



Köpa molntjänster i offentlig sektor

Handbok – Innehåller exempel på språk för
offertförfrågan för ett molnramavtal

Meddelanden

Det här är endast ett informationsdokument. Det har inte tagits fram i enlighet med juridiska krav för offentliga upphandlingar inom någon särskild region. Kunderna ansvarar själva för att göra egna oberoende utvärderingar av informationen i det här dokumentet och vid all användning av en molnleverantörs produkter eller tjänster. Detta dokument ger inte upphov till någon garanti, några sakförhållanden, avtalsmässiga åtaganden, betingelser eller försäkringar.

Exempel på dokument och språk ska inte tolkas som juridisk rådgivning eller vägledning. Molnkunder ska rådgöra med juridisk rådgivare om sina förpliktelser enligt gällande lag i det land där de är verksamma. CISPE frånsäger sig uttryckligen alla garantier eller förpliktelser eller skador relaterade till eller som orsakas på grund av informationen i detta dokument.

Köpa molntjänster i offentlig sektor

Om CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, <https://cispe.cloud>) är en ideell oberoende branschorganisation. Vi representerar tjänsteleverantörer av molninfrastruktur i Europa och arbetar med branschaktörer och beslutsfattare för att tillhandahålla vägledning och utbildning om molntjänster och deras roll i branschen, det offentliga livet och samhället i allmänhet.

I vår växande gemenskap ingår företag som är verksamma i alla EU-länder och som har sitt globala huvudkontor i 16 europeiska länder. Organisationen är öppen för företag om de kan uppvisa att minst en av deras tjänster uppfyller kraven i CISPE:s uppförandekod för dataskydd. Vi:

- förordar fördelarna med offentlig upphandlingspolitik för molnet först inom EU och EU:s medlemsstater
- främjar enhetliga säkerhetskrav och tekniska standarder som omfattar hela EU
- stödjer omfattande integritetskrav med en uppförandekod
- arbetar för att hålla EU:s marknad för molninfrastruktur öppen, konkurrenskraftig och fri från låsning
- förhindrar oskäligen skyldigheter för innehållsövervakning i EU:s rättsliga ramverk.

Våra medlemmar tillhandahåller och upprätthåller de nödvändiga ”byggstenarna för IT” som gör det möjligt för regeringen, offentliga myndigheter och företag att bygga sina egna system och tillhandahålla nödvändiga tjänster till miljarder medborgare. Där hjälper vi till med att möjliggöra utvecklingen av avancerad teknik och tjänster som använder artificiell intelligens (AI), sammankopplade föremål, självkörande fordon och 5G samt nästa generations teknik för cellulär uppkoppling.

Uppförandekod för molninfrastruktur tjänster

CISPE:s kod togs fram innan EU:s dataskyddsförordning (GDPR) började gälla. Den överensstämmer med de strikta kraven i GDPR för att hjälpa leverantörer av molninfrastruktur med att uppfylla och erbjuda ett starkt ramverk som hjälper kunder att välja molnleverantörer och lita på deras tjänster. CISPE:s uppförandekod omfattar fler än 100 tjänster som tillhandahålls av över 30 molnföretag med huvudkontor i fler än 16 EU-medlemsstater och som används av miljontals slutanvändare och konsumenter. <https://cispe.cloud/code-of-conduct/>

CISPE och den offentliga sektorn

CISPE bidrar till den europeiska debatten om offentliga riktlinjer och arbetar för att säkerställa ökad förståelse av rollen som, bidraget från och potentialen hos Europas molninfrastrukturbransch.

Modellen för offentlig upphandling ska bestämma processen för anpassning och användning av molntjänster, men upphandlingen av molntjänster skiljer sig från de flesta upphandlingarna av traditionell teknik som den offentliga sektorn känner till. Hanteringen av upphandlingar måste omprövas: CISPE uppmuntrar beslutsfattare inom EU att utveckla en mer ambitiös och framtidsinriktad hantering på EU-nivå som baseras på politiska initiativ om ”moln först” för att bidra till att främja tillväxten av den inre marknaden för molninfrastruktur i Europa och optimera tillväxtmålen för den digitala inre marknaden (DSM).

Denna handbok är utformad för att tillhandahålla användbar vägledning och support till offentliga myndigheter vid upphandling av molntjänster.

Köpa molntjänster i offentlig sektor

Mer information

CISPE-medlemmar: <https://cispe.cloud/members>

Styrelse: <https://cispe.cloud/board-of-directors>

Molntjänster som omfattas av CISPE:s uppförandekod: <https://cispe.cloud/publicregister>

Innehåll

Meddelanden	2
Om CISPE	3
Innehåll	4
Sammanfattning av och syfte med handboken	1
1.0 Översikt över ett molnramavtal	3
2.0 Översikt över offertförfrågan för molntjänster	7
2.1 Upprätta offertförfrågan för molntjänster	7
2.1.1 Inledning och strategiska mål	7
2.1.2 Tidslinje för respons på offertförfrågan	9
2.1.3 Definitioner	10
2.1.4 Detaljerad beskrivning av köpmodellen och konkurrensen inom ramavtalet	11
2.1.5 Minsta krav på anbudsgivare – administrativt	15
2.2 Tekniskt	17
2.2.1 Minsta krav	18
2.2.2 Jämförelse mellan leverantörer	21
2.2.3 Upphandling	22
2.3 Säkerhet	24
2.3.1 Minsta krav	24
2.3.2 Jämförelse mellan leverantörer	28
2.3.3 Upphandling	28
2.4 Priser	29
2.4.1 Minsta krav	29
2.4.2 Jämförelse mellan leverantörer	31
2.5 Konfiguration av/villkor för avtalets fullgörande	33
2.5.1 Villkor	33
2.5.2 Välja mellan mottagare efter projekt	36
2.5.3 Introduktion och utträde	36
3.0 Bästa praxis/lärdomar	36
3.1 Molnstyrning	37
3.2 Budgetera för molnet	37
3.3 Förstå partnerns affärsmodell	39
3.4 Molnmäklare	39
3.5 Inköps-/marknadsundersökning av offertförfrågan som hålls i förtid	40
Bilaga A – Tekniska krav för att jämföra olika anbudsgivare	41
1. Molnleverantörens profil	41
2. Global infrastruktur	41

Köpa molntjänster i offentlig sektor

3. Infrastruktur	42
3.1 Databehandling.....	42
3.2 Nätverk	45
3.3 Lagring	49
4. Administration	53
5. Säkerhet.....	54
6. Efterlevnad	56
7. Migreringar	61
8. Fakturering	63
9. Hantering.....	63
10. Support	65
Bilaga B - Demonstration.....	67

v 2020 05 11

Sammanfattning av och syfte med handboken

Syftet med den här **handboken för att köpa molntjänster** är att tillhandahålla vägledning till de molnkunder som vill köpa molntjänster genom en konkurrenskraftig upphandling (**offertförfrågan för molntjänster**), men saknar expertisen att upprätta ett molnramavtal.

Det här är endast ett informationsdokument. Det har inte tagits fram i enlighet med juridiska krav för offentliga upphandlingar inom något särskilt land eller särskild region.

Handboken beskriver även språk för ytterligare urvalskriterier för **avrop** eller **minitävlingar** vid upphandling genom ett molnramavtal. Avsnitten i handboken är ordnade för att efterlikna en allmän offertförfrågan för IT. Exempel på allmän offertförfrågan och språk för urvalskriterier åtföljs av kommentarer som förklarar varför en offertförfrågan för moln skiljer sig från en traditionell offertförfrågan för IT.

”Molntjänster” syftar på alla molntekniker och relaterade tjänster som en slutanvändare kan behöva åtkomst till. Det inbegriper konsulttjänster eller professionella/hanterade tjänster för att stödja och köra en migreringsåtgärd till molnet och stödja arbetsbelastningar i molnet, utöver själva molninfrastrukturen, och molntjänster på marknadsplatser, till exempel SaaS-produkter (Software as a Service).

Uppkomsten av molntjänster som standardval för den offentliga sektorns IT utgör ett tillfälle att modernisera befintliga upphandlingsstrategier. Molnriktade upphandlingar kan bidra till att enheter i den offentliga sektorn kan dra nytta av fördelarna med molnet, till exempel åtkomst till avancerad innovation, ökad hastighet och flexibilitet, förbättrad säkerhet, regelefterlevnad och styrning, samtidigt som effektiviteten och kostnadsbesparingarna ökar.

Traditionella metoder för IT-upphandling vid köp av maskinvara, programvara och datacenter är inte desamma som vid köp av molntjänster. Hanteringen av bland annat priser, avtalsstyrning, villkor, säkerhet, tekniska krav och servicenivåavtal ser annorlunda ut i en molnmodell. Om befintliga upphandlingsmetoder används i dessa fall minskar eller elimineras fördelarna med molnet.

Ett av de bästa sätten för effektiv offentlig upphandling av molntjänster är med ett **molnramavtal** – en tilldelning av en uppsättning moln till flera organisationer där berättigade inköpare som är kopplade till den upphandlande organisationen kan upphandla molntekniker och relaterade tjänster som uppfyller och passar deras behov. Om sådana ramavtal används som avtalsinstrument går det att upphandla molntjänster på ett effektivt sätt. Det resulterar i att upphandlarorganisationer och slutanvändarenheter får åtkomst till en fullständig uppsättning molntjänster och i slutänden drar nytta av fördelarna med molnet: flexibilitet, omfattande stordriftsfördelar, skalbarhet för ökad tillgänglighet till lägre kostnader, ett brett spektrum funktioner, hög innovationstakt, förmåga att anpassa sig till nya geografiska platser.

Observera att **det här dokumentet fokuserar på inköp av molntekniker för IaaS (Infrastructure as a Service) och PaaS (Platform as a Service) som tillhandahålls av en molntjänstleverantör (CISP)**. Sådan molnteknik kan köpas direkt från en molntjänstleverantör eller genom en återförsäljare till en molntjänstleverantör. *Ytterligare överväganden om offertförfrågan krävs för distributörer av molntjänster på marknadsplatser (PaaS och SaaS) och för molnkonsulttjänster.*

Köpa molntjänster i offentlig sektor

Observera även att det här dokumentet inte omfattar varje aspekt av att skapa ett heltäckande ramverk för molninköp. Det finns många andra dokument från branschen och analytiker som behandlar frågor som bästa praxis för molninköp, att budgetera för moln, molnstyrning osv. och vi rekommenderar starkt att sådana råd och dokument tas i beaktande under utvecklingen av en övergripande strategi för molninköp.

Tabell 1 nedan beskriver handboken om offertförfrågan för molntjänster och var exempel på språk för offertförfrågan finns för varje del av en offertförfrågan för molntjänster.

Tabell 1 – Sammanfattning av avsnitten i handboken om offertförfrågan för molntjänster

Avsnitt	Översikt och exempel på språk för offertförfrågan
1.0 Översikt över ett molnramavtal	En översikt över modellen för ett molnramavtal (områden, tillvägagångssätt för att delta och upphandling)
2.0 Översikt över offertförfrågan för molntjänster	Exempel på språk för allmän offertförfrågan som omfattar avsnitten nedan, tillsammans med kommentarer som förklarar den logiska grunden bakom strukturen hos offertförfrågan för molntjänster och språket som används.
2.1 Upprätta offertförfrågan för molntjänster	2.1.1 Inledning och strategiska mål 2.1.2 Tidslinje för respons på offertförfrågan 2.1.3 Definitioner 2.1.4 Detaljerad beskrivning av köpmodellen och konkurrensen inom ramavtalet 2.1.5 Minsta krav på anbudsgivare – administrativt
2.2 Tekniskt	2.2.1 Minsta krav 2.2.2 Jämförelse mellan leverantörer 2.2.3 Upphandling
2.3 Säkerhet	2.3.1 Minsta krav 2.3.2. Jämförelse mellan leverantörer 2.3.3 Upphandling
2.4 Priser	2.4.1 Minsta krav 2.4.2 Jämförelse mellan leverantörer
2.5 Konfiguration av/villkor för avtalets fullgörande	2.5.1 Villkor 2.5.2 Välja mellan mottagare per projekt 2.5.3 Introduktion och utträde
3.0 Bästa praxis/lärdomar	3.1 Molnstyrning 3.2 Budgetera för molnet 3.3 Förstå partnernes affärsmodell 3.4 Molnmäklare 3.5 Inköps-/marknadsundersökning av offertförfrågan som hålls i förtid
Bilaga A – Tekniska krav för att jämföra olika anbudsgivare	En lista över allmänna krav på molnteknik för avrop eller minitävlingar
Bilaga B - Demonstration	Ett exempelskript för bedömning av produktvisning av molnteknik (molndemonstrationer som en del av avrop eller minitävling)

1.0 Översikt över ett molnramavtal

Ett väl utformat molnramavtal kan möjliggöra inköpet av molntjänster på ett sätt som gynnar både de deltagande organisationerna i den offentliga sektorn och molnleverantörerna. Några av fördelarna med ett väl utformat molnramavtal är följande:

- **Samarbetsinriktat:**
 - Flera organisationer som samlas för att lägga beställningar för liknande krav är praktiskt, effektivt, sänker kostnaderna och förenklar beställningsprocessen. Det skapar ett effektivt sätt att samla krav från flera olika organisationer i den offentliga sektorn för vanlig molnteknik och tillhörande molntjänster, till exempel marknadsplatslösningar och konsulttjänster.
- **Komplett sortiment av molntjänster**
 - Det kan omfatta alla konsulttjänster/professionella tjänster/hanterade tjänster som behövs för att ge fullständigt stöd åt och helt genomföra migreringen till molnet och stödja arbetsbelastningar i molnet, utöver molnteknik från molntjänstleverantörer och marknadsplatstjänster.
 - Sådan molnteknik kan köpas direkt från en molntjänstleverantör eller genom en utvald återförsäljare.
- **Avtalsstyrning:**
 - Det samlar organisationer/inköpare kring en gemensam uppsättning villkor och kring ett och samma tilldelningsbeslut, i stället för att ha olika för varje organisation.
 - Det är också till fördel för leverantörerna eftersom det bara finns en upphandlingsprocess, en uppsättning villkor och en beställningsmekanism att hantera, i stället för att varje organisation inom offentlig sektor har en egen.
 - Det ökar flexibiliteten. För att skapa, godkänna och upprätthålla ett effektivt molnavtal inom befintliga statliga policyer/föreskrifter krävs experimentering och möjligheten till snabba justeringar. Det är mycket mer fördelaktigt att skapa ett ramavtal som gör att den offentliga sektorn och molnleverantörer kan samarbeta för att förbättra avtalet – avtalsmässigt, mekaniskt och effektivt. Ett flerårigt avtal som inte fungerar och inte kan justeras leder till en dålig upplevelse för den offentliga sektorns slutanvändare, upphandlingsorganisationer och molnleverantörer.
- **Val:**
 - Det ger inköpare möjligheten att välja mellan flera behöriga molntjänstleverantörer och sätter ribban högt för alla molntjänster och tillhörande tjänster, till exempel en molnmarknadsplats för PaaS/SaaS och molnkonsulttjänster.
 - Det ger kontroll över flera leverantörer i ett ramverk genom att säkerställa att varje mottagares standard granskas nog.

Ett ramavtal för att köpa molntjänster fungerar bäst när det omfattar kärntekniker för IaaS/PaaS från molntjänstleverantörer, tillsammans med en marknadsplats för PaaS/SaaS och konsulttjänster som den

Köpa molntjänster i offentlig sektor

offentliga sektorns slutanvändare får åtkomst till när de behöver det för att hjälpa dem att planera, överföra, använda och upprätthålla en arbetsbelastning i molnet. Därför föreslår vi att en offertförfrågan för molntjänster för att upprätta ett molnramavtal delas in i tre områden enligt nedan:

- **OMRÅDE 1 – MOLNTEKNIK**

Molnteknik som köps direkt från en molntjänstleverantör eller genom en utvald återförsäljare till en molntjänstleverantör.

- **OMRÅDE 2 – MARKNADSPLATS**

Åtkomst till en marknadsplats för PaaS- och SaaS-tjänster.

- **OMRÅDE 3 – MOLNKONSULTTJÄNSTER**

Molnrelaterade konsulttjänster (utbildning, professionella tjänster, hanterade tjänster osv.) och teknisk support.

*Som nämnts tidigare fokuserar det här dokumentet på molntekniker för IaaS och PaaS (**OMRÅDE 1**) som tillhandahålls av en molntjänstleverantör (köps direkt från en molntjänstleverantör eller genom en återförsäljare till en molntjänstleverantör). Separata kvalificeringskrav för leverantörer krävs för leverantörer i områdena 2 och 3 i en offertförfrågan för molntjänster.*

Bild 1 nedan ger en överblick över hur en väl utformad offertförfrågan för molntjänster, indelad i dessa tre områden, kan leda till att ett molnramavtal ger enheter i offentliga sektorn ökad flexibilitet (både tekniskt och avtalsmässigt), insyn i och kontroll över kostnader och molnanvändning, tillsammans med möjligheten att ha alla molntjänster som krävs för att skapa och upprätthålla de tjänster som de behöver.

Köpa molntjänster i offentlig sektor

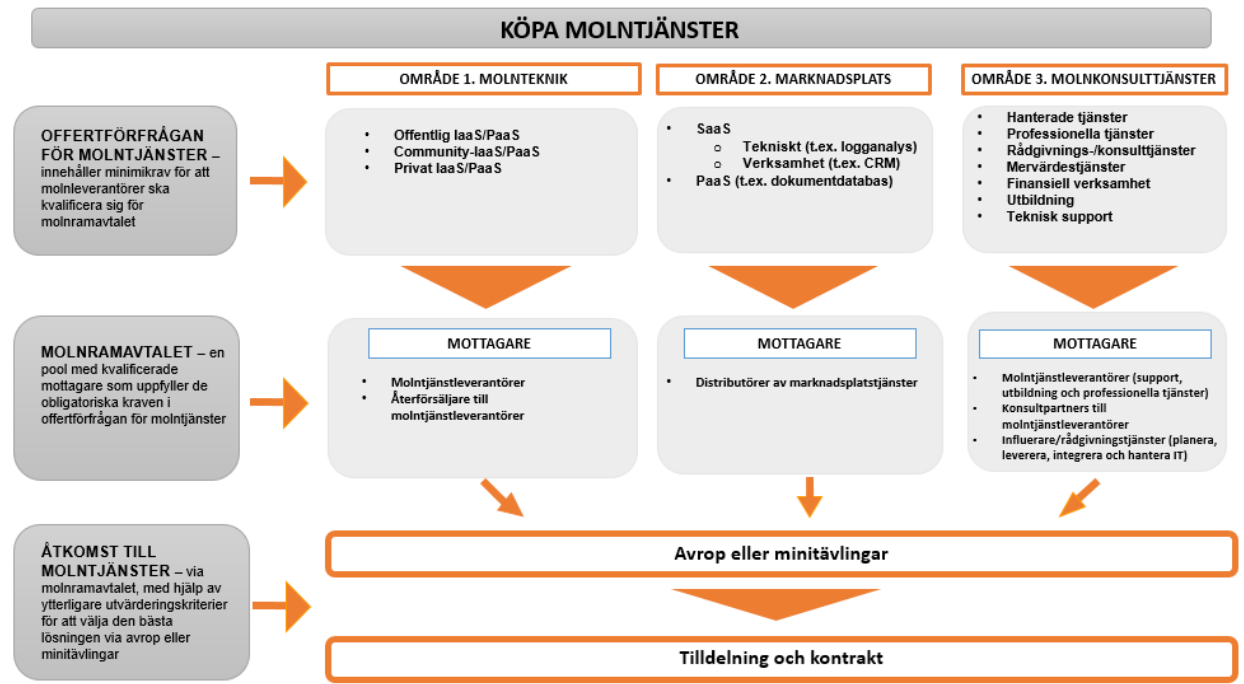


Bild 1 – En framgångsrik offertförfrågan för molntjänster delas in i tre områden. Varje område innehåller kategorier eller ”typer av erbjudanden” i respektive område för att säkerställa en teknisk och avtalsmässig lösning som uppfyller slutanvändarnas krav vid upphandlingen av molnramavtalet.

Obs!

- Varje område kan tilldelas flera mottagare.
- OMRÅDE 3 kan tilldelas via en annan offertförfrågan eller möjligtvis via ett befintligt avtal för konsulttjänster.

OMRÅDE 1 Kategorier

I framgångsrika molnramavtal får molntjänstleverantörer beskriva modellen för molnet de erbjuder, uppdelad i kategorier inom varje område. Vi rekommenderar att branschstandarden för molntjänster används ([väsentliga molnegenskaper enligt National Institute of Standards and Technology \(NIST\)](#)) – för definitionerna av **offentligt** moln, **community**moln och **privat** moln. Genom att strukturera ett molnramavtal på det här sättet kan upphandlingsbyråer och offentliga organ som använder ramverket välja bland flera olika molnmodeller som passar deras behov.

Se *avsnitt 2.1.3 Definitioner* för NIST-definitionen av varje molnmodell i OMRÅDE 1 (offentlig IaaS/PaaS, community IaaS/PaaS och privat IaaS/PaaS).

Tillvägagångssätt för att delta – avrop eller minitävlingar?

Krav på leverantören för en offertförfrågan för molntjänster bör omfatta viktiga delar och minsta standarder och inte inbegripa standarder som ”kan vara bra att ha”. Om ytterligare standarder utöver de

Köpa molntjänster i offentlig sektor

grundläggande läggs till för att kvalificera leverantörer för ramverket kan det leda till att vissa leverantörer inte kan lämna anbud och inköparna får färre deltagare att välja mellan.

Genom att följa offertförfrågan och efterföljande lösning för molnramavtalet kan organ i offentliga sektorn som är part i ramverket beställa eller göra avrop på de molntjänster de behöver när de behövs. Om ett avropsavtal läggs till under ett ramavtal kan köpare finjustera krav med ytterligare funktionsspecifikationer för avrop och samtidigt behålla fördelarna i ramavtalet.

Om det anses nödvändigt kan en liten tävling anordnas för att identifiera den bästa leverantören för en särskild arbetsbelastning eller ett särskilt projekt. En liten tävling innebär att en kund öppnar upp för ytterligare konkurrens under ramavtalet genom att bjuda in alla leverantörer inom ett område att svara på en uppsättning krav. Kunden bjuder in alla kapabla leverantörer inom området att lämna anbud, varför det är viktigt med minsta krav för mottagare i en offertförfrågan för molntjänster eftersom det säkerställer alternativ med hög standard inom ett särskilt område.

*Observera att det är viktigt att det finns **olika uppsättningar av villkor** för avtal för varje område enligt bild 1 ovan. Ett "tillvägagångssätt där en lösning passar alla" i upphandling för alla områden leder till problem med teknisk genomförbarhet och kompatibilitet.*

2.0 Översikt över offertförfrågan för molntjänster

Det här avsnittet beskriver modellen och omfattningen av offertförfrågan för molntjänster, bland annat: strategiska mål, deltagare, definitioner, tidslinje och administrativa minsta krav. Vi påminner om att fokus i den här handboken ligger på **OMRÅDE 1 – MOLNTEKNIK**.

2.1 Upprätta offertförfrågan för molntjänster

Vi rekommenderar starkt att enheter i den offentliga sektorn är tydliga med sina mål på högre nivå och krav i inledningen till offertförfrågan för molntjänster.

2.1.1 Inledning och strategiska mål

För att få fram de strategiska målen på ett tydligt sätt är det bra praxis att i inledningen till offertförfrågan för molntjänster förklara **(1)** de affärsområden och fördelar som organisationen vill uppnå genom användningen av molnet; **(2)** ramavtalets struktur – vem köper, vem driver, vem budgeterar osv.; **(3)** en tydlig förståelse för modellen med delat ansvar mellan den offentliga sektorn och molnleverantörerna, vilket är kärnan i en framgångsrik upphandling och användning av molnet, och **(4)** typen av relation som skapas mellan molntjänstleverantörer (CISP:er), distributörer av marknadsplatstjänster, konsultpartners, statliga upphandlingsbyråer och statliga slutanvändare. Att förklara de här fyra punkterna hjälper organisationer att ta fram en offertförfrågan som passar deras behov bäst. Dessutom säkerställer det att både kunden och leverantörerna är på det klara med offertförfrågans mål.

En offertförfrågan för moln skiljer sig avsiktligt från traditionella offertförfrågningar för IT. Molntechniken är inte en likvärdig ersättning för traditionella databehandlingsmetoder – den inför ett helt nytt sätt att konsumera teknik. Väl utformade offertförfrågningar för molntjänster kan hjälpa enheter i den offentliga sektorn att röra sig snabbt för att dra nytta av molnet.

Av alla aspekter som vi nämner som bra praxis vid inköp av moln är nog en tydlig förståelse för modellen för delat ansvar den bästa utgångspunkten. Modellen för delat ansvar¹ används för det mesta när man diskuterar säkerhet och överensstämmelse i molnet, men denna uppdelning av ansvarsområden gäller alla delar av molntjänsterna. En offertförfrågan för molntjänster bör tydligt visa vad i en molnmiljö som ligger på molntjänstleverantörens ansvar och vad som förblir kundens ansvar. En molntjänstleverantör tillhandahåller till exempel funktionerna för att övervaka resurser och program som körs i molnet, **men** det är kundens ansvar att faktiskt använda funktionerna som molntjänstleverantören tillhandahåller, eftersom en molntjänstleverantör som är verksam i stor skala inte är utformad för att göra detta för miljontals kunder.

Dessutom bör molnkunder förstå hur en molntjänstleverantörs partnersätverk hjälper kunder att använda molnet och hantera sina ansvarsområden. En leverantör av hanterade tjänster (MSP) kan till exempel hjälpa en kund att konfigurera och använda övervakningsfunktioner från en molntjänstleverantör för att uppfylla deras unika krav på efterlevnad och granskning.

Enkelt uttryckt är ansvarsområdena i molnmodellen följande:

¹ Se avsnitt 5 i CISPE:s uppförandekod för leverantörer av molninfrastruktur tjänster: <https://cispe.cloud/website-cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf>

Köpa molntjänster i offentlig sektor

En molntjänstleverantör tillhandahåller molntekniken

En kund använder molntekniken

Konsultföretag (i tillämpliga fall) hjälper en kund att få åtkomst till och använda molntekniken

”Konsultföretag” är företag med konsulttjänster och hanterade/professionella tjänster som hjälper kunder att utforma, skapa, bygga, migrera och hantera deras arbetsbelastningar och program i molnet. Sådana företag är bland annat systemintegratörer, strategiska konsulter, byråer, leverantörer av hanterade tjänster och återförsäljare av mervärde.

Att ”handla” molntjänster kan jämföras vid att handla i en fysisk järnhandel. I en järnhandel finns det ett omfattande utbud av material och verktyg för att bygga det du vill. Du kan bygga ett skåp, en simbassäng eller ett helt hus – det är upp till dig. När du köper material och verktyg kan personalen i järnhandeln ge dig välgrundade råd, men de följer inte med dig hem och bygger något åt dig. Det här gör att du har några alternativ:

1. Köpa material och verktyg själv och bygga på egen hand.
2. Köpa material och verktyg själv och anlita någon att bygga eller köra något åt dig.
3. Anlita någon att bygga/köra något åt dig och låta dem tillhandahålla material och verktyg som en del i det övergripande erbjudandet.

Om en organisation har den interna kompetensen att skapa och hantera en molnmiljö och molnlösningar själv, då behöver den egentligen bara få åtkomst till den standardiserade molntekniken och verktygen från molntjänstleverantören (direkt från en molntjänstleverantör eller genom en återförsäljare till en molntjänstleverantör – se **OMRÅDE 1**). Nödvändig programvara för SaaS och PaaS bör vara tillgänglig på en molnmarknadsplats (**OMRÅDE 2**). Om ytterligare konsulttjänster eller hjälp med migrering, implementering eller hantering behövs kan en molntjänstleverantörs partnernetverk stå till tjänst (**OMRÅDE 3**).

Exempel på språk för offertförfrågan: inledning och strategiska mål

Molntjänster ger organisationer i den offentliga sektorn snabb åtkomst till ett brett utbud av flexibla och kostnadseffektiva IT-resurser där du bara betalar för det du använder. Organisationer kan tillhandahålla rätt typ och storlek på de resurser som de behöver för att komma igång med nya bra idéer eller driva sina IT-avdelningar, samtidigt som de slipper stora investeringar i maskinvara eller långsiktiga avtal för programvarulicenser.

<ORGANISATION> har ett krav för åtkomst till dessa typer av kommersiellt tillgänglig molnteknik för att tillgodose företagets behov i ett brett spektrum av kopplade organisationer.

Huvudsyftet med den här offertförfrågan är att tilldela ett parallellt <RAMAVTAL> utan ensamrätt med upp till <x> leverantörer som representerar olika molntekniker och molnrelaterade tjänster.

1. **OMRÅDE 1.** Molntjänstleverantörer (CISP:er) eller återförsäljare till en molntjänstleverantör för köp av molnteknik
2. **OMRÅDE 2.** Leverantörer av marknadsplatstjänster.

Köpa molntjänster i offentlig sektor

3. **OMRÅDE 3.** Leverantörer av konsulttjänster för att tillhandahålla ytterligare kunskap vid migrering till och användning av dessa erbjudanden från molntjänstleverantörer

I **OMRÅDE 1** måste organisationer som lämnar anbud (molntjänstleverantörer eller återförsäljare till en molntjänstleverantör) redovisa hur deras erbjudande uppfyller dessa mål:

- **Flexibilitet** – Göra IT-resurser tillgängliga för slutanvändare på bara några minuter i stället för de traditionella tidslinjerna på veckor och månader.
- **Innovation** – Ha omedelbar åtkomst till den nyaste och mest innovativa tekniken på marknaden.
- **Kostnad** – Byta ut anläggningskostnader mot rörliga kostnader (t.ex. CapEx till OpEx). Du betalar endast för de resurser som förbrukas.
- **Budget** – Visa fakturerings- och användningsinformation både på detaljnivå och översiktligt, visualisera utgiftsmönster över tid och prognostisera framtida utgifter.
- **Elasticitet** – Få lägre rörliga kostnader från de större stordriftsfördelarna som molnet ger.
- **Kapacitet** – Slipp gissa om infrastrukturens kapacitetsbehov.
- **Sluta förlita dig på datacenter** – Fokusera på våra medborgare snarare än på grovgöret i form av hanteringen av fysiska servrar.
- **Säkerhet** – Formalisera kontodesignen med bättre synlighet och granskningsmöjligheter av resurser och slipp kostnaden för att skydda anläggningar och fysisk maskinvara.
- **Delat ansvar** – Lätta på den operativa bördan då molntjänstleverantören driver, hanterar och styr komponenterna från värdoperativsystemet och virtualiseringskiktet ned till den fysiska säkerheten i anläggningarna där tjänsterna tillhandahålls.
- **Automatisering** – Bygg in automation i molnarkitekturen för bättre möjlighet att bygga ut systemet säkrare, snabbare och mer kostnadseffektivt.
- **Molnstyrning** – (1) börja med en fullständig inventering av alla IT-tillgångar, (2) hantera alla dessa tillgångar centralt och (3) skapa varningar gällande användning/fakturering/säkerhet/osv. – alla med möjlighet till tillgångsspårning, lagerhantering, ändringshantering, logghantering och -analys samt övergripande synlighet och molnstyrning.
- **Kontroll** – Få fullständig insyn i hur IT-tjänster konsumeras och var de kan finjusteras med avseende på säkerhet, tillförlitlighet, prestanda och kostnad.
- **Reverserbarhet** – Verktyg och tjänster för portabilitet som hjälp vid migrering till och från molntjänstleverantörens infrastruktur, för att minimera låsningen till en viss leverantör och respektera branschens uppförandekoder
- **Dataskydd** – Möjlighet att bevisa efterlevnad av dataskyddsförordningen (GDPR) genom en särskild uppförandekod för molninfrastruktur-tjänster inom branschen: [CISPE:s uppförandekod för dataskydd](#).
- **Transparens** – Kunder bör ha rätt att få veta var infrastrukturerna som används för att behandla och lagra deras data finns (stadsområde).

2.1.2 Tidslinje för respons på offertförfrågan

Det är bra praxis att förse anbudsgivarna med en tidslinje över förväntad anbudsaktivitet vid upprättandet av ett molnramavtal och tillhörande offertförfrågan för molntjänster. Ju mer engagemang i branschen

Köpa molntjänster i offentlig sektor

desto bättre. Det hjälper till att säkerställa att det finns en tydlig förståelse bland alla parter för offertförfrågans krav och för hur alla leverantörstjänster passar in i molntjänstmodellen.

Observera att offertförfrågans tidslinje följer lokala lagar och juridiska skyldigheter. Listan nedan är avsedd att fungera som en guide med bästa praxis snarare än att vara en normativ lista över aktiviteter och tidsramar.

Exempel på språk för offertförfrågan: tidslinje för respons

Se offertförfrågans tidslinje nedan för offertförfrågan för molntjänster:

Tidslinje för offertförfrågan för molntjänster
<ul style="list-style-type: none">• <i>Version av begäran om information (RFI):</i>• <i>Respons på begäran om information:</i>• <i>Version av utkast för offertförfrågan (RFP):</i>• <i>Utkast för offertförfrågan senast:</i>• <i>Branschens konsultationsfas: <tidslinjer></i>• <i>Version av förkvalificerad offertförfrågan:</i>• <i>Respons på förkvalificerad offertförfrågan:</i>• <i>Version av offertförfrågan:</i>• <i>Runda 1 Frågor senast:</i>• <i>Runda 1 Svar:</i>• <i>Runda 2 Frågor senast:</i>• <i>Runda 2 Svar:</i>• <i>Respons på offertförfrågan senast:</i>• <i>Period för förtydligande av förfrågan:</i>• <i>Förhandlingsperiod:</i>• <i>Datum för försök till tilldelning:</i>• <i>Tilldelningsbeslut:</i>• <i>Avtalets varaktighet (alternativ till förlängning):</i>

Observera att offertförfrågans tidslinje följer lokala lagar och juridiska skyldigheter. Listan nedan är avsedd att fungera som en guide med bästa praxis snarare än att vara en normativ lista över aktiviteter och tidsramar.

2.1.3 Definitioner

En offertförfrågan för molntjänster ska innehålla en detaljerad lista med definitioner. Denna lista omfattar leverantörroller (t.ex. molntjänstleverantör, molnåterförsäljare, leverantörspartner), allmänna teknikkoncept (databehandling, lagring, IaaS/PaaS, SaaS) och andra viktiga delar av avtalet. Här är ett exempel på en definitionslista:

Exempel på språk för offertförfrågan: definitioner

Köpa molntjänster i offentlig sektor

Definitionerna nedan är definitioner för molntjänster enligt National Institute of Standards and Technology (NIST).²

- **Infrastructure as a Service (IaaS).** Funktionen som konsumenten tillhandahålls är att etablera bearbetning, lagring, nätverksanslutning och andra fundamentala databehandlingsresurser där kunden kan distribuera och köra valfri programvara som operativsystem och program. Konsumenten hanterar eller styr inte den underliggande molninfrastrukturen men har kontroll över operativsystem, lagring och distribuerade program, och har möjligtvis begränsad kontroll över utvalda nätverkskomponenter (som värdbaserade brandväggar).
- **Platform as a Service (PaaS).** Funktionen som konsumenten tillhandahålls är att distribuera program som skapats av konsumenten eller förvärvade program som skapats med hjälp av programmeringsspråk, bibliotek, tjänster och verktyg som stöds av leverantören till molninfrastrukturen.³ Konsumenten hanterar eller styr inte den underliggande molninfrastrukturen som nätverk, servrar, operativsystem eller lagring, men har kontroll över distribuerade program och möjligtvis konfigurationsinställningarna för miljön där programmen körs.
- **Software as a Service (SaaS).** Funktionen som konsumenten tillhandahålls är att använda leverantörens program som körs i en molninfrastruktur. Programmen är tillgängliga från flera olika klientenheter via antingen ett tunt klientgränssnitt, som en webbläsare (t.ex. webbaserad e-post) eller ett programgränssnitt. Konsumenten hanterar eller styr inte den underliggande molninfrastrukturen som nätverk, servrar, operativsystem, lagring eller ens individuella programfunktioner, med det möjliga undantaget för begränsade konfigurationsinställningar för användarspecifika program.
- **Offentligt moln.** Molninfrastrukturen tillhandahålls för fri användning av allmänheten. Den kan ägas, hanteras och drivas av ett företag, en akademisk organisation eller en myndighetsorganisation, eller en kombination av dessa. Den finns lokalt hos molnleverantören.
- **Communitymoln.** Molninfrastrukturen tillhandahålls för exklusiv användning av en specifik konsumentcommunity från organisationer som har gemensamma intressen (som uppdrag, säkerhetskrav, policy och efterlevnadsöverväganden). Den kan ägas, hanteras och drivas av en eller flera av organisationerna i communityn, en tredje part eller en kombination av dessa och kan finnas både lokalt och externt.
- **Hybridmoln.** Molninfrastrukturen är en kombination av två eller fler olika molninfrastrukturer (privat, community eller offentligt) som förblir unika enheter, men som binds samman av standardiserad eller egen teknik som möjliggör data- och programportabilitet (till exempel kapacitetsstyrd omdirigering till molnet för lastbalansering mellan moln).
- **Privat moln.** Molninfrastrukturen tillhandahålls för exklusiv användning av en enda organisation som består av flera konsumenter (till exempel affärsenheter). Den kan ägas, hanteras och drivas av organisationen, en tredje part eller en kombination av dessa och kan finnas både lokalt och externt.

2.1.4 Detaljerad beskrivning av köpmodellen och konkurrensen inom ramavtalet

Som beskrivs ovan bör organisationer i den offentliga sektorn identifiera modellen för hur ett ramavtal fungerar som en köpmekanism för molnteknik och relaterade tjänster för implementering och hantering. Detta ska framgå tydligt i offertförfrågan för molntjänster så att molnteknikleverantörer, relaterade organisationer som erbjuder konsulttjänster, marknadsplatsdistributörer och upphandlingsenheter förstår sina respektive roller.

Vad gäller ramavtalets omfattning och följande avrop och minitävlingar bör organisationer överväga följande:

² <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Köpa molntjänster i offentlig sektor

- Vem ska ansvara för integreringstjänster och hanterade tjänster som inbegriper användningen av molntekniken under avtalet?
- Är det ett krav för en återförsäljare/partner till molntjänstleverantören att tillhandahålla tjänster med mervärde utöver upprätthållandet av en avtalsmässig relation med molntjänstleverantören och tillhandahålla samlingsfaktureringsstjänster och direktåtkomst i rätt tid till användnings- och faktureringsdata relaterade till användningen av molnleverantörens tjänster?
- Behövs en återförsäljare av fullständiga tjänster med mervärde, en systemintegratör eller en leverantör av hanterade tjänster eller någon annan typ av IT-arbetstjänster?

Det är viktigt att notera att en molntjänstleverantör inte är en systemintegratör (SI) eller leverantör av hanterade tjänster (MSP). Många kunder i den offentliga sektorn behöver en molntjänstleverantör för sina IaaS/PaaS och överlåter konsulttjänster och praktisk planering, migrering och hantering till en systemintegratör eller leverantör av hanterade tjänster. Nedan visas en bild av uppdelningen av rollerna och ansvarsområdena i molntjänstmodellen i **bild 2**.

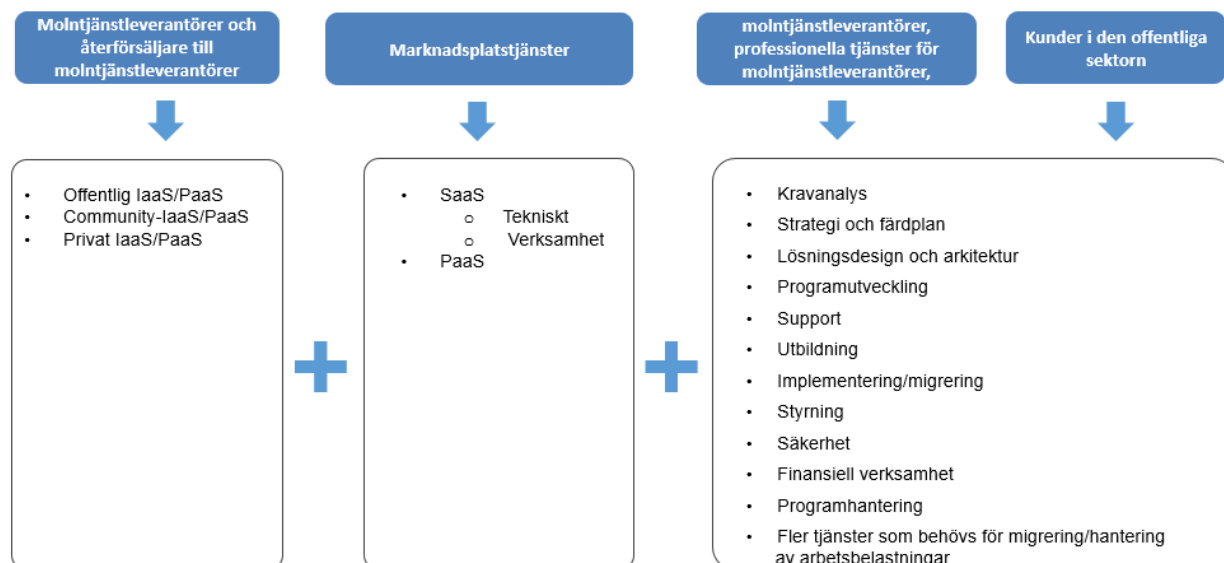


Bild 2 – En offertförfrågan för molntjänster ska förse slutanvändare med en uppsättning molntjänster som de behöver. Kunder i den offentliga sektorn behöver en molntjänstleverantör för molnteknik och eventuellt en marknadsplats för PaaS- och SaaS-produkter. Därefter kan kunderna bestämma hur stor roll de vill anta i leveransen av molntjänster och hur mycket de har tänkt överlåta till ett konsultföretag/systemintegratör/leverantör av hanterade tjänster/osv.

Exemplet på språk nedan är format efter rollerna och ansvarsområdena som visas i bild 2 ovan. Ett molnramavtal och tillhörande offertförfrågan för molntjänster ska säkerställa att köpare har möjlighet att på ett lämpligt sätt bedöma varje leverantörs erbjudande, så att de kan välja bland de tjänster som behövs för arbetsbelastningen/projektet. Detta görs på bästa sätt genom att dela upp tjänsterna i de redan nämnda områdena och genom att vara tydlig med hur avrop och minitävlingar utförs under ramavtalet.

Köpa molntjänster i offentlig sektor

Exempel på språk för offertförfrågan: köpmodell

Detta avtal fungerar som ett **ramverk** för köp. Detta molnramavtal innehåller flera **områden** som definieras av <ORGANISATION> för molnteknik och relaterade marknadsplatstjänster/-produkter, konsulttjänster, professionella tjänster/systemintegration/hanterade tjänster/migrering, professionella tjänster, utbildning och support som definieras av <ORGANISATION> och kan användas av flera berättigade köpare med koppling till <ORGANISATION>. Detta förenklar upphandlingen samtidigt som det optimerar stordriftsfördelarna.

När ramavtalet är upprättat kan organisationer köpa den specifika molntekniken och de molnrelaterade tjänsterna de vill ha när de behöver dem, i stället för att köpa dem genom separata upphandlingar. Ett sådant tillvägagångssätt minskar de administrativa kraven och minskar upphandlingens komplexitet och cykeltid avsevärt.

Ramavtalets giltighet är högst <X> år, inklusive eventuella förnyelser. Den längsta giltigheten för ett ramavtal för avrop är normalt <X> månader. Det kan förlängas till <X> månader och sedan ytterligare <X> månader, med de korrekta interna godkännandena som behövs för en sådan förlängning. Detta anges för varje specifikt **avrop**.

RAMVERKET är indelat i **3 (tre) områden**.

1. **OMRÅDE 1: MOLNTEKNIKER** – molnleverantörens teknik (direkt från molntjänstleverantör, från återförsäljare eller från återförsäljare med tjänster/support med mervärde):
 - i. **IaaS- och PaaS-tjänster** – en uppsättning molntekniker som databehandling, lagring, nätverk, databas, analys, programtjänster, distribution, hantering, utveckling, sakernas internet (IoT) osv.). Innehåller paketerade molntekniklösningar som DR/COOP, Archive, Big Data & Analytics, DevOps osv.
2. **OMRÅDE 2: MARKNADSPLATS** – samtliga PaaS- och SaaS-tjänster/-produkter som redovisning, CRM, design, HR, GIS och mappning, HPC, BI, innehållshantering, logganalys osv.
3. **OMRÅDE 3: MOLNTJÄNSTER** – samtliga konsulttjänster (hanterade tjänster, professionella tjänster, rådgivnings-/konsulttjänster, tjänster med mervärde, FinOps, teknisk support) relaterade till molnmigrering- och användning. Dessa tjänster kan omfatta planering, design, migrering, hantering, support, kvalitetssäkring, säkerhet, utbildning osv.

Leverantörer kan skicka sina erbjudanden till flera områden.

Leverantörer kan skicka sina erbjudanden och relaterade priser i vilket format som helst.

KONKURRENS INOM RAMVERKET OCH TILLDELNING AV AVTAL

AVROP

Organ i den offentliga sektorn som är part i ramavtalet kan beställa eller göra avrop på tjänsterna som de behövde vid behov. Om ett avropsavtal läggs till under ramavtalet kan köpare finjustera krav med ytterligare funktionsspecifikationer för avrop och samtidigt behålla fördelarna i ramavtalet.

Avtal som tilldelas genom ramavtal kan visa ett tydligt revisionsspår vad gäller krav som används för att välja en leverantör inom varje område. Slutköpare registrerar kommunikationen med leverantörer, bland annat eventuellt tidigt marknadsengagemang, förtydligade frågor, e-postmeddelanden och personliga samtal.

1. SKRIVA AVROPSKRAV OCH SÖKA INTERNT GODKÄNNANDE FÖR KÖP

Köpa molntjänster i offentlig sektor

Alla slutköpare som är berättigade att använda ramavtalet skapar gemensamma team med företagslutanvändare, upphandlingsspecialister och tekniska experter för att förbereda en lista över vad som behövs och vad som önskas. Dessa krav bidrar till att fastställa vilka områden som är tillämpliga och vilken leverantör som är bäst kvalificerad att uppfylla kraven. Köpare överväger följande vid utarbetandet av kraven:

- Tillgängliga medel för att använda tjänsten
- Tekniska och upphandlingsrelaterade krav för projektet
- Kriterier som valet ska baseras på.

2. SÖKA EFTER TJÄNSTER

Köpare under ramavtalet använder en ramverkskatalog online (en portal där de kvalificerade mottagarna för ramavtalet och deras tjänster presenteras) för att hitta produkter/tjänster som tillgodoser deras identifierade behov. De väljer lämpliga områden och söker sedan efter tjänster.

3. GRANSKA OCH UTVÄRDERA TJÄNSTER

Köpare under ramavtalet granskar tjänstebeskrivningarna för att hitta de tjänster som bäst tillgodoser behoven baserat på både krav och budget. Varje tjänstebeskrivning innehåller följande:

- Dokument med tjänstebeskrivning eller länkar till tjänstedefinitioner
- Dokument med villkor
- Dokument med pris (länkar till offentliga priser accepteras under förutsättning att ett dokument med en fullständig prislista/pris finns tillgänglig på begäran)

Priset är kostnaden för tjänstens vanligaste konfiguration. Däremot baseras pris ofta på volym, så köpare bör alltid titta på leverantörens dokument för pris eller allmänna priser och priskalkylatorverktyg för att ta reda på det faktiska priset för det som köps och det övergripande värdet för köparen (till exempel tjänster för optimering och resulterande kostnadssänkningar).

Köpare under ramavtalet kan prata med leverantörer för att be dem att förklara sina tjänstebeskrivningar, villkor, pris eller dokument med/modell för tjänstedefinitioner. Ett register med eventuella samtal med leverantörer kommer att föras.

4. VÄLJ EN TJÄNST OCH TILLDELA ETT AVTAL

En leverantör

Om endast en leverantör uppfyller kraven kan ett avtal tilldelas till denna.

Flera leverantörer

Om det finns flera tjänster på en slutlista väljer köparen den tjänst som har det ekonomiskt mest fördelaktiga anbudet (MEAT). Se kriterierna i följande tabell för den MEAT-baserade bedömningen. Köpare kan bestämma vilka detaljerade egenskaper som ska användas och hur de ska viktas.

Observera att köparen kan behöva:

- titta på kombinationer av flera leverantörer
- hämta specifik information om volym- eller företagsrabatter och kostnadsoptimerade tjänster för leverantörer.

Köpa molntjänster i offentlig sektor

Bedömningen av leverantörer ska alltid vara rättvis och transparent. Valet baseras på vem som lämpar sig bäst och leverantörer/tjänster utesluts inte utan att hänvisa tillbaka till projektkraven.

Tabell 2 – MEAT-baserad bedömning

Tilldelningskriterier
<i>Kostnad för hela livscykeln: kostnadseffektivitet, pris och löpande kostnader</i>
<i>Tekniska fördelar och funktioners lämplighet: täckning, nätverkskapacitet och prestanda enligt relevanta tjänstenivåer</i>
<i>Hantering av tjänster efter försäljning: hjälpcentral, dokumentation, funktion för kontohantering och försäkras om leverans av ett tjänsteutbud</i>
<i>Icke-funktionella egenskaper</i>

MINITÄVLINGAR

Om det anses nödvändigt kan en liten tävling anordnas för att identifiera den bästa leverantören för en särskild arbetsbelastning eller ett särskilt projekt. En liten tävling innebär att en kund öppnar upp för ytterligare konkurrens under ramavtalet genom att bjuda in alla leverantörer inom ett område att svara på en uppsättning krav. Kunden bjuder in alla kapabla leverantörer inom området att lämna anbud. Se ytterligare jämförelseinformation i avsnitten nedan angående teknik, säkerhet och pris/värde.

AVTAL

Både köparen och leverantören undertecknar ett exemplar av avtalet innan tjänsten kan användas. Den längsta giltigheten för ett ramavtal är normalt <x> månader. Det kan förlängas till <x> månader och sedan ytterligare <x> månader, med de korrekta interna godkännandena som behövs för en sådan förlängning.

Ett exemplar av avtalet måste undertecknas av alla intresserade parter (köparen och leverantören) innan tjänsten kan användas.

2.1.5 Minsta krav på anbudsgivare – administrativt

Ett enkelt och tydligt språk för ramavtalets krav på leverantören hjälper till att säkerställa att det inte förekommer anbud från traditionella datacenter eller maskinvaruleverantörer som förpackar en traditionell lösning som ett "moln". Deltagare i offertförfrågan ska visa hur de uppfyller de minsta administrativa kraven på anbudsgivare.

Observera återigen att det här dokumentet fokuserar på **OMRÅDE 1 – MOLNTEKNIK**. Vi har dock lagt till ytterligare information om **OMRÅDE 2 – MARKNADSPLATS** och **OMRÅDE 3 – MOLNTJÄNSTER** när den bidrar till att ge ett övergripande sammanhang vad gäller krav och omfattning för offertförfrågan. Det är till exempel viktigt att inkludera de minsta kraven på leverantören för en återförsäljare till en molntjänstleverantör/leverantör av hanterade tjänster/systemintegratör/konsultföretag/osv. och det hjälper till att säkerställa att de (1) är direkt kopplade till molntjänstleverantören som återförsäljare eller kanalpartner, (2) är certifierade av en molntjänstleverantör att sälja direktåtkomst till molntjänstleverantörens erbjudanden till tredjepartsenheter och (3) har certifieringar från de molntjänstleverantörer som fastställer deras kunskaper och expertis

Exempel på språk för offertförfrågan: minsta krav på anbudsgivare – administrativt

Detta ramavtal tilldelar avtal till flera leverantörer i följande kategorier. Leverantörerna måste vara kommersiella molntjänstleverantörer, en tredjepartsåterförsäljare till en molntjänstleverantör, en distributör av marknadsplatstjänster eller en leverantör av tjänster för att använda en molntjänstleverantör (till exempel konsulttjänster, migreringstjänster, hanterade tjänster, FinOps osv.). Identifiera rollerna du lämnar anbud för:

Köpa molntjänster i offentlig sektor

OMRÅDE 1

___ – Direktleverantör (molntjänstleverantör) av offentliga molntjänster (IaaS OCH PaaS)

___ – Direktleverantör (molntjänstleverantör) av communitymolntjänster (IaaS OCH PaaS)

___ – Direktleverantör (molntjänstleverantör) av privata molntjänster (IaaS OCH PaaS)

___ – Tredjepartsåterförsäljare till en molntjänstleverantör (möjlighet att ge direktåtkomst till en molntjänstleverantörs erbjudanden om onlinemoln).

- Identifiera för vilket av molntjänstleverantörens erbjudanden som du kan sälja direktåtkomst till tjänsten: _____
- Tillhandahåll ett brev från molntjänstleverantören om att du är en auktoriserad återförsäljare av deras erbjudanden: _____

OMRÅDE 2

___ – Direktleverantör av marknadsplatstjänster som körs via en molntjänstleverantör (PaaS eller SaaS)

___ – Distributör av marknadsplatstjänster som körs via en molntjänstleverantör (PaaS eller SaaS)

OMRÅDE 3

___ – Molntjänstleverantör som tillhandahåller professionella tjänster

___ – Leverantör av molntjänstleverantörens tekniska support

___ – Partner till molntjänstleverantör som tillhandahåller tjänster för användning eller drift via en molntjänstleverantör

___ – Partner till molntjänstleverantör som tillhandahåller tjänster för användning eller drift via en molntjänstleverantör

Identifiera typen av erbjudande:

- Hanterade tjänster av arbetsbelastningar hos en molntjänstleverantör (J/N): _____
 - Identifiera specialiteter (i tillämpliga fall): _____
- Professionella tjänster: (J/N): _____
- Konsulttjänster – utbildning (J/N): _____
- Konsulttjänster – strategi (J/N): _____
- Konsulttjänster – migrering (J/N): _____
- Konsulttjänster – molnstyrning (J/N): _____
- Konsulttjänster – FinOps (J/N): _____
- Konsulttjänster – övrigt (identifiera): _____

Identifiera molnleverantören som du tillhandahåller tjänster för: _____

Tillhandahåll ett brev från molntjänstleverantören som bekräftar att du är fastställd partner enligt molntjänstleverantörens modell: _____

OMRÅDE 1 MINSTA ADMINISTRATIVA KRAV

Köpa molntjänster i offentlig sektor

Molntjänstleverantörer (CISP:er)

För att kvalificeras som en molntjänstleverantör måste kraven nedan uppfyllas.

Föreslagna krav på molntjänstleverantören	Anledning
Information om organisationen, till exempel namn, juridisk struktur, registrerings-/DUNS-nummer, momsregistreringsnummer osv.	
Företagets storlek, ekonomisk och finansiell ställning ³	Kunden kan avgöra om molntjänstleverantören kan fullgöra avtalet.
Skäl till uteslutning, till exempel kriminella/bedrägliga aktiviteter osv.	
Fallstudier/kundreferenser (ange nödvändigt antal/typ)	Kunden kan mäta molntjänstleverantörens erfarenhet av att tillhandahålla tjänsterna som krävs.
Företagets sociala ansvar	Detta ska vara offentliga versioner som molntjänstleverantören tillhandahåller.
Offentliga hållbarhetsåtaganden och praxis	Kunden kan se att en molntjänstleverantör strävar efter att driva sin verksamhet på ett så miljövänligt sätt som möjligt
Molntjänstleverantören måste uppvisa styrkt erfarenhet inom innovation och lansering av nya, användbara tjänster och funktioner under de senaste fem åren, särskilt inom PaaS, maskininlärning och analys, big data, hanterade tjänster och optimerade funktioner för molnanvändning. Offentliga ändringsloggar eller uppdateringsflöden kan användas som bevis.	Visar att molntjänstleverantören arbetar för att snabbt förse kunder med nya produkter och sedan snabbt iterera och förbättra produkter. Det hjälper kunderna att behålla en avancerad och modern IT-infrastruktur utan att behöva göra kapitalkrävande investeringar

Återförsäljare till/partneravtal med molntjänstleverantör

<ORGANISATION> kräver att den primära leverantören har direkt koppling till molntjänstleverantören som en återförsäljare eller kanalpartner, certifierad av en molntjänstleverantör för att sälja direktåtkomst till molntjänstleverantörens erbjudanden till tredjepartsenheter, med certifieringar från de molntjänstleverantörer som fastställer deras kunskap och expertis. Detta eliminerar kravet på att <ORGANISATION> ska granska villkoren och tjänsterna som är kopplade till ytterligare en nivå av underleverantörer mellan ramavtalets primära leverantör och molntjänstleverantören. Detta krav minskar komplexiteten som ytterligare nivåer av återförsäljare medför när (1) <ORGANISATION> utför due diligence för att säkerställa en tydlig tilldelning av ansvarsområden avseende tjänsterna som ska tillhandahållas och (2) <ORGANISATION> utför dagliga aktiviteter, bland annat förbrukningen av molntjänster

2.2 Tekniskt

En offertförfrågan för molntjänster bör höja ribban för molntjänstleverantörer genom att kräva att de ska tillhandahålla den standardiserade molnteknik som behövs för att kunden ska kunna skapa sin anpassade lösning. Som tidigare nämnt är skillnaden mellan vad som är standardiserat och vad som är anpassat väldigt viktigt när det gäller en offertförfrågan för molntjänster. Molntjänstleverantörer erbjuder standardiserade

³ Observera att företagsinformation på översiktlig nivå används i en offertförfrågan för molntjänster, snarare än antalet anställda i företaget eller den interna teamstrukturen. Med molnteknik finns det ingen korrelation mellan garantier kring tjänsternas prestanda och antalet anställda. I stället beaktas företagets övergripande storlek när det gäller att uppfylla kraven i offertförfrågningar för moln (lämplig skala) och bevisad erfarenhet/resultat.

Köpa molntjänster i offentlig sektor

tjänster till miljontals kunder, så anpassningar i en offertförfrågan för molntjänster fokuserar på lösningar och resultat med det lilla extra snarare än de underliggande metoder, den infrastruktur eller maskinvara som används för att erbjuda molntjänsterna som används för att uppnå lösningsresultat.

2.2.1 Minsta krav

Traditionella IT-upphandlingar förlitar sig ofta på verksamhetskrav som arbetats fram genom en rad arbetssessioner som dokumenterar hur organisationen för närvarande sköter sin verksamhet. Även under de bästa förhållandena är det svårt att få dessa krav riktigt bra. I lyckade fall dokumenterar dessa kravsessioner den tidigare affärsprocessen som kan vara föråldrad och ineffektiv. Om dessa krav sedan utgör en del av offertförfrågan som molntjänstleverantören replikerar kan den enda lösningen bli en skraddarsydd lösning. Denna modell är inkompatibel med molnupphandlingar.

Organisationer i den offentliga sektorn ska förstå sina affärs mål och prestanda behov, men inte vara föreskrivande i en offertförfrågan så att de dikterar systemets design och funktion. I stället bör organisationen sikta på det som passar verksamheten bäst. Organisationer bör inte fokusera på att bedöma förslag gällande hundratals eller till och med tusentals föreskrivande krav som kanske inte leder till framgångsrika tjänster, utan snarare inkludera bedömningskriterier baserade på hur bra tekniken och tillhörande tjänster uppfyller eller förbättrar affärs målen, oavsett om de uppnår prestanda behoven eller inte, och möjligheten att finjustera affärsreglerna genom konfiguration.

Offertförfrågningar för moln bör ställa de rätta frågorna för att hitta de bästa lösningarna. Eftersom inga fysiska tillgångar köps i en molnmodell resulterar det i att många upphandlingskrav för traditionella datacenter inte är tillämpbara. Om datacenterfrågor återanvänds leder det oundvikligen till gamla datacentersvar, vilket leder till att molntjänstleverantörerna inte kan lämna anbud eller till sämre utformade avtal som aktivt hindrar kunder i offentlig sektor från att dra nytta av molnets kapacitet och fördelar.

En offertförfrågan för molntjänster fokuserar på de huvudsakliga kraven som ställs på en molntjänstleverantör och molntjänster, vilket säkerställer att leverantörerna som kvalificeras för OMRÅDE 1 håller hög nivå. Kraven ska inte heller vara allt för föreskrivande för att inte begränsa den offentliga sektorns åtkomst till ett brett utbud av kvalificerade molntjänstleverantörer.

Exempel på språk för offertförfrågan: molnleverantörens funktioner

Se även de minsta administrativa kraven för molntjänstleverantörer för OMRÅDE 1 ovan.

Föreslagna krav på molntjänstleverantören	Anledning
<i>Infrastruktur</i>	
<i>Molntjänstleverantörens infrastruktur ska innehålla minst två kluster av datacenter. Varje kluster måste bestå av minst två datacenter som är sammankopplade via en länk med korta svarstider för att aktiva distributioner med hög tillgänglighet och implementeringar av DR-BC-scenarion ska vara möjliga. Datacentren som utgör varje kluster måste vara fysiskt isolerade och feloberoende av varandra.</i>	<i>Molntjänstleverantören måste kunna erbjuda en infrastruktur som klarar av att skapa program med hög tillgänglighet där enskilda fel punkter kan undvikas.</i>

Köpa molntjänster i offentlig sektor

Molntjänstleverantören ska tillhandahålla logiskt och geografiskt isolerade regioner. Molntjänstleverantören får inte replikera kunddata utanför dessa regioner.	Kraven för datalagring innebär att kunden ska ha full kontroll över var deras data finns.
Molntjänstleverantören måste kunna ha direkt, särskild och privat anslutning mellan molntjänstleverantörens datacenter.	Privat anslutning är ett grundläggande krav för att kunna bygga en säker hybridinfrastruktur.
Molntjänstleverantören ska tillhandahålla tillräckliga mekanismer, bland annat kryptering av data under överföring.	Kunden kan kräva att det ska finnas en funktion som ser till att data som inte är krypterade inte kan överföras.
Minsta antal certifieringar för molntjänstleverantörer	
Molntjänstleverantören måste vara certifierad enligt ISO 27001	Granskning, certifiering och ackreditering från tredje part säkerställer att kunder kan testa tjänsternas (och i synnerhet plattformens) kvalitet, säkerhet och tillförlitlighet. Det är nödvändigt att ett minsta antal certifieringar uppfylls.
CISP bör tillhandahålla funktioner och tjänster som kan användas i enlighet med GDPR, vilket gör det möjligt för kunder att bygga applikationer som uppfyller GDPR.	Kunden måste kunna skapa eller köra program i enlighet med GDPR, så det är en förutsättning att de tjänster och verktyg som erbjuds uppfyller GDPR.
Molntjänstleverantören måste göra granskningsrapporter från tredje part tillgängliga, till exempel SOC-rapport 1 och 2 (som omfattar de platser och tjänster som används av EC), för att se till att molntjänstleverantörens kontroller och rutiner är transparenta.	Molntjänstleverantören måste vara transparent gällande hur programmet körs och hanteras. SOC-rapporter är viktiga för att säkerställa tillit och transparens
Tjänstegenskaper	
Molntjänstleverantörens infrastruktur måste vara tillgänglig via programmeringsgränssnitt (API:er) och webbaserade hanteringskonsoler.	Självhanterad åtkomst och programmeringsgränssnitt är en obligatorisk standard för molntjänstleverantörer för att i största möjliga mån undvika mellanhänder mellan användaråtkomsten och själva leverantören.
Molntjänstleverantören måste erbjuda en grundläggande uppsättning tjänster med bland annat: objektlagring, hanterade relationsdatabaser, hanterade icke-relationsdatabaser, hanterade lastbalanserare, övervakning och integrerad automatisk skalning.	Det räcker inte med ett erbjudande om virtuella datorer för att kvalificera en leverantör som en molnleverantör. Molnleverantörer bör erbjuda en uppsättning PaaS- och IaaS-tjänster för att förbättra kundens program och göra det snabbare.
Molntjänstleverantören måste tillåta att kunden fritt får ändra användningen och konfigurationen av leverantörens tjänster och flytta data inom och utanför molntjänstleverantören (självhanterat erbjudande).	Självhanterad åtkomst till tjänster och data är ett fast krav som gör att kunden kan vara helt självständig.
Molntjänstleverantören måste godkänna fakturering av leverantörens tjänster baserat på förbrukningen.	Med förbrukningsbaserad användning kan kunden kostnadsoptimera sina arbetsbelastningar, minska riskerna och använda molntjänstleverantören för kortvariga program och koncepttest.
Data- och systemsäkerhet	
Molntjänstleverantören måste tillåta kunden att få full kontroll över egna data, ge kunden friheten att välja var	Kunden måste ha kontroll över var data lagras, hur åtkomsten till innehållet ska hanteras och användaråtkomst till tjänster och resurser

Köpa molntjänster i offentlig sektor

<i>data lagras (stadsområde) och garantera att inga kunddata flyttas såvida en sådan flytt inte initierats av kunden själv.</i>	
<i>Molntjänstleverantören måste ge kunden full kontroll över säkerhetspolicyer, bland annat gällande konfidentialitet, integritet och tillgång till kundens data och system.</i>	<i>Kunden måste kunna definiera och implementera sina säkerhetsstandarder i hela arbetsbelastningen. Det räcker inte med att lita på att leverantören ska hantera kundens data på rätt sätt.</i>
Kostnadskontroll	
<i>Molntjänstleverantören måste ha mekanismer och verktyg som låter kunden övervaka utgifter över tid. Verktygen måste kunna utföra grundläggande segmentering av kostnader baserat på arbetsbelastning, tjänst och konto.</i>	
<i>Molntjänstleverantören måste erbjuda verktyg som varnar kunden när ett tröskelvärde för kostnader överskrids.</i>	
<i>Molntjänstleverantören måste skicka detaljerade fakturor till kunden. Det måste gå att strukturera fakturan på ett sådant sätt att det går att dela upp kostnaderna efter arbetsbelastning, miljö och konto.</i>	

Molntjänstleverantören måste dessutom svara på frågorna om tekniska krav nedan.

LÖSNINGAR

Molntjänstleverantören ska redovisa hur denna kan tillhandahålla förkonfigurerade mallar och programvarulösningar som antingen körs hos eller är integrerade med molntjänstleverantören för följande lösningar:

- Lagring
- DevOps
- Säkerhet/efterlevnad
- Big data/analys
- Affärsprogram
- Telekommunikation och nätverk
- Geospatiala data
- IoT
- [Annat]

Tillhandahåll en översikt över hur molntjänstleverantören har använts för följande arbetsbelastningar:

- Haveriberedskap
- Utveckling och testning
- Arkivering
- Säkerhetskopiering och återställning
- Big Data
- Högpresterande databehandling (HPC)
- Sakernas internet (IoT)
- Webbplatser
- Serverlös databehandling
- DevOps
- Innehållsleverans
- [Annat]

Köpa molntjänster i offentlig sektor

2.2.2 Jämförelse mellan leverantörer

Utöver de minsta kraven i offertförfrågan för molntjänster är det viktigt att tillhandahålla kriterier som molntjänstleverantörens teknik kan jämföras med under en konkurrensutvärdering.

Offertförfrågningar för molntjänster bör efterfråga de molnfunktioner som en organisation behöver, med en förståelse för att kunden använder sådana funktioner för att skapa sin lösning. Funktioner utöver den standard som en molntjänstleverantör kan tillhandahålla (till exempel förkonfigurerade lösningar via molntjänstleverantören eller automatiserade funktioner) kan användas till en mer meningsfull analys av "alternativ med mervärde" eller "bästa värde" i en offertförfrågan för molntjänster.

Den offentliga sektorn kräver ofta konkurrens mellan anbudsgivare genom att använda utvärderingskriterier som bästa värde, ekonomiskt mest fördelaktigt anbud (MEAT) eller lägst pris. När enheter i den offentliga sektorn planerar för den här delen av en offertförfrågan för molntjänster är det viktigt att bygga upp en strategi som tar hänsyn till molnets unika funktioner. Det är till exempel inte ett effektivt sätt att jämföra erbjudanden genom att bara jämföra standardartiklar i molnleverantörernas erbjudanden (till exempel angående databehandling eller lagring). Vi rekommenderar i stället starkt ett fokus på mer övergripande lösningar, till exempel de som anges ovan i avsnitt 2.2.1. Enheter i den offentliga sektorn kan då titta på molnspecifika krav, till exempel de som anges i *Bilaga A – Tekniska krav för att jämföra olika anbudsgivare*.

I offertförfrågningar bör de nödvändiga molnegenskaperna som behövs för att skapa molnlösningen framgå. För att göra detta kan organisationer i den offentliga sektorn dra nytta av nödvändiga molnegenskaper enligt National Institute of Standards and Technology (NIST), utöver användningen av rapporter från tredjepartsanalytiker för att säkerställa att molntjänstleverantören har ett erbjudande som passar bäst för ett "äkta moln" och som drivs i massiv skala.

Exempel på språk för offertförfrågan – jämförelse mellan leverantörer

Molntjänstleverantören måste svara på ALLA frågor om tekniska krav i bilaga A.

Deltagarna måste ha följande attribut och beskriva hur deras anbud för molntjänster stämmer överens med de fem nödvändiga egenskaperna för molntjänster⁴.

- 1) **Självhantering på begäran:** Deltagaren måste erbjuda möjligheten till ensidigt tillhandahållande av databehandlingsfunktioner automatiskt, till exempel servertid och nätverkslagring, efter behov och utan krav på mänsklig interaktion med varje tjänstleverantör. Deltagaren ska erbjuda beställningsaktiviteten möjligheten till ensidigt (dvs. utan leverantörsgranskning eller -godkännande) tillhandahållande av tjänster. Förklara hur detta fungerar med ditt erbjudande eller det erbjudande du representerar.*
- 2) **Allmän nätverksåtkomst:** Deltagaren måste erbjuda flera alternativ för nätverksanslutning, varav ett måste vara internetbaserat. Förklara hur detta fungerar med ditt erbjudande eller det erbjudande du representerar.*
- 3) **Resurssammanslagning:** Deltagarens molntjänstleverantör måste erbjuda sammanslagna databehandlingsresurser som hanterar flera konsumenter genom att använda en modell för flera klienter med olika virtuella resurser som tilldelas och omtilldelas dynamiskt i enlighet med konsumentens begäran. Användaren kan ange en plats på en övergripande abstraktionsnivå (exempelvis land, region eller datacenterplats). Deltagaren ska stödja skalning av dessa resurser inom några minuter eller timmar efter en förfrågan. Förklara hur detta fungerar med ditt erbjudande eller det erbjudande du representerar.*

⁴ <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Köpa molntjänster i offentlig sektor

- 4) **Snabb elasticitet:** Deltagarens molntjänstleverantör ska stödja etablering av tjänster och avetablering av funktioner (upp- och nedskalning), så att tjänsten blir tillgänglig inom en viss tid (högst "x" timmar) efter en förfrågan. Deltagaren ska stödja faktureringsjusteringar till följd av dessa förfrågningar varje timme eller varje dag.
- 5) **Mätning av tjänsten:** Deltagaren ska erbjuda insyn i användningen av tjänsten via en instrumentpanel online eller liknande elektroniska medel.

Dessutom måste molntjänstleverantören:

- vara en etablerad ledare i att tillhandahålla molntjänster enligt Gartner Magic Quadrant för IaaS⁵
- tillhandahålla rapporter från branschetablerade tredjepartsanalytiker som visar molntjänstleverantörens beprövade funktioner och tillförlitlighet.

Slutligen används de scenarier som anges i bilaga B för att jämföra molntjänstleverantörer.

2.2.2.1 Servicenivåavtal (SLA)

Molntjänstleverantörer tillhandahåller kommersiella SLA:er till miljontals kunder och kan därför inte erbjuda anpassade SLA:er, vilket är fallet med en lokal datacentermodell. Men molntjänstleverantörernas kunder kan (ofta med hjälp av molntjänstleverantörernas partners) utforma sin egen molnanvändning så att den utnyttjar kommersiella SLA:er för att uppfylla kundspecifika krav och unika SLA:er.

Offertförfrågningar för molntjänster ska se till att molntjänstleverantörerna erbjuder de funktioner och den vägledning som krävs för att använda deras tjänster och kommersiella SLA:er, så att de enskilda slutanvändarna kan uppfylla prestanda- och tillgänglighetskraven.

Exempel på språk för offertförfrågan: servicenivåavtal

Tillhandahålla information om och länkar till molntjänstleverantörens inställning till servicenivåavtal (SLA).

<ORGANISATION> ska upprätthålla medvetenheten om molntjänstleverantörens servicenivåavtal och distribuera viktiga arbetsbelastningar och program på ett sådant sätt att de fortsätter att fungera om ett servicenivåavtal inte fullgörs.

<ORGANISATION> ansvarar för att upprätthålla lämpligt servicenivåavtal relaterat till utrustning som ägs av <ORGANISATION> eller tjänster som drivs av <ORGANISATION> och används med molntjänstleverantören.

Molntjänstleverantören ska förse <ORGANISATION> med funktionerna för att ha kontinuerlig insyn i och rapportera om servicenivåavtalets prestanda och dokumenterad bästa praxis för att dra nytta av molntjänstleverantörens infrastruktur för att skapa tjänster för prestanda, hållbarhet och tillförlitlighet.

2.2.3 Upphandling

Molntjänstleverantörens villkor utformas för att återspegla hur en molntjänstmodell fungerar (inga fysiska tillgångar köps och molntjänstleverantörer bedriver sin verksamhet i massiv skala och erbjuder standardiserade tjänster). Av den anledningen är det viktigt att molntjänstleverantörens villkor införlivas och används i största möjliga utsträckning. Se avsnitt 2.5 nedan för mer information om villkor och upphandling.

⁵ <https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb>

Köpa molntjänster i offentlig sektor

2.2.3.1 Nya och föränderliga tjänster

Molntjänstleverantörer tillhandahåller prestanda som en tjänst. Till skillnad från traditionella lokala lösningar som kräver uppgraderingar och underhållskontrakt som upphör att gälla kan molnleverantörer helt enkelt tillhandahålla den standardiserade tjänsten. För att molnmodellen ska uppnå stordriftsfördelar lanseras uppgraderingar och ändringar av underliggande infrastruktur till alla, inte till individuella användare, och kunderna väljer sedan vilka tjänster de använder. Tjänsten är smidigare än tidigare lokala system och molnleverantörer lägger ständigt till nya förbättrade tjänster som kunderna kan använda som de vill.

Om en molntjänstleverantörs nya eller förbättrade tjänster inte kan läggas till efter en offertförfrågans sista inlämningsdag begränsar organisationer i den offentliga sektorn sig själva från att dra nytta av nya tjänster och förbättrade funktioner tills nästa iteration för ett ramavtal släpps. Vi rekommenderar därför att tillhandahållandet av tjänsterna som beskrivs i ramavtalet är brett, så att nya tjänster från molntjänstleverantören kan läggas till efter sista inlämningsdag. EU:s upphandlingslag kan begränsa att nya tjänster från molntjänstleverantören som är väsentligt annorlunda läggs till i ramavtalet, men uppdateringar och nya versioner av tjänster som inte anses vara väsentliga ändringar kan läggas till utan att orsaka några problem med upphandlingen.

Exempel på språk för offertförfrågan: nya och föränderliga tjänster

Molntjänstleverantören ska tillhandahålla en kostnadseffektiv lösning som använder både bevisad och stabil virtualiseringsteknik och banbrytande teknik som uppdateras kontinuerligt. <ORGANISATION> bekräftar och godkänner att molntekniken kan tillhandahållas som en delad tjänst till <ORGANISATION> och andra klienter till molntjänstleverantören med en gemensam kod eller gemensam miljö och molntjänstleverantören kan vid olika tidpunkter ändra, lägga till eller ta bort funktioner, prestanda eller andra egenskaper hos molntjänsterna. Om sådan ändring, tillägg eller borttagning görs ska specifikationerna för molntjänsten ändras i enlighet med det.

*Omfattningen av denna leveransbeställning inkluderar alla befintliga och nya eller förbättrade tjänster från molntjänstleverantören **INOM RAMEN FÖR RAMVERKET**. Molntjänster från en molntjänstleverantör som är tillgängliga för kommersiella kunder ska göras tillgänglig för <ORGANISATION>.*

2.2.3.2 Låsning till en viss leverantör/reverserbarhet

Molnteknik minskar låsningar till en viss leverantör eftersom inga fysiska tillgångar köps och kunderna när som helst kan flytta sina data från en molnleverantör till en annan.

En viss grad av låsning till leverantören är dock ofrånkomlig vid köp av molntjänster eftersom alla moln inte är likadana. Av den anledningen kan en molntjänstleverantör erbjuda tjänster och funktioner som en annan helt enkelt inte kan tillhandahålla och på så sätt minska möjligheten att få likvärdiga tjänster från en annan leverantör. Ett försiktigt tillvägagångssätt är att begära att molntjänstleverantörer tillhandahåller de nödvändiga funktionerna och tjänsterna för att få utträde från molnet med dokumentation över hur dessa tjänster ska användas. Det fungerar som en rimlig "utträdesstrategi", eftersom det är omöjligt för en molntjänstleverantör att känna till kundens unika användning av de standardiserade tjänsterna och därmed tillhandahålla en anpassad utträdesplan.

En uppförandekod inom branschen för att hantera "dataportering" och att "byta molnleverantör" är under utveckling för att uppfylla kraven i artikel 6 i EU:s "Förordning om det fria flödet av icke-personuppgifter" och ska användas som ett verktyg för att visa sådan reverserbarhet när den är allmänt tillgänglig. En sådan hänvisning kommer att finnas på CISPE:s webbplats.

Köpa molntjänster i offentlig sektor

Exempel på språk för offertförfrågan: introduktion och utträde

<ORGANISATION> söker förslag med en rimlig utträdesstrategi för att förhindra låsning. <ORGANISATION> köper inte fysiska tillgångar och molntjänstleverantören erbjuder möjligheten att röra IT-stacken uppåt och nedåt. Molntjänstleverantören tillhandahåller verktyg och tjänster för portabilitet som hjälp vid migrering till och från molntjänstleverantörens plattform, för att minimera låsning. Detaljerad dokumentation över hur molntjänstleverantörens verktyg och tjänster för portabilitet används fungerar som en rimlig utträdesplan.

Molntjänstleverantören ska inte ha **krav** på minimiåtaganden eller långsiktiga avtal.

Data som lagras hos en tjänstleverantör kan när som helst exporteras av kunden. Molntjänstleverantören ska tillåta <ORGANISATION> att flytta data till och från molntjänstleverantörens lagring efter behov. Molntjänstleverantören ska även tillåta att virtuella maskinbilder laddas ned och porteras till en ny molnleverantör. <ORGANISATION> kan exportera sina maskinbilder och använda dem lokalt eller hos en annan leverantör (i enlighet med begränsningarna i relevanta programvarulicenser).

2.3 Säkerhet

Molntjänstleverantören och molnkunderna delar ansvaret för säkerhet och efterlevnad. I denna modell ansvarar kunderna för att strukturera och skydda de program och data som de implementerar i infrastrukturen, medan molntjänstleverantörerna ansvarar för att tillhandahålla tjänsterna på en säker och kontrollerad plattform, samt att tillhandahålla en rad ytterligare säkerhetsfunktioner. Molnleverantörens och kundens ansvar i denna modell beror på molndistributionsmodellen (IaaS/PaaS/SaaS) och kunden ska vara införstådd med sitt ansvar i varje modell.

Det är viktigt att denna modell med delat ansvar förstås för att kunna utforma en lyckad offertförfrågan för molntjänster. Organisationer i den offentliga sektorn ska se till att de vet vad molntjänstleverantören ansvarar för, vad de själva ansvarar för och var konsultpartners/oberoende programleverantörspartners och deras lösningar kan hjälpa till.

2.3.1 Minsta krav

Nyckelordet för säkerhet i molnet är **funktioner**. Organisationer i den offentliga sektorn ska kräva att molntjänstleverantörer tillhandahåller de säkerhetsfunktioner som krävs för att säkerställa att kunderna kan ta sitt ansvar i modellen för delat ansvar. Som visas i listan nedan med representativa krav ombeds molntjänstleverantören att erbjuda en standardiserad funktion som kunden kan använda för att göra sin unika molnmiljö säker.

- **Tillhandahålla** nätverksbrandväggar och **funktioner** för brandväggar för webbprogram för att skapa privata nätverk och kontrollera åtkomsten till instanser och program.
- **Tillhandahålla** anslutnings**alternativ** som möjliggör privata eller särskilda anslutningar från kontoret eller den lokala miljön.
- **Tillhandahålla en funktion** för att implementera en strategi för djupförsvar och förhindra DDoS-angrepp.
- Tillgängliga **funktioner** för datakryptering i lagrings- och databastjänster.
- **Tillhandahålla** flexibla **alternativ** för nyckelhantering med möjligheten att välja om du vill att molntjänstleverantören ska hantera krypteringsnycklarna eller ge kunden fullständig kontroll över nycklarna.
- **Tillhandahålla API:er** så att kunden kan integrera kryptering och dataskydd med tjänsterna som utvecklats eller distribuerats i en molntjänstleverantörs miljö.
- **Tillhandahålla** distributions**verktyg** för att skapa resurser från en molntjänstleverantör eller ta dem ur bruk enligt organisationens standarder.

Köpa molntjänster i offentlig sektor

- **Tillhandahålla verktyg** för inventerings- och konfigurationshantering som identifierar molntjänstleverantörens resurser och sedan spårar och hanterar ändringar hos dessa resurser över tid.
- **Tillhandahålla verktyg och funktioner** som gör att kunder kan se precis vad som händer i deras miljö från molntjänstleverantören.
- **Ge djup insyn** i API-anrop, som vem, vad, när och varifrån anrop har gjorts.
- **Tillhandahålla alternativ** för loggaggregering som effektiviserar granskningar och efterlevnadsrapportering.
- **Tillhandahålla en funktion** för att konfigurera varningsmeddelanden när specifika händelser inträffar eller tröskelvärden överskrids
- **Tillhandahålla funktioner** som definierar, upprätthåller och hanterar policyer för användaråtkomst i molntjänstleverantörens tjänster.
- **Tillhandahålla en funktion** för att definiera individuella användarkonton med behörigheter i molntjänstleverantörens resurser
- **Tillhandahålla en funktion** för att integrera och organisera affärskataloger för att minska administrationspåslag och ge slutanvändaren en bättre upplevelse.

Fler krav finns i *Bilaga A – Tekniska krav för att jämföra olika* anbudsgivare.

Funktioner utöver minimumstandarden för säkerhet kan användas för en mer meningsfull analys av "alternativ med mervärde" eller "bästa värde" i en offertförfrågan. Ju fler inbyggda eller automatiska funktioner för säkerhet desto bättre. Se *Bilaga A – Tekniska krav för att jämföra olika* anbudsgivare för krav angående jämförelser mellan olika anbudsgivare.

Organisationer i den offentliga sektorn bör titta på molnackrediteringscertifieringar och -bedömningar för att försäkra sig om att molntjänstleverantören har implementerat de obligatoriska säkerhetskontrollerna. Överväg till exempel en molntjänstleverantör som har validerats och certifierats av en oberoende revisionsenhet för att bekräfta efterlevnad av certifieringsstandarden ISO 27001. ISO 27001 Annex A, domän 14 behandlar de specifika kontroller som en molntjänstleverantör ska följa enligt ISO-kraven för anskaffning, utveckling och underhåll av system. Dessa kontroller omfattar sannolikt de flesta, om inte alla, kontroller för anskaffning, utveckling och underhåll av system som vanligtvis efterfrågas av en organisation i en IT-relaterad offertförfrågan. Därför är det rimligt att en organisation endast kräver att en molntjänstleverantör är certifierad enligt ISO 27001, snarare än att göra dubbla insatser och ange kontrollkrav för anskaffning, utveckling och underhåll av system i en offertförfrågan för molntjänster.

Detta tillvägagångssätt att dra nytta av rapporter om överensstämmelse från tredje part kan tillämpas på de flesta kontroller för säkerhet och överensstämmelse, till exempel GDPR, ISO, SOC osv.

Exempel på språk för offertförfrågan: säkerhet

Molntjänstleverantören ska upplysa <ORGANISATION> om sina generiska säkerhetsprocesser och tekniska begränsningar så att lämpligt skydd och flexibilitet kan uppnås mellan <ORGANISATION> och tjänstleverantören.

Molntjänstleverantören ska ange sina roller och ansvarsområden gällande säkerhet och efterlevnad:

- Beskriv molntjänstleverantörens och <ORGANISATION>s säkerhetsrelaterade roller och ansvarsområden i det föreslagna erbjudandet. Var tydlig med uppdelningen av ansvarsområden och presentera molntjänstleverantörens tjänster för att hjälpa <ORGANISATION> att skapa och automatisera säkerhetsfunktioner i sin molnmiljö.
- Svara på de tekniska specifikationerna i **BILAGA A** relaterade till <ORGANISATION>s säkerhetskrav.

ÄGARE AV OCH KONTROLL ÖVER <ORGANISATION>S INNEHÅLL

Köpa molntjänster i offentlig sektor

Beskriv hur molntjänstleverantörens funktioner kan skydda <ORGANISATION>s datasekretess. Inkludera de kontroller som används för att skydda <ORGANISATION>s innehåll. Molntjänstleverantören måste tillhandahålla stark regional isolering så att objekten som lagras i en region aldrig lämnar regionen, såvida inte <ORGANISATION> uttryckligen överför dem till en annan region

- *<ORGANISATION> hanterar åtkomsten till sitt innehåll, sina tjänster och resurser. Molntjänstleverantören ska tillhandahålla en uppsättning avancerade funktioner för åtkomst, kryptering och inloggning som hjälper <ORGANISATION> att sköta detta effektivt. Molntjänstleverantören öppnar eller använder inte <ORGANISATION>s innehåll i något annat syfte än som krävs enligt lag och för att upprätthålla molntjänstleverantörens tjänster och tillhandahålla <ORGANISATION> och dess slutanvändare dessa.*
- *<ORGANISATION> väljer i vilken region innehållet ska lagras. Molntjänstleverantören flyttar eller replikerar inte <ORGANISATION>s innehåll utanför den valda regionen förutom om detta krävs enligt lag, och efter behov för att upprätthålla molntjänstleverantörens tjänster och tillhandahålla <ORGANISATION> och dess slutanvändare dessa.*
- *<ORGANISATION> väljer hur innehållet ska skyddas. Molntjänstleverantören måste tillhandahålla stark kryptering för <ORGANISATION>s innehåll vid överföring eller vilande innehåll och erbjuda <ORGANISATION> alternativet att hantera sina egna krypteringsnycklar.*
- *Molntjänstleverantören måste ha ett säkerhetsgaranti-program med global bästa praxis för integritet och dataskydd. Detta för att hjälpa <ORGANISATION> att inrätta, använda och tillvarata molntjänstleverantörens säkerhetskontrollmiljö. Säkerhetsskyddet och kontrollprocesserna måste valideras oberoende genom ett antal bedömningar som genomförs av oberoende tredje part.*

Med certifieringar och bedömningar för molnackreditering får organisationerna i den offentliga sektorn en försäkran om att molntjänstleverantörerna har effektiva fysiska och logiska säkerhetskontroller på plats. När dessa ackrediteringar används i offertförfrågningar effektiviserar det upphandlingen och bidrar till att undvika betungande processer som behöver göras flera gånger, eller godkännandeflöden som kanske inte krävs för en molnmiljö.

Offertförfrågningar för moln ska ge molntjänstleverantörer en möjlighet att bevisa att de uppfyller ackrediteringar och bedömningar för efterlevnad. Som nämndes ovan överlappar dessa ackrediteringar varandra mycket vad beträffar deras riskscenarier och riskhanteringsmetoder. Eftersom kontroller och krav har slagits ihop i sådana ackrediteringar går det snabbare att hantera efterlevnad i en offertförfrågan genom att kräva att molntjänstleverantörer ska uppfylla ackrediteringarna i stället för att göra dubbla insatser med att ange sådana enskilda kontroller (**varav många kan vara hämtade från tidigare offertförfrågningar som gäller för lokala datacenter och därför kanske inte är tillämpbara för molntjänster**).

OBS! Det är dessutom väldigt viktigt att förstå hur rapporterna som anges nedan kan nås. SOC-rapporterna 1 och 2 är till exempel vanligtvis känsliga dokument. Förstå de avtal som krävs för att få åtkomst till dem (t.ex. sekretessavtal – NDA) och be inte bara om att dessa dokument ska skickas som en del av responsen på offertförfrågan (dessa dokument kan offentliggöras genom lagen om offentliga handlingar eller liknande lag som äventyrar molnsäkerheten).

Exempel på språk för offertförfrågan: efterlevnad

Användningen av erkända standarder för säkerhet, efterlevnad och användning som härleds från bästa praxis inom molntjänsttjänster, bland annat datahantering, datasäkerhet, konfidentialitet, tillgänglighet osv., effektiviserar upphandlingen av molnteknik.

Köpa molntjänster i offentlig sektor

<ORGANISATION> utvärderar unika erbjudanden mot godkända standarder för säkerhet, efterlevnad och användning som anges nedan och i **bilaga A**. Genom att förlita sig på leverantörens efterlevnadscertifiering för varje standard kan **<ORGANISATION>** använda minsta efterlevnad av standarden som utgångspunkt vid utvärderingen av förslaget.

Fördelen med att kräva att molntjänstleverantören ska fortsätta att uppfylla den minsta standarden under hela avtalets giltighetstid är att tjänsteftlevnaden förblir aktuell.

Molntjänstleverantören som lämnar anbud (direkt eller genom en återförsäljare) ska kunna uppvisa att denna uppfyller följande intyg, rapporter och certifieringar från oberoende tredje part (Obs! Om något av dessa intyg, rapporter och certifieringar har begränsningar i fråga om utlämnande på grund av säkerhetsfrågor ska **<Organisation>** samarbeta med molntjänstleverantören för att komma överens om ett sätt att få åtkomst till dem):

Certifieringar/intyg	Lagar, förordningar och sekretess	Anpassningar/ramverk
<input type="checkbox"/> C5 (Tyskland)		<input type="checkbox"/> CDSA
<input type="checkbox"/> CISPE:s uppförandekod för dataskydd (GDPR)		
<input type="checkbox"/> DIACAP	<input type="checkbox"/> EU:s dataskyddsdirektiv	<input type="checkbox"/> CIS
<input type="checkbox"/> DoD SRG-nivå 2 och 4	<input type="checkbox"/> EU:s modellklausuler	<input type="checkbox"/> Informationstjänster om straffrätt (CJIS)
<input type="checkbox"/> HDS (Frankrike, sjukvård)		
<input type="checkbox"/> FedRAMP	<input type="checkbox"/> FERPA	<input type="checkbox"/> CSA
<input type="checkbox"/> FIPS 140-2	<input type="checkbox"/> GDPR	<input type="checkbox"/> EU-US Privacy Shield
<input type="checkbox"/> ISO 9001	<input type="checkbox"/> GLBA	<input type="checkbox"/> EU Safe Harbor
<input type="checkbox"/> ISO 27001	<input type="checkbox"/> HIPAA	<input type="checkbox"/> FISC
<input type="checkbox"/> ISO 27017	<input type="checkbox"/> HITECH	<input type="checkbox"/> FISMA
<input type="checkbox"/> ISO 27018	<input type="checkbox"/> IRS 1075	<input type="checkbox"/> G-Cloud [Storbritannien]
<input type="checkbox"/> IRAP [Australien]	<input type="checkbox"/> ITAR	<input type="checkbox"/> GxP (FDA CFR 21 del 11)
<input type="checkbox"/> MTCS nivå 3 [Singapore]	<input type="checkbox"/> PDPA – 2010 [Malaysia]	<input type="checkbox"/> ICREA
<input type="checkbox"/> PCI DSS nivå 1	<input type="checkbox"/> PDPA – 2012 [Singapore]	<input type="checkbox"/> IT Grundschutz [Tyskland]
<input type="checkbox"/> SEC-regel 17-a-4(f)	<input type="checkbox"/> PIPEDA [Kanada]	<input type="checkbox"/> MARS – E
<input type="checkbox"/> SecNumCloud (Frankrike)		
<input type="checkbox"/> SOC1/ISAE 3402	<input type="checkbox"/> Privacy Act [Australien]	<input type="checkbox"/> MITA 3.0
<input type="checkbox"/> SOC2/SOC3	<input type="checkbox"/> Privacy Act [Nya Zeeland]	<input type="checkbox"/> MPAA
	<input type="checkbox"/> Spansk DPA-auktorisering	<input type="checkbox"/> NIST
	<input type="checkbox"/> U.K. DPA - 1988	<input type="checkbox"/> Nivåer på Uptime Institute

Listan ovan är endast avsedd för illustrativa syften och bör inte betraktas som uttömmande för de certifieringar och standarder som kan gälla för molntjänster.

2.3.2 Jämförelse mellan leverantörer

Precis som när det gäller de tekniska kriterierna i avsnitten ovan, utöver de minsta säkerhetskraven i en offertförfrågan för molntjänster, är det viktigt att tillhandahålla kriterierna som molntjänstleverantörens säkerhetsfunktioner och -tjänster kan jämföras med under en konkurrensutvärdering.

Se *Bilaga A – Tekniska krav för att jämföra olika* anbudsgivare för exempel på molntjänstleverantörens säkerhetskrav. Vi rekommenderar starkt att funktionerna nedan betraktas som viktiga säkerhetsaspekter när organisationer i den offentliga sektorn utvärderar molntjänstleverantörer:

Exempel på språk för offertförfrågan: viktiga säkerhetsaspekter

- *Molntjänstleverantörens förståelse för modellen för delat ansvar och dokumentation som hjälper kunder att förstå uppdelningen av säkerhetsansvar för molntjänstleverantörens funktioner och tjänster (till exempel med hänsyn till GDPR)*
- *Bevisad historik över molntjänstleverantörens infrastruktursäkerhet med offentlig, generisk dokumentation om molntjänstleverantörens säkerhetsställning och fysiska/logiska kontroller*
- *Molntjänstleverantörens specifika support för molnsäkerhet*
- *Tjänster som gör det möjligt för kunderna att formalisera kontodesignen, automatisera säkerheten och styrningskontrollen samt effektivisera granskningsprocessen*
- *Möjligheten att skapa, tillhandahålla och hantera en samling resurser i en malliknande modell (innehåller säkerhetsmallar med guldstandard som skapats av en molntjänstleverantör/partner till en molntjänstleverantör)*
- *Möjligheten att skapa en tillförlitlig och repeterbar drift för kontrollerna*
- *Funktioner för fortlöpande granskning i realtid*
- *Möjligheten att kontrollera policyer för molnstyrning med hjälp av tekniska skript*
- *Möjligheten att skapa tvingande funktioner som inte kan åsidosättas av användare som inte har rätt att modifiera de funktionerna*
- *Möjligheten att ta fram en tillförlitlig implementering av det som tidigare skrivits in i policyer, standarder och bestämmelser, och samtidigt kunna skapa en säkerhet och överensstämmelse som är möjlig att upprätthålla, något som i sin tur leder till en funktionell och tillförlitlig molnstyrningsmodell för IT-miljöerna*
- *Tjänster som skyddar mot vanliga, mest förekommande DDoS-angrepp (Distributed Denial of Service) mot nätverks- och transportlager tillsammans med möjligheten att skriva anpassade regler för att minska avancerade angrepp mot programlager*
- *Hanterad tjänst för upptäckt av hot*

2.3.3 Upphandling

Som beskrivs ovan utformas molntjänstleverantörens villkor för att återspegla hur en molntjänstmodell fungerar (inga fysiska tillgångar köps och molntjänstleverantörer bedriver sin verksamhet i massiv skala och erbjuder standardiserade tjänster). Av den anledningen är det viktigt att molntjänstleverantörens villkor införlivas och används i största möjliga utsträckning. Se avsnitt 2.5 nedan för mer information om villkor och upphandling.

Vad gäller säkerhet rekommenderar vi återigen starkt att låta molntjänstleverantörer kontinuerligt uppdatera sina erbjudanden eller att leverantörer tillåts lägga till produkter efter den sista

Köpa molntjänster i offentlig sektor

inlämningsdagen, så länge de uppfyller offertförfrågans ursprungliga parametrar. Detta visar att säkerhetsfunktioner och -tjänster utvecklas snabbt och att molntjänstleverantörer ofta lanserar säkerhetsfokuserade tjänster som i många fall är kostnadsfria att använda. Observera att det är viktigt att fastställa en lägsta säkerhetsnivå (se de minsta kraven ovan) så att inte ändringar i säkerhetserbjudanden leder till en försämring.

Modellen för delat ansvar är givetvis kärnan för säkerheten i en offertförfrågan för molntjänster. Varje part måste vara tydlig med sitt säkerhetsansvar och molntjänstleverantörer bör ha skyldigheten att dokumentera molntjänstleverantörens/kundens säkerhetsansvar för molnteknik från en molntjänstleverantör, tillsammans med dokumentation som hjälper kunder att implementera och automatisera bästa praxis för säkerhet.

Ett molnramavtal ska vara flexibelt nog att kunna avlägsna en leverantör om denna inte uppfyller de minsta kraven på säkerhet och efterlevnad som anges i offertförfrågan för molntjänster.

2.4 Priser

Organisationer i den offentliga sektorn behöver ett avtal som gör att de kan betala för tjänster när de förbrukas för att kunna hantera variationer i efterfrågan – med den molnstyrning och synlighet som krävs kring användning och utgifter.

Det är viktigt att offertförfrågningar för molntjänster tittar på värdet och den totala ägandekostnaden (TCO), i stället för att bara göra en "lika mot lika"-jämförelse av enhetspriserna. Den traditionella metoden att titta på det lägsta enhetspriset fungerar inte i molnmodellen och tenderar därför att inte leda till det ekonomiskt mest fördelaktiga anbudet eller det övergripande lägsta priset.

*För att underlätta utvärderingen av molntjänstleverantörers priser kan det hjälpa att först låta molntjänstleverantörerna förkvalificera sig eller gå vidare till slutomgången via ett **minsta krav angående priser**, så att molntjänstleverantörer med liknande funktioner kan kvalificera sig för ramavtalet. Utvärderingsprocessen för avrop och minitävlingar kan sedan titta på ett urval av exempel på typiska molnarkitekturer och **prisscenarier** som stämmer överens med några typiska arbetsbelastningar och låta molntjänstleverantörerna prissätta dem. Demonstrationer med livetester rekommenderas också för att kunna jämföra prestanda och elasticitet hos molntjänstleverantörernas tjänster. Se bilaga B för ett exempel på ett demonstrationstestskript för molnteknik.*

2.4.1 Minsta krav

Prisavsnittet i en offertförfrågan för molntjänster har fyra viktiga delar:

1. **Nyttjandepreis:** Molnkunder införlivar en modell för betalning per förbrukning. Den innebär att kunderna i slutet av varje månad bara betalar för det de använder, vilket är optimalt för användnings- och resursmätvärden.
2. **Transparent pris:** Molntjänstleverantörens pris ska vara offentligt och transparent.
3. **Dynamiskt pris:** Ta med flexibilitet att låta priset skifta beroende på marknadspriset. Den här metoden drar nytta av molnprisernas dynamiska och konkurrensutsatta natur och stöder innovation och prissänkningar.

Köpa molntjänster i offentlig sektor

4. **Kontrollerade utgifter:** Molntjänstleverantören ska erbjuda verktyg för rapportering, övervakning och prognoser som låter kunderna 1) övervaka förbrukning och utgifter både översiktligt och på detaljnivå, 2) få aviseringar när förbrukning och utgifter uppnår anpassningsbara gränsvärden och 3) uppskatta förbrukning och utgifter för att kunna planera framtida molnbudgetar.

Exempel på språk för offertförfrågan: priser

<ORGANISATION> begär att deltagande molntjänstleverantörer inkluderar sin föreslagna metod och prismodell för att tillhandahålla var och en av sina tjänster till slutanvändare som en kommersiell molnfunktion.

Molntjänstleverantören ska tillhandahålla följande:

- Dokument med tjänstebeskrivning eller länkar till tjänstedefinitioner
- Dokument med villkor
- Dokument med pris (länkar till offentliga priser accepteras, under förutsättning att ett dokument med en fullständig prislista/pris finns tillgänglig på begäran)

Priset är kostnaden för tjänstens vanligaste konfiguration. Molntjänstleverantörer ska erbjuda alternativ för volymbaserade rabatter och priskalkylatorverktyg för att ta reda på det faktiska priset för det som köps och det övergripande värdet för köparen (till exempel tjänster för optimering och resulterande kostnadsänkningar).

Köpare under ramavtalet kan prata med leverantörer för att be dem att förklara sina tjänstebeskrivningar, villkor, pris eller dokument med/modell för tjänstedefinitioner. Ett register med eventuella samtal med leverantörer kommer att föras.

Ytterligare priskrav

- Tillhandahålla molnteknik med en dynamisk prismodell som ger största möjliga affärsflexibilitet och möjlighet till skalbarhet och tillväxt.
- Prisattribut måste innehålla följande:
 - Erbjuds priser i en tjänst på begäran som baseras på betalning per förbrukning? Beskriv er prismodell.
 - Kan ni uppnå ytterligare rabatter genom massanvändning eller -inköp? Beskriv hur.
 - Är priserna offentliga och transparenta? Inkludera länkar till offentliga priser.
 - Är priserna dynamiska och svarar de snabbt och effektivt på marknadskonkurrensen?
 - Erbjuder ni bästa praxis och resurser för att spåra utgifter?
 - Erbjuder ni bästa praxis och resurser för kostnadsoptimering?

Pristransparens

På grund av den ständigt nedåtgående pristrenden inom kommersiell molnteknik som drivs av innovation och konkurrens får molntjänstleverantörens uppmätta enhetskostnad för tjänster som betalas av <ORGANISATION> under ramavtalet inte överskrida molnleverantörens enhetspriser som publicerats på molnleverantörens webbplats som gäller när tjänstenheten förbrukas av kunden.

Varningar/rapporter om budgetering och fakturering

För att påvisa leverans och användning av molnteknik ska molntjänstleverantörerna tillhandahålla <ORGANISATION> med verktyg för att upprätta detaljerade faktureringsrapporter som bryter ned kostnader per timme, dag eller månad; för varje konto i en organisation; per produkt eller produktresurs eller enligt kunddefinierade taggar. <ORGANISATION> erkänner att modellen för delat ansvar för molnet innebär att <ORGANISATION> ansvarar för att använda funktioner och verktyg för budgetering och fakturering för att uppfylla unika krav på prognostisering och rapportering.

Köpa molntjänster i offentlig sektor

- *Tillhandahålla information om hur <ORGANISATION> kan visa faktureringsinformation både på detaljnivå och översiktligt, visualisera mönster i utgifter för molntjänstleverantörers resurser över tid och prognostisera framtida utgifter.*
- *Tillhandahålla information om hur <ORGANISATION> kan filtrera vyn för användning/fakturering per tjänst, länkat konto eller enligt anpassade taggar som tillämpats på resurser och skapa faktureringsvarningar som skickar aviseringar när användningen av tjänsterna närmar sig eller överskrider av <ORGANISATION> angivna tröskelvärden/budgetar.*
- *Tillhandahålla information om hur <ORGANISATION> kan prognostisera volymen förbrukade molntjänster under en angiven prognostiserad tidsperiod baserat på tidigare användning. Molntjänstleverantören ska erbjuda en uppskattning av fakturabeloppet till <ORGANISATION> från molntjänstleverantören och göra det möjligt för <ORGANISATION> att använda larm och budgetar för den förväntade förbrukningen, för att få bättre kontroll över kostnader och utgifter.*

2.4.2 Jämförelse mellan leverantörer

Organisationer i den offentliga sektorn kräver ofta konkurrens mellan anbudsgivare genom att använda utvärderingskriterier som bästa värde, ekonomiskt mest fördelaktigt anbud (MEAT) eller lägsta pris. Vid planeringen av prissättningen av ramavtalets avrop eller minitävlingar är det viktigt att utforma ett tillvägagångssätt som tar hänsyn till molnets unika funktioner. Det är till exempel inte effektivt att jämföra offerter genom att bara jämföra standardartiklar i molnleverantörernas erbjudanden (t.ex. databehandling eller lagring) eftersom det inte tar hänsyn till funktioner som prestanda, kostnadsoptimering genom att använda molntjänster och övervakningsverktyg från molntjänstleverantören eller olika tjänster som molntjänstleverantörer kan erbjuda kostnadsfritt. Dessutom kan en molntjänstleverantörs katalogpriser innehålla tiotusentals standardartiklar och prismodellerna kan skilja sig från en tjänst till en annan och mellan olika leverantörer.

Analysera den totala ägandekostnaden

Vi rekommenderar större fokus på den totala ägandekostnaden (TCO) för definierade användningsfall eftersom den tar hänsyn till alla aspekter i en molnlösning (bland annat partnertjänster, standardiserade rabatter för molntjänstleverantörer, tekniska funktioner som kan öka prestandan och minska/optimera kostnader osv.).

Jämföra scenarier

Utvärderingsprocessen kan även beakta vanliga scenarier som motsvarar vanliga system eller program. Sådana scenarier (till exempel webbvårdskap eller implementeringen av HR-system med x antal användare osv.) kan innehålla variabler som resursernas hastighet och skala, programmets eller lösningens prestanda, tider för lagringsåtkomst, små volymer av komplexa data jämfört med enkla databehandlingsuppgifter med stora volymer osv. Programmen eller systemen kan även ha vanliga scenarier som bearbetning av stora volymer vid skatteåterbäring, nödaviseringar som översvämningsvarningar. Scenarierna ska innehålla omfattningen av tekniken och tjänsterna som kunden kan använda under projektet. På så sätt kan kunden jämföra den uppskattade övergripande kostnaden för projektet.

Jämför scenarier ekonomiskt och tekniskt

Det är även viktigt att ta hänsyn till tekniska fördelar vid jämförelse av priser mellan molntjänstleverantörernas erbjudanden. En molntjänstleverantör kan till exempel göra det möjligt för kunder att skapa en aktiv topologi för haveriberedskap (DR) tack vare att dess modell har datacenter i kluster inom en geografisk region. En molntjänstleverantör som inte har den här typen av redundans och datacenterkonfiguration kan vara x % dyrare med tanke på kostnaderna för invägda behov för

Köpa molntjänster i offentlig sektor

haveriberedskap. Se alternativen nedan för en direkt "lika mot lika"-jämförelse som ett exempel på varför ett holistiskt tillvägagångssätt för prissättning som innehåller tekniska funktioner är viktigt vid utvärderingen av molntjänstleverantörer.

Exempel: En kund vill jämföra priset på objektlagring som tillhandahålls av kvalificerade molntjänstleverantörer i ett ramavtal. Priset på objektet för "lagringsenheten" från molntjänstleverantör 1 är 0,023 €/GB. Priset på samma "enhet" från molntjänstleverantör 2 är 0,01 €/GB. Vid en enkel jämförelse av enheter skulle inte kunden ställa viktiga frågor som:

1. Hur många redundanta kopior av objektet finns tillgängliga om ett fel uppstår? I exemplet ovan är molntjänstleverantör 1 utformad för att klara en parallell dataförlust på två olika anläggningar och har flera datakopior. I fallet med molntjänstleverantör 2 skapas inga redundanta kopior.
2. Vilken nivå av hållbarhet har de lagrade objekten? Molntjänstleverantör 1 erbjuder 99.999999999 % medan molntjänstleverantör 2 erbjuder 99 %.
3. Ta hänsyn till kostnaden för ägandets hela livscykel för det övergripande projektet eller arbetsbelastningen och hur funktioner för kostnadsoptimering kan sänka kostnaderna för hur data lagras och används (att öka användningen av en molntjänstleverantörs serverlösa funktioner kan till exempel sänka kostnaderna med x %).

Detta är bara några av många andra tekniska överväganden som spelar in vid prissättning, i synnerhet när det gäller säkerhet och efterlevnad.

Överväganden för prisscenarier

Baspriser – dessa är generellt molntjänstleverantörers offentliga priser. Molntjänstleverantörer ska ange dessa priser officiellt. Däremot, som beskrivs ovan, kan kunder be om att kanske tre till fem specifika scenarier (eller så många som kunden anser rimliga) prissätts av alla leverantörer för att effektivt jämföra molntjänstleverantörerna. Scenarierna ska innehålla den omfattning av tjänster och teknik som kunden sannolikt använder under projektets gång. På så sätt kan kunden jämföra den övergripande uppskattade kostnaden för projektet. Jämförelser mellan standardartiklar/SKU:er brukar vara mer problematiska än nyttiga för kunder och leverantörer (kunderna måste jämföra tiotusentals standardartiklar hos alla molntjänstleverantörer och leverantörerna måste dels förse kunden med den här detaljnivån och sedan hantera den när det faktiska priset endast fastställs utifrån förbrukningen av tjänsten).

Det är ett måste att utvärdera en molntjänstleverantörs övergripande uppsättning funktioner för molnkunder som vill ha bästa värde. Molntjänstkunder kan till exempel ha flera tjänster som antingen är kostnadsfria eller generellt kostnadsfria och en prisutvärdering bör ta hänsyn till sådana tjänster, samt att andra molntjänstleverantörer kanske tar betalt för liknande funktioner.

Utvärderingskriterier kan skrivas på ett sätt som gör att molntjänstleverantörerna kan göra avrop på sina funktioner av typen "inklusive x standard" och hur sådana tjänster påverkar den övergripande kostnaden. Utvärderingskriterier kan även titta på molntjänstleverantörens volymbaserade/bundna priser och kommersiellt tillgängliga rabatter som reserverade instanser/spot-instanser. Exempelvis:

- x % besparing om kunden köper reserverad databehandlingskapacitet (ett år, tre år osv.)
- x % rabatt på bundna/volymbaserade priser

Köpa molntjänster i offentlig sektor

- x % besparing på arkitekturgranskningar och optimering av infrastrukturen, till exempel att byta till ett mer lämpligt databehandlingsalternativ
- Som beskrivs ovan är det viktigt att ta hänsyn till kostnaden för hela livscykeln och hur funktioner för kostnadsoptimering kan sänka kostnaderna

PRISSCENARIO

Anbudsgivare måste ange priser för scenariot nedan, endast i utvärderingssyfte. Det faktiska priset baseras på förbrukningen av tjänster på begäran som baseras på betalning per användning.

Nedan visas representativa krav för att identifiera priser och de presenteras med den uttryckliga förståelsen att dessa nominala krav kan ändras under avtalets giltighetstid. Ange priser för både 12 och 36 månader på begäran och 12 och 36 månader reserverad kapacitet.

Ange:

- Namnet på den föreslagna lösningen:
- Anbudsgivarens bästa pris:
- Tider för tjänsten: dygnet runt, alla dagar på året
- Tjänstens tillgänglighet: 99,95 %

Prisscenarier kan även innehålla exempel från befintliga kunder med liknande arbetsbelastning som har optimerat sina utgifter över ett/två/tre år genom att använda molntjänstleverantörens övervaknings- och optimeringsverktyg, införa optimerade molnlösningar och genom molntjänstleverantörens prissänkningar.

2.5 Konfiguration av/villkor för avtalets fullgörande

Molntekniker och -åtgärder från en molntjänstleverantör har standardiserad utformning och därför är även avtalsvillkoren standardiserade. Däremot är det möjligt att justera dessa avtal marginellt för att anpassa dem till lokala lagar och regelverk.

Traditionella metoder för IT-upphandling innehåller ofta strikta regler om att sökanden måste uppfylla många eller alla krav i upphandlingen, annars blir de avvisade. Eller så innehåller de en strikt delmängd obligatoriska krav. När den här typen av inköpsmetod används för molnteknik, som egentligen består av en uppsättning standardiserade komponenter och verktyg som hjälper till att utforma en anpassad lösning, brukar upphandlingar misslyckas.

2.5.1 Villkor

Det första steget vid upphandling med en offertförfrågan för molntjänster är att granska och förstå molntjänstleverantörens befintliga kommersiella villkor, som ofta finns officiellt på molntjänstleverantörens webbplats. Enheter i den offentliga sektorn godkänner i allt större utsträckning molntjänstleverantörers kommersiella villkor. En del av det här arbetet med att förstå villkoren är inriktat på möten med molntjänstleverantörer och deras partners för att gå in djupare på deras tillvägagångssätt. Den viktiga frågan är "varför" molntjänstleverantörer använder specifika villkor. Vissa av villkoren kan se ut att skilja sig från traditionella IT-villkor, men det finns väldigt specifika anledningar till "varför" de ingår i ett molnavtal. Om de offentliga villkoren inte godkänns har molntjänstleverantörer ofta avtal för företagskunder som kan modifieras något.

Utöver granskningen av molntjänstleverantörens villkor är det viktigt att förstå befintliga policyer, regelverk eller lagar (t.ex. de som berör teknik, dataklassificering, sekretess, personal osv.). Det finns ofta befintliga

Köpa molntjänster i offentlig sektor

policyer/regelverk/lagar som är utformade för att köpa och använda traditionella IT-erbjudanden, och de kan stämma dåligt överens med en molntjänstleverantörs modell. Ett exempel är att endast tillåta användningen av molnteknik som inkluderades i det ursprungliga anbudet för ramavtal via offertförfrågan för molntjänster. Molntjänstleverantörer lägger ständigt till nya tjänster och nya funktioner. Det är inte rimligt för slutkunden att åtkomsten till de nya tjänsterna hindras bara för att ni följer ett traditionellt tillvägagångssätt för IT-produktuppdateringar. Om så är fallet är det viktigt att ha ingående diskussioner med molntjänstleverantörerna där dessa policyer/regelverk eller lagar behandlas.

Använd diskussioner om offertförfrågan som hålls i förväg

Som anges ovan bör du ta dig tid att träffa molntjänstleverantörer och relaterade leverantörer innan en offertförfrågan utarbetas för att förstå deras villkor och presentera din enhets tillvägagångssätt, policyer, regelverk och lagar. Den viktigaste delen av dessa diskussioner är att båda sidor förstår "varför" de relevanta villkoren fungerar som de gör. Villkor för moln skiljer sig till exempel från villkor för traditionella datacenter, hanterade tjänster, maskinvara, förseglad licensprogramvara och systemintegration. I och med att det handlar om enskilda modeller med ständig innovation kräver deras affärsmodeller att offertförfrågans process är tillräckligt flexibel för att genom förhandlingar och diskussioner kunna få ett förtydligande.

Genom möjligheten att kunna förtydliga villkor genom diskussioner eller förhandlingar får organisationer i den offentliga sektorn ökad förståelse för molnmodeller och undviker problemet med att avvisa leverantörer som kanske faktiskt kan tillgodose organisationens behov. En vanlig process är att organisationen identifierar vissa villkor i förväg som den är villig att diskutera och förhandla innan tilldelning. Genom att förhandla godtagbara villkor med anbudsgivarna i förväg säkerställer organisationen att den får det anbud som passar bäst och löser problem som annars skulle kunna resultera i att ett effektivt förslag avvisades. Enheter i den offentliga sektorn kan även granska deras policyer, regelverk och lagar, och båda sidor kan få ökad förståelse för hur molnanvändningen passar in i dessa modeller. Det finns ofta sätt att arbeta med de befintliga klausulerna. Om det däremot finns ett problematiskt område kan båda teamen samarbeta för att hitta en lösning (det är bättre att ta dessa diskussioner i god tid innan en eventuell offertförfrågan och efterföljande avtalsförhandling).

Förhandlingsflexibilitet

För att kunna skriva avtal i enlighet med lokala lagar och samtidigt förlita sig på standardiserade avtalsvillkor från molntjänstleverantören rekommenderar vi att ni (1) ber de sökande om deras standardavtal, (2) inte antar opassande avtalsvillkor vid upprättandet av ramavtalet för offertförfrågan för molntjänster och (3) erbjuder ett förhandlingsalternativ för alla bestämmelser för konsulttjänster och förslag som ska ingå i ramavtalet (förutom de obligatoriska klausulerna enligt lag givetvis).

OBS! Omfattningen av delat ansvar ingår i molnmodellen och ska beaktas i avtalets villkor (t.ex. att molntjänstleverantören bekräftar att kunden äger sina data, oavsett var de lagras, och tillhandahåller verktyg som säkerställer att valet av dataplatser är begränsat – **MEN** – att det är kundens eller partners ansvar att använda dessa verktyg).

*Observera att det är viktigt att det finns **olika uppsättningar av villkor** för avtal för varje område i ett molnramavtal. Ett "tillvägagångssätt där en lösning passar alla" i upphandlingen för alla områden leder till problem med teknisk genomförbarhet och kompatibilitet.*

Köpa molntjänster i offentlig sektor

Som tidigare nämnt är offertförfrågningar med obligatoriska villkor som inte kan förhandlas generellt ett "allt eller inget"-förslag för leverantörer som kan leda till att förslag som i andra fall skulle godkännas i stället avvisas. Organisationer i den offentliga sektorn bör noga överväga konsekvenserna av att använda obligatoriska villkor, såvida det inte är ett krav enligt lag. Organisationer bör vara säkra på att ett obligatoriskt krav eller villkor behövs eftersom framtida förhandlingar åsidosätts av deras klassificering som obligatoriskt. Obligatoriska krav eller villkor bör användas i minsta möjliga mån för att ge organisationen den flexibilitet som behövs för att anskaffa den bästa tekniken och lösningen.

Tänk på att molntjänstleverantörernas molnteknik är helt standardiserad och levereras på ett fullständigt automatiserat sätt. Därför kan en molntjänstleverantör inte ändra några villkor som skulle kräva en underliggande anpassning av tjänsten. Dessutom är priserna för tjänsterna vanligtvis offentliga och standardiserade för alla användare, vilket innebär att en molntjänstleverantör inte bara kan justera priser för att absorbera mer risker på en viss kunds bekostnad.

Indirekta inköp

Ett alternativ till att köpa molnteknik direkt från en molntjänstleverantör är att köpa den från en återförsäljare till en molntjänstleverantör i stället. Mer information om återförsäljare till en molntjänstleverantör finns i avsnittet 2.1.3 ovan.

Exempel på språk för offertförfrågan: villkor

Molntjänstleverantörer eller representerande leverantörer måste tillhandahålla sina offentliga villkor och ge feedback på viktiga villkor från <ORGANISATION>.

<ORGANISATION> avser att ingå ett skriftligt avtal med den anbudsgivare som tilldelats avtalet baserat på anbudsgivarens avtalsvillkor. Anbudsgivaren ska förse <ORGANISATION> med en uppsättning föreslagna avtalsvillkor som organisationen kan granska och som representerar dess bästa kommersiella och juridiska förslag. Anbudsgivare och <ORGANISATION> kan diskutera båda villkorsuppsättningarna under fasen för <DISKUSSION/FÖRHANDLING>.

- *Övergripande, huvudsakliga villkor för ramverket ska som mest bestå av följande komponenter:*
 - *Ramverkets varaktighet*
 - *Ramverkets styrning*
 - *Ramverkets prestanda*
 - *Ramverkets avslutande*
 - *Ramverkets omfattning*
 - *Beställningsprocess*
 - *Sekretessbestämmelser*
 - *Kategorispecifik IP och information*
 - *Minska tekniska krav som molntjänstleverantörerna ska uppfylla, till exempel standarder, ackreditering, säkerhet och dataskydd*
- *Det finns olika villkor för varje område i ramavtalet*
- *Detaljerna i molntjänstleverantörernas tjänster kan övervägas och hanteras vid avropet*
- *Tillåt avtalsändringar – villkoren bör inte hindra kunder och leverantörer från att komma överens om avtalsändringar för att lägga till nya tjänster eller förbättringar. I och med molntjänsternas föränderliga natur blir tjänstförbättringar kontinuerligt tillgängliga, vilket bidrar till att ge kunderna ökad effektivitet.*
- *Servicenivåavtal (SLA) bör inte specificeras av kunden. Kundens villkor bör inte definiera kommissionsspecifika, skräddarsydda servicenivåavtal som skiljer sig från molntjänstleverantörernas leveransmodeller för*

Köpa molntjänster i offentlig sektor

standardtjänster. Genom att tillåta molntjänstleverantörers standard servicenivåavtal kan molntjänstleverantörerna hålla nere kostnaderna och lägga över dem på kunderna samtidigt som kunderna kan lita på att molntjänstleverantören kan fullgöra servicenivåavtalet.

- *Tak för ansvarsskyldighet bör vara proportionerliga. Ansvarsskyldigheten bör vara proportionerlig till de tjänster som köps och det bör inte finnas oproportionerligt höga tak. Oproportionerligt höga tak skulle utgöra ett hinder för molntjänstleverantörer att acceptera projekt med lågt värde. Dessa projekt är ofta en bra inledning och ett "testfall" som kunder kan använda för att avgöra om vissa molnlösningar är effektiva för deras organisation eller inte.*
- *Kunder bör äga sina egna data. Kunder bör kontrollera och äga sina data och ha möjligheten att bestämma på vilken geografisk plats de lagras. Det gör att kunderna slipper bli låsta till en viss leverantör och fritt kan flytta data till nya leverantörer.*

2.5.2 Välja mellan mottagare efter projekt

Organ i den offentliga sektorn som är part i ramverket kan vid behov beställa eller göra avrop på tjänster de behöver. Om ett avropsavtal läggs till under ett ramavtal kan köpare finjustera krav med ytterligare funktionsspecifikationer för avrop och samtidigt behålla fördelarna i ramavtalet.

Om det anses nödvändigt kan en liten tävling anordnas för att identifiera den bästa leverantören för en särskild arbetsbelastning eller ett särskilt projekt. En liten tävling innebär att en kund öppnar upp för ytterligare konkurrens under ramverket genom att bjuda in alla leverantörer inom ett område att svara på en uppsättning krav. Kunden bjuder in alla kapabla leverantörer inom området att lämna anbud, varför det är viktigt med minsta krav för mottagare i en offertförfrågan för molntjänster eftersom det säkerställer alternativ med hög standard inom ett särskilt område.

Observera återigen att det är viktigt att det finns olika uppsättningar villkor för avtal för varje områdeskategori för typen av erbjudande (till exempel offentlig IaaS/PaaS, community IaaS/PaaS, privat IaaS/PaaS) eftersom ett "tillvägagångssätt där en lösning passar alla" i upphandlingen för varje område leder till problem med genomförbarhet och kompatibilitet.

Se avsnitt 2.1.4 för exempel på språk för offertförfrågan när det gäller att välja mellan mottagare.

2.5.3 Introduktion och utträde

Något som bör övervägas vid upprättandet av ett molnramavtal är möjligheten att använda ett dynamiskt upphandlingssystem (DPS). Med en DPS-modell antas alla leverantörer som uppfyller de minsta kraven för ramavtalet till ramverket. Det finns ingen fast gräns för hur många leverantörer som kan delta i ramverket och till skillnad från den traditionella ramverksmodellen kan leverantörer även delta i "DPS-ramverket" när som helst under dess livstid.

Vi rekommenderar starkt att enheter i den offentliga sektorn sätter höga standarder för att säkerställa kvalitet och försäkra på tjänsterna från kvalificerade leverantörer. Däremot bör standarderna inte vara så specifika att de utesluter molntjänstleverantörer på ett sätt som inte garanterar rättvis konkurrens. Målet är i slutändan att undvika att mätta slutanvändarna med en enorm mängd alternativ, samtidigt som standarden på de molntekniker som erbjuds ska vara hög.

3.0 Bästa praxis/lärdomar

Nedan lyfter vi fram några lärdomar kring hur ett lyckat molnramavtal med en välskrivna offertförfrågan för molntjänster upprättas.

Köpa molntjänster i offentlig sektor

3.1 Molnstyrning

Styrning i molnet är ett delat ansvar. Molntjänstleverantörer tillhandahåller funktioner och tjänster för att bygga in molnstyrning i varje aspekt av molnmiljön, medan kunder bidrar med sina befintliga standarder för molnstyrning och lär sig hur molnet underlättar molnstyrning.

I molnet har kunderna möjlighet att få den IT-miljö de vill ha snarare än att bara hantera den de miljö har. Molnkunder kan (1) starta med en full uppsättning av alla IT-tillgångar, (2) hantera alla dessa tillgångar centralt och (3) skapa varningar om användning/fakturering/säkerhet osv. Alla dessa viktiga fördelar med molnet bidrar till att kunderna får en optimerad – och i möjligaste mån automatiserad – arkitektur utan att ständigt behöva införskaffa och installera ny maskinvara. Det sköts av molntjänstleverantören, så att kunder kan flytta sitt fokus från odifferentierad infrastrukturhantering till verksamhetskritisk drift.

Ett bra sätt att se på ett moln från en molntjänstleverantör är som ett mycket stort API. När du startar en ny server eller ändrar en säkerhetsinställning gör du egentligen bara API-anrop. Varje ändring av miljön loggas och registreras (alla uppgifter om "vem, vad, var och när" för varje ändring registreras). Det ger en molnstyrning, kontroll och inblick som bara är möjlig i en molnmiljö. Det får kunderna att tänka om gällande sina befintliga modeller för IT-styrning och fastställa hur de kan effektiviseras och förbättras med de fördelar som molnet kan ge.

Molnstyrning kan även innebära att kommunicera och införliva de positiva processändringarna och den nya kompetensen som följer med molnet. Projektledare är till exempel vana vid att vänta månader på att en IT-miljö ska byggas ut och kan därför överskatta scheman för att ta fram en miljö för utveckling eller tester i molnet (som i molnet kan gå på bara några minuter). Det är en utvecklingsprocess att anpassa sig till denna nyfunna flexibilitet och det sker program för program. Sådana lärdomar bör delas, så att ett molnramavtal kan fortsätta att utvecklas på ett sådant sätt att kraven passar nya processer och flexibilitet.

3.2 Budgetera för molnet

När det gäller att strukturera molnpriser som baseras på betalning per förbrukning och som passar den offentliga sektorns anskaffnings- och budgetkrav har vi kommit fram till att det underlättar att samla molntjänstleverantörens tjänster i en enda standardartikel (databehandling, lagring, nätverk, databas, IoT osv.), alla under en standardartikel för **molnteknik**. Detta tillvägagångssätt ger flexibiliteten att erbjuda kunderna molntjänstleverantörens alla aktuella och nya tekniker i realtid. Det ger även snabb åtkomst till de resurser som kunden behöver, när de behöver dem. Det ger även möjlighet att hantera varierande behov, vilket leder till en optimerad användning och låga kostnader.

Organisationer i den offentliga sektorn kan lägga till ytterligare standardartiklar för beställningar från andra områden i ett molnramverk om de skulle behöva konsulttjänster/professionella eller hanterade tjänster, programvara från en marknadsplats, tjänster för molnsupport och utbildning inom erbjudanden från molntjänstleverantörer.

Det går att åstadkomma ytterligare flexibilitet i upphandlingen genom att använda valfria avtalsstandardartiklar i lämpliga resurskategorier för att möjliggöra framtida tillväxt. Om en organisation vill samla molntekniker med konsulttjänster/professionella eller hanterade tjänster i en enda standardartikel går det att göra med en standardartikel som "molnteknik och annat arbete".

Köpa molntjänster i offentlig sektor

Nedan visas ett representativt exempel på detta tillvägagångssätt. I exemplet nedan motsvarar varje enhet i standardartikeln ”#1001 – Molnteknik” 1,00 € per ”molnteknik” som används. Varje månad kan beställningsökningar finansieras baserat på aktuella och prognostiserade användningsprognoser.

Tabell 3 – Exempel på prisstruktur för en standardartikel.

ARTIKELNR	LEVERANSER/TJÄNSTER	KVANTITET	ENHET	ENHETSPRIS	MÄNGD
1001	Molnteknik	1 000	Var	1 €	1 000 €
1002	Konsulttjänster	1	Per vecka	3 000 €	3 000 €
1003	Molnsupport	1	Per månad	1 000 €	1 000 €
1004	Molnutbildning	1	Per dag	3,00 €	3 000 €
1005	Molnmarknadsplats	10	Var	10 €	100 €

Ett exempel på hur den här strukturen kan fungera: En organisation i den offentliga sektorn samarbetar med en molntjänstleverantör för att uppskatta hur många molntekniktjänster som organisationen ska använda. Organisationen och leverantören enas om 10 miljoner euro över 5 år, vilket blir 2 miljoner euro per år. Organisationen förbinder sig till det första årsbeloppet på 2 miljoner euro. Varje månad skickas en faktura och pengarna dras från fonden för att betala den. Det finns ett kreditutnyttjande mot kontot. Molntjänstleverantörens övervaknings- och prognostiseringsverktyg används till att övervaka förbrukningen av återstående medel. Om återstående medel blir låga begär organisationen ytterligare medel från finansdirektören för att använda dessa till att behålla tjänsterna.

Exempel på språk för offertförfrågan: priser – upphandling

BETALNINGSVILLKOR

Betalningsvillkoren måste struktureras enligt principen att bara betala för de resurser som används av <ORGANISATION> enligt nedan:

1. Månadsbetalning som baseras på faktisk användning/förbrukning av tjänster och i enlighet med molntjänstleverantörens officiella priser.

MINSTA GARANTI OCH HÖGSTA UTGIFTER

Eftersom det är omöjligt för <ORGANISATION> att fastställa exakt hur många av en molntjänstleverantörs resurser som kommer att förbrukas under en viss tid, specificeras beställningar med enhetskvantiteter med fast pris för en enda beställningsstandardartikel för ”molnteknik”.

Varje enhet av standardartikeln som beställs motsvarar <1,00 €> av den beställda molntekniken. Inkrementella beställningar läggs regelbundet via ändringar av beställningen i flera kvantiteter för att erbjuda <ORGANISATION> flexibiliteten att förbeställa flera kvantiteter med ”euro-belopp” av molntjänstleverantörens molnteknik baserat på den uppskattade användningen för behov som varar olika länge. Kvantiteter förbeställs regelbundet av <ORGANISATION> för belopp som räcker till att täcka den uppskattade kostnaden för molnteknik som ska användas till att uppfylla flera olika krav.

Artikelnr	Beskrivning	Kvantitet	Enhet	Pris
01	Molntjänstleverantörens molnteknik	1 000	EA	1 000,00 €

Köpa molntjänster i offentlig sektor

MINSTA BESTÄLLNING/INKREMENTELL BESTÄLLNING

Beställningar läggs regelbundet för flera kvantiteter på <10 000> enheter av standardartiklar baserat på <ORGANISATION>s uppskattade användning av molnteknik. Det här arrangemanget ger <ORGANISATION> flexibiliteten att förbeställa <10 000> enheter av "molnteknik" för att hantera driften i enlighet med principen "betala per användning" för molntjänster.

En första ökning på <100 000> enheter till ett pris på <100 000 €> beställs när avropet läggs. Det minsta antalet totala enheter av standardartiklar som kan läggas på en enda inkrementell beställning med en eller flera standardartiklar är <x>. Det största antalet enheter som kan beställas under leveransbeställningen får inte överstiga <x>, men får aldrig överstiga avropsvärdet när det kombineras med alla tidigare beställda enheter. <ORGANISATION> ansvarar för att säkerställa att alla beställningar håller sig inom gränserna som anges i detta avsnitt.

MAXIMAL BESTÄLLNING

Det totala största beställningsvärdet är <x> och får bestå av upp till <x> enheter av en och samma standardartikel som kostar <x> per enhet. Värdet baseras på en uppskattning av <ORGANISATION>s behov under prestandaperioden, men kan inte garanteras.

3.3 Förstå partners affärsmodell

Enheter i den offentliga sektorn bör försöka förstå modellerna som molntjänstleverantörer använder för att tillhandahålla sina erbjudanden, och att partners som levererar konsulttjänster, hanterade tjänster, återförsäljartjänster och mycket mer är mycket viktiga för processen. Många kunder behöver en molnleverantör för sin infrastruktur, och anlitar en systemintegratör eller leverantör av hanterade tjänster för det praktiska arbetet med planering, migrering och hantering. Med tanke på denna blandning av tjänster kan det finnas krav som inte gäller för molnleverantörer, t.ex. tillämpning av klausuler i huvudavtalet på underleverantörer.

Ett exempel på varför det är viktigt att förstå hur partner och återförsäljare arbetar i relation till molntjänstleverantören är att det vid vissa typer av upphandlingar finns klausuler som kräver att den primära leverantören för vidare vissa obligatoriska klausuler till alla sina partners/underleverantörer. Molntjänstleverantörer tillhandahåller vanligtvis inte tjänster och offererar inte som formella underleverantörer, eftersom de erbjuder en standardiserad tjänst på en enorm skala som inte är skraddarsydd efter en viss slutanvändares unika krav (inklusive behoven hos en kund i den offentliga sektorn enligt ett avtal för den offentliga sektorn). I en modell för indirekta upphandlingar (upphandlingar av molntjänster genom en återförsäljare för en molntjänstleverantör) kan en molntjänstleverantör avvisa dessa klausuler från sin återförsäljare som icke tillämpbara för en leverantör av kommersiella tjänster i det andra ledet. I detta fall utför inte molntjänstleverantören själv arbetet som avtalet avser. I stället använder en av molntjänstleverantörens partner dennes infrastruktur för att utföra arbetet. Molntjänstleverantören fungerar därför som en kommersiell leverantör (inte en underleverantör) till en partners verksamhet. I en direkt upphandlingsmodell (köpa molntjänster direkt från en molntjänstleverantör) avvisar vanligtvis en molntjänstleverantör dessa "obligatoriska" klausuler som passar en vanlig underleverantör av handelsvaror på grund av de upphandlade tjänsternas kommersiella natur och det faktum att de flesta molntjänstleverantörer inte behöver underleverantörer för att leverera sina kommersiella tjänster.

3.4 Molnmäklare

Konceptet molnmäklare i betydelsen att minska låsningen till en viss leverantör kan vara problematiskt. Molnmäklare kan låta som en bra idé i teorin, men i praktiken skulle det antagligen medföra mer komplexitet och förvirring än verkligt värde.

Köpa molntjänster i offentlig sektor

Det är oundvikligt att göra kompromisser under utformningen av program som samtidigt eller utbytbart fungerar i flera moln (**det finns ingen Rosettasten för molnet**). Det här tillvägagångssättet kan skapa ett onödigt lager av komplexitet mellan kunder i den offentliga sektorn och deras molntjänster, och äventyra de effektiviseringar och säkerhetsvinster som man försöker uppnå. Det leder i sin tur till minskad skalbarhet och flexibilitet, ökade kostnader och avstannande innovation.

3.5 Inköps-/marknadsundersökning av offertförfrågan som hålls i förtid

När en enhet i den offentliga sektorn planerar en offertförfrågan för molntjänster bör den inkludera intressenterna från alla aspekter av organisationen – högre chefer, affärsintressenter, avdelningarna för teknik, ekonomi, upphandling, juridik och avtal – från början av processen. Detta tillvägagångssätt säkerställer att alla intressenter förstår molnmodellen och därför också kan ompröva traditionella metoder för IT-upphandling på ett välgrundat sätt.

Vad gäller kontakten med branschen rekommenderar vi att enheter i den offentliga sektorn tar sig tid att ha djupgående samtal för att samla in feedback från branschen – molntjänstleverantörer, partners till molntjänstleverantörer, marknadsplatsleverantörer av PaaS/SaaS och branschexperter. En sådan dialog kan till exempel ske i form av branschdagar eller säkerhets- och upphandlingsseminarier. Ett annat effektivt sätt att få en ingående förståelse för molnupphandling är att publicera en begäran om information eller ännu hellre ett utkast på en offertförfrågan. De innehåller ofta potentiella problem som kan identifieras, diskuteras och justeras innan den slutgiltiga offertförfrågan för molntjänster släpps.

Bilaga A – Tekniska krav för att jämföra olika anbudsgivare

Nedan anger vi några generella krav på molnteknik som kan användas för att jämföra molntjänstleverantörer under avrop eller minitävlingar i ett molnramavtal.

1. Molnleverantörens profil

	<i>Krav</i>
1.	MARKNADSERFARENHET: <i>Hur många år har molnleverantören varit verksam inom molnmarknadssegmentet?</i>
2.	ÖPPENHET OCH DATASKYDD: <i>Följer molnleverantören uppförandekoderna för dataskydd och reverserbarhet? Följer molnleverantören principerna för öppen källkod och öppen API-utveckling?</i>

2. Global infrastruktur

	<i>Krav</i>
1.	GLOBAL RÄCKVIDD: <i>Erbjuder molnleverantören en global infrastruktur för att hjälpa användare att få korta svarstider och hantera stora dataflöden?</i>
2.	REGIONER: <i>Har molnleverantören regional närvaro i de geografiska områden som krävs?</i>
3.	DOMÄNER/ZONER: <i>Använder sig molnleverantören av konceptet domäner eller zoner, där flera datacenter grupperas via ett nätverk med korta svarstider för att ge högre tillgänglighet och feltolerans?</i> <ul style="list-style-type: none"> <i>Ange i så fall antalet domäner eller zoner och antalet datacenter i det aktuella geografiska området</i>
4.	AVSTÅND FRÅN DOMÄNER/ZONER: <i>Bygger molnleverantören sina domäner eller zoner med datacenter som är fysiskt åtskilda för att stödja redundans, hög tillgänglighet och korta svarstider?</i>
5.	BYGGDA DATACENTER: <i>Erbjuder molnleverantören datacenter som är isolerade från fel i andra datacenter, med redundant strömförsörjning, kylning och nätverk?</i>
6.	REPLIKERING AV DATACENTER: <i>Erbjuder molnleverantören datareplikering i datacentren inom en domän eller zon med automatisk redundans?</i>
7.	REPLIKERING AV DOMÄN/ZON: <i>Erbjuder molnleverantören datareplikering i domäner eller zoner inom en region?</i>

Köpa molntjänster i offentlig sektor

3. Infrastruktur

3.1 Databehandling

	Krav
1.	DATABEHANDLING – REGELBUNDEN INSTANS – ALLMÄNNA ÄNDAMÅL: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• Allmänna ändamål – optimerad för allmänna program och balanserar resurser för databehandling, minne och nätverk.<ul style="list-style-type: none">○ Vilken är den största instansen i så fall?
2.	DATABEHANDLING – REGELBUNDEN INSTANS – MINNESOPTIMERAD: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• Minnesoptimerad – optimerad för minnesintensiva program<ul style="list-style-type: none">○ Vilken är den största instansen i så fall?
3.	DATABEHANDLING – REGELBUNDEN INSTANS – DATABEHANDLINGSOPTIMERAD: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• Databehandlingsoptimerad – optimerad för databehandlingsintensiva program<ul style="list-style-type: none">○ Vilken är den största instansen i så fall?
4.	DATABEHANDLING – REGELBUNDEN INSTANS – LAGRINGSOPTIMERAD: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• Lagringsoptimerad – erbjuder stor kapacitet för lokal lagring<ul style="list-style-type: none">○ Vilken är i så fall den maximala kapaciteten (dvs. 5, 10, 20, 50 TB) och det maximala antalet diskar (hårddiskar/SSD-enheter) som kan tillhandahållas och kopplas till en instans?
5.	DATABEHANDLING – REGELBUNDEN INSTANS – GRAFIKOPTIMERAD: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• Grafik till låg kostnad – erbjuder grafikaccelerering till låg kostnad för databehandlingsinstanser<ul style="list-style-type: none">○ Vilken är den största instansen i så fall?
6.	DATABEHANDLING – REGELBUNDEN INSTANS – GPU-OPTIMERAD: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• GPU – erbjuder maskinvara för grafikprocessorer (GPU) för grafikintensiva program<ul style="list-style-type: none">○ Hur många GPU-enheter och vilka GPU-modeller kan molnleverantören erbjuda per instans i så fall?
7.	DATABEHANDLING – REGELBUNDEN INSTANS – FPGA-OPTIMERAD: Erbjuder molnleverantören följande instanstyper? <ul style="list-style-type: none">• FPGA – erbjuder fältprogrammerbara grindmatriser (FPGA) för att utveckla och distribuera anpassade maskinvaruaccelereringar för program.<ul style="list-style-type: none">○ Hur många FPGA-enheter kan molnleverantören erbjuda per instans i så fall?
8.	DATABEHANDLING – OMDIRIGERBAR INSTANS: Erbjuder molnleverantören omdirigerbara instanser som ger prestanda för en processor (CPU) på basnivå med möjligheten att nå högre än basnivån?

Köpa molntjänster i offentlig sektor

	<ul style="list-style-type: none"> • Vilken är den största dirigerbara instansen i så fall?
9.	<p>DATABEHANDLING – I/O-INTENSIV INSTANS:</p> <p>Erbjuder molnleverantören instanser som använder icke-flyktig minnesexpress (NVMe), solid state-hårddiskar (SSD-enheter) optimerade för korta svarstider, mycket höga slumpmässiga I/O-prestanda och höga sekventiella läsprestanda?</p> <ul style="list-style-type: none"> • Vilken är i så fall den maximala kapaciteten för inmatnings-/utmatningsåtgärder per sekund (IOPS) för den största instansen?
10.	<p>DATABEHANDLING – TILLFÄLLIG LOKAL LAGRING:</p> <p>Stödjer molnleverantören att lokal lagring för databehandlingsinstanser används för tillfällig lagring av information som ofta ändras?</p>
11.	<p>DATABEHANDLING – STÖD FÖR FLERA NÄTVERKSKORT:</p> <p>Stödjer molnleverantören att flera (primära och extra) nätverkskort (NIC) tilldelas för en given instans?</p> <ul style="list-style-type: none"> • Vilket är i så fall det maximala antalet NIC per instans?
12.	<p>DATABEHANDLING – INSTANSTILLHÖRIGHET:</p> <p>Erbjuder molnleverantören användare möjligheten att på ett logiskt sätt gruppera instanser i samma datacenter?</p>
13.	<p>DATABEHANDLING – INSTANSANTITILLHÖRIGHET:</p> <p>Erbjuder molnleverantören användare möjligheten att på ett logiskt sätt gruppera instanser och placera dem i olika datacenter inom en region?</p>
14.	<p>DATABEHANDLING – SJÄLVHANTERAD ETABLERING:</p> <p>Erbjuder molnleverantören självhanterad etablering av flera instanser samtidigt, antingen via ett programmeringsgränssnitt, en hanterad konsol eller en webbportal?</p>
15.	<p>DATABEHANDLING – ANPASSNING:</p> <p>Erbjuder molnleverantören anpassningsbara instanser, dvs. möjligheten att modifiera konfigurationsinställningar som virtuella processorer (vCPU) och RAM (Random Access Memory)?</p>
16.	<p>DATABEHANDLING – KLIENTORGANISATIONER:</p> <p>Erbjuder molnleverantören instanser för enstaka klientorganisationer som körs på maskinvara som är avsedd för en enda användare?</p> <ul style="list-style-type: none"> • Vilken är i så fall den största tillgängliga instansen för enstaka klientorganisationer?
17.	<p>DATABEHANDLING – VÄRDITILLHÖRIGHET:</p> <p>Erbjuder molntjänstleverantören möjligheten att starta en instans och specificera att denna instans alltid startar om på samma fysiska värd?</p>
18.	<p>DATABEHANDLING – VÄRDANTITILLHÖRIGHET:</p> <p>Erbjuder molnleverantören möjligheten att dela upp och köra specifika instanser på olika fysiska värddar?</p>
19.	<p>DATABEHANDLING – AUTOMATISK SKALNING:</p> <p>Erbjuder molnleverantören möjligheten att automatiskt öka antalet instanser under behovstoppar för att bibehålla prestanda (dvs. "utskalning")?</p>
20.	<p>DATABEHANDLING – MEKANISM FÖR IMPORT AV AVBILDNINGAR:</p> <p>Erbjuder molnleverantören användare möjligheten att importera befintliga avbildningar och spara dem som nya, privat tillgängliga avbildningar som sedan kan användas för att etablera nya instanser i framtiden?</p> <ul style="list-style-type: none"> • Vilka format stöds i så fall?
21.	<p>DATABEHANDLING – MEKANISM FÖR EXPORT AV AVBILDNINGAR:</p>

Köpa molntjänster i offentlig sektor

	<p>Stödjer molnleverantören möjligheten att ta en befintlig instans som körs eller en kopia av en instans och exportera instansen till ett virtuellt datorformat?</p> <ul style="list-style-type: none"> • Vilka format stöds i så fall?
22.	<p>DATABEHANDLING – STÖRNINGAR I TJÄNSTEN:</p> <p>Erbjuder molnleverantören mekanismer för att undvika att instansen drabbas av avbrott eller driftstopp när leverantören utför någon typ av underhåll på maskinvara eller tjänster på värdnivå?</p>
23.	<p>DATABEHANDLING – INSTANSOMSTART:</p> <p>Erbjuder molnleverantören mekanismer för att automatiskt starta om instanser på en fungerande värd om den ursprungliga fysiska värden slutar att fungera?</p>
24.	<p>DATABEHANDLING – AVISERINGAR:</p> <p>Om något inträffar som gör att databehandlingen måste återhämta sig, har molnleverantören möjlighet att informera användaren om att detta har inträffat och kan användaren på egen hand välja att få eller avstå från denna kommunikation?</p>
25.	<p>DATABEHANDLING – SCHEMALÄGGNING AV HÄNDELSER:</p> <p>Erbjuder molnleverantören möjligheten att kunna schemalägga händelser för användarens instanser, till exempel att starta om, stoppa, starta eller ta instansen ur drift?</p>
26.	<p>DATABEHANDLING – MEKANISM FÖR SÄKERHETSKOPIERING OCH ÅTERSTÄLLNING:</p> <p>Erbjuder molnleverantören en integrerad mekanism för säkerhetskopiering och återställning?</p>
27.	<p>DATABEHANDLING – MEKANISM FÖR ÖGONBLICKSBILDER:</p> <p>Erbjuder molnleverantören en manuell mekanism för ögonblicksbilder på begäran?</p>
28.	<p>DATABEHANDLING – METADATA:</p> <p>Erbjuder molnleverantören en tjänst för instansmetadata som gör att användare kan ange godtyckliga nyckelvärdepar för instansen?</p>
29.	<p>DATABEHANDLING – ANROP OM METADATA:</p> <p>Erbjuder molnleverantören en tjänst för instansmetadata med ett API (Application Programming Interface) som instansen kan anropa för att få information om sig själv?</p>
30.	<p>DATABEHANDLING – MEKANISM FÖR ATT LÄMNA ANBUD:</p> <p>Erbjuder molnleverantören en mekanism för att lämna anbud på billigare instanser som omedelbart kan skapas för att köra mindre viktiga arbetsbelastningar?</p>
31.	<p>DATABEHANDLING – MEKANISM FÖR SCHEMALÄGGNING:</p> <p>Erbjuder molnleverantören ett sätt att regelbundet schemalägga och reservera extra databehandlingskapacitet, dvs. varje dag, vecka eller månad?</p>
32.	<p>DATABEHANDLING – RESERVATIONSMEKANISM:</p> <p>Erbjuder molnleverantören ett sätt att reservera extra databehandlingskapacitet för framtiden (dvs. ett år, två år, tre år osv.)?</p>
33.	<p>DATABEHANDLING – LINUX-OPERATIVSYSTEM:</p> <p>Stödjer molnleverantören de senaste två långsiktiga kompatibla versionerna av minst en Linux-distribution för företag (som Red Hat eller SUSE) och en vanlig kostnadsfri Linux-distribution (som Ubuntu, CentOS eller Debian)?</p>
34.	<p>DATABEHANDLING – WINDOWS-OPERATIVSYSTEM:</p> <p>Stödjer molnleverantören minst två stora Windows Server-versioner (Windows Server 2017 och Windows Server 2016)?</p>

Köpa molntjänster i offentlig sektor

35.	<p>DATABEHANDLING – LICENS PORTABILITET:</p> <p>Erbjuder molnleverantören licensportabilitet och -support?</p> <ul style="list-style-type: none"> Ange i så fall programvaruleverantör, programvarunamn, utgåvor och dess versioner.
36.	<p>DATABEHANDLING – BEGRÄNSNINGAR FÖR TJÄNSTEN:</p> <p>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller databehandlingsavsnittet ovan?</p> <p>Exempel:</p> <p>Maximalt antal instanser per konto</p> <p>Maximalt antal dedikerade värdar per konto</p> <p>Maximalt antal reserverade IP-adresser (internetprotokoll)</p>

3.2 Nätverk

	Krav
1.	<p>NÄTVERK – VIRTUELLA NÄTVERK:</p> <p>Stödjer molnleverantören möjligheten att skapa ett logiskt, isolerat virtuellt nätverk som representerar ett företags egna nätverk i molnet?</p>
2.	<p>NÄTVERK – ANSLUTNING I SAMMA REGION:</p> <p>Stödjer molnleverantören att två virtuella nätverk i samma region ansluts för att dirigera trafik mellan dem med hjälp av privata IP-adresser (internetprotokoll)?</p>
3.	<p>NÄTVERK – ANSLUTNING I OLIKA REGIONER:</p> <p>Stödjer molnleverantören att två virtuella nätverk i olika regioner ansluts för att dirigera trafik mellan dem med hjälp av privata IP-adresser (internetprotokoll)?</p>
4.	<p>NÄTVERK – PRIVAT UNDERNÄT:</p> <p>Erbjuder molnleverantören möjligheten att skapa helt isolerade (privata) virtuella nätverk och undernät där instanser kan etableras utan någon offentlig IP-adress (internetprotokoll) eller internetdirigering?</p>
5.	<p>NÄTVERK – ADRESSINTERVALL FÖR VIRTUELLA NÄTVERK:</p> <p>Stödjer molnleverantören IP-adressintervall som anges i begäran om kommentarer (RFC) 1918 och officiellt dirigerbara CIDR-block (Classless Inter-Domain Routing)?</p>
6.	<p>NÄTVERK – FLERA PROTOKOLL:</p> <p>Stödjer molnleverantören flera protokoll, bland annat TCP (Transmission Control Protocol), UDP (User Datagram Protocol) och ICMP (Internet Control Message Protocol)?</p>
7.	<p>NÄTVERK – AUTOMATISK TILLDELNING AV IP-ADRESSER:</p> <p>Stödjer molnleverantören möjligheten att automatiskt tilldela offentliga IP-adresser till instanser?</p>
8.	<p>NÄTVERK – RESERVERADE STATISKA IP-ADRESSER:</p> <p>Stödjer molnleverantören att IP-adresser kopplas till ett användarkonto och inte en särskild instans? IP-adressen ska förbli kopplad till kontot tills den uttryckligen frigörs.</p>
9.	<p>NÄTVERK – STÖD FÖR IPV6:</p> <p>Stödjer molnleverantören IPv6 (IPv6), antingen på gateway- eller instansnivå, och visas denna funktion för användarna?</p>
10.	<p>NÄTVERK – FLERA IP-ADRESSER PER NÄTVERKSKORT:</p>

Köpa molntjänster i offentlig sektor

	<i>Stödjer molnleverantören möjligheten att tilldela en primär och en sekundär IP-adress till ett nätverkskort (NIC) som är kopplat till en given instans?</i>
11.	NÄTVERK – FLERA NÄTVERKSKORT: <i>Stödjer molnleverantören möjligheten att tilldela flera nätverkskort (NIC) till en given instans?</i>
12.	NÄTVERK – MOBILITET FÖR NÄTVERKSKORT OCH IP-ADRESSER: <i>Stödjer molnleverantören möjligheten att flytta nätverkskort (NIC) och IP-adresser mellan instanser?</i>
13.	NÄTVERK – STÖD FÖR SR-IOV: <i>Stödjer molnleverantören möjligheter som SR-IOV (Single Root Input/Output Virtualization) för högre prestanda (dvs. paket per sekund – PPS), korta svarstider och lägre jitter?</i>
14.	NÄTVERK – INKOMMANDE FILTRERING: <i>Stödjer molnleverantören möjligheten att lägga till eller ta bort regler för inkommande trafik till instanser?</i>
15.	NÄTVERK – UTGÅENDE FILTRERING: <i>Stödjer molnleverantören möjligheten att lägga till eller ta bort regler för utgående trafik från instanser?</i>
16.	NÄTVERK – ACL: <i>Erbjuder molnleverantören åtkomstkontrollistor (ACL) för att kontrollera inkommande och utgående trafik till undernät?</i>
17.	NÄTVERK – STÖD FÖR FLÖDESLOGGAR: <i>Erbjuder molnleverantören möjligheten att registrera flödesloggar med nätverkstrafik?</i>
18.	NÄTVERK – NAT: <i>Erbjuder molnleverantörer en hanterad lösning med gateway för nätverksöversättning (NAT) för att möjliggöra anslutning av instanser i ett privat nätverk till internet eller andra molntjänster, men hindrar internet från att initiera en anslutning till dessa instanser?</i>
19.	NÄTVERK – KONTROLL AV KÄLLA/MÅL: <i>Har molnleverantören möjlighet att avaktivera kontroll av källa/mål på nätverkskort (NIC)?</i>
20.	NÄTVERK – STÖD FÖR VPN: <i>Stödjer molnleverantören anslutning av virtuella privata nätverk (VPN) mellan molnleverantören och användarens datacenter?</i>
21.	NÄTVERK – VPN-TUNNLAR: <i>Stödjer molnleverantören flera anslutningar av virtuella privata nätverk (VPN) per nätverk?</i>
22.	NÄTVERK – STÖD FÖR IPSEC VPN: <i>Erbjuder molnleverantören användare åtkomst till molntjänster via antingen en VPN-tunnel (virtuellt privat nätverk) med IPsec (internetprotokollsäkerhet) eller en VPN-tunnel (virtuellt privat nätverk) med SSL (Secure Sockets Layer) via offentligt internet?</i>
23.	NÄTVERK – STÖD FÖR BGP: <i>Använder molnleverantören BGP (Border Gateway Protocol) för att förbättra redundans i VPN-tunnlar (virtuellt privat nätverk) med IPsec (internetprotokollsäkerhet)?</i>
24.	NÄTVERK – PRIVAT DEDIKERAD ANSLUTNING: <i>Erbjuder molnleverantörer en direkt, privat anslutningstjänst mellan molnleverantörens platser och användarens datacenter, kontor eller samlokaliseringssmiljö som klarar stora och snabba dataöverföringar?</i>
25.	NÄTVERK – LASTBALANSERING FÖR KLIENTDELEN:

Köpa molntjänster i offentlig sektor

	<i>Erbjuder molnleverantören en lastbalanseringstjänst för klientdelen (mot internet) som tar emot begäran från klienter över internet och fördelar dem mellan instanser som är registrerade i lastbalanseringen?</i>
26.	NÄTVERK – LASTBALANSERING FÖR SERVERDELEN: <i>Erbjuder molnleverantören en lastbalanseringstjänst för serverdelen (privat) som dirigerar trafik till instanser som körs i privata undernät?</i>
27.	NÄTVERK – LASTBALANSERING I LAGER 7: <i>Erbjuder molnleverantören en lastbalanseringstjänst i lager 7 (Hypertext Transfer Protocol – HTTP) som klarar lastbalansering av nätverkstrafik över flera instanser?</i>
28.	NÄTVERK – LASTBALANSERING I LAGER 4: <i>Erbjuder molnleverantören en lastbalanseringstjänst i lager 4 (Transmission Control Protocol – TCP) som klarar nätverkstrafik för lastbalansering över flera instanser?</i>
29.	NÄTVERK – SESSIONSTILLHÖRIGHET FÖR LASTBALANSERING: <i>Erbjuder molnleverantören en lastbalanseringstjänst med stöd för sessionstillhörighet?</i>
30.	NÄTVERK – DNS-BASERAD LASTBALANSERING: <i>Erbjuder molnleverantören en lastbalanseringstjänst som klarar lastbalanseringstrafik till instanser som körs på flera värdar som tillhör en enda domän?</i>
31.	NÄTVERK – LASTBALANSERINGSLOGGAR: <i>Erbjuder molnleverantören loggar som registrerar detaljerad information om alla förfrågningar som skickas till en lastbalanserare?</i>
32.	NÄTVERK – DNS: <i>Erbjuder molnleverantören en DNS-tjänst (Domain Name System) med mycket hög tillgänglighet och skalbarhet?</i>
33.	NÄTVERK – LATENSBASERAD DNS-DIRIGERING: <i>Erbjuder molnleverantören en DNS-tjänst (Domain Name System) med stöd för latensbaserad dirigering (dvs. DNS-tjänsten svarar på DNS-frågor med de resurser som ger bästa möjliga svarstid)?</i>
34.	NÄTVERK – GEOGRAFISKT BASERAD DNS-DIRIGERING: <i>Erbjuder molnleverantören en DNS-tjänst (Domain Name System) med stöd för geografiskt baserad dirigering (dvs. DNS-tjänsten svarar på DNS-frågor baserat på användarnas geografiska plats)?</i>
35.	NÄTVERK – REDUNDANSBASERAD DNS-DIRIGERING: <i>Erbjuder molnleverantören en DNS-tjänst (Domain Name System) med stöd för redundansbaserad dirigering (dvs. DNS-tjänsten dirigerar DNS-frågor till den resurs som för tillfället är aktiv, medan en andra resurs väntar och endast aktiveras om den första resursen slutar fungera)?</i>
36.	NÄTVERK – TJÄNST FÖR DOMÄNREGISTRERING: <i>Erbjuder molnleverantören tjänster för domännamnsregistrering (dvs. användare kan söka efter och registrera tillgängliga domännamn)?</i>
37.	NÄTVERK – DNS HÄLSOKONTROLLER: <i>Erbjuder molnleverantören en DNS-tjänst (Domain Name System) som använder hälsokontroller för att övervaka resursernas tillstånd och prestanda?</i>

Köpa molntjänster i offentlig sektor

38.	<p>NÄTVERK – DNS OCH LASTBALANSERINGSINTEGRERING:</p> <p>Erbjuder molnleverantören en DNS-tjänst (Domain Name System) som integreras med molnleverantörens lastbalansering?</p>
39.	<p>NÄTVERK – VISUELL REDIGERARE:</p> <p>Erbjuder molnleverantören ett verktyg som gör det möjligt för användare att utforma policyer för trafikhantering?</p>
40.	<p>NÄTVERK FÖR INNEHÅLLSLEVERANS (CDN)</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) för att distribuera innehåll med korta svarstider och hög dataöverföringshastighet?</p>
41.	<p>NÄTVERK – CDN OCH CACHEMINNEN SOM UPPHÖR:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) som gör det möjligt att ta bort objekt från cacheminnen på gränsheter innan de upphör, bland annat funktioner som att ogiltigförklara och versionshantera objekt?</p>
42.	<p>NÄTVERK – CDN OCH EXTERNA URSPRUNG:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) med stöd för anpassade ursprung, t.ex. en HTTP-server (Hypertext Transfer Protocol)?</p>
43.	<p>NÄTVERK – CDN OCH OPTIMERING:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) med detaljerad kontroll för att konfigurera servrar med flera ursprung och cachelagringsegenskaper för olika URL-adresser (Uniform Resource Locators)?</p>
44.	<p>NÄTVERK – CDN MED GEOGRAFISK BEGRÄNSNING:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) med stöd för geografisk begränsning, dvs. som hindrar användare i ett visst geografiskt område från att få åtkomst till innehåll?</p>
45.	<p>NÄTVERK – CDN OCH TOKEN:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) med stöd för undertecknade URL-adresser (Uniform Resource Locators) som vanligtvis skulle innehålla ytterligare information, till exempel utgångsdatum/-tid, för att ge användare mer kontroll över åtkomsten till deras innehåll?</p>
46.	<p>NÄTVERK – CDN OCH CERTIFIKAT:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) med stöd för anpassade SSL-certifikat (Secure Sockets Layer) för att på ett säkert sätt leverera innehåll via HTTPS (Hypertext Transfer Protocol Secure) från gränsheter?</p>
47.	<p>NÄTVERK – CDN OCH CACHEMINNEN MED FLERA NIVÅER:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) som tillämpar en metod för cacheminnen med flera nivåer med användningen av regionala cacheminnen på gränsheter för att minska svarstiderna?</p>
48.	<p>NÄTVERK – CDN OCH KOMPRIMERING:</p> <p>Erbjuder molnleverantören en CDN-tjänst (nätverk för innehållsleverans) med stöd för filkomprimering?</p>
49.	<p>NÄTVERK – CDN OCH KRYPTERAD UPPLADDNING:</p> <p>Erbjuder molnleverantören ett CDN (nätverk för innehållsleverans) där användarna på ett säkert sätt kan ladda upp känsliga data så att sådan information endast kan visas av vissa komponenter och tjänster i användarens ursprungliga infrastruktur?</p>
50.	<p>NÄTVERK – SLUTPUNKTER:</p> <p>Erbjuder molnleverantörens nätverkstjänst användare med slutpunkter som kan dirigera trafik via leverantörens interna nätverk anslutning (dvs. privata anslutningar) för att sänka kommunikationskostnaderna och förbättra trafiksäkerheten?</p>

Köpa molntjänster i offentlig sektor

51.	<p>NÄTVERK – BEGRÄNSNINGAR FÖR TJÄNSTEN:</p> <p>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller nätverksavsnittet ovan?</p> <p>Exempel:</p> <p>Maximalt antal virtuella nätverk per konto</p> <p>Maximal storlek på ett virtuellt nätverk</p> <p>Maximalt antal undernät per konto</p> <p>Maximalt antal lastbalanserare per konto</p> <p>Maximalt antal poster i åtkomstkontrollistan (ACL)</p> <p>Maximalt antal VPN-tunnlar (virtuellt privat nätverk)</p> <p>Maximalt antal ursprung per distribution</p> <p>Maximalt antal certifikat per lastbalanserare</p>
-----	---

3.3 Lagring

	Krav
1.	<p>BLOCKLAGRINGSTJÄNST:</p> <p>Erbjuder molnleverantören lagringsvolymen på blocknivå för användning med databehandlingsinstanser?</p>
2.	<p>BLOCKLAGRING – IOPS:</p> <p>Erbjuder molnleverantören möjligheten att köpa ett uttryckligt prestandamål eller en prestandanivå för blocklagringsvolymen, till exempel ett visst antal inmatnings-/utmatningsfunktioner per sekund (IOPS) eller datavolymer i megabyte per sekund (MB/S)?</p>
3.	<p>BLOCKLAGRING – SOLID STATE-HÅRDDISKAR (SSD):</p> <p>Stödjer molnleverantören säkerhetskopierade lagringsmedia på SSD-enheter (solid state-hårddisk) som ger svarstider på bara några millisekunder?</p> <ul style="list-style-type: none"> Vilket är i så fall det maximala antalet SSD-enheter som kan kopplas per instans?
4.	<p>BLOCKLAGRING – SKALNING:</p> <p>Erbjuder molnleverantören möjligheten att öka storleken på en befintlig blocklagringsvolym utan att behöva etablera en ny volym och kopiera/flytta data?</p>
5.	<p>BLOCKLAGRING – ÖGONBLICKSBILDER:</p> <p>Erbjuder molnleverantören en funktion för ögonblicksbilder för den här blocklagringstjänsten?</p>
6.	<p>BLOCKLAGRING – DATAELIMINERING:</p> <p>Stödjer molnleverantören fullständig eliminering av data sådan att data inte längre kan läsas eller är tillgängliga för obehöriga användare eller tredje part?</p>
7.	<p>BLOCKLAGRING – VILANDE KRYPTERING:</p> <p>Erbjuder molnleverantören kryptering på serversidan av vilande data för data som lagras i volymer och deras ögonblicksbilder?</p> <ul style="list-style-type: none"> Vilken krypteringsalgoritm används i så fall?
8.	<p>OBJEKTLAGRINGSTJÄNST:</p> <p>Erbjuder molnleverantören säker och varaktig objektlagring med hög skalbarhet för lagring och hämtning från webben oavsett datavolym?</p>

Köpa molntjänster i offentlig sektor

9.	<p>OBJEKTLAGRING – OREGELBUNDEN ÅTKOMST:</p> <p>Erbjuder molnleverantören en lagringstjänstnivå till lägre pris som är avsedd för att lagra objekt och filer som används sällan?</p>
10.	<p>OBJEKTLAGRING – KORTARE VARAKTIGHET:</p> <p>Erbjuder molnleverantören en reducerad redundansnivå till ett lägre pris där en användare kan lagra icke-kritiska objekt som är enkla att återskapa?</p>
11.	<p>OBJEKTLAGRING – MINDRE FREKVENT ÅTKOMST:</p> <p>Erbjuder molnleverantören en nivå för data som används mindre frekvent, men som fortfarande kräver snabb åtkomst?</p>
12.	<p>OBJEKTLAGRING – OBJEKTNIVÅER:</p> <p>Erbjuder molnleverantören en funktion för objektlagringsnivåer, dvs. möjligheten att rekommendera överföring av ett objekt mellan objektlagringsklasser eller -nivåer baserat på hur ofta det används?</p>
13.	<p>OBJEKTLAGRING – HANTERING AV LIVSCYKELN:</p> <p>Stödjer molnleverantören hanteringen av ett objekts livscykel genom att använda en livscykelkonfiguration som definierar hur objekt hanteras under dess livstid, från skapande till borttagning?</p>
14.	<p>OBJEKTLAGRING – POLICYDRIVEN HANTERING:</p> <p>Erbjuder molnleverantören möjligheten att skapa och använda policyer för att hantera lagrade data, livscykeln och nivåinställningarna?</p>
15.	<p>OBJEKTLAGRING – PLATS- OCH TIDSBASERADE POLICYER:</p> <p>Erbjuder molnleverantören användare möjligheten att skapa policyer som kan begränsa åtkomsten till data baserat på var och när användaren begär åtkomsten?</p>
16.	<p>OBJEKTLAGRING – WEBBPLATSVÄRDSKAP:</p> <p>Stödjer molnleverantören att statiska webbplatser körs från objektlagringstjänsten?</p>
17.	<p>OBJEKTLAGRING – VILANDE KRYPTERING:</p> <p>Stödjer molnleverantören kryptering på serversidan (SSE) av vilande data, där molnleverantören hanterar krypteringsnycklarna?</p> <ul style="list-style-type: none"> • Vilken krypteringsalgoritm används i så fall?
18.	<p>OBJEKTLAGRING – KRYPTERING MED ANVÄNDARNYCKLAR:</p> <p>Erbjuder molnleverantören funktioner för kryptering på serversidan (SSE) med hjälp av krypteringsnycklar som kunden tillhandahåller?</p>
19.	<p>OBJEKTLAGRING – NYCKELHANTERAD TJÄNST:</p> <p>Stödjer molnleverantören kryptering från serversidan (SSE) genom att använda en nyckelhanteringstjänst som skapar krypteringsnycklar, definierar policyer som kontrollerar hur nycklar kan användas och granskar nyckelanvändningen för att bevisa att de används på rätt sätt?</p>
20.	<p>OBJEKTLAGRING – HUVUDNYCKEL PÅ KLIENTSIDAN:</p> <p>Erbjuder molnleverantören användare möjligheten att behålla kontrollen över krypteringsnycklarna och kryptera/dekryptera objekt på klientsidan?</p>
21.	<p>OBJEKTLAGRING – STARK KONSEKVENNS:</p> <p>Stödjer molnleverantören konsekvens för direkt synlighet för PUT-åtgärder för nya objekt?</p>
22.	<p>OBJEKTLAGRING – DATAPLATS:</p> <p>Erbjuder molnleverantören en stark regional isolering, så att objekt som lagras i en region aldrig lämnar regionen såvida inte användaren uttryckligen överför dem till en annan region?</p>

Köpa molntjänster i offentlig sektor

23.	<p>OBJEKTLAGRING – REPLIKERING:</p> <p>Erbjuder molnleverantören en funktion för replikering i olika regioner, som automatiskt replikerar objekt mellan olika regioner som användaren väljer själv?</p>
24.	<p>OBJEKTLAGRING – VERSIONSHANTERING:</p> <p>Stödjer molnleverantören versionshantering, dvs. möjligheten att lagra och upprätthålla flera versioner av samma objekt?</p>
25.	<p>OBJEKTLAGRING – MÖJLIGHET ATT NEKA BORTTAGNING:</p> <p>Erbjuder molnleverantören en användare möjligheten att markera att ett objekt inte kan tas bort?</p>
26.	<p>OBJEKTLAGRING – MFA-BORTTAGNING:</p> <p>Stödjer molnleverantören MFA (multifaktorautentisering) för borttagningsåtgärder som ett extra säkerhetsalternativ?</p>
27.	<p>OBJEKTLAGRING – UPPLADDNING AV FLERA DELAR:</p> <p>Erbjuder molnleverantören möjligheten att ladda upp ett objekt som en uppsättning delar, där varje del är en sammanhängande del av objektets data och dessa objektindelar kan laddas upp oberoende av varandra och i valfri ordning?</p>
28.	<p>OBJEKTLAGRING – TAGGAR:</p> <p>Erbjuder molnleverantören möjligheten att skapa och koppla föränderliga, dynamiska taggar på objektnivå?</p>
29.	<p>OBJEKTLAGRING – AVISERINGAR:</p> <p>Erbjuder molnleverantören möjligheten att skicka aviseringar när vissa händelser inträffar på objektnivå (dvs. åtgärder som att lägga till/ta bort)?</p>
30.	<p>OBJEKTLAGRING – LOGGAR:</p> <p>Erbjuder molnleverantören möjligheten att generera revisionsloggar som innehåller detaljer om enskilda förfrågningar, till exempel vem som gjorde förfrågningen, när förfrågningen gjordes, begärd åtgärd, svarsstatus och felkod?</p>
31.	<p>OBJEKTLAGRING – INVENTERING AV OBJEKT:</p> <p>Erbjuder molnleverantören en funktion för objektinventering för att ge användare möjligheten att snabbt visualisera objekt och deras status, så att användare snabbt kan se vilka objekt som har offentlig åtkomst?</p>
32.	<p>OBJEKTLAGRING – INVENTERING AV METADATA:</p> <p>Erbjuder molnleverantören en funktion för objektinventering för att ge användare möjligheten att snabbt visualisera objektens metadata?</p>
33.	<p>OBJEKTLAGRING – OPTIMERING AV UPPLADDNINGAR:</p> <p>Erbjuder molnleverantören möjligheten att dirigera data från gränsheter till lagringstjänsten med hjälp av en optimerad nätverkssökväg?</p>
34.	<p>OBJEKTLAGRING – FRÅGEFUNKTION:</p> <p>Erbjuder molnleverantören användare möjligheten att köra frågor mot objektlagringstjänsten med hjälp av SQL-uttryck (Structured Query Language)?</p>
35.	<p>OBJEKTLAGRING – HÄMTNING AV DELMÄNGDER:</p>

Köpa molntjänster i offentlig sektor

	<i>Erbjuder molnleverantören användare möjligheten att hämta endast en delmängd av data från ett objekt med hjälp av enkla SQL-uttryck (Structured Query Language)?</i>
36.	FILLAGRINGSTJÄNST: <i>Erbjuder molnleverantören en enkel och skalbar fillagringstjänst som används med databehandlingsinstanser i molnet?</i>
37.	FILLAGRING – REDUNDANS: <i>Lagrar molnleverantören filsystemobjekten redundant (dvs. katalog, fil och länk) i flera datacenter eller anläggningar för att få högre tillgänglighet och varaktighet?</i>
38.	FILLAGRING – DATAELIMINERING: <i>Stödjer molnleverantören fullständig eliminering av fillagringsdata så att de inte längre är läsbara eller tillgängliga för obehöriga användare eller tredje part?</i>
39.	FILLAGRING – HÖG TILLGÄNGLIGHET: <i>Erbjuder molnleverantörens hanterade filsystem hög tillgänglighet?</i>
40.	FILLAGRING – NFS: <i>Stödjer molnleverantören NFS-protokoll (Network File System)?</i>
41.	FILLAGRING – SMB: <i>Stödjer molnleverantören SMB-protokoll (Server Message Block)?</i>
42.	FILLAGRING – VILANDE KRYPTERING: <i>Har molnleverantörens fillagringstjänst stöd för vilande kryptering?</i>
43.	FILLAGRING – KRYPTERING VID ÖVERFÖRING: <i>Har molnleverantörens fillagringstjänst stöd för kryptering av data vid överföring?</i>
44.	FILLAGRING – DATAMIGRERINGSVERKTYG: <i>Erbjuder molnleverantören något datamigreringsverktyg som gör att användare kan flytta data från lokala system till det molnbaserade filsystemet?</i>
45.	ARKIVLAGRINGSTJÄNST: <i>Erbjuder molnleverantören en lagringstjänst till mycket lågt pris som är avsedd för att arkivera objekt och filer som används sällan och nästan är oföränderliga?</i>
46.	ARKIVLAGRING – FELTOLERANS: <i>Erbjuder molnleverantörens arkitektur feltolerans i arkivlagringstjänsten?</i>
47.	ARKIVLAGRING – OFÖRÄNDERLIGHET: <i>Stödjer molnleverantören oföränderlighet av arkiverade objekt och filer?</i>
48.	ARKIVLAGRING – WORM: <i>Erbjuder molnleverantören en WORM-funktion (Write Once Read Many)?</i>
49.	ARKIVLAGRING – HÄMTNING AV DELMÄNGDER: <i>Erbjuder molnleverantören användare möjligheten att endast hämta en delmängd data från ett arkiverat objekt med hjälp av enkla SQL-uttryck (Structured Query Language)?</i>
50.	ARKIVLAGRING – SNABB HÄMTNING: <i>Erbjuder molnleverantören användare flera alternativ för datahämtningar med olika kostnader och hämtningstider?</i>

Köpa molntjänster i offentlig sektor

51.	ARKIVLAGRING – VILANDE KRYPTERING: <i>Har molnleverantörens arkivlagringstjänst stöd för vilande kryptering?</i>
52.	LAGRING – TJÄNSTENS BEGRÄNSNINGAR: <i>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller lagringsavsnittet ovan?</i> <i>Exempel:</i> <i>Maximal volymstorlek</i> <i>Maximalt antal enheter kopplade till en instans</i> <i>Maximal antal inmatnings-/utmatningsfunktioner per sekund (IOPS)</i> <i>Maximal objektstorlek</i> <i>Maximalt antal objekt per lagringskonto</i> <i>Maximalt antal ögonblicksbilder</i>

4. Administration

	Krav
1.	ADMINISTRATION – ANVÄNDARE OCH GRUPPER: <i>Erbjuder molnleverantören en tjänst för att skapa och hantera användare och grupper som använder infrastrukturen och resurserna?</i>
2.	ADMINISTRATION – ÅTERSTÄLLA LÖSENORD: <i>Erbjuder molnleverantören användare möjligheten att återställa sitt lösenord själva?</i>
3.	ADMINISTRATION – BEHÖRIGHETER: <i>Erbjuder molnleverantören möjligheten att lägga till behörigheter för användare och grupper på resursnivå?</i>
4.	ADMINISTRATION – TILLFÄLLIGA BEHÖRIGHETER: <i>Erbjuder molnleverantören möjligheten att skapa behörigheter som gäller under en viss tid?</i>
5.	ADMINISTRATION – TILLFÄLLIGA INLOGGNINGSUPPGIFTER: <i>Erbjuder molnleverantören användare möjligheten att skapa och ge betrodda användare tillfälliga säkerhetsinloggningsuppgifter som är konfigurerade att gälla från några minuter till flera timmar?</i>
6.	ADMINISTRATION – ÅTKOMSTKONTROLL: <i>Erbjuder molnleverantören detaljerade åtkomstkontroller till resurserna i infrastrukturen?</i> <ul style="list-style-type: none"><i>Vilka villkor kan i så fall användas av dessa kontroller (dvs. tid på dagen, ursprunglig IP-adress osv.)?</i>
7.	ADMINISTRATION – INBYGGDA POLICYER: <i>Innehåller molnleverantörens infrastruktur inbyggda policyer för åtkomstkontroll som kan kopplas till användare och grupper?</i>
8.	ADMINISTRATION – ANPASSADE POLICYER: <i>Erbjuder molnleverantörens infrastruktur möjligheten att skapa och anpassa policyer för åtkomstkontroll som kan kopplas till användare och grupper?</i>
9.	ADMINISTRATION – POLICYSIMULATOR: <i>Erbjuder molnleverantören en mekanism för att testa effekterna av policyer för åtkomstkontroll innan sådana policyer läggs till i produktionen?</i>

Köpa molntjänster i offentlig sektor

10.	<p>ADMINISTRATION – MOLN-MFA:</p> <p>Stödjer molnleverantören användningen av MFA (multifaktorautentisering) som ytterligare ett lager av åtkomstkontroll och autentisering i infrastrukturen?</p>
11.	<p>ADMINISTRATION – BEGRÄNSNINGAR FÖR TJÄNSTEN:</p> <p>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller administrationsavsnittet ovan?</p> <p>Exempel:</p> <p>Maximalt antal användare</p> <p>Maximalt antal grupper</p> <p>Maximalt antal hanterade policyer</p>

5. Säkerhet

	Krav
1.	<p>SÄKERHET – BAKGRUNDSKONTROLLER:</p> <p>Görs bakgrundskontroller på all personal hos molnleverantören som har tillgång till tjänstens infrastruktur (fysisk eller inte)?</p>
2.	<p>SÄKERHET – FYSISK ÅTKOMST:</p> <p>Begränsar molnleverantören de anställda från att komma åt tjänstens infrastruktur, såvida det inte föreligger ett särskilt problem, en ändringsbegäran eller någon liknande formell behörighet?</p>
3.	<p>SÄKERHET – ÅTKOMSTLOGGAR:</p> <p>Skapar molnleverantören loggar med de anställdas åtkomst till sin infrastruktur, där sådan åtkomst alltid loggas och loggarna lagras i minst 90 dagar?</p>
4.	<p>SÄKERHET – VÄRDINLOGGNINGAR:</p> <p>Begränsar molnleverantören de anställda från att logga in på databehandlingsvärdar och istället automatiserar alla uppgifter som utförs på en databehandlingsvärd där innehållet i dessa automatiserade jobb loggas och loggarna lagras i minst 90 dagar?</p>
5.	<p>SÄKERHET – KRYPTERINGSNYCKLAR:</p> <p>Erbjuder molnleverantören en tjänst för att skapa och kontrollera krypteringsnycklar som används för att kryptera användardata?</p>
6.	<p>SÄKERHET – HANTERING AV ÅTKOMSTNYCKLAR:</p> <p>Erbjuder molnleverantören möjligheten att identifiera när en åtkomstnyckel senast användes, rotera gamla nycklar och ta bort inaktiva användare?</p>
7.	<p>SÄKERHET – NYCKLAR FRÅN KUNDER:</p> <p>Erbjuder molnleverantören användare möjligheten att importera nycklar från den egna infrastrukturen för nyckelhantering till molntjänstleverantörens nyckelhanteringstjänst?</p>
8.	<p>SÄKERHET – INTEGRERING MED TJÄNSTER FÖR KRYPTERINGSNYCKLAR:</p> <p>Kan molnleverantörens nyckelhanteringstjänst integreras med andra molntjänster för att tillhandahålla en funktion för vilande datakryptering?</p>
9.	<p>SÄKERHET – HSM:</p> <p>Erbjuder molnleverantören särskilda fysiska säkerhetsmoduler (HSM), dvs. maskinvaruenheter som tillhandahåller säker nyckellagring och krypteringsåtgärder i en säkerhetsmodul som inte kan manipuleras?</p>

Köpa molntjänster i offentlig sektor

10.	<p>SÄKERHET – VARAKTIGHET FÖR KRYPTERINGSNYCKLAR:</p> <p>Stödjer molnleverantören varaktighet för nycklar, bland annat genom att lagra flera kopior så att nycklarna är tillgängliga när de behövs?</p>
11.	<p>SÄKERHET – SSO:</p> <p>Erbjuder molnleverantören en hanterad SSO-tjänst (Single Sign-On) som ger användare centralt hanterad åtkomst till flera konton och företagsprogram?</p>
12.	<p>SÄKERHET – CERTIFIKAT:</p> <p>Erbjuder molnleverantören en hanterad tjänst för att tillhandahålla, hantera och distribuera SSL- (Secure Sockets Layer)/TLS-certifikat (Transport Layer Security)?</p>
13.	<p>SÄKERHET – FÖRNYELSE AV CERTIFIKAT:</p> <p>Underlättar molnleverantörens certifikatshanteringstjänst förnyelse av certifikat?</p>
14.	<p>SÄKERHET – CERTIFIKAT MED JOKERTECKEN:</p> <p>Stödjer molnleverantörens certifikatshanteringstjänst användningen av certifikat med jokertecken?</p>
15.	<p>SÄKERHET – CERTIFIKATUTFÄRDARE:</p> <p>Fungerar molnleverantörens certifikatshanteringstjänst även som en certifikatutfärdare (CA)?</p>
16.	<p>SÄKERHET – ACTIVE DIRECTORY:</p> <p>Erbjuder molnleverantören en hanterad Microsoft AD-tjänst (Active Directory) i molnet?</p>
17.	<p>SÄKERHET – LOKAL ACTIVE DIRECTORY:</p> <p>Stödjer molnleverantörens hanterade Microsoft AD-tjänst (Active Directory) integrering med lokal Microsoft AD (Active Directory)?</p>
18.	<p>SÄKERHET – LDAP:</p> <p>Stödjer molnleverantörens hanterade Microsoft AD-tjänst (Active Directory) LDAP (Lightweight Directory Access Protocol)?</p>
19.	<p>SÄKERHET – ACTIVE DIRECTORY:</p> <p>Stödjer molnleverantörens hanterade Microsoft AD-tjänst (Active Directory) SAML (Security Assertion Markup Language)?</p>
20.	<p>SÄKERHET – HANTERING AV INLOGGNINGSUPPGIFTER:</p> <p>Erbjuder molnleverantören en hanterad tjänst som hjälper användare att enkelt rotera, hantera och hämta inloggningsuppgifter, till exempel API-nycklar (Application Programming Interface), inloggningsuppgifter till databaser och andra hemligheter?</p>
21.	<p>SÄKERHET – WAF:</p> <p>Erbjuder molnleverantören en brandvägg för webbprogram (WAF) som hjälper till att skydda webbprogram mot vanligt förekommande hot på webben som kan påverka tillgängligheten, äventyra säkerheten eller förbruka kostsamma resurser?</p>
22.	<p>SÄKERHET – DDOS:</p> <p>Erbjuder molnleverantören en tjänst som skyddar mot vanliga, mest förekommande DDoS-angrepp (Distributed Denial of Service) mot nätverks- och transportlager tillsammans med möjligheten att skriva anpassade regler för att minska avancerade angrepp mot programlager?</p>
23.	<p>SÄKERHET – SÄKERHETREKOMMENDATIONER:</p> <p>Erbjuder molnleverantören en tjänst för att automatiskt bedöma potentiella sårbarheter i program och resurser?</p>
24.	<p>SÄKERHET – UPPTÄCKT AV HOT:</p>

Köpa molntjänster i offentlig sektor

	<i>Erbjuder molnleverantören en hanterad tjänst för upptäckt av hot?</i>
25.	<p>SÄKERHET – BEGRÄNSNINGAR FÖR TJÄNSTEN:</p> <p><i>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller säkerhetsavsnittet ovan?</i></p> <p><i>Exempel:</i></p> <p><i>Maximalt antal kundhuvudnycklar</i></p> <p><i>Maximalt antal fysiska säkerhetsmoduler (HSM-enheter)</i></p>

6. Efterlevnad

Listan nedan är endast avsedd för illustrativa syften och bör inte betraktas som uttömmande för de certifieringar och standarder som kan gälla för molntjänster.

Ange hur många uppsättningar internationella och branschspecifika efterlevnadsstandarder som molnleverantören har uppfyllt:

Certifieringar/intyg	Lagar, förordningar och sekretess	Anpassningar/ramverk
<input type="checkbox"/> C5 [Tyskland]	<input type="checkbox"/> EU:s dataskyddsdirektiv	<input type="checkbox"/> CDSA
<input type="checkbox"/> CISPE:s uppförandekod för dataskydd	<input type="checkbox"/> EU:s modellklausuler	
<input type="checkbox"/> DIACAP	<input type="checkbox"/> FERPA	<input type="checkbox"/> CIS
<input type="checkbox"/> DoD SRG-nivå 2 och 4	<input type="checkbox"/> GDPR	<input type="checkbox"/> Informationstjänster om straffrätt (CIJS)
<input type="checkbox"/> FedRAMP	<input type="checkbox"/> GLBA	<input type="checkbox"/> CSA
<input type="checkbox"/> FIPS 140-2	<input type="checkbox"/> HIPAA	<input type="checkbox"/> EU-US Privacy Shield
<input type="checkbox"/> HDS (Frankrike, sjukvård)	<input type="checkbox"/> HITECH	<input type="checkbox"/> EU Safe Harbor
<input type="checkbox"/> ISO 9001	<input type="checkbox"/> IRS 1075	<input type="checkbox"/> FISC
<input type="checkbox"/> ISO 27001	<input type="checkbox"/> ITAR	<input type="checkbox"/> FISMA
<input type="checkbox"/> ISO 27017	<input type="checkbox"/> PDPA – 2010 [Malaysia]	<input type="checkbox"/> G-Cloud [Storbritannien]
<input type="checkbox"/> ISO 27018	<input type="checkbox"/> PDPA – 2012 [Singapore]	<input type="checkbox"/> GxP (FDA CFR 21 del 11)
<input type="checkbox"/> IRAP [Australien]	<input type="checkbox"/> PIPEDA [Kanada]	<input type="checkbox"/> ICREA
<input type="checkbox"/> MTCS nivå 3 [Singapore]	<input type="checkbox"/> Privacy Act [Australien]	<input type="checkbox"/> IT Grundschutz [Tyskland]
<input type="checkbox"/> PCI DSS nivå 1	<input type="checkbox"/> Privacy Act [Nya Zeeland]	<input type="checkbox"/> MARS – E
<input type="checkbox"/> SEC-regel 17-a-4(f)	<input type="checkbox"/> Spansk DPA-auktorisering	<input type="checkbox"/> MITA 3.0
<input type="checkbox"/> SOC1/ISAE 3402	<input type="checkbox"/> U.K. DPA - 1988	<input type="checkbox"/> MPAA

Köpa molntjänster i offentlig sektor

SOC2/SOC3

VPAT/avsnitt 508

NIST

Nivåer på Uptime Institute

Storbritanniens molnsäkerhetsprinciper

Genom att använda efterlevnadsrapporterna ovan kan organisationer i den offentliga sektorn utvärdera unika erbjudanden mot godkända standarder för säkerhet, efterlevnad och drift. Sådana rapporter kan visa att molntjänstleverantören, genom att uppfylla dem, uppfyller de kontroller för datacenterverksamhet som krävs för den offentliga molntjänstleverantören. Genom att kräva efterlevnad av sådana rapporter får enheter i den offentliga sektorn en garanti om att nedanstående kontroller genomförs.

- **Granskad åtkomst:** Molntjänstleverantören bör begränsa den fysisk åtkomsten till de personer som måste befinna sig på en plats av en motiverad affärsanledning. Om åtkomst tillåts bör den återkallas så snart det nödvändiga arbetet är utfört.
- **Kontrollerat och övervakat inträde:** Det bör vara en kontrollerad process att gå in i datacenterlagret. Molntjänstleverantören bör ha personalingångar med säkerhetsvakter och utse övervakare som övervakar vakter och besökare via säkerhetskameror. När godkända personer är på plats bör de få en bricka som kräver multifaktorautentisering och begränsar åtkomsten till områden godkända på förhand.
- **Arbetare på molntjänstleverantörens datacenter:** Molntjänstleverantörens anställda som regelbundet behöver åtkomst till ett datacenter bör få behörighet till relevanta områden i anläggningen baserat på arbetsfunktion. Åtkomsten bör granskas regelbundet. Personallistor bör granskas regelbundet av en ansvarig för områdesåtkomst för att säkerställa att varje anställds behörighet fortfarande är nödvändig. Anställda som inte har ett pågående affärsbehov av att vara på ett datacenter bör genomgå besöksprocessen.
- **Övervakning av obehörigt inträde:** Molntjänstleverantörer bör kontinuerligt övervaka obehörigt inträde på datacenteregendomar med hjälp av videoövervakning, intrångsdetektering och övervakningssystem med åtkomstloggar. Ingångar bör säkras med enheter som aktiverar ett ljudlarm om en dörr tvingas upp eller hålls öppen.
- **Global säkerhet för molntjänstleverantörens datacenter:** Molntjänstleverantörens bör ha säkerhetscenter i olika delar av världen som ansvarar för att övervaka, prioritera och driva säkerhetsprogram för molntjänstleverantörens datacenter. De bör se över hanteringen av fysisk åtkomst och resultat från intrångsdetekteringen och samtidigt ge säkerhetsteam på lokala datacenter global support dygnet runt. De bör även utföra kontinuerliga övervakningsaktiviteter som att spåra åtkomstaktivitet, häva åtkomstbehörigheter och vara tillgängliga för att reagera på och analysera potentiella säkerhetsincidenter.
- **Åtkomstgranskning per lager:** Åtkomsten till infrastrukturlagret bör vara begränsad baserat på affärsbehov. Genom att använda en åtkomstgranskning per lager beviljas inte inträde till varje lager som standard. Åtkomst till ett särskilt lager bör endast beviljas om det finns ett specifikt behov av att komma åt det specifika lagret.
- **Underhåll av utrustning är en del av den regelbundna verksamheten:** Molntjänstleverantörens team bör köra diagnostiska tester på datorer, nätverk och reservutrustning för att säkerställa att de fungerar för tillfället och i en nödsituation. Rutinmässiga underhållskontroller på datacenterutrustning och -verktyg bör vara en del av den regelbundna verksamheten på molntjänstleverantörens datacenter.
- **Reservutrustning för nödsituationer:** Reserver för vatten, ström, telekommunikation och internetanslutning bör vara utformade med redundans så att molntjänstleverantören kan upprätthålla kontinuerliga åtgärder i en nödsituation. Elektriska kraftsystem bör vara fullständigt redundanta så att enheter med oavbruten strömförsörjning kan aktiveras för vissa funktioner om ett avbrott skulle inträffa, samtidigt som generatorer kan förse hela anläggningen med reservström. Människor och system bör övervaka och reglera temperaturen och fuktigheten för att förhindra överhettning, vilket i sin tur minskar risken för avbrott i tjänsterna.
- **Teknik och människor samarbetar för ökad säkerhet:** Det bör finnas obligatoriska processer för att få behörighet att gå in i datalagret. Detta inkluderar att behöriga personer granskar och godkänner en persons åtkomstansökan. Dessutom bör hot och elektroniska intrångsdetekteringssystem övervaka och automatiskt utlösa varningar om identifierade hot eller misstänkt aktivitet. Om till exempel en dörr hålls öppen eller tvingas upp utlöses ett larm. Molntjänstleverantören bör placera ut säkerhetskameror och lagra video i enlighet med juridiska krav och efterlevnadskrav.

Köpa molntjänster i offentlig sektor

- **Förhindra fysiska och tekniska intrång:** Åtkomstpunkter till serverrum bör skyddas med elektroniska styrenheter som kräver multifaktorautentisering. Molntjänstleverantören bör även vara beredd på att förhindra tekniska intrång. Molntjänstleverantörens servrar bör kunna varna anställda om det görs försök att ta bort data. I det osannolika fallet att ett intrång sker ska servern avaktiveras automatiskt.
- **Servrar och media får stor uppmärksamhet:** Molntjänstleverantören bör klassificera lagringsenheter som används till att lagra kunddata som kritiska med stor inverkan och behandla dem i enlighet med detta under hela livscykeln. Molntjänstleverantören bör ha stränga standarder för hur enheterna ska installeras, underhållas och till slut förstöras när de inte längre är användbara. När en lagringsenhet har nått slutet av sin livslängd ska molntjänstleverantören utränga media genom att använda tekniken som anges i NIST 800-88. Molntjänstleverantören fortsätter att kontrollera media som har lagrat kunddata tills de har utrangerats på ett säkert sätt.
- **Granskare från tredje part verifierar molntjänstleverantörens rutiner och system:** Molntjänstleverantören bör granskas av externa granskare för att undersöka datacenter på djupet och fastställa att molntjänstleverantören följer de upprättade regler som krävs för att erhålla säkerhetscertifikaten. Beroende på efterlevnadsprogrammet och dess krav kan externa granskare intervjua molntjänstleverantörens anställda om hur de hanterar och kasserar media. Granskare kan även titta på video från säkerhetskamerorna och observera ingångar och hallar i ett datacenter. De kan även undersöka utrustning, till exempel molntjänstleverantörens elektroniska åtkomstkontrollenheter och säkerhetskameror.
- **Förberedd för det oväntade:** Molntjänstleverantören bör proaktivt förbereda sig för potentiella miljöhot, till exempel naturkatastrofer och bränder. Två sätt som molntjänstleverantören kan skydda datacenter på är genom att installera automatiska sensorer och responsiv utrustning. Enheter som känner av vatten bör installeras för att varna anställda om problem medan automatiska pumpar arbetar med att avlägsna vätska och förhindra skador. På liknande sätt minskar automatisk brandavkänning och brandutrustning riskerna och kan meddela molntjänstleverantörens anställda och brandmän om eventuella problem.
- **Hög tillgänglighet via flera åtkomstzoner:** Molntjänstleverantören bör tillhandahålla flera åtkomstzoner för ökad feltolerans. Varje åtkomstzon bör bestå av ett eller flera datacenter, vara fysiskt åtskilda och ha redundansström och nätverk. Åtkomstzoner bör vara anslutna till varandra via snabba, privata fiberoptiska nätverk för att kunna hantera program som automatiskt skapar redundans mellan åtkomstzonerna utan avbrott.
- **Simulera avbrott och mäta svarstider:** Molntjänstleverantören bör ha en plan för kontinuerlig drift i form av en driftsprocessguide som beskriver hur avbrott som orsakas av naturkatastrofer kan undvikas och minskas, med detaljerade åtgärder som ska vidtas före, under och efter en händelse. För att minska risken och förbereda sig för det oväntade bör molntjänstleverantören testa planen för kontinuerlig drift regelbundet med övningar som simulerar olika situationer. Molntjänstleverantören bör dokumentera hur personalen och processerna fungerar och sedan gå igenom lärdomar och eventuella korrigeringar åtgärder som kan behövas för att förbättra responsen. Molntjänstleverantörens personal bör vara utbildad och redo att snabbt återhämta sig från avbrott med en metodisk återhämtningsprocess för att minska ytterligare driftstopp på grund av fel.
- **Hjälp med att uppfylla effektivitetsmål:** Förutom att hantera miljörisiker bör molntjänstleverantören även införa hållbarhetsöverväganden i datacentrets utformning. Molntjänstleverantören bör tillhandahålla detaljer om sitt åtagande för att använda förnybar energi i sina datacenter och tillhandahålla information om hur kunderna och de egna datacentren kan minska koldioxidutsläppen.
- **Välja plats:** Innan molntjänstleverantören väljer en plats bör denna göra en första miljömässig och geografisk bedömning. Platserna för datacenter bör väljas med omsorg för att minska miljörisiker, till exempel översvämning, extremt väder och seismisk aktivitet. Molntjänstleverantörens åtkomstzoner bör byggas oberoende och vara fysiskt åtskilda.
- **Redundans:** Datacenter bör utformas för att förebygga och tolerera fel samtidigt som de bibehåller servicenivåerna. Om ett fel inträffar bör automatiska processer flytta trafiken från det berörda området. Viktiga program bör distribueras i en N+1-standard, så att det finns tillräckligt med kapacitet för att lastbalansera trafik till de återstående platserna om ett datacenter skulle sluta att fungera.
- **Tillgänglighet:** Molntjänstleverantören bör identifiera kritiska systemkomponenter som krävs för att upprätthålla systemets tillgänglighet och få igång driften igen om ett avbrott inträffar. Kritiska systemkomponenter bör säkerhetskopieras till flera isolerade platser. Varje plats eller åtkomstzon bör vara utformad för att fungera oberoende med hög tillförlitlighet. Åtkomstzoner bör vara anslutna så att program automatiskt kan skapa redundans mellan åtkomstzonerna utan avbrott. Stor motståndskraft och servicetillgänglighet bör vara inbyggd i systemdesignen.

Köpa molntjänster i offentlig sektor

Datacenterdesignen med åtkomstzoner och datareplikering bör ge molntjänstleverantörens kunder extremt korta återställningstider och mål för återställningspunkter samt högsta möjliga servicetillgänglighet.

- **Kapacitetsplanering:** Molntjänstleverantören bör övervaka tjänstanvändningen kontinuerligt för att distribuera infrastruktur som stödjer åtaganden och krav på tillgänglighet. Molntjänstleverantören bör upprätthålla en modell för kapacitetsplanering som bedömer molntjänstleverantörens användning och krav på infrastrukturen minst en gång i månaden. Denna modell bör stödja planeringen av framtida krav och innefatta överväganden som informationsbehandling, telekommunikationer och lagring av revisionsloggar.

KONTINUERLIG DRIFT och HAVERIBEREDSKAP

- **Plan för kontinuerlig drift:** Molntjänstleverantörens plan för kontinuerlig drift bör beskriva åtgärder för att undvika och minska miljöavbrott. Den ska innehålla driftsdetaljer om åtgärder som ska vidtas före, under och efter en händelse. Planen för kontinuerlig drift bör testas i form av bland annat simuleringar av olika situationer. Under och efter testningen bör molntjänstleverantören dokumentera personalens och processernas prestationer, korrigerande åtgärder och lärdomar med syftet att ständigt förbättra dem.
- **Pandemirespons:** Molntjänstleverantören bör införa policyer och rutiner för pandemirespons i haveriberedskapsplaneringen för att snabbt kunna reagera på hot om smittsamma sjukdomar. Strategier för att minska riskerna omfattar alternativa personalmodeller för att överföra kritiska processer till resurser utanför regionen och aktivering av en krishanteringsplan som stödjer viktig affärsverksamhet. Pandemiplaner bör hänvisa till internationella hälsovårdsmyndigheter och -föreskrifter, bland annat kontaktpunkter för internationella myndigheter.

ÖVERVAKNING och LOGGNING

- **Granskning av åtkomst till datacenter:** Åtkomsten till datacenter bör granskas regelbundet. Åtkomst ska återkallas automatiskt när en anställd bortförs från molntjänstleverantörens HR-system. När en anställds eller leverantörs åtkomst upphör i enlighet med varaktigheten för den godkända förfrågningsen ska denna åtkomst återkallas, även om personen fortfarande är anställd hos molntjänstleverantören.
- **Loggar över åtkomst till datacenter:** Fysisk åtkomst till molntjänstleverantörens datacenter bör loggas, övervakas och lagras. Molntjänstleverantören bör korrelera information som hämtas från logiska och fysiska övervakningssystem för att öka säkerheten i mån av behov.
- **Övervakning av åtkomst till datacenter:** Molntjänstleverantören bör övervaka datacenter med hjälp av globala säkerhetscenter som ansvarar för att övervaka, prioritera och driva säkerhetsprogram. De bör tillhandahålla global support dygnet runt och övervaka åtkomstaktiviteter på datacentret, utrusta lokala team och andra supportteam så att de kan reagera på säkerhetsincidenter genom att prioritera, konsultera, analysera och skicka respons.

ÖVERVAKNING och DETEKTERING

- **CCTV:** Fysiska åtkomstpunkter till serverrum bör filmas av CCTV-kameror (Closed Circuit Television Camera). Bildmaterialet ska lagras i enlighet med juridiska krav och efterlevnadskrav.
- **Ingångar till datacenter:** Fysisk åtkomst bör kontrolleras vid byggnadens ingångar av professionell säkerhetspersonal med hjälp av övervakning, detekteringssystem och andra elektroniska medel. Behörig personal bör använda mekanismer för multifaktorautentisering för åtkomst till datacenter. Ingångar till serverrum bör säkras med enheter som aktiverar ett ljudlarm för att inleda incidentrespons om en dörr tvingas upp eller hålls öppen.
- **Intrångsdetektering:** Elektroniska intrångsdetekteringssystem bör installeras i datalagret för att övervaka, upptäcka och automatiskt varna rätt personal om säkerhetsincidenter. Ingångar och utgångar till serverrum bör säkras med enheter som kräver att varje person uppvisar multifaktorautentisering innan inträde eller utträde beviljas. Dessa enheter aktiverar ett ljudlarm om dörren tvingas upp utan autentisering eller hålls öppen. Dörrlarmenheter bör även konfigureras att upptäcka instanser där en person lämnar eller går in i ett datalager utan att uppvisa multifaktorautentisering. Larm bör omedelbart skickas till molntjänstleverantörens säkerhetscenter som arbetar dygnet runt för att omedelbart logga, analysera och svara.

ENHETSHANTERING

Köpa molntjänster i offentlig sektor

- **Hantering av tillgångar:** Molntjänstleverantörens tillgångar bör hanteras centralt via ett inventeringshanteringssystem som lagrar och spårar ägare, plats, status, underhåll och beskrivande information om molntjänstleverantörens tillgångar. Efter upphandling ska tillgångar skannas och spåras, och tillgångar som underhålls ska kontrolleras och övervakas för ägarskap, status och lösning.
- **Destruktion av media:** Molntjänstleverantören bör klassificera mediagringenheter som används för att lagra kunddata som kritiska med stor inverkan och behandla dem därefter under hela deras livscykel. Molntjänstleverantören bör ha stränga standarder för hur enheterna ska installeras, underhållas och till slut förstöras när de inte längre är användbara. När en lagringseenhet har nått slutet av sin livslängd ska molntjänstleverantören utränga media genom att använda tekniken som anges i NIST 800-88. Molntjänstleverantören ska fortsätta att kontrollera media som har lagrat kunddata tills de har utrangerats på ett säkert sätt.

SYSTEM FÖR OPERATIVT STÖD

- **Ström:** Molntjänstleverantörens elektriska kraftsystem i datacentren bör vara fullständigt redundanta och kunna upprätthållas utan att driften påverkas, dygnet runt. Molntjänstleverantören bör säkerställa att datacentren är utrustade med reservströmförsörjning som ser till att det finns ström för att upprätthålla driften om ett elektriskt fel skulle inträffa och påverka kritiska och nödvändiga belastningar i anläggningen.
- **Klimat och temperatur:** Molntjänstleverantörens datacenter bör använda mekanismer för att kontrollera klimatet och hålla en lämpligt driftstemperatur för servrar och annan maskinvara för att förhindra överhettning och minska risken för serviceavbrott. Personal och system bör övervaka och reglera temperaturen och fuktigheten till lämpliga nivåer.
- **Brandavkänning och -bekämpning:** Molntjänstleverantörens datacenter bör vara utrustade med automatisk brandavkänning och brandutrustning. Brandavkänningssystem bör använda rökavkänningssensorer i nätverks- och infrastrukturutrymmen samt mekaniska utrymmen. Dessa områden bör dessutom skyddas med brandbekämpningssystem.
- **Läckagedetektering:** För att upptäcka vattenläckor bör molntjänstleverantören utrusta datacentren med funktioner för att upptäcka vatten. Om vatten upptäcks bör det finnas mekanismer som tar bort vattnet för att förhindra eventuella vattenskadorna.

UNDERHÅLL AV INFRASTRUKTUR

- **Underhåll av utrustning:** Molntjänstleverantören bör övervaka och utföra förebyggande underhåll på elektrisk och mekanisk utrustning för att upprätthålla systemens kontinuerliga drift på molntjänstleverantörens datacenter. Rutiner för underhåll av utrustning bör utföras av behöriga personer och i enlighet med ett dokumenterat underhållsschema.
- **Miljöhantering:** Molntjänstleverantören bör övervaka elektriska och mekaniska system och utrustning för att omedelbart kunna identifiera problem. Detta bör utföras med kontinuerliga revisionsverktyg och information från molntjänstleverantörens fastighetsförvaltningssystem och elektriska övervakningssystem. Förebyggande underhåll bör utföras för att upprätthålla utrustningens fortsatta funktion.

STYRNING OCH RISK

- **Pågående riskhantering på datacenter:** Molntjänstleverantörens säkerhetscenter bör utföra regelbundna hot- och sårbarhetsgranskningar av datacentren. Pågående bedömningar och minskade risker för potentiella sårbarheter bör utföras i form av riskbedömningsaktiviteter på datacentret. Denna bedömning bör utföras utöver riskbedömningsprocessen på företagsnivå som används för att identifiera och hantera risker för hela företaget. Denna process bör även ta hänsyn till regionala regler och miljörisker.
- **Säkerhetsintyg från tredje part:** Tredjepartstestning av molntjänstleverantörens datacenter, som dokumenterats i tredjeparttrapporterna, bör säkerställa att molntjänstleverantören har implementerat lämpliga säkerhetsåtgärder i enlighet med upprättade regler som krävs för att erhålla säkerhetscertifikat. Beroende på efterlevnadsprogram och dess krav kan externa granskare utföra tester på kassering av media, granska videor från säkerhetskameror, observera ingångar och hallar i ett datacenter, testa elektroniska åtkomstkontrollenheter och undersöka datacentrets utrustning.

Köpa molntjänster i offentlig sektor

7. Migreringar

	Krav
1.	<p>MIGRERINGSTJÄNST:</p> <p>Hur många olika tjänster för datamigrering erbjuder molnleverantören?</p>
2.	<p>MIGRERINGAR – CENTRALISERAD ÖVERVAKNING:</p> <p>Erbjuder molnleverantören organisationer en centraliserad (dvs. en översikt) tjänst som de kan använda för att spåra och övervaka statusen för migrering av servrar och program?</p>
3.	<p>MIGRERINGAR – INSTRUMENTPANEL:</p> <p>Erbjuder molnleverantörens migreringsverktyg en instrumentpanel som snabbt visualiserar migreringsstatus, relaterade mätvärden och migreringshistorik?</p>
4.	<p>MIGRERINGAR – VERKTYG FRÅN MOLNLEVERANTÖREN:</p> <p>Erbjuder molnleverantörens migreringsverktyg integration med andra migreringsverktyg från molnleverantören som kan utföra migrering av servrar och program?</p>
5.	<p>MIGRERINGAR – VERKTYG FRÅN TREDJE PART:</p> <p>Erbjuder molnleverantörens migreringsverktyg möjligheten att införa migreringsverktyg från tredje part?</p> <ul style="list-style-type: none"> • Vilka migreringsverktyg från tredje part stöds i så fall?
6.	<p>MIGRERINGAR – MIGRERINGAR I FLERA REGIONER:</p> <p>Erbjuder molnleverantörens migreringsverktyg möjligheten att spåra och övervaka migrering av servrar och program som sker i andra regioner?</p>
7.	<p>MIGRERINGAR – SERVERMIGRERING:</p> <p>Erbjuder molnleverantörens migreringsverktyg ett sätt att migrera lokala, virtualiserade servrar till molnet?</p> <ul style="list-style-type: none"> • Vilka virtualiserade miljöer stöds för tillfället i så fall?
8.	<p>MIGRERINGAR – SERVERUPPTÄCKT:</p> <p>Erbjuder molnleverantörens migreringsverktyg möjligheten att automatiskt hitta lokala, virtuella servrar som ska migreras till molnet?</p>
9.	<p>MIGRERINGAR – DATA FÖR SERVERPRESTANDA:</p> <p>Erbjuder molnleverantörens migreringsverktyg möjligheten att samla in och visa servrars eller virtuella maskiners prestanda som CPU- (processor) eller RAM-användning (Random Access Memory)?</p>
10.	<p>MIGRERINGAR – DATABAS MED UPPTÄCKTER:</p> <p>Kan molnleverantörens migreringsverktyg lagra alla insamlade data i en centraliserad databas?</p> <ul style="list-style-type: none"> • Kan organisationer exportera dessa data i så fall? Till vilka format?
11.	<p>MIGRERINGAR – VILANDE KRYPTERING:</p> <p>Krypterar molnleverantören all vilande information och lagrar den i databasen med upptäckter?</p>
12.	<p>MIGRERINGAR – INKREMENTELL SERVERREPLIKERING:</p> <p>Erbjuder molnleverantörens migreringsverktyg automatiserad, inkrementell serverreplikering i realtid vid servermigrering eller migrering av virtuella datorer som ett sätt att se till att alla ändringar som görs på servern eller i den virtuella datorn ingår i den slutliga migrerade avbildningen?</p> <ul style="list-style-type: none"> • Hur länge kan denna tjänst köras i så fall?
13.	<p>MIGRERINGAR – VMWARE:</p>

Köpa molntjänster i offentlig sektor

	<i>Stödjer molnleverantörens migreringsverktyg migreringar av VMWare virtuella maskiner från lokala platser till molnet?</i>
14.	MIGRERINGAR – HYPER-V: <i>Stödjer molnleverantörens migreringsverktyg migreringar av Hyper-V virtuella maskiner från lokala platser till molnet?</i>
15.	MIGRERINGAR – PROGRAMUPPTÄCKT: <i>Kan molnleverantörens migreringsverktyg upptäcka och gruppera program innan de migreras?</i>
16.	MIGRERINGAR – BEROENDEMAPPNING: <i>Kan molnleverantörens migreringsverktyg upptäcka beroenden mellan servrar och program innan de migreras?</i>
17.	MIGRERINGAR – MIGRERING AV DATABAS: <i>Kan molnleverantörens migreringsverktyg migrera lokala databaser till molnet?</i>
18.	MIGRERINGAR – DRIFTSTOPP VID MIGRERING AV DATABAS: <i>Kan molnleverantörens migreringsverktyg utföra en databasmigrering till molnet med minsta möjliga driftstopp, dvs. att källdatabasen är fullt fungerande under migreringen?</i>
19.	MIGRERINGAR – KÄLLDATABAS: <i>Stödjer molnleverantörens migreringsverktyg olika databaskällor som Oracle, SQL Server osv.?</i> <ul style="list-style-type: none">• <i>Ange alla källdatabaser som kan migreras till molnet i så fall.</i>
20.	MIGRERINGAR – HETEROGENA MIGRERINGAR: <i>Kan molnleverantörens migreringsverktyg utföra migreringar av heterogena databaser, dvs. från en källdatabas till en annan måldatabas, till exempel från Oracle till SQL Server?</i> <ul style="list-style-type: none">• <i>Ange alla möjliga kombinationer för heterogen databasmigrering i så fall.</i>
21.	MIGRERINGAR – DATAMIGRERING I PETABYTESKALA: <i>Erbjuder molnleverantören en datatransportlösning i petabyteskala som med säkra redskap överför stora mängder data till och från molnet?</i>
22.	MIGRERINGAR – DATAMIGRERING I EXABYTESKALA: <i>Erbjuder molnleverantören en datatransportlösning i exabyteskala för att flytta extremt stora mängder data till molnet?</i>
23.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG: <i>Erbjuder molnleverantören en tjänst för att smidigt integrera en kunds datacenter med molnlagringstjänster som accepterar överföring och lagring av data i molnleverantörens lagringstjänst?</i>
24.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – OBJEKTLAGRING: <i>Erbjuder molnleverantörens säkerhetskopieringstjänst för företag integrering med leverantörens tjänst för objektlagring i molnet?</i>
25.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – FILÅTKOMST: <i>Erbjuder molnleverantörens säkerhetskopieringstjänst för företag användare möjligheten att lagra och hämta objekt med hjälp av filprotokoll som NFS (Network File System)?</i>
26.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – BLOCKÅTKOMST: <i>Erbjuder molnleverantörens säkerhetskopieringstjänst för företag användare möjligheten att lagra och hämta objekt med hjälp av blockprotokoll som iSCSI (Internet Small Computer Systems Interface)?</i>
27.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – BANDÅTKOMST:

Köpa molntjänster i offentlig sektor

	<i>Erbjuder molnleverantörens säkerhetskopieringstjänst för företag användare möjligheten att säkerhetskopiera sina data via ett virtuellt bandbibliotek och lagra dessa bandkopior i leverantörens moln?</i>
28.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – KRYPTERING: <i>Erbjuder molnleverantörens säkerhetskopieringstjänst möjligheten att kryptera vilande data och data vid överföring?</i>
29.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – INTEGRERING AV PROGRAMVARA FRÅN TREDJE PART: <i>Kan molnleverantörens säkerhetskopieringstjänst för företag integreras med vanlig säkerhetskopieringsprogramvara från tredje part?</i>
30.	MIGRERINGAR – BEGRÄNSNINGAR FÖR TJÄNSTEN: <i>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller migreringsavsnittet ovan?</i> <i>Exempel:</i> <i>Maximalt antal simultana migreringar av virtuella datorer</i> <i>Maximalt antal datatransportlösningar som kan beställas</i>

8. Fakturering

	Krav
1.	FAKTURERING – SPÅRNING OCH RAPPORTERING: <i>Erbjuder molnleverantören en fakturerings tjänst med spårning och rapportering för att hjälpa användare att hantera och övervaka sin användning av molnerbjudanden?</i>
2.	FAKTURERING – LARM OCH AVISERINGAR: <i>Erbjuder molnleverantören en mekanism för att ställa larm med aviseringar för att varna användare när deras utgifter har överskridit ett specifikt tröskelvärde?</i>
3.	FAKTURERING – KOSTNADSSTYRNING: <i>Erbjuder molnleverantören en mekanism för att skapa och visa diagram som sammanfattat kostnader och utgifter?</i>
4.	FAKTURERING – BUDGETAR: <i>Erbjuder molnleverantören en mekanism för att visa och hantera budgetar och prognostisera uppskattade kostnader?</i>
5.	FAKTURERING – SAMMANSTÄLLD ÖVERSIKT: <i>Erbjuder molnleverantören en mekanism för att sammanställa fakturering från flera konton under ett primärt betalningskonto?</i>
6.	FAKTURERING – BEGRÄNSNINGAR FÖR TJÄNSTEN: <i>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller faktureringsavsnittet ovan?</i> <i>Exempel:</i> <i>Maximalt antal konton som kan grupperas tillsammans</i> <i>Maximalt antal larm som kan skapas</i> <i>Maximalt antal budgetar som kan hanteras</i>

9. Hantering

	Krav

Köpa molntjänster i offentlig sektor

1.	<p>HANTERING – ÖVERVAKNINGSTJÄNST:</p> <p>Erbjuder molnleverantören en övervakningstjänst för att hantera molnresurser och -program som samlar in, övervakar och rapporterar med hjälp av fördefinierade mätvärden?</p>
2.	<p>HANTERING – LARM:</p> <p>Erbjuder molnleverantörens övervakningstjänst användare möjligheten att ställa in larm?</p>
3.	<p>HANTERING – ANPASSADE MÄTVÄRDEN:</p> <p>Erbjuder molnleverantörens övervakningstjänst användare möjligheten att skapa och övervaka anpassade mätvärden?</p>
4.	<p>HANTERING – ÖVERVAKNINGSUPPLÖSNING:</p> <p>Erbjuder molnleverantörens övervakningstjänst flera nivåer av övervakningsupplösning, ned till minutnivå?</p>
5.	<p>HANTERING – TJÄNST FÖR API-SPÅRNING:</p> <p>Erbjuder molnleverantören en tjänst som loggar, övervakar och lagrar aktivitet mot molnresurser på både konsolen och på API-nivå (Application Programming Interface) för ökad synlighet?</p> <ul style="list-style-type: none"> • Vilka av molnleverantörens tjänster kan integreras med denna spårningstjänst i så fall?
6.	<p>HANTERING – AVISERING:</p> <p>Erbjuder molnleverantören möjligheten att skicka ut aviseringar baserade på API-aktivitet (Application Programming Interface)?</p>
7.	<p>HANTERING – KOMPRIMERING:</p> <p>Erbjuder molnleverantören en mekanism för att komprimera loggar som genererats av API-spårningssystemet (Application Programming Interface) för att hjälpa användare att sänka lagringskostnader relaterade till denna tjänst?</p>
8.	<p>HANTERING – REGIONAGGREGERING:</p> <p>Erbjuder molnleverantören möjligheten att registrera API-aktivitet (Application Programming Interface) för konton i alla regioner och leverera denna information på ett samlat sätt för enkel användning?</p>
9.	<p>HANTERING – RESURSinVENTERING:</p> <p>Erbjuder molnleverantören en tjänst för att bedöma, granska och utvärdera konfigurationerna av resurser som distribuerats av en användare?</p>
10.	<p>HANTERING – KONFIGURATIONSÄNDRINGAR:</p> <p>Registrerar molnleverantören automatiskt konfigurationsändringar för resurser när de sker?</p>
11.	<p>HANTERING – KONFIGURATIONSISTORIK:</p> <p>Erbjuder molnleverantören möjligheten att undersöka resursers konfiguration vid tidigare tillfällen?</p>
12.	<p>HANTERING – KONFIGURATIONSREGLER:</p> <p>Erbjuder molnleverantören riktlinjer och rekommendationer för efterlevnad gällande etablering, konfigurering och kontinuerlig övervakning?</p>
13.	<p>HANTERING – RESURSMALLAR:</p> <p>Erbjuder molnleverantören användare möjligheten att skapa, tillhandahålla och hantera en samling resurser i en malliknande form?</p>
14.	<p>HANTERING – REPLIKERING AV RESURSMALLAR:</p> <p>Erbjuder molnleverantören möjligheten att snabbt replikera dessa resursmallar i olika regioner för att potentiellt använda dem i haveriberedskapssituationer (DR)?</p>
15.	<p>HANTERING – MALLDESIGNER:</p>

Köpa molntjänster i offentlig sektor

	<i>Erbjuder molnleverantören ett lättanvänt grafiskt verktyg med dra och släpp-funktion som skyndar på processen att skapa sådana resursmallar?</i>
16.	HANTERING – TJÄNSKATALOG: <i>Erbjuder molnleverantören en tjänst för att skapa och hantera en katalog med tjänster, dvs. servrar, virtuella datorer, programvara, databaser osv.?</i>
17.	HANTERING – KONSOLÅTKOMST: <i>Erbjuder molnleverantören ett webbaserat användargränssnitt för att underlätta hanteringen och övervakningen av molntjänster?</i>
18.	HANTERING – CLI-ÅTKOMST: <i>Erbjuder molnleverantören ett enhetligt verktyg för att hantera och konfigurera flera molntjänster från kommandoradsgränssnittet (CLI) och möjliggöra automatisk hantering av uppgifter med hjälp av skript?</i>
19.	HANTERING – MOBIL ÅTKOMST: <i>Erbjuder molnleverantören en smartphoneapp som gör att användare kan ansluta till molntjänsten och hantera sina resurser?</i> <ul style="list-style-type: none"> • Är denna app tillgänglig för både iOS och Android i så fall?
20.	HANTERING – BÄSTA PRAxis: <i>Har molnleverantören en tjänst som hjälper användare att jämföra sin molnanvändning med bästa praxis?</i>
21.	HANTERING – BEGRÄNSNINGAR FÖR TJÄNSTEN: <i>Har molnleverantören några begränsningar (dvs. gränser för tjänsten) vad gäller hanteringsavsnittet ovan?</i> <i>Exempel:</i> <i>Maximalt antal konfigurationsregler per konto</i> <i>Maximalt antal larm som kan skapas</i> <i>Maximalt antal loggar som kan lagras</i>

10. Support

	Krav
1.	SUPPORT – TJÄNST: <i>Erbjuder molnleverantören support när som helst, dygnet runt, alla dagar i veckan och alla dagar om året via telefon, chatt och e-post?</i>
2.	SUPPORT – SUPPORTNIVÅER: <i>Erbjuder molnleverantören olika supportnivåer?</i>
3.	SUPPORT – NIVÅTILLDELNING: <i>Erbjuder molnleverantören användare möjligheten att själva tilldela resurserna/tjänsterna som används till olika supportnivåer baserade på detaljerad klassificering och inte genom att tvinga användare att ha separata molnkonton för att uppnå olika supportnivåer?</i>
4.	SUPPORT – FORUM: <i>Erbjuder molnleverantören olika offentliga supportforum där kunder kan diskutera sina problem?</i>
5.	SUPPORT – ÖVERSIKT ÖVER TJÄNSTENS TILLSTÅND:

Köpa molntjänster i offentlig sektor

	<i>Erbjuder molnleverantören en översikt över tjänstens tillstånd som visar uppdaterad information om tjänstens tillgänglighet i olika regioner?</i>
6.	SUPPORT – ANPASSAD INSTRUMENTPANEL: <i>Erbjuder molnleverantören en instrumentpanel som visar en anpassad översikt över tjänsternas prestanda och tillgänglighet för användarens specifika resurser?</i>
7.	SUPPORT – INSTRUMENTPANELSHISTORIK: <i>Erbjuder molnleverantören historik över tjänstetillståndsöversikten från ett år tillbaka?</i>
8.	SUPPORT – MOLNRÅDGIVARE: <i>Erbjuder molnleverantören en tjänst som fungerar som en anpassad molnexpert och hjälper till att jämföra resursernas användning med bästa praxis?</i>
9.	SUPPORT – TAM: <i>Erbjuder molnleverantören en chef för tekniska konton (TAM) som tillhandahåller teknisk expertis för alla molntjänster?</i>
10.	SUPPORT – PROGRAMSUPPORT FRÅN TREDJE PART: <i>Erbjuder molnleverantören support för vanliga operativsystem och vanliga programstackkomponenter?</i>
11.	SUPPORT – OFFENTLIGT API: <i>Erbjuder molnleverantören ett offentligt API (Application Programming Interface) för programmatisk hantering av supportärenden för att skapa, redigera och stänga sådana ärenden?</i>
12.	SUPPORT – DOKUMENTATION AV TJÄNSTEN: <i>Erbjuder molnleverantören offentlig teknisk dokumentation av bra kvalitet för alla tjänster, bland annat men inte begränsat till användarhandböcker, självstudier, vanliga frågor och versionsanteckningar?</i>
13.	SUPPORT – CLI-DOKUMENTATION: <i>Erbjuder molnleverantören offentlig teknisk dokumentation av bra kvalitet för sitt kommandoradsgränssnitt (CLI)?</i>
14.	SUPPORT – REFERENSARKITEKTURER: <i>Erbjuder molnleverantören en kostnadsfri samling av referensarkitekturdokument online för att hjälpa kunder att utforma specifika lösningar genom att kombinera flera av molnleverantörens molntjänster?</i>
15.	SUPPORT – REFERENSIMPLEMENTERINGAR: <i>Erbjuder molnleverantören en kostnadsfri samling dokument online som innehåller detaljerade, testade och validerade stegvisa procedurer, bland annat bästa praxis, för att implementera vanliga lösningar (dvs. DevOps, Big Data, datavaruhus, Microsoft-arbetsbelastningar, SAP-arbetsbelastningar osv.) i sina molnerbjudanden?</i>

Bilaga B - Demonstration

Att använda demonstrationer kan vara ett effektivt sätt för slutanvändare att testa molnerbjudanden och att vid tilldelningsbeslutet se vad som bäst passar organisationens affärsbehov. Nedan visas ett exempel på ett demonstrationstestskript för molnteknik.

1. *Demonstrera på ett översiktligt sätt molntjänstleverantörernas konsol och offentliga erbjudanden/resurser:*
 - *Lagringsfunktioner*
 - *Databehandlingsfunktioner*
 - *Databasfunktioner och -typer*
 - *Nätverk*
 - *Hanterings- och analysverktyg*
 - *Säkerhet*
 - *Andra funktioner*
2. *Beskriv hur du använder molntekniken som används i demonstrationen.*
3. *Visa hur du utför denna demonstration i realtid med hjälp av molnerbjudandet.*
4. *Konton:*
 - *Beskriv systemet med kontonycklar (rot och användare) som används i demonstrationen.*
 - *Visa hur du hanterar och skyddar dina kontonycklar*
5. *Visa hur du väljer den fysiska plats där dina arbetsbelastningar/data lagras.*
6. *Visa skalan för ditt erbjudande genom att ange lösningar för databehandling i stor skala och lagring.*
7. *Visa hur en slutanvändare begär olika tjänster ur molnerbjudandet. Visa följande:*
 - *Hur konton etableras*
 - *Hur säkerhetsbestämmelser aktiveras*
 - *Hur huvudkonton kan delas in i underkonton*
 - *Hur din IAM (Identity and Access Management) kan separera åtkomsten till olika resurser:*
 - *Hur du skyddar ett konto*
 - *Skapa användare och grupper*
 - *Lägg till en policy*
 - *Ställ in lösenord*
8. *Visa hur virtuella miljöer kan isoleras ur ett säkerhets- och nätverksperspektiv:*
 - *Skapa undernät*
 - *Internetdirigering*
9. *Visa hur du kan skapa en miljö på två eller flera skilda, isolerade platser.*
 - *Visa lastbalansering mellan miljöerna.*
10. *Visa möjligheten att använda flera metoder för att interagera med molntjänster (t.ex. API (Application Program Interface), webbkonsol, kommandorad).*
11. *Lagring:*
 - *Beskriv de olika lagringsalternativen*
 - *Visa typer av tillgänglig lagring (t.ex. block, objekt) och processer för datalivscyklar*
 - *Etablera en lagringsvolym och visa hur data laddas och hämtas*
 - *Skapa en lagringsvolym på X GB med och utan databehandlingsalternativ*
 - *Visa och validera behörigheter för att få åtkomst till dessa volymer.*
12. *Databehandling:*
 - *Beskriv databehandlingsalternativen – databehandlingsresursernas storlek och funktioner*
 - *Visa hur en databehandlingsresurs aktiveras och avaktiveras*
 - *Visa egenskaper (möjligheten att köra X instanser samtidigt, val av nätverk, skydd mot oavsiktligt avslutande, klientorganisationer osv.)*

Köpa molntjänster i offentlig sektor

- Visa ett databehandlingsalternativ med motsvarande X kärnor och X GB RAM
 - Visa belastningsbaserad skalning av resurser genom att köra en arbetsbelastning
 - Visa funktioner för automatisk skalning
 - Visa hur databehandlingen kan stoppas och återupptas senare
 - Visa hur ett databehandlingsalternativ kan bli större eller mindre med bibehållen konfiguration
 - Visa hur ett databehandlingsalternativ kan kopieras
 - Visa hur säkerhetsgrupper konfigureras
 - Beskriv vilka operativsystem som är tillgängliga i molntjänstleverantörens erbjudande
 - Visa ett exempel på en installation av Linux-operativsystem
 - Beskriv dina funktioner för att lägga till avbildningar i databehandlingserbjudanden
 - Vilka avbildningsformat stöds?
 - Visa hur du skulle läsa in och använda en avbildning
 - Visa serverlös databehandling
 - Visa möjligheten att köra ett kluster av databehandlingsinstanser med varierande priser baserade på en spotmarknad
13. Databas:
- Beskriv de databasfunktioner som erbjuds
 - Visa funktioner för MySQL, MS SQL Server, Oracle och Postgres
 - Visa funktioner för valfritt datalager
 - Visa funktioner för att säkerhetskopiera resurser
14. Nätverk: visa funktioner för programvarudefinierade nätverksalternativ och nätverkshantering
15. Hantering och analys
- Beskriv dina funktioner för molnhantering och -analys
 - Visa övervakningsalternativ
 - Visa dina funktioner för Hadoop-ramverk
16. Säkerhet: visa nätverkssäkerheten
- Beskriv tillgängliga säkerhetslösningar
 - Brandväggar
 - Säkerhetsgrupper
 - Gateway
 - Åtkomstkontrollistor för nätverk (NACL)
 - Systemloggar
 - Kryptering
 - Tillgängliga efterlevnadsackrediteringar
 - Nyckellagring
 - Andra funktioner
17. Tillhandahållande: visa hur du kan skapa en samling relaterade molnresurser och tillhandahålla dem på ett ordnat och förutsägbart sätt med hjälp av en mall som kan återanvändas
18. Programvara: visa dina funktioner för att ge åtkomst till och använda vanlig programvara
19. Visa hur du kan genomföra dataöverföring i stor skala
20. Visa faktureringsalternativ, bland annat:
- Sammanfattningsvy, detaljerad vy, vy enligt taggade resurser
 - Prognostiserade utgifter/användning baserade på aktuella utgifter/användning
21. Visa tillgängliga funktioner för support och rådgivning
- Vilka supportalternativ är tillgängliga?
 - Finns det funktioner för att kontrollera och ge rekommendationer kring användningen av tjänsten?

Köpa molntjänster i offentlig sektor

Visa eventuella andra funktioner i erbjudandet som du tror får erbjudandet att sticka ut från mängden.