk risk vid låg kontroll
Data	Kan vi kontrollera, förstå, skydda och flytta vår information?	Data kan inte exporteras, verifieras eller återskapas med sammanhang
Identitet	Kan vi kontrollera användare, grupper, roller och åtkomst?	Åtkomstmodellen blir inlåst i plattformen
Drift	Kan vi förstå, påverka och byta driftmodell?	Organisationen saknar insyn, alternativ och återställningsförmåga
Integrationer	Kan vi förändra vårt digitala ekosystem?	Verksamhetsprocesser låses till en viss leverantör
Exit	Kan vi lämna eller byta väg kontrollerat?	Avtalsmässig uppsägning finns, men praktisk exit saknas

3.1 Data

Datakontroll handlar inte bara om var data lagras. Det handlar om att kunna förstå, skydda, exportera och återskapa informationsmiljön.

För digitala samarbetsmiljöer är metadata ofta lika viktig som själva dokumentet. Ett dokument kan exporteras som fil, men organisationen behöver även veta vad som händer med ägare, behörigheter, versioner, kommentarer, delningslänkar, taggar, klassning och aktivitetsloggar.

En praktisk bedömning bör skilja mellan fem datalager:

Lager	Exempel	Varför det spelar roll
Primärdata	Dokument, filer, kalkylark, presentationer	Det mest uppenbara exportobjektet
Metadata	Ägare, datum, taggar, klassning	Krävs för sammanhang och livscykel
Behörighetsdata	Grupper, roller, delningslänkar	Krävs för att återskapa åtkomstkontroll
Aktivitetsdata	Loggar, kommentarer, versionshistorik	Krävs för spårbarhet och revision
Verksamhetskontext	Projektstruktur, mallar, processer	Krävs för att arbetet ska fungera efter flytt

Nyckelfrågan är inte bara “kan vi exportera filer?”. Frågan är “kan vi återskapa informationsmiljön?”.

3.2 Identitet

Identitet är en central inlåsningspunkt. I moderna arbetsmiljöer styr identiteten åtkomst till dokument, möten, chatt, projekt, integrationer, administration och AI-funktioner.

Identitetskontroll omfattar hela livscykeln: användare, grupper, roller, flerfaktorsautentisering, enkel inloggning, externa användare, servicekonton, privilegierad åtkomst, avveckling av användare och återkommande behörighetsgranskning.

Om organisationen inte kontrollerar sin identitetsmodell kontrollerar den inte fullt ut sin digitala miljö.

Identitet bör därför ses som en migrationsförsäkring. Ju mer dokumenterad, federerad och portabel identitetsmodellen är, desto lättare blir det att byta samarbetsplattform, driftmodell eller leverantör.

3.3 Drift

Drift är mer än serverplacering. Den omfattar infrastruktur, applikationsdrift, uppdateringar, backup, återställning, övervakning, support, incidenthantering, underleverantörer, loggning och ansvarsfördelning.

Digital suveränitet kräver inte att organisationen driver allt själv. Men organisationen bör förstå driftmodellen tillräckligt väl för att kunna bedöma risk, ansvar, kontinuitet och alternativ.

En viktig princip är tydlig ansvarsgräns: var slutar leverantörens ansvar och var börjar kundens? En driftad eller hanterad tjänst betyder sällan att kunden saknar ansvar. Kunden ansvarar ofta fortfarande för informationsklassning, behörigheter, användarhantering, integrationer, verksamhetsprocesser och beslut om riskacceptans.

> **Leverantören kan sköta driften, men organisationen äger fortfarande risken.**

Detta är särskilt viktigt för ledning och verksamhetsägare. En extern leverantör kan leverera tjänsten, men organisationen måste fortfarande kunna visa att risker är kända, kontroller är valda och ansvarsfördelningen är förstådd.

Backup utan testad återställning är inte en färdig kontroll. Det är ett antagande.

3.4 Integrationer

Integrationer skapar nytta men också beroenden. De kopplar samman samarbetsmiljön med identitet, ärendehantering, kundsystem, ekonomisystem, e-signering, AI, rapportering, loggplattformar, arkiv och verksamhetsapplikationer.

Integrationsskuld uppstår när dessa kopplingar växer fram utan tydlig ägare, dokumentation, testbarhet eller exitplan.

En integrationskatalog bör minst beskriva syfte, ägare, datatyper, system, autentisering, gränssnitt, driftansvar, felhantering, loggning, testmetod och exitpåverkan.

Det som inte finns i en integrationskatalog är svårt att styra. Det som är svårt att styra är svårt att lämna.

3.5 Exit

Exit är det tydligaste testet av digital suveränitet.

Många organisationer har avtalsmässig rätt att lämna en tjänst. Färre har praktisk förmåga att göra det.

Exit handlar inte bara om att säga upp ett avtal. Det handlar om att kunna återta kontroll över data, metadata, identiteter, behörigheter, dokumenthistorik, loggar, integrationer, arbetsflöden, arkiv och verksamhetsprocesser.

En praktisk exitplan bör innehålla ett konkret körschema för:

1 beslut och omfattning,
2 inventering av data, metadata, behörigheter och integrationer,
3 export och verifiering,
4 målmiljö,
5 migrering,
6 verksamhetsacceptans,
7 avveckling,
8 radering eller arkivering enligt avtal,
9 efterkontroll.

Exit ska inte behandlas som slutet av relationen. Exit är beviset på att relationen bygger på valfrihet.

---

4. Mognad och risk: från nuläge till prioritering

Digital suveränitet blir användbar först när organisationen kan bedöma två saker samtidigt:

1 Hur mycket kontroll har vi i dag?
2 Vilka risker uppstår där kontrollen är låg?

Mognadsmodellen och riskmatrisen ska därför inte behandlas som två separata övningar. De hör ihop. Mognaden visar var organisationen står. Riskmatrisen visar varför det spelar roll.

4.1 Fem mognadsnivåer

Molnkontorets mognadsmodell använder fem nivåer.

Nivå	Namn	Kort beskrivning	Typiskt nästa steg
1	Konsument / reaktiv	Organisationen använder digitala tjänster utan tydlig kontroll över beroenden	Kartläggning
2	Medveten	Organisationen känner till vissa beroenden men saknar full styrning	Dokumentation och ägarskap
3	Kontrollerad	Centrala beroenden, ansvar och kontroller är dokumenterade	Testning och verifiering
4	Strategisk	Kontroll används i arkitektur, upphandling, AI-strategi och förvaltning	Ledningsstyrning och återkommande uppföljning
5	Suverän	Organisationen har reell handlingsfrihet och kan byta väg kontrollerat	Optimering utan överstyrning

Målet är inte alltid nivå 5. För lågkänsliga standardtjänster kan nivå 2 eller 3 räcka. För verksamhetskritiska samarbetsmiljöer, känslig information eller samhällsviktiga processer bör organisationen normalt eftersträva minst nivå 3 och i vissa fall nivå 4.

Den viktiga poängen är att mognad inte ska räknas som ett enkelt genomsnitt. En organisation kan ha nivå 4 i drift men nivå 1 i exit. Det innebär fortfarande en strategisk svaghet.

4.2 Typiska risker vid låg digital suveränitet

Alla suveränitetsrisker är inte akuta cyberhot. Många är långsamma beroenden som växer fram över tid.

Risk	Typisk konsekvens	Berörda dimensioner	Prioriterad kontroll
Leverantörsinlåsning	Svårt eller dyrt att byta leverantör	Data, drift, integrationer, exit	Exitplan, exporttest, öppna format
Jurisdiktion och tredjelandsrisk	Osäker rättslig och regulatorisk kontroll	Data, drift	Dataflödeskarta, underbiträdeskontroll, krypteringsstyrning
Kompetens- och personberoende	Svag kontinuitet och beroende av enskilda personer	Drift, integrationer, exit	Dokumentation, ansvarsmatris, genomgångar
Proprietära format och låg	Data kan exporteras men inte	Data, exit	Exportformat, importtest,

portabilitet	användas effektivt		metadatakontroll
Identitets- och åtkomstrisk	Obehörig åtkomst eller svag spårbarhet	Identitet, data	Flerfaktorsautentisering, enkel inloggning, behörighetsgranskning, avveckling av användare
Integrationsskuld	Dolda beroenden och svår migration	Integrationer, drift, exit	Integrationskatalog, gränssnittsinventering, ägarskap
AI- och dataanvändningsrisk	Otydlig dataanvändning och ny inlåsning	Data, identitet, integrationer	AI-policy, dataflödeskarta, avgränsning per informationsklass

Riskmatrisen ska inte användas mekaniskt. Den ska användas som diskussionsunderlag mellan ledning, IT, informationssäkerhet, dataskydd, upphandling och verksamhet.

4.3 Exempel: en effektiv men inlåst miljö

Anta att en organisation använder en större global samarbetsplattform. Plattformen fungerar väl för användarna, har hög teknisk säkerhet och är etablerad i organisationens vardag.

En första suveränitetsprofil visar:

Dimension	Nivå	Kommentar
Data	3	Dokument kan exporteras, men metadata och behörigheter är oklara
Identitet	3	Enkel inloggning och flerfaktorsautentisering finns, men externa användare granskas inte systematiskt
Drift	2	Driftmodellen är känd på hög nivå men support- och underleverantörsled är otydliga
Integrationer	2	Flera verksamhetskritiska integrationer saknar ägare
Exit	1	Ingen praktiskt testad exitplan finns

Detta är inte nödvändigtvis ett akut problem. Men det är en strategisk signal. Organisationen är operativt effektiv men svag vid förändring.

Rimliga första åtgärder är inte att byta plattform direkt. Rimliga första åtgärder är att ta fram integrationskatalog, genomföra behörighetsgranskning, testa export av en projektmapp och dokumentera en första exitplan med körschema.

4.4 Från fynd till åtgärd

En suveränitetsbedömning bör alltid sluta i små, tydliga åtgärder.

Fynd	Risk	Åtgärd	Ägare	Tid
Exitplan saknas	Leverantörsinlåsning	Ta fram första exitplan med körschema	IT + upphandling	60 dagar
Externa användare granskas inte	Obehörig åtkomst	Genomför behörighetsgranskning	Systemägare	30 dagar
Återställning har inte testats	Kontinuitetsrisk	Genomför återläsningstest	Driftansvarig	60 dagar
Integrationer saknar ägare	Förändrings- och migrationsrisk	Skapa integrationskatalog	IT-arkitekt	90 dagar
AI-dataflöden är okända	Okontrollerad behandling	Kartlägg aktiva AI-funktioner	Informationssäkerhet	60 dagar

Det första målet är inte att bli “fullt suverän”. Det första målet är att sluta vara beroende utan att veta om det.

---

5. Strategiska vägval: komplettera, avgränsa eller ersätta

Digital suveränitet leder inte automatiskt till ett teknikbyte. Ofta är det första steget att stärka kontrollen över befintlig miljö. I andra fall är det mer rationellt att komplettera med kontrollerade arbetsytor. I vissa fall bör en befintlig plattform ersättas helt eller delvis.

Det avgörande är inte vilken plattform organisationen använder i dag. Det avgörande är vilken handlingsfrihet organisationen behöver i morgon.

5.1 Vägval 1: Stärk befintlig plattform

Detta är rätt väg när nuvarande plattform fungerar, användarna är beroende av den och risknivån är acceptabel.

Fokus bör då ligga på:

- bättre dokumentation,
- behörighetsgranskningar,

- tydligare AI-policy,
- exitplan,
- integrationskatalog,
- uppdaterad informationsklassning,
- och leverantörsuppföljning.

Detta är ofta snabbaste vägen från reaktiv användning till dokumenterad kontroll. Det är också en lågtröskelväg för organisationer som inte är redo för ny plattform men behöver bättre styrning.

Typiskt scenario:

> **En kommun eller ett bolag använder redan en etablerad molnplattform för majoriteten av sitt dagliga arbete. Den ska inte avvecklas. Däremot saknas överblick över externa användare, känsliga arbetsytor, AI-funktioner och praktisk exit.**

Rimligt första steg är en suveränitetsbedömning, inte en migration.

5.2 Vägval 2: Komplettera med kontrollerade arbetsytor

Organisationen kan behålla befintlig standardplattform men flytta känsligare samarbetsytor till en mer kontrollerad miljö.

Det kan gälla:

- styrelsearbete,
- nämndmaterial,
- upphandlingar,
- beredskap,
- ledningsdokument,
- känsliga projekt,
- leverantörsdialoger,
- eller samverkan med externa parter.

Detta är ofta den mest praktiska modellen. Allt behöver inte flyttas, men det som kräver högre kontroll hanteras separat.

Typiskt scenario:

> **Organisationen är nöjd med sin huvudsakliga digitala arbetsplats, men vissa processer har högre krav på datakontroll, åtkomst, svensk eller europeisk drift, spårbarhet och exit. Då kan**

> **en kontrollerad samarbetsyta införas som komplement.**

Fördelen är att organisationen kan minska risk där det betyder mest utan att störa all daglig produktivitet.

5.3 Vägval 3: Flytta känsliga processer till svensk eller europeisk drift

I vissa fall är det inte tillräckligt att bara stärka styrning ovanpå befintlig plattform. Organisationen kan behöva flytta specifika processer till en miljö där drift, support, underleverantörer och dataflöden är tydligare avgränsade.

Detta är särskilt relevant när informationen är känslig, när externa parter deltar eller när organisationen behöver kunna visa tydligare kontroll i upphandling, revision, DPIA eller informationssäkerhetsarbete.

Typiskt scenario:

> **Ett kommunalt bolag hanterar styrelsehandlingar, upphandlingsunderlag och teknisk dokumentation i en miljö där drift, supportkedja och AI-dataflöden är svåra att beskriva. Organisationen vill inte byta hela arbetsplattformen, men behöver en mer kontrollerad miljö för vissa processer.**

Detta vägval kräver tydliga regler för vad som ska ligga var. Annars skapas förvirring. Informationsklassning och enkel användarvägledning blir centrala.

5.4 Vägval 4: Ersätt befintlig plattform där kontrollbehovet kräver det

Molnkontoret behöver inte ersätta befintliga plattformar, men det kan göra det.

För vissa organisationer eller informationsklasser kan risk, kostnad, jurisdiktion, AI-dataflöden, upphandlingskrav eller leverantörsinlåsning motivera ett mer fullständigt byte.

Ersättning bör inte drivas som teknikbyte för teknikens skull. Den bör drivas när nuvarande plattform inte ger tillräcklig kontroll, portabilitet eller långsiktig handlingsfrihet.

Typiskt scenario:

> **En organisation har byggt mycket av sin interna och externa dokumenthantering i en plattform där licensmodell, AI-funktioner, exportmöjligheter och leverantörsberoenden inte längre matchar verksamhetens riskaptit. Ett kontrollerat alternativ blir då inte bara ett komplement, utan en möjlig ersättare.**

Ett sådant byte bör ske stegvis. Börja med en avgränsad process, testa export, verifiera behörigheter och bygg migrationsförmåga innan större delar flyttas.

5.5 Vägval 5: Kundägd eller dedikerad drift

För vissa verksamheter kan kundägd, dedikerad eller starkt avgränsad drift vara relevant.

Det betyder inte att organisationen måste göra allt själv. Det kan innebära att en partner driftar en miljö där kunden har större kontroll över:

- data,
- identitet,
- konfiguration,
- underleverantörer,
- loggning,
- backup,
- återställning,
- och exit.

Detta kan vara relevant för högre informationsklassning, samhällsviktig verksamhet, krav på svensk eller europeisk kontroll eller tydliga regulatoriska behov.

5.6 Beslutsprinciper

Följande principer gör vägvalet enklare.

Princip	Praktisk innebörd
Kontroll ska följa informationsklass	Allt behöver inte samma kontrollnivå
Exit ska designas före kris	Det är billigare att planera handlingsfrihet innan den behövs
Identitet är strategisk infrastruktur	En låst identitetsmodell gör hela miljön svår att flytta
Integrationer ska dokumenteras tidigt	Odokumenterade integrationer blir snabbt dolda beroenden
AI ska bedömas som dataflöde	AI är inte bara funktionalitet; det är ny åtkomst och ny behandling
Hybrid är normalt	En organisation kan ha olika miljöer för olika informationsklasser

Den praktiska frågan är inte:

> **Ska vi använda molntjänster?**

Den praktiska frågan är:

> **Vilka digitala tjänster ska vi använda för vilken information, med vilken kontrollnivå och med**

> **vilken exitförmåga?**

6. Molnkontorets operativa modell

De fem dimensionerna i detta whitepaper är inte bara ett analysverktyg. De är också grunden för hur Molnkontoret paketerar sina tjänster.

Molnkontoret utgår från att de flesta organisationer inte behöver börja med ett stort plattformsbyte. De behöver först förstå var kontrollen redan finns, var beroendena är otydliga och vilka arbetsytor som kräver högre suveränitet.

Därför kan Molnkontoret användas på tre nivåer: som analys, som avgränsad pilot och som långsiktig kontrollerad samarbetsmiljö.

6.1 Analys av öppen källkod och digital suveränitet

När det passar: Organisationen vill förstå nuläge, risker och möjligheter innan den fattar beslut om ny plattform, pilot, upphandling eller kompletterande miljö.

Vad vi gör: Molnkontoret kartlägger organisationens digitala beroenden utifrån de fem dimensionerna: data, identitet, drift, integrationer och exit. Analysen fokuserar på praktisk kontroll, inte på abstrakt teknikjämförelse.

Vad kunden får:

- suveränitetsprofil enligt femdimensionell modell,
- identifierade risker och beroenden,
- bedömning av data, identitet, drift, integrationer och exit,
- rekommenderad kontrollnivå per informationsklass,
- prioriterad åtgärdsplan,
- beslutsunderlag för ledning, IT, upphandling och informationssäkerhet.

Vad kunden slipper: Osäkerhet inför plattformsval, otydliga beroenden, svaga upphandlingsunderlag och diskussioner där tekniken hamnar före verksamhetsrisken.

Typiskt resultat: Organisationen får en tydlig bild av vilka beroenden som är acceptabla, vilka som bör reduceras och om nästa steg bör vara förstärkt styrning, kontrollerad pilot eller alternativ samarbetsmiljö.

6.2 Pilot för kontrollerad samverkan

När det passar: Organisationen vill testa en kontrollerad samarbetsyta i liten skala innan större beslut fattas.

Exempel på pilotområden:

- styrelse eller ledning,
- nämndarbete,
- upphandling,
- beredskap,
- känsligt projekt,
- extern leverantörsyta,
- samverkan mellan flera organisationer.

Vad vi gör: Molnkontoret sätter upp en avgränsad samarbetsyta med definierad åtkomst, dokumenterade dataflöden, tydlig driftmodell och enkel styrning. Piloten utformas för att visa både funktion och kontroll.

Vad kunden får:

- förkonfigurerad samarbetsyta,
- roll- och behörighetsmodell,
- dokumenterade dataflöden,
- support- och åtkomstmodell,
- backup- och återställningsupplägg,
- enkel styrningsdokumentation,
- export- och exittest för pilotens omfattning,
- rekommendation inför eventuell breddning.

Vad kunden slipper: Ett stort införande innan nyttan är verifierad. Piloten visar i liten skala om organisationen får bättre kontroll utan att störa hela den digitala arbetsplatsen.

Typiskt resultat: Organisationen får ett praktiskt bevis på hur kontrollerad samverkan kan fungera utan att först byta ut hela sin digitala arbetsplats.

6.3 Långsiktig och kontrollerad samarbetsmiljö

När det passar: Organisationen vill ha en långsiktig, kontrollerad samarbetsmiljö utan att själv bära hela drift- och förvaltningsbördan.

Vad vi gör: Molnkontoret levererar eller stödjer en samarbetsmiljö där drift, åtkomst, dokumentation, support, export och förvaltning är en del av tjänstens styrning från början.

Vad kunden får:

- svensk eller europeisk driftmodell,
- tydlig ansvarsgräns mellan kund, leverantör och eventuella underleverantörer,
- återkommande behörighetsgranskning,
- rapportering av drift, säkerhet och förändringar,
- stöd för DPIA-underlag och informationsklassning,
- integrations- och exportdokumentation,
- planerad exit och återkommande kontrollpunkter,
- möjlighet till kundägd, dedikerad eller partnerdriven drift beroende på behov.

Vad kunden slipper: En miljö som fungerar operativt men inte går att förklara, granska eller lämna. Målet är inte bara att erbjuda samarbete, utan att göra samarbetet styrbart över tid.

Typiskt resultat: Organisationen får en modern samarbetsmiljö som inte bara fungerar i vardagen, utan också kan granskas, styras och lämnas kontrollerat.

6.4 Tekniken är medlet, inte huvudbudskapet

Molnkontorets tekniska grund bygger på öppna och portabla principer. Det kan handla om öppna komponenter för filsamverkan, dokumentredigering, identitet, lagring, drift och automatiserad förvaltning.

Det tekniska valet är viktigt, men det är inte huvudbudskapet för ledningen.

Den viktigaste effekten är att organisationen minskar risken för plötsliga prishöjningar, svårförklarade dataflöden, otydlig AI-användning och leverantörsinlåsning.

Öppen teknik är en försäkring mot att kontrollen koncentreras till en enda leverantör. Molnkontorets roll är att göra den kontrollen användbar för verksamheten genom paketering, dokumentation, driftmodell och tydlig ansvarsfördelning.

6.5 Vad Molnkontoret inte kräver

Molnkontoret kräver inte att organisationen omedelbart lämnar sin befintliga plattform.

Molnkontoret kräver inte att all information flyttas.

Molnkontoret kräver inte att kunden själv bygger upp full driftorganisation.

Molnkontoret kräver inte att digital suveränitet behandlas som ett ideologiskt ställningstagande.

Rätt första steg är ofta mindre: förstå beroenden, välj kontrollnivå, testa en avgränsad samarbetsyta och bygg handlingsfrihet där den gör störst nytta.

7. Nästa steg: 30 dagar till bättre kontroll

Det första steget är inte ett teknikbyte. Det första steget är att ta reda på vilka beroenden som redan finns.

7.1 En enkel självskattning för ledningsgruppen

Ta med denna checklista till nästa ledningsmöte. Be IT, informationssäkerhet, dataskydd och upphandling svara **ja**, **delvis**, **nej** eller **vet ej**.

Om majoriteten av svaren är **vet ej** eller **delvis** finns en strategisk sårbarhet som kräver ledningens uppmärksamhet. Det betyder inte att organisationen måste byta plattform direkt. Det betyder att ledningen saknar ett tillräckligt beslutsunderlag om sina digitala beroenden.

Område	Ledningsfrågor	Ja	Delvis	Nej	Vet ej
Data	Vet vi var vår data lagras? Vet vi vilka metadata som skapas? Kan vi exportera data och metadata i användbart format? Har vi testat återställning?	☐	☐	☐	☐
Identitet	Vet vi vem som äger identiteterna? Har vi fungerande inloggnings- och behörighetsstyrning? Har vi rutin för externa användare och avveckling av användare? Genomför vi återkommande behörighetsgranskning?	☐	☐	☐	☐
Drift	Vet vi vem som driftar tjänsten? Vet vi vilka underleverantörer som används? Finns tydlig ansvarsmatris? Har återställning testats?	☐	☐	☐	☐
Integrationer	Har vi en katalog över våra viktigaste integrationer? Vet vi vilka integrationer som är verksamhetskritiska? Finns ägare för tekniska kopplingar och systemkonton?	☐	☐	☐	☐
Exit	Finns exitplan? Har exit testats? Vet vi vilka data och metadata som inte kan exporteras? Vet vi vad exit kostar och hur lång tid den tar?	☐	☐	☐	☐

Tolkning:

- “Vet ej” betyder att frågan behöver utredas innan ledningen kan fatta ett tryggt beslut.
- “Delvis” betyder att kontrollen finns i någon form, men att ansvar, dokumentation eller test behöver stärkas.
- “Nej” betyder att området bör prioriteras i en åtgärdsplan.
- “Ja” bör kunna styrkas med dokumentation, ansvarig ägare eller genomfört test.

7.2 Första 30 dagarna

En realistisk start kräver inte ett stort program. Den kräver en tydlig första inventering.

Prioritera:

1 Lista de viktigaste samarbetsmiljöerna.

2 Identifiera ägare för varje miljö.

3 Kartlägg externa användare och delningslänkar.

4 Identifiera känsliga arbetsytor.

5 Lista kända integrationer.

6 Samla avtal och underbiträdeslistor.

7 Bedöm om AI-funktioner är aktiverade.

8 Välj en arbetsyta för export- eller återställningstest.

Efter 30 dagar bör organisationen åtminstone kunna svara på:

- Vilka samarbetsmiljöer använder vi?
- Vilka är mest verksamhetskritiska?
- Vilka har högst informationsrisk?
- Var saknar vi kontroll i dag?

7.3 Efter 60 och 90 dagar

Efter 60 dagar bör organisationen ha dokumenterat de viktigaste kontrollpunkterna: dataflöden, identitet, driftansvar, integrationsägare och första exitbedömning.

Efter 90 dagar bör organisationen ha testat handlingsfrihet i liten skala: export av projektmapp, återställning, borttag av extern användare eller avveckling av en enklare integration.

Det räcker ofta för att skilja antaganden från faktisk kontroll.

7.4 Slutsats

Digital suveränitet handlar inte om att säga nej till molnet. Det handlar om att använda digitala tjänster utan att förlora kontrollen över data, identitet, drift och framtida vägval.

För svenska organisationer blir frågan mer akut av fyra skäl:

1 digitala samarbetsmiljöer har blivit verksamhetskritiska,

2 regelverken kräver mer dokumenterad styrning,

3 AI skapar nya dataflöden och beroenden,

4 leverantörsinlåsning blir dyrare ju längre den får växa.

Den praktiska frågan är därför inte:

> **Vilken teknik använder vi?**

Den praktiska frågan är:

> **Vilken handlingsfrihet behåller vi?**

Nästa steg behöver inte vara ett plattformsbyte. Det kan vara en avgränsad bedömning av var kontrollen redan finns, var beroendena är otydliga och vilka arbetsytor som bör hanteras med högre suveränitet. För många organisationer räcker det som första beslutspunkt: vad kan vi fortsätta använda, vad bör vi komplettera och vad bör vi inte längre lägga i en standardplattform?

Molnkontoret hjälper organisationer att besvara den frågan, först som analys och pilot, därefter som kontrollerad samarbetsmiljö där det behövs.

Källor

[1] NIST, *SP 800-145: The NIST Definition of Cloud Computing*. https://csrc.nist.gov/pubs/sp/800/145/final

[2] Integritetsskyddsmyndigheten, *Grundläggande principer enligt GDPR*. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

[3] Integritetsskyddsmyndigheten, *Överföring av personuppgifter till tredjeland*. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/

[4] Integritetsskyddsmyndigheten, *GDPR och AI*. https://www.imy.se/verksamhet/ai/gdpr-och-ai/

[5] Integritetsskyddsmyndigheten, *AI-förordningen*. https://www.imy.se/verksamhet/ai/ai-forordningen/

[6] Regeringen, *Nu skärps kraven på svensk cybersäkerhet*. https://www.regeringen.se/pressmeddelanden/2026/01/nu-skarps-kraven-pa-svensk-cybersakerhet/

[7] MSB, *Det här är cybersäkerhetslagen*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/det-har-ar-nis2-direktivet/

[8] MSB, *Cybersäkerhetslagen för ledningen*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/nis2-for-ledningen/

[9] European Commission, *Data Act*. https://digital-strategy.ec.europa.eu/en/policies/data-act

[10] European Commission, *Data Act explained*. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

[11] European Commission, *Common European Data Spaces*. https://digital-strategy.ec.europa.eu/en/policies/data-spaces

[12] European Commission, *Strengthening Europe's Tech Sovereignty*. https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en

[13] European Commission, *Cloud and AI Development Act*. https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act

[14] European Commission, *Sovereign Cloud Framework explained*. https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en

[15] European Commission, *Cloud Sovereignty Framework – Implementation guidance*. https://commission.europa.eu/document/download/2ad80a48-166f-4c77-a513-80c53ca2a128_en?filename=Cloud+Sovereignty+Framework+-+Implementation+guidance.pdf

[16] NIST, *The NIST Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/cyberframework

[17] ISO, *ISO/IEC 27001 – Information security management systems*. https://www.iso.org/standard/27001

[18] OWASP, *API Security Top 10 2023*. https://owasp.org/API-Security/editions/2023/en/0x11-t10/