



Köpa molntjänster i offentlig sektor

Handbok – Med exempel på formuleringar till
offertförfrågningar för ett ramavtal för molntjänster

Version 2: februari 2022

Observera

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.

Exempeldokument och exempel på 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.

Om CISPE

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

I vår växande organisation ingår företag som är verksamma i alla EU-länder och som har sina globala huvudkontor i 16 europeiska länder. Organisationen är öppen för företag som kan uppvisa att minst en av deras tjänster uppfyller kraven i CISPE:s Data Protection Code of Conduct. Vi:

- förespråkar om fördelarna med offentlig upphandlingspolitik som prioriterar molntjänster inom EU och dess medlemsstater
- samarbetar med molninfrastruktursektorn för att den ska uppnå klimatneutralitet senast 2030
- främjar enhetliga säkerhetskrav och tekniska standarder som omfattar hela EU
- stödjer omfattande integritetskrav med en uppförandekod för dataskydd
- arbetar för att hålla EU:s marknad för molninfrastruktur öppen, konkurrenskraftig och fri från inlåsningar
- 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 infrastrukturtjänster i molnet

CISPE:s Data Protection Code of Conduct distribuerades offentligt i september 2016, innan tillämpningen av EU:s allmänna dataskyddsförordning (GDPR). Den överensstämmer med de strikta kraven i dataskyddsförordningen för att hjälpa leverantörer av molninfrastruktur med att operationalisera efterlevnaden av förordningen och erbjuda ett starkt ramverk för att hjälpa kunderna med att välja molnleverantörer och kunna lita på deras tjänster. CISPE:s Code of Conduct har [validerats av Europeiska dataskyddsstyrelsen](#) (EDPB) i maj 2021 och [godkänts av den franska CNIL](#) juni 2021 i egenskap av behörig myndighet. <https://www.codeofconduct.cloud/>

Climate Neutral Data Centre Pact

CISPE samarbetade med Europeiska kommissionen i slutet av 2019 för att utveckla en uppsättning mätvärden och ett självregleringsinitiativ för att säkerställa datacentrens klimatneutralitet innan 2030. Detta initiativ har utvecklats tillsammans med European Data Centre Association (EUDCA) och andra branschorganisationer och aktörer på marknaden för datacenter. Det lanserades januari 2021 som ”Climate Neutral Data Centre Pact” <https://www.climateneutraldatacentre.net/>

Initiativet för rättvis programvara

Tillsammans med den franska CIO-föreningen CIGREF och med stöd av andra branschorganisationer för CIO:er och leverantörer över hela Europa har CISPE lanserat [Ten Principles of Fair Software Licensing for Cloud Customers](#), några principer för bästa praxis för företag som söker sig till molnet för tillväxt, innovation och flexibilitet och som utmanar sina mjukvaruleverantörer att se till att hänvisa till rättvisa licensvillkor. <https://www.fairsoftware.cloud/>

GAIA-X

CISPE var en av de tjugotvå grundande medlemmarna i GAIA-X – det europeiska initiativet för att skapa ett öppet, transparent och säkert digitalt ekosystem. CISPE har därför redan från början varit engagerad i GAIA-X-organisationens vision och principer. Generalsekreteraren från CISPE har blivit omvald juni 2021 att sitta i GAIA-X-styrelsen. Några av de verktyg som det hänvisas till i handboken, t.ex. [CISPE:s Data Protection Code of Conduct](#) och [SWIPO:s uppförandekod för IaaS](#), är användbara för att visa att GAIA-X-principerna följs. <https://www.gaia-x.eu>

CISPE och den offentliga sektorn

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

Även om offentliga upphandlingsmodeller bör vara avgörande för processen att införa och använda molntjänster skiljer sig upphandling av molntjänster från de flesta traditionella teknikupphandlingar 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 för att fokusera på molnet i första hand 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 stöd till offentliga myndigheter vid upphandling av molntjänster.

Mer information

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

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

Molntjänster som omfattas av CISPE:s Code of Conduct:

<https://www.codeofconduct.cloud/public-register/>

Innehållsförteckning

Observera	2
Om CISPE	3
Innehållsförteckning	5
Sammanfattning av och syfte med handboken	1
1.0 Översikt över ett ramavtal för molntjänster	4
2.0 Översikt över offertförfrågan för molntjänster	7
2.1 Upprätta offertförfrågningar för molntjänster	7
2.1.1 Inledning och strategiska mål	7
2.1.2 Tidslinje för svar på offertförfrågan	10
2.1.3 Definitioner	10
2.1.4 Detaljerad beskrivning av inköpsmodellen och konkurrens inom ramavtalet	11
2.1.5 Minimikrav för anbudsgivare – administration	15
2.2 Teknik	17
2.2.1 Minimikrav	18
2.2.2 Jämföra leverantörer	21
2.2.3 Upphandling	23
2.3 Säkerhet	24
2.3.1 Minimikrav	24
2.3.2 Jämföra leverantörer	30
2.3.3 Upphandling	30
2.4 Prissättning	31
2.4.1 Minimikrav	31
2.4.2 Jämföra leverantörer	33
2.5 Utformning av/villkor för avtalets fullgörande	35
2.5.1 Villkor	35
2.5.2 Villkor för programvara	38
2.5.3 Välja mellan utvalda leverantörer per projekt	39
2.5.4 Introduktion och utträde	40
3.0 Bästa praxis/lärdomar	40
3.1 Molnstyrning	40
3.2 Budgetera för molnet	41
3.3 Förstå affärsmodell med partner	43
3.4 Molnmäklare	43
3.5 Inköps-/marknadsundersökning inför offertförfrågan	43
3.6 Hållbarhet	44
Bilaga A – Tekniska krav för att jämföra olika anbudsgivare	45
1. Molnleverantörens profil	45
2. Global infrastruktur	45
3. Infrastruktur	46

3.1 Beräkningskapacitet.....	46
3.2 Nätverk	49
3.3 Lagring	53
4. Administration	57
5. Säkerhet.....	58
6. Lagefterlevnad	60
7. Migreringar.....	65
8. Fakturering	67
9. Hantering.....	68
10. Support	69
Bilaga B – Teknisk utvärdering i realtid.....	71
Plattform – exempel på en teknisk utvärdering i realtid	73
Arbetsbelastning: Webbapplikation – exempel på teknisk utvärdering i realtid.....	82

Sammanfattning av och syfte med handboken

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

Det här dokumentet är endast menat att ge information. 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 **förnyad konkurrensutsättning** vid inköp genom ett ramavtal för molntjänster. Avsnitten i handboken är ordnade för att efterlikna en allmän offertförfrågan för IT. Exempel på allmänna offertförfrågningar och formuleringar för urvalskriterier åtföljs av kommentarer som förklarar varför en offertförfrågan för molntjänster skiljer sig från en traditionell offertförfrågan för IT.

Efter offentliggörandet av EU-kommissionens molnstrategi som visar hur EU:s institutioner och organ ska modernisera sin IT-infrastruktur genom en strategi som fokuserar på molnet i första hand överlämnade CISPE handboken till EU-kommissionen juli 2019 under evenemanget *“How to transform governments through a smart cloud policy”*.



Version 2 av handboken innehåller ny vägledning kring dataskydd (avsnitt 2.3.1.1), byte av molnleverantör och dataportering (avsnitt 2.3.1.2), villkor för programvara (avsnitt 2.5.2), hållbarhet i molnet (avsnitt 3.6) och en uppdaterad bilaga B – Teknisk utvärdering i realtid.

***“Molntjänster”** syftar på all molnteknik och relaterade tjänster som en slutanvändare kan behöva ha åtkomst till. Det inbegriper konsulttjänster eller professionella/förvaltade tjänster för att stödja och genomföra en migrering till molnet och stödja arbetsbelastningar i molnet, utöver själva molninfrastrukturen, och molntjänster på marknadsplatser, till exempel program som tjänst (SaaS).*

Att molntjänster håller på att bli standardvalet för den offentliga sektorns IT skapar tillfälle att modernisera befintliga upphandlingsstrategier. Upphandlingar med fokus på molntjänster kan bidra till att enheter i den offentliga sektorn kan dra nytta av fördelarna med molnet, till exempel möjlighet att ligga i framkant med innovationen, ökad hastighet och flexibilitet, förbättrad säkerhet och lagefterlevnad. Samtidigt blir effektiviteten och kostnadsbesparingarna allt större.

Traditionella metoder för IT-upphandlingar för 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 försvinner fördelarna med molnet.

Ett av de bästa sätten att genomföra en effektiv offentlig upphandling av molntjänster är med ett **ramavtal för molnet** – en tilldelning av ett utbud av molntjänster till flera organisationer där berättigade köpare som är kopplade till den upphandlande organisationen kan införskaffa molnteknik och relaterade tjänster som uppfyller och passar deras behov. Om sådana ramavtal används som verktyg för avtalet går det att upphandla molntjänster på ett effektivt sätt. Det resulterar i att de köpande organisationerna och slutanvändarna 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, en stor mängd olika funktioner, nyskapande i snabb takt och förmågan att skala ut till nya geografiska platser.

Observera att **det här dokumentet fokuserar på inköp av molntekniker för infrastruktur som tjänst (IaaS) och plattform som tjänst (PaaS) som tillhandahålls av en molntjänstleverantör (CISP)**. Sådan molnteknik kan köpas direkt från en molntjänstleverantör eller genom en återförsäljare till en leverantör. *Ytterligare överväganden kring offertförfrågningar krävs för distributörer av molntjänster på marknadsplatser (PaaS och SaaS) och för konsulttjänster för molnet.*

Observera även att det här dokumentet inte omfattar varje aspekt av att skapa ett heltäckande ramverk för inköp av molntjänster. Det finns många andra dokument från branschen och analytiker som behandlar frågor som bästa praxis för inköp av molntjänster, 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 inköp av molntjänster. I **tabell 1** nedan beskriver handboken offertförfrågningar för molntjänster och var exempel på formuleringar för varje del av en offertförfrågan för molntjänster går att hitta.

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

Avsnitt	Översikt och exempel på formuleringar för offertförfrågningar
1.0 Översikt över ett ramavtal för molntjänster	En översikt över modellen för ett ramavtal för molntjänster (områden, tillvägagångssätt för att delta och avtal).
2.0 Översikt över offertförfrågan för molntjänster	Exempel på formuleringar för allmänna offertförfrågningar som omfattar avsnitten nedan, tillsammans med kommentarer som förklarar tanken bakom strukturen i offertförfrågningar för molntjänster och formuleringarna som används.
2.1 Upprätta offertförfrågningar för molntjänster	2.1.1 Inledning och strategiska mål 2.1.2 Tidslinje för svar på offertförfrågan 2.1.3 Definitioner 2.1.4 Detaljerad beskrivning av inköpsmodellen och konkurrens inom ramavtalet 2.1.5 Minimikrav för anbudsgivare – administration
2.2 Teknik	2.2.1 Minimikrav 2.2.2 Jämföra leverantörer 2.2.3 Upphandling

Avsnitt	Översikt och exempel på formuleringar för offertförfrågningar
2.3 Säkerhet	2.3.1 Minimikrav 2.3.1.1 Dataskydd 2.3.1.2 Byte av molnleverantör och dataportering 2.3.2 Jämföra leverantörer 2.3.3 Upphandling
2.4 Prissättning	2.4.1 Minimikrav 2.4.2 Jämföra leverantörer
2.5 Utformning av/villkor för avtalets fullgörande	2.5.1 Villkor 2.5.2 Villkor för programvara 2.5.3 Välja mellan utvalda leverantörer per projekt 2.5.4 Introduktion och utträde
3.0 Bästa praxis/lärdomar	3.1 Molnstyrning 3.2 Budgetera för molnet 3.3 Förstå affärsmodell med partner 3.4 Molnmäklare 3.5 Inköps-/marknadsundersökning inför offertförfrågan 3.6 Hållbarhet
Bilaga A – Tekniska krav för att jämföra olika anbudsgivare	En lista över allmänna krav på molntechniken för avrop eller förnyad konkurrensutsättning
Bilaga B – Teknisk utvärdering i realtid	Ett exempel på frågeställningar för produkter inom molntechnik som visar hur man kan göra bedömningar (molndemonstrationer som en del av avrop eller förnyad konkurrensutsättning)

1.0 Översikt över ett ramavtal för molntjänster

Ett väl utformat ramavtal för molntjänster kan öppna upp för 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 ramavtal för molnet är:

- **Samarbetsinriktat:**
 - Att flera organisationer samlas för att lägga beställningar med 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 för att helt genomföra migreringen till molnet och stödja arbetsbelastningar i molnet, utöver molnteknik från leverantörer och marknadsplatstjänster.
 - Sådan molnteknik kan köpas direkt från en molntjänstleverantör eller genom en utvald återförsäljare.
- **Avtalsstyrning:**
 - Det samlar organisationer/köpare kring en gemensam uppsättning villkor och kring ett och samma tilldelningsbeslut, i stället för att ha olika för varje organisation.
 - Fördelen för leverantörerna är att det bara finns en upphandlingsprocess, en uppsättning villkor och regler och ett beställningsförfarande att hantera, i stället för att varje organisation inom offentlig sektor har en egen upphandlingsprocess.
 - Det ger flexibilitet. För att skapa, godkänna och upprätthålla ett effektivt molnavtal inom befintliga statliga policyer/förordningar krävs experimentering och möjligheten till snabba justeringar. Det är mycket mer fördelaktigt att skapa ett ramavtal som gör att den offentliga sektorn och molnleverantörerna 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, upphandlingsorganisationerna och molnleverantörerna.
- **Val:**
 - Det ger köparen möjligheten att välja mellan flera kvalificerade leverantörer och sätter ribban högt för alla molntjänster och tillhörande tjänster, till exempel en marknadsplats för PaaS/SaaS och konsulttjänster för molnet.
 - Det ger kontroll över flera leverantörer i ett ramverk genom att säkerställa att varje utvald leverantörs standard granskas noga.

Ett ramavtal för att köpa molntjänster fungerar bäst när det omfattar kärnteknik för IaaS/PaaS från molntjänstleverantörerna, tillsammans med en marknadsplats för PaaS/SaaS och konsulttjänster som den 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 att upprätta ett ramavtal för molntjänster delas in i följande tre områden:

- **OMRÅDE 1 – MOLNTEKNIK**

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

- **OMRÅDE 2 – MARKNADSPLATS**

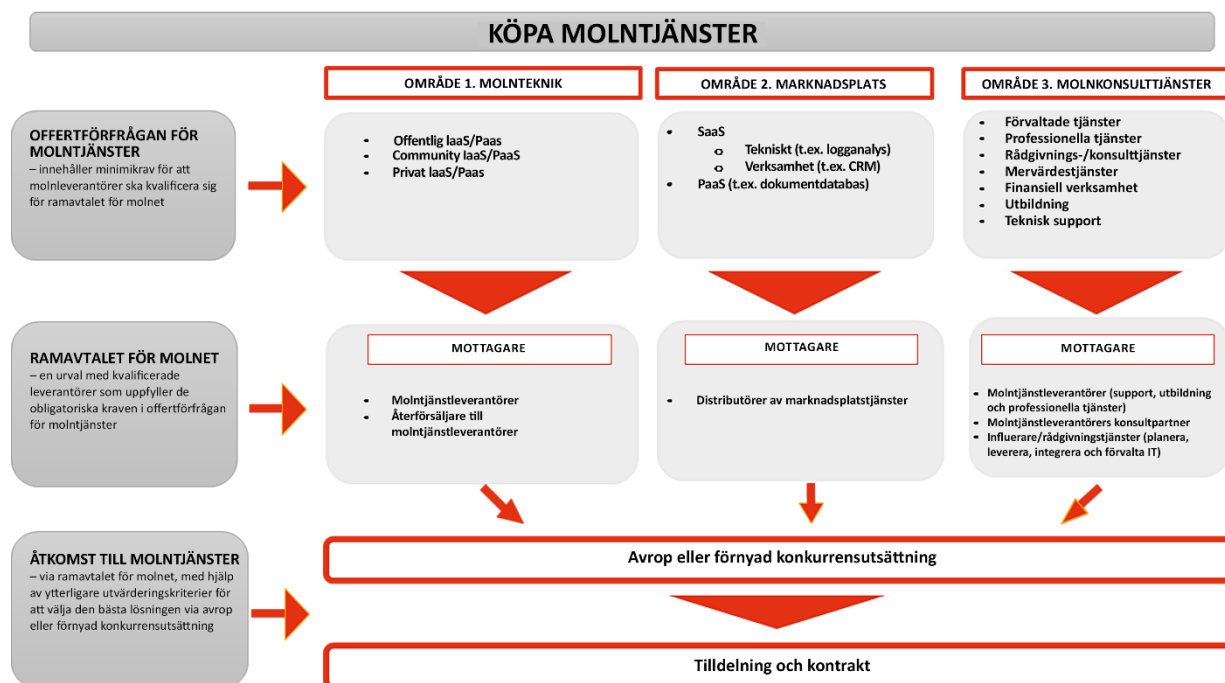
Åtkomst till en marknadsplats för PaaS- och SaaS-tjänster.

- **OMRÅDE 3 – KONSULTTJÄNSTER FÖR MOLNET**

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

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

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



Figur 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 ramavtalet för molntjänster.

Obs!

- Flera leverantörer kan väljas i varje område.
- OMRÅDE 3 kan tilldelas via en annan offertförfrågan eller möjligtvis via ett befintligt avtal för konsulttjänster.

Kategorier i OMRÅDE 1

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

Se avsnittet 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 förnyad konkurrensutsättning?

Krav på leverantören för en offertförfrågan för molntjänster bör omfatta viktiga delar och lägsta standarder. De bör inte inbegripa standarder som "kan vara bra att ha". Om ytterligare standarder utöver de grundläggande läggs till för att kvalificera leverantörer för ramverket kan det leda till att vissa leverantörer inte kan lämna anbud och köparna får färre deltagare att välja mellan.

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

Om det anses nödvändigt kan en förnyad konkurrensutsättning anordnas för att identifiera den bästa leverantören för en särskild arbetsbelastning eller ett särskilt projekt. En förnyad konkurrensutsättning innebär att en kund går vidare med upphandlingen enligt 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. Det är därför viktigt att använda sig av minimikrav för deltagare i en offertförfrågan för molntjänster eftersom det säkerställer alternativ med hög standard inom ett särskilt område.

*Observera att det är viktigt att avtalen har **olika uppsättningar villkor** för varje område enligt figur 1 ovan. Ett tillvägagångssätt där man använder samma lösning för upphandlingar i alla områden leder till problem med teknisk genomförbarhet och kompatibilitet.*

2.0 Översikt över offertförfrågan för molntjänster

Det här avsnittet beskriver offertförfrågningar för molntjänster samt deras modell och omfattning, bland annat: strategiska mål, deltagare, definitioner, tidslinje och minsta administrativa villkor. Vi vill åter igen uppmärksamma att den här handboken lägger fokus på **OMRÅDE 1 – MOLNTEKNIK**.

2.1 Upprätta offertförfrågningar för molntjänster

Vi rekommenderar starkt att organ i den offentliga sektorn är tydliga med sina övergripande mål och krav i inledningen till sin 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 en offertförfrågan för molntjänster förklara **(1)** de affärsmål och fördelar som organisationen vill uppnå genom att använda molnet; **(2)** ramavtalets struktur – vem köper, vem tar hand om driften, vem budgeterar osv.; **(3)** en tydlig förståelse för modellen för delat ansvar mellan den upphandlande myndigheten och molntjänstleverantörer, vilket är nyckeln till en framgångsrik upphandling och användning av molnet samt **(4)** den typ 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 så bra som möjligt. Dessutom säkerställer det att både kunderna och leverantörerna är på det klara med vad som ska levereras enligt offertförfrågan.

En offertförfrågan för moln skiljer sig avsiktligt från traditionella offertförfrågningar för IT. Molntechniken är inte en enkel 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 agera snabbt för att dra nytta av molnet.

Bland alla aspekter som vi nämner som bra praxis vid inköp av molntjänster 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 lågefterlevnad i molnet, men denna uppdelning av ansvarsområdena gäller alla delar av molntechniken. En offertförfrågan för molntjänster bör tydligt visa vad i en molnmiljö som är leverantörens ansvar och vad som förblir kundens ansvar. En molntjänstleverantör erbjuder till exempel funktioner för att övervaka resurser och program som körs i molnet, **men** det är kundens ansvar att faktiskt använda funktionerna som leverantören tillhandahåller, eftersom en leverantör som är verksam i stor skala inte är utformad för att göra detta åt miljontals kunder.

Dessutom bör molnkunder förstå hur leverantörens partnernätverk hjälper kunder att använda molnet och hantera sina ansvarsområden. En managed service provider (MSP) kan till exempel hjälpa en kund att konfigurera och använda övervakningsfunktioner från en molntjänstleverantör för att uppfylla deras unika krav på lågefterlevnad och granskningar.

Enkelt uttryckt är ansvarsområdena i molnmodellen följande:

¹ Se avsnitt 5 i CISPE:s Code of Conduct for Cloud Infrastructure Service Providers: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Leverantören tillhandahåller molntekniken

Kunden använder molntekniken

Konsultföretag (om det är relevant) hjälper en kund att få åtkomst till och använda molntekniken

”Konsultföretag” är företag med konsulttjänster och förvaltade/professionella tjänster som hjälper kunder att utforma, skapa, bygga, migrera och hantera deras arbetsbelastningar och program i molnet. Bland sådana företag finns bland annat systemintegratörer, strategiska konsulter, byråer, managed service providers och återförsäljare av mervärdestjänster.

Att ”handla” molntjänster kan jämföras med att handla i ett fysiskt byggvaruhus. I ett byggvaruhus finns det ett stort 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 byggvaruhuset ge dig välgrundade råd, men de följer inte med dig hem och bygger saker åt dig. Det här gör att du har några olika alternativ:

1. Köp material och verktyg själv och bygg på egen hand.
2. Köp material och verktyg själv och anlita någon att bygga och/eller driva något åt dig.
3. Anlita någon att bygga/driva något åt dig och låt dem införskaffa material och verktyg som en del av deras erbjudande.

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

Exempel på formuleringar 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 man bara betalar för det man använder. Organisationer kan etablera rätt typ och storlek på resurserna 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 krav på åtkomst till denna typ av kommersiellt tillgänglig molnteknik för att tillgodose företagets behov i ett brett spektrum av anknutna organisationer.

Huvudsyftet med den här offertförfrågan är att parallellt tilldela <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 leverantör för köp av molnteknik.
2. **OMRÅDE 2.** Leverantörer av marknadsplatstjänster.

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

I **OMRÅDE 1** måste organisationer som lämnar anbud (från molntjänstleverantörer eller återförsäljare) 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 senaste och mest innovativa tekniken på marknaden.
- **Kostnad** – Byta ut kapitalutgifter mot rörliga kostnader (t.ex. CapEx till OpEx). Att endast betala för de resurser som förbrukas.
- **Budget** – Visa fakturerings- och användningsinformation både på detaljnivå och översiktligt, visualisera mönster i utgifterna över tid och förutsäga framtida utgifter.
- **Elasticitet** – Få lägre rörliga kostnader från stordriftsfördelarna som molnet ger.
- **Kapacitet** – Slippa gissa när det gäller infrastrukturens kapacitetsbehov.
- **Sluta förlita sig på datacenter** – Kunna fokusera på våra medborgare snarare än på grovgörat med att hantera fysiska servrar.
- **Säkerhet** – Formalisera kontodesignen med bättre synlighet och granskningsmöjligheter av resurser och slipp kostnaden av att skydda anläggningar och fysisk maskinvara.
- **Delat ansvar** – Lätta på den operativa bördan då molntjänstleverantören driver, hanterar och styr komponenterna från värdoperativsystemet och virtualiseringslagret ned till den fysiska säkerheten i anläggningarna där tjänsterna drivs.
- **Automatisering** – Inbyggd automatisering i molnarkitekturen för att ge bättre möjligheter att bygga ut systemet säkrare, snabbare och mer kostnadseffektivt.
- **Molnstyrning** – (1) Ge en fullständig inventering av alla IT-tillgångar från första början, (2) hantera alla dessa tillgångar centralt och (3) skapa aviseringar gällande användning/fakturerings/säkerhet/osv. – allt med möjlighet till tillgångsspårning, lagerhantering, ändringshantering, hantering och analys av loggar 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.
- **Möjlighet till förändring** – Verktyg och tjänster för förflyttning 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 Data Protection Code of Conduct](#).
- **Transparens** – Kunder bör ha rätt att få veta var infrastrukturerna som används för att behandla och lagra deras data befinner sig (stadsområde).
- **Klimatneutralitet** – Kunder bör samarbeta med leverantörer som vidtar bevisade, specifika åtgärder för att uppfylla målen för klimatneutralitet innan 2030 och som har undertecknat Climate Neutral Data Centre Pact. Detta kommer att hjälpa kunderna att uppnå sina egna mål för klimatneutralitet.

2.1.2 Tidslinje för svar på offertförfrågan

Det är bra att förse anbudsgivarna med en tidslinje över förväntad anbudsaktivitet vid upprättandet av ett ramavtal för molntjänster och tillhörande offertförfrågan för molntjänster. Ju fler inom branschen som visar intresse 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 bör följa lokala lagar och juridiska skyldigheter. Listan nedan är avsedd att fungera som vägledning för bästa praxis snarare än att vara en normativ lista över aktiviteter och tidsramar.

Exempel på formuleringar för offertförfrågan: tidslinje för svar

Se tidslinjen för offertförfrågan för molntjänster nedan:

<i>Tidslinje för offertförfrågan för molntjänster</i>
<i>Begäran om information (RFI) offentliggörs:</i> <i>Svar på begäran om information:</i> <i>Utkast till offertförfrågan (RFP) offentliggörs:</i> <i>Deadline för utkast till svar på offertförfrågan:</i> <i>Fas för branschkonsultation: <tidslinjer></i> <i>Offertförfrågan för förhandsurvalet offentliggörs:</i> <i>Svar på förhandsurvalets offertförfrågan:</i> <i>Offertförfrågan offentliggörs:</i> <i>Deadline för första omgången frågor:</i> <i>Svar på första omgången frågor:</i> <i>Deadline för andra omgången frågor:</i> <i>Svar på andra omgången frågor:</i> <i>Deadline för svar på offertförfrågan:</i> <i>Period för förtydligande av offert:</i> <i>Förhandlingsperiod:</i> <i>Datum för offentliggörande av beslut om tilldelning:</i> <i>Kontraktstilldelning:</i> <i>Avtalets varaktighet (alternativ till förlängning):</i>

2.1.3 Definitioner

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

Exempel på formuleringar för offertförfrågningar: definitioner

Definitionerna nedan är tagna ur National Institute of Standards and Technology (NIST) Definition of Cloud Computing.²

- **Infrastruktur som tjänst (IaaS).** Funktionen som konsumenten får är att etablera resurser för bearbetning, lagring, nätverksanslutning och andra fundamentala databehandlingsresurser där kunden kan distribuera och köra valfri programvara. Det kan inkludera operativsystem och program. Konsumenten hanterar eller styr inte den underliggande molninfrastrukturen men har kontroll över operativsystem, lagring och distribuerade program. Hen har möjligtvis begränsad kontroll över utvalda nätverkskomponenter (som värdbaserade brandväggar).
- **Plattform som tjänst (PaaS).** Konsumenten får kapaciteten att implementera program som skapats eller förvärvats av konsumenten på molninfrastrukturen. Dessa program skapas med hjälp av programmeringsspråk, bibliotek, tjänster och verktyg som stöds av leverantören. Konsumenten hanterar eller kontrollerar inte den underliggande molninfrastrukturen, inklusive nätverk, servrar, operativsystem eller lagring, men har kontroll över de installerade programmen och eventuella konfigurationsinställningar för miljön.
- **Program som tjänst (SaaS).** Konsumenten får kapaciteten 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 programmets begränsade användarspecifika konfigurationsinställningar.
- **Offentligt moln.** Molninfrastrukturen är öppen för att användas av allmänheten. Den kan ägas, hanteras och drivas av ett företag, en akademisk organisation, en myndighetsorganisation, eller en kombination av dessa. Den finns hos molnleverantörens lokaler.
- **Communitymoln.** Molninfrastrukturen tillhandahålls för exklusiv användning av en specifik grupp konsumenter från organisationer som har gemensamma intressen (som aspekter av uppdrag, säkerhetskrav, policy och lagefterlevnad som måste övervägas). Den kan ägas, förvaltas och drivas av en eller flera av organisationerna i communityn, en tredje part eller en kombination av dessa och kan finnas både på plats och externt.
- **Hybridmoln.** Molninfrastrukturen är en kombination av två eller flera olika molninfrastrukturer (privat, community eller offentligt) som förblir unika enheter, men som binds samman av standardiserad eller egen teknik som gör det möjligt att flytta data och program (till exempel utökbara moln 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 på plats och externt.

2.1.4 Detaljerad beskrivning av inköpsmodellen och konkurrens inom ramavtalet

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

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

Vad gäller ramavtalets omfattning och de avrop och förnyade konkurrensutsättningar som följer det bör organisationer överväga följande:

- Vem ska ansvara för integrering och förvaltnade tjänster som inbegriper användningen av molntekniken under avtalet?
- Är det ett krav för en återförsäljare eller en partner till molntjänstleverantören att tillhandahålla mervärdestjänster utöver upprätthållandet av en avtalsmässig relation med leverantören och tillhandahålla tjänster för samlingsfakturerings och snabb direktåtkomst till användnings- och faktureringsdata relaterade till användningen av molnleverantörens tjänster?
- Behövs en återförsäljare av fullständiga mervärdestjänster, en systemintegratör eller en managed service provider eller någon annan typ av tjänster för IT-arbete?

Det är viktigt att notera att en molntjänstleverantör inte är en systemintegratör (SI) eller managed service provider (MSP). Många kunder i den offentliga sektorn behöver en molntjänstleverantör för sina IaaS/PaaS och överlåter konsulttjänster och praktisk planering, migrering och förvaltning till en systemintegratör eller leverantör av förvaltnade tjänster. Uppdelningen av rollerna och ansvarsområdena i molntjänstmodellen visas nedan i **figur 2**.



Figur 2 – En offertförfrågan för molntjänster ska förse slutanvändare med ett utbud av de molntjänster som de behöver. Kunder i den offentliga sektorn behöver en leverantör för molnteknik och eventuellt en marknadsplats för PaaS- och SaaS-produkter. Därefter kan kunderna bestämma hur stor del de vill ta av leveransen av molntjänster och hur mycket de har tänkt överlåta till något konsultföretag, någon systemintegratör, leverantör av förvaltnade tjänster, osv.

Exempelformuleringarna nedan är formade efter rollerna och ansvarsområdena som visas i figur 2 ovan. Ett ramavtal för molnet och tillhörande offertförfrågan för molntjänster ska säkerställa att köparna har möjlighet att på ett lämpligt sätt bedöma varje leverantörs erbjudande, så att de kan välja bland de tjänster som behövs för arbetsbelastningen eller 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 förnyad konkurrensutsättning utförs under ramavtalet.

Exempel på formuleringar för offertförfrågan: inköpsmodell

Detta avtal fungerar som ett **ramverk** för inköp. Detta ramavtal för molnet innehåller flera **områden**, som definieras av <ORGANISATION>, för molnteknik och relaterade tjänster/produkter från en marknadsplats, konsulttjänster, professionella tjänster/systemintegration/hanterade tjänster/migrering, professionella tjänster, utbildning och support som definieras av <ORGANISATION> och kan användas av flera berättigade anknutna 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 giltighetstid är högst <X> år, inklusive eventuella förnyelser. Den längsta giltighetstiden för ett ramavtal för avrop är normalt <X> månader. Det kan förlängas med <X> månader och sedan med ytterligare <X> månader, med rätt interna godkännanden som behövs för en sådan förlängning. Detta anges för varje specifikt **avrop**.

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

1. **OMRÅDE 1: MOLNTEKNIK** – det omfattande utbudet av molnleverantörens teknik (direkt från molntjänstleverantören, från återförsäljare eller från återförsäljare som erbjuder mervärdestjänster/support):
 - i. **IaaS- och PaaS-tjänster** – ett utbud av molnteknik som beräkningskapacitet, lagring, nätverk, databas, analys, programtjänster, distribution, förvaltning, utveckling, sakernas internet (IoT) osv. Innehåller paketerade molntekniklösningar som DR/COOP, Archive, stordata och analys, DevOps osv.
2. **OMRÅDE 2: MARKNADSPLOTS** – samtliga tjänster och produkter för PaaS/SaaS som redovisning, kundvårdssystem, design, HR, GIS och mappning, högpresterande databehandling, omvärldsbevakning, innehållshantering, logganalys osv.
3. **OMRÅDE 3: KONSULTTJÄNSTER FÖR MOLNET** – samtliga konsulttjänster (förvaltade tjänster, professionella tjänster, rådgivnings-/konsulttjänster, mervärdestjänster, FinOps, teknisk support) relaterade till migrering till och användning av molnet. Dessa tjänster kan omfatta planering, design, migrering, förvaltning, support, kvalitetssäkring, säkerhet, utbildning osv.

Leverantörer kan skicka sina erbjudanden inom flera områden.

Leverantörer kan skicka sina erbjudanden och relaterade priser i valfritt format.

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 behöver vid behov. Om ett avropsavtal läggs till under ramavtalet kan köpare finjustera sina krav med ytterligare funktionsspecifikationer för avrop och samtidigt behålla fördelarna med ramavtalet.

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

1. SKRIVA AVROPSKRAV OCH SÖKA INTERNT GODKÄNNANDE FÖR KÖP

Alla slutköpare som är berättigade att använda ramavtalet skapar gemensamma team med företagens slutanvändare, 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 när de utarbetar kraven:

- tillgängliga medel för att använda tjänsten
- projektets tekniska och upphandlingsrelaterade krav
- 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 fastställda 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 när det gäller både krav och budget. Varje tjänstebeskrivning innehåller följande:

- dokument med tjänstebeskrivning eller länkar till dessa beskrivningar
- dokument med villkor
- dokument med priser (länkar till offentliga priser accepteras under förutsättning att en prislista eller ett dokument med samtliga priser finns tillgängligt på begäran).

Priset är kostnaden för tjänstens vanligaste upplägg. Däremot baseras pris ofta på volym, så köpare bör alltid titta på dokumentet med leverantörens priser eller deras allmänna priser och verktyg för att räkna ut dem. På så sätt går det att ta reda på det faktiska priset för det som köps in och det övergripande värdet för köparen (till exempel tjänster för optimering och deras kostnadsminskningar).

Köpare under ramavtalet kan prata med leverantörer för att be dem att förklara sina tjänstebeskrivningar, villkor, priser eller dokument med och modeller för tjänstedefinitioner. En logg 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 angivna egenskaper som ska användas och hur de ska viktas.

Observera att köparen kan behöva:

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

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

FÖRNYAD KONKURENSUTSÄTTNING

Om det anses nödvändigt kan en förnyad konkurrensutsättning anordnas för att fastställa den bästa leverantören för en särskild arbetsbelastning eller ett särskilt projekt. En förnyad konkurrensutsättning innebär att en kund går vidare med upphandlingen enligt ramavtalet genom att bjuda in alla leverantörer inom ett område att svara på en uppsättning krav. Kunden bjuder in alla kapabla leverantörer inom området till att lämna anbud. Se ytterligare jämförelseinformation i avsnitten nedan angående teknik, säkerhet och pris/värde.

AVTAL

Både köparen och leverantören måste underteckna ett exemplar av avtalet innan tjänsten kan användas. Den längsta giltighetstiden för ett ramavtal är normalt <x> månader. Det kan förlängas med <x> månader och sedan med ytterligare <x> månader, med rätt interna godkännanden som behövs för en sådan förlängning.

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

2.1.5 Minimikrav för anbudsgivare – administration

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 lägger fram en traditionell lösning som ett "moln". Deltagare i offertförfrågan ska visa hur de uppfyller de lägsta administrativa kraven på anbudsgivare.

Observera återigen att det här dokumentet lägger fokus på **OMRÅDE 1 – MOLNTEKNIK**. Vi har dock lagt till ytterligare information om **OMRÅDE 2 – MARKNADSPLATS** och **OMRÅDE 3 – KONSULTTJÄNSTER FÖR MOLNET** när den bidrar till att ge ett övergripande sammanhang vad gäller krav och omfattning för offertförfrågan. Det är till exempel viktigt att inkludera de lägsta kvalificeringskraven på en återförsäljare till en molntjänstleverantör/leverantör av förvaldade tjänster/systemintegratör/konsultföretag/osv. och det bidrar till att säkerställa att de (1) är direkt kopplade till leverantören som återförsäljare eller kanalpartner, (2) är certifierade av leverantören att sälja direktåtkomst till deras erbjudanden till tredje part och (3) har certifieringar från dessa molntjänstleverantörer som fastställer deras kunskaper och expertis.

Exempel på formuleringar för offertförfrågan: minimikrav för anbudsgivare – administration

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 leverantörs molninfrastruktur (till exempel konsulttjänster, migreringstjänster, förvaldade tjänster, FinOps osv.). Ange rollerna som du lämnar anbud för:

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 för onlinemoln).

- Identifiera för vilket tjänsteerbjudande från molntjänstleverantörens som du kan sälja direktåtkomst till: _____
- Tillhandahåll ett brev från molntjänstleverantören om att du är en behörig 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 en molntjänstleverantörs tekniska support
- _____ – Partner till molntjänstleverantör som tillhandahåller tjänster för användning av eller drift via en molntjänstleverantör
- _____ – Influera/rådgivningstjänster för användning av eller drift via en molntjänstleverantör

Ange typen av erbjudande:

- Förvaltade tjänster för arbetsbelastningar hos en molntjänstleverantör (Ja/Nej): _____
 - Ange specialiteter (i tillämpliga fall): _____
- Professionella tjänster (Ja/Nej): _____
- Konsulttjänster – utbildning (Ja/Nej): _____
- Konsulttjänster – strategi (Ja/Nej): _____
- Konsulttjänster – migrering (Ja/Nej): _____
- Konsulttjänster – molnstyrning (Ja/Nej): _____
- Konsulttjänster – FinOps (Ja/Nej): _____
- Konsulttjänster – övrigt (ange vad): _____

Identifiera molnleverantörerna som du tillhandahåller tjänster för: _____

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

OMRÅDE 1 MINIMIKRAV FÖR ADMINISTRATION**Molntjänstleverantörer (CISP:er)**

För att kvalificeras som en molntjänstleverantör måste kraven nedan uppfyllas.

Föreslagna krav på molntjänstleverantörer	Motivering
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 fullfölja avtalet.
Skäl till uteslutning, till exempel kriminalitet, bedrägerier osv.	
Fallstudier/kundreferenser (ange nödvändigt antal/typ).	Kunden får möjlighet att mäta molntjänstleverantörens erfarenhet av att tillhandahålla tjänsterna som krävs.
Företagets sociala ansvar.	Dessa bör vara offentligt tillgängliga versioner som molntjänstleverantören tillhandahåller.
Offentligt tillgängliga åtaganden och metoder kring hållbarhet.	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, stordata, förvaltade tjänster och funktioner för optimerad molnanvändning. Offentliga ändringsloggar eller uppdateringsflöden kan användas för att påvisa detta.	Visar att molntjänstleverantören arbetar för att snabbt förse kunder med nya produkter och sedan snabbt upprepat omarbета och förbättra produkter. Det hjälper kunderna att bibehålla en avancerad och modern IT-infrastruktur utan att behöva göra kapitalkrävande investeringar.

Återförsäljare/partner till CISP

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

2.2 Teknik

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 skraddarsydd lösning. Som tidigare nämnt är skillnaden mellan vad som är standardiserat och vad som är skraddarsytt väldigt viktig när det gäller en offertförfrågan för molntjänster. Molntjänstleverantörer

³ Observera att företagsinformationen som används i en offertförfrågan för molntjänster är på en översiktlig nivå, snarare än antalet anställda i företaget eller den interna teamstrukturen. När det gäller molnteknik finns det ingen korrelation mellan garantier om 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.

erbjuder standardiserade tjänster till miljontals kunder, så anpassningar i en offertförfrågan för molntjänster fokuserar på lösningar och resultat som tillägger något utöver standarden, snarare än de underliggande metoderna, den infrastruktur eller den maskinvara som används för att erbjuda molntjänsterna som används för att uppnå resultat med lösningarna.

2.2.1 Minimikrav

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 till kraven helt rätt. I lyckade fall dokumenterar dessa kravsessioner den tidigare verksamhetsprocessen som i sig kan vara föråldrad och ineffektiv. Om dessa krav sedan utgör en del av offertförfrågan som molntjänstleverantören har att gå på kan den enda möjliga lösningen vara en skräddarsydd lösning. Denna modell är inte kompatibel med molnupphandlingar.

Organisationer i den offentliga sektorn ska förstå sina affärsmål och prestandabehov, men inte vara preskriptiva i en offertförfrågan på så sätt att de dikterar systemets design och funktion. I stället bör organisationen sikta in sig 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 affärsmålen, oavsett om de uppnår prestandabehoven eller inte, och möjligheten att finjustera affärsreglerna genom konfiguration.

*Offertförfrågningar för moln bör ställa rätt frågor för att hitta de bästa lösningarna. Eftersom inga fysiska tillgångar köps in i en molnmodell slutar det med att många upphandlingskrav för traditionella datacenter inte är tillämpliga. **Att återanvända frågor för datacenter leder oundvikligen till gamla svar för datacenter**, 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 på molntjänster, vilket säkerställer att leverantörerna som kvalificerar sig för OMRÅDE 1 ligger på en hög nivå. Kraven ska inte heller vara allt för preskriptiva, så att de inte begränsar den offentliga sektorns åtkomst till ett brett utbud av kvalificerade molntjänstleverantörer.

Exempel på formuleringar för offertförfrågningar: molnleverantörens förmågor

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

Föreslagna krav på molntjänstleverantörer	Motivering
Infrastruktur	
<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 distributioner med hög tillgänglighet och aktiv redundans samt 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 systemkritiska svaga punkter kan undvikas.</i>

Molntjänstleverantören ska tillhandahålla logiskt och geografiskt isolerade regioner. Molntjänstleverantören får inte replikera kunddata utanför dessa regioner.	Kraven på dataresidens innebär att kunden ska ha full kontroll över var deras data befinner sig.
Molntjänstleverantören måste kunna ha direkt, dedikerad och privat anslutning mellan molntjänstleverantörens olika datacenter.	Privat anslutning är ett grundläggande krav för att kunna bygga en säker hybridinfrastruktur.
Molntjänstleverantören ska tillhandahålla nog med 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.
Minimikrav på molntjänstleverantörens certifieringar	
Molntjänstleverantören måste vara certifierad enligt ISO 27001.	Granskning, certifiering och ackreditering från tredje part säkerställer att kunder kan säkerställa tjänsternas (och i synnerhet plattformens) kvalitet, säkerhet och tillförlitlighet. Det är nödvändigt att ett minimikrav på certifieringar uppfylls.
Molntjänstleverantören måste följa CISPE:s Data Protection Code of Conduct för att kunna tillhandahålla funktioner och tjänster som kan användas i enlighet med GDPR och som gör det möjligt för kunderna att bygga program i enlighet med GDPR.	Kunden måste kunna bygga eller driva program i enlighet med 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 öppen med hur programmet drivs och hanteras. SOC-rapporter är viktiga för att säkerställa tillit och transparens.
Molntjänstleverantören måste agera i enlighet med Climate Neutral Data Centre Pact.	Climate Neutral Data Centre Pact innebär att molntjänstleverantören ska uppnå klimatneutralitet senast 2030 och därmed göra det möjligt för användaren att nå sina egna hållbarhetsmål. Granskning utförd av tredjepartsrevisorer är obligatoriskt för leverantörer med över 250 heltidsekvivalent anställda (ej små och medelstora företag).
Molntjänstleverantören måste följa SWIPO:s uppförandekod för portabilitet inom IaaS.	SWIPO:s uppförandekod för portabilitet inom IaaS säkerställer att tjänsterna uppfyller kraven i artikel 6, "Dataportering", i förordningen om det fria flödet av andra data än personuppgifter.
Tjänstegenskaper	
Molntjänstleverantörens infrastruktur måste vara tillgänglig via programmeringsgränssnitt (API:er) och webbaserade hanteringskonsoler.	Självbetjäningsåtkomst 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, förvaldade relationsdatabaser, andra förvaldade databaser, förvaldade lastbalanserare, övervakning och integrerad automatisk skalning.	Det räcker inte med ett erbjudande om virtuella maskiner för att kvalificera en leverantör som en molnleverantör. Molnleverantörer bör erbjuda en uppsättning PaaS- och IaaS-tjänster för att förbättra kundens program och göra dem snabbare.

Molntjänstleverantören måste låta kunden fritt ändra användningen och konfigurationen av leverantörens tjänster och flytta data inom och utanför molntjänstleverantörens moln (erbjudande med självbetjänande tjänster).	Självbetjäningsåtkomst 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 användning.	Med användningsbaserad fakturering kan kunden kostnadsoptimera sina arbetsbelastningar, minska riskerna och använda molntjänstleverantören för kortvariga program och koncepttest.
Data- och systemsäkerhet	
Molntjänstleverantören måste låta kunden få full kontroll över sina egna data, ge kunden friheten att välja var data lagras (stadsområde) och garantera att inga kunddata flyttas såvida en sådan flytt inte initierats av kunden själv.	Kunden måste ha kontroll över var data lagras, hur åtkomsten till innehållet ska hanteras och användaråtkomst till tjänster och resurser.
Molntjänstleverantören måste ge kunden full kontroll över säkerhetspolicier, bland annat gällande sekretess, integritet och åtkomst till kundens data och system.	Kunden måste kunna definiera och implementera sina säkerhetsstandarder för alla sina arbetsbelastningar. Det räcker inte med att lita på att leverantören ska hantera kundens data på rätt sätt.
Kostnadskontroll	
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.	
Molntjänstleverantören måste erbjuda verktyg som varnar kunden när kostnaderna överskrider ett tröskelvärde.	
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.	

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/lagefterlevnad
- stordata/analys
- företagsprogram
- telekommunikation och nätverk
- geospatiala lösningar
- IoT
- [övrigt].

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

- haveriberedskap
- utveckling och testning

- arkivering
- säkerhetskopiering och återställning
- stordata
- databehandling med höga prestanda (HPC)
- sakernas internet (IoT)
- webbplatser
- serverlös databehandling
- DevOps
- innehållsleverans
- [övrigt].

2.2.2 Jämföra leverantörer

Utöver minimikraven i offertförfrågan för molntjänster är det viktigt att sätta upp kriterier som gör att de olika molntjänstleverantörernas teknik kan jämföras i 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 "hur prisvärd" i en offertförfrågan för molntjänster.

Den offentliga sektorn kräver ofta konkurrens mellan anbudsgivare genom att använda utvärderingskriterier som hur prisvärd, 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 beräkningskapacitet eller lagring). Vi rekommenderar i stället 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 egenskaperna som behövs för att skapa molnlösningen framgå. För att göra detta kan organisationer i den offentliga sektorn dra nytta av de väsentliga molnegenskaper som National Institute of Standards and Technology (NIST) har publicerat, utöver att använda analysrapporter från tredje part för att säkerställa att molntjänstleverantören har ett erbjudande som passar bäst för ett "äkta moln" och som drivs i massiv skala.

Exempel på formuleringar för offertförfrågan – jämföra 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 väsentliga egenskaperna för molntjänster⁴.

- 1) **Självbetjäning på begäran:** deltagaren måste erbjuda möjligheten till ensidigt etablerande av beräkningskapacitet automatiskt, till exempel servertid och nätverkslagring, efter behov och utan krav på mänsklig interaktion med varje tjänstleverantör. Deltagaren ska erbjuda möjligheten till att ensidigt beställa

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

(dvs. utan leverantörens granskning eller godkännande) etablering 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 sammanslagen beräkningskapacitet som hanterar flera konsumenter genom att använda en modell med delade miljöer för olika virtuella resurser som tilldelas och omtilldelas dynamiskt i enlighet med vad konsumenten begär. Användaren kan ange en plats på en övergripande abstraktionsnivå (exempelvis land, region eller datacenterområde). 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) **Snabb elasticitet:** deltagarens molntjänstleverantör ska ha stöd för funktioner som etablerar och tar bort etablerade tjänster (skala upp och ned), så att tjänsten finns tillgänglig inom en viss tidsram (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.

Utöver detta måste molntjänstleverantören:

- vara en etablerad ledare i att tillhandahålla molntjänster enligt Gartners Magic Quadrant for 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 molntjänstleverantörerna.

2.2.2.1 Servicenivåavtal (SLA)

Molntjänstleverantörer tillhandahåller kommersiella servicenivåavtal till miljontals kunder och kan därför inte erbjuda anpassade avtal, som det går att göra med en lokal datacentermodell. Men molntjänstleverantörernas kunder kan (ofta med hjälp av molntjänstleverantörernas partner) utforma sin egen molnanvändning så att den utnyttjar kommersiella servicenivåavtal för att uppfylla kundspecifika krav och unika avtal.

Offertförfrågningar för molntjänster ska se till att molntjänstleverantörerna erbjuder de funktioner och den vägledning som krävs för att använda deras tjänster och kommersiella servicenivåavtal, så att de enskilda slutanvändarna kan uppfylla kraven på prestanda och tillgänglighet.

Exempel på formuleringar för offertförfrågan: servicenivåavtal

Tillhandahåll information om och länka 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 i fall där ett servicenivåavtal inte fullgörs.

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

<ORGANISATION> ansvarar för att upprätthålla ett 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 hur servicenivåavtalet fungerar i drift 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.

2.2.3.1 Nya och föränderliga tjänster

Molntjänstleverantörer tillhandahåller prestanda som en tjänst. Till skillnad från traditionella lösningar på plats 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 de tidigare lokala systemen och molnleverantörer lägger ständigt till nya förbättrade tjänster som kunderna kan använda hur 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 version av ett ramavtal släpps. Vi rekommenderar därför att tillhandahållandet av tjänsterna som beskrivs i ramavtalet inte är begränsande, 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 formuleringar 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 kunder hos 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 molntjänstens specifikationer ändras i enlighet med det.

*Omfattningen av denna beställning inkluderar alla befintliga och nya eller förbättrade tjänster från molntjänstleverantören **INOM AVTALETS RAMVERK**. Molntjänster från molntjänstleverantören som är tillgängliga för kommersiella kunder ska göras tillgängliga för <ORGANISATION>.*

2.2.3.2 Låsning till en viss leverantör och möjlighet till förändring

Molnteknik innebär mindre 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 en leverantör är dock ofrånkomlig vid köp av molntjänster eftersom alla moln inte är likadana. En molntjänstleverantör kan erbjuda tjänster och funktioner som en annan helt enkelt inte kan tillhandahålla. På så sätt minskar möjligheten att få likvärdiga tjänster från en annan leverantör. Ett klokt tillvägagångssätt är att begära att molntjänstleverantörer tillhandahåller de nödvändiga funktionerna och tjänsterna för att lämna deras moln med dokumentation över hur dessa tjänster ska användas. Det kan fungera 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.

Se avsnitt 2.3.1.2 för information om branschens uppförandekoder gällande "dataportering" och "byte av molnleverantör" för att uppfylla kraven i artikel 6 i EU:s förordning om det fria flödet av andra data än personuppgifter.

Exempel på formuleringar 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 kan fungera som en rimlig utträdesplan.

*Molntjänstleverantören ska inte ha **obligatoriska** minimiåtaganden eller **obligatoriska** 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 hämtas och förs över till en ny molnleverantör. <ORGANISATION> kan exportera sina maskinbilder och använda dem på plats eller hos en annan leverantör (i enlighet med begränsningarna i relevanta programvarulicenser).

2.3 Säkerhet

Molntjänstleverantören och molnkunderna delar på ansvaret för säkerhet och lagefterlevnad. 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 modellen för molndistribution (IaaS/PaaS/SaaS). Det är viktigt att kunden är införstådd med sitt ansvar i varje modell.

Det är viktigt att förstå modellen för delat ansvar för att kunna utforma en lyckad offertförfrågan för molntjänster. Organisationer i den offentliga sektorn bör säkerställa att de vet vad molntjänstleverantören ansvarar för, vad de själva ansvarar för och var konsultpartner/oberoende programleverantörspartner och deras lösningar kan hjälpa till.

2.3.1 Minimikrav

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 funktioner** för nätverksbrandväggar och web application firewalls för att skapa privata nätverk och kontrollera åtkomsten till instanser och program.
- **Tillhandahålla anslutningsalternativ** som möjliggör privata eller dedikerade anslutningar från kontoret eller den lokala miljön.
- **Tillhandahålla en funktion** för att implementera en detaljerad strategi för säkerhet och förhindra DDoS-angrepp.
- Tillgängliga **funktioner** för datakryptering i lagrings- och databastjänster.
- **Tillhandahålla flexibla alternativ** för nyckelhantering med möjligheten att välja om man 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 distributionsverktyg** för att skapa resurser från en molntjänstleverantör eller ta dem ur bruk enligt organisationens standarder.
- **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 får insyn i vad som händer i deras miljö hos molntjänstleverantören.
- **Göra det möjligt** att få en djup **insyn** i API-samtal, till exempel vem, vad, när och varifrån samtal har gjorts.
- **Tillhandahålla alternativ** för loggaggregering som effektiviserar granskning och rapportering om lagefterlevnad.
- Tillhandahålla en funktion för att konfigurera varningsmeddelanden när specifika händelser inträffar eller tröskelvärden överskrids.
- **Tillhandahålla funktioner** som definierar, upprätthåller och hanterar principer för användaråtkomst i alla tjänster hos molntjänstleverantören.
- **Tillhandahålla en funktion** för att definiera individuella användarkonton med egna behörigheter i molntjänstleverantörens resurser.
- **Tillhandahålla en funktion** för att integrera och organisera affärskataloger för att minska administrativa omkostnader och ge slutanvändaren en bättre upplevelse.

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

Funktioner utöver minimistandarden för säkerhet kan användas för en mer betydelsefull analys av "alternativ med mervärde" eller "hur prisvärd" i en offertförfrågan. Ju fler inbyggda eller automatiska funktioner som finns för säkerhet desto bättre. Se *Bilaga A – Tekniska krav för att jämföra olika anbudsgivare* för krav angående att jämföra olika anbudsgivare.

Organisationer i den offentliga sektorn bör titta på certifieringar och bedömningar för molnackreditering 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 revisor för att bekräfta efterlevnad av certifieringsstandard ISO 27001. ISO 27001 Annex A, område 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 för att dra nytta av rapporter om lagefterlevnad från tredje part kan tillämpas på de flesta säkerhets- och efterlevnadskontroller, till exempel: CISPE GDPR Code of Conduct, ISO, SOC osv.

Exempel på formuleringar 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 lagefterlevnad:

- Beskriv de säkerhetsrelaterade roller och ansvarsområden som molntjänstleverantören och <ORGANISATION> har 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 säkerhetskraven hos <ORGANISATION>.

ÄGARE AV OCH KONTROLL ÖVER INNEHÅLL SOM TILLHÖR <ORGANISATION>

Beskriv hur molntjänstleverantörens funktioner kan skydda datasekretessen åt <ORGANISATION>. Inkludera de kontroller som används för att skydda innehåll som tillhör <ORGANISATION>. 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> kommer att hantera 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 på ett effektivt sätt. Molntjänstleverantören öppnar eller använder inte innehåll som tillhör <ORGANISATION> i något annat syfte än de som krävs enligt lag och för att upprätthålla molntjänstleverantörens tjänster och tillhandahålla <ORGANISATION> och dess slutanvändare dessa.
- <ORGANISATION> väljer i vilka regioner innehållet ska lagras. Molntjänstleverantören flyttar eller replikerar inte innehåll som tillhör <ORGANISATION> 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 innehåll som tillhör <ORGANISATION> vid överföring eller i vila och erbjuda <ORGANISATION> alternativet att hantera sina egna krypteringsnycklar.
- Molntjänstleverantören måste ha ett program för säkerhetsgaranti med global bästa praxis för integritet och dataskydd. Detta för att hjälpa <ORGANISATION> att inrätta, använda och tillvarata molntjänstleverantörens miljö för säkerhetskontroll. Säkerhetsskyddet och kontrollprocesserna måste valideras 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 blir upphandlingen mer effektiv och de 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 lagefterlevnad. Som nämndes ovan täcker dessa ackrediteringar till stor del samma områden kring 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 datacenter på plats och därför kanske inte går att tillämpa på molntjänster).

OBS! Det är även väldigt viktigt att förstå hur man kan komma åt rapporterna som anges nedan. SOC-rapport 1 och 2 är till exempel vanligtvis känsliga dokument. Se till att du förstår 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 svaret på offertförfrågan (dessa dokument kan offentliggöras genom lagar om offentliga handlingar eller liknande lag som äventyrar molnsäkerheten).

Exempel på formuleringar för offertförfrågan: lagefterlevnad

Användningen av erkända standarder för säkerhet, lagefterlevnad och drift som härleds från bästa praxis inom molntjänststugor, bland annat datahantering, datasäkerhet, sekretess, tillgänglighet osv., gör upphandlingen av molnteknik mer effektiv.

<ORGANISATION> utvärderar unika erbjudanden mot godkända standarder för säkerhet, lagefterlevnad och drift 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 minimistandarden under hela avtalets giltighetstid är att tjänsteafterlevnaden 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
☐ C5 (Tyskland)		☐ CDSA
☐ CISPE:s Data Protection Code of Conduct (GDPR)		
☐ CNDP (Climate Neutral Data Centre Pact)		
☐ DIACAP	☐ EU:s dataskyddsdirektiv	☐ CIS
☐ Nivå 2 och 4 i DoD SRG	☐ EU:s modellklausuler	☐ Informationstjänster om straffrätt (CJIS)
☐ HDS (Frankrike, sjukvård)		
☐ FedRAMP	☐ FERPA	☐ Cybersäkerhetsakten
☐ FIPS 140-2	☐ GDPR	☐ EU-US Privacy Shield
☐ ISO 9001	☐ GLBA	☐ EU Safe Harbor
☐ ISO 27001	☐ HIPAA	☐ FISC
☐ ISO 27017	☐ HITECH	☐ FISMA

☐ ISO 27018	☐ IRS 1075	☐ G-Cloud [Storbritannien]
☐ IRAP [Australien]	☐ ITAR	☐ GxP (del 11 i FDA CFR 21)
☐ Nivå 3 av MTCS [Singapore]	☐ PDPA – 2010 [Malaysia]	☐ ICREA
☐ Nivå 1 av PCI DSS	☐ PDPA – 2012 [Singapore]	☐ IT Grundschutz [Tyskland]
☐ SEC Rule 17-a-4(f)	☐ PIPEDA [Kanada]	☐ MARS – E
☐ SecNumCloud (Frankrike)		
☐ SOC1/ISAE 3402	☐ Privacy Act [Australien]	☐ MITA 3.0
☐ SOC2/SOC3	☐ Privacy Act [Nya Zeeland]	☐ MPAA
☐ SWIPO:s uppförandekod för IaaS		
	☐ Spansk DPA-auktorisering	☐ NIST
	☐ Storbritanniens DPA – 1988	☐ Nivåer från Uptime Institute
	☐ VPAT/avsnitt 508	☐ Storbritanniens Cloud Security Principles

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

2.3.1.1 Dataskydd

En viktig aspekt när du använder molntjänster är att behandlingen av personuppgifter sker i enlighet med EU:s gällande lagstiftning kring dataskydd, inklusive dataskyddsförordningen (GDPR). GDPR är en principbaserad förordning och innehåller därför ingen sektorsspecifik vägledning för att säkerställa lagefterlevnad. Dataskyddsförordningen uppmuntrar dock till att tillämpa verktyg för lagefterlevnad, t.ex. uppförandekoder, för att ge sådan vägledning. CISPE har i samarbete med den franska dataskyddsmyndigheten (CNIL) utarbetat en uppförandekod för dataskydd (CISPE-koden⁶) som godkänts av den Europeiska dataskyddsstyrelsen och som är allmänt tillämplig i Europa. Syftet med koden är att hjälpa molntjänstleverantörer med att följa GDPR och vägleda kunderna i bedömningen av om en leverantör är lämplig för den behandling av personuppgifter som kunden vill utföra.

- Koden är endast inriktad på IaaS-sektorn och behandlar IaaS-leverantörernas specifika roller och ansvarsområden.
- Den bidrar till att klargöra aspekterna av rättvis och öppen behandling och lämpliga säkerhetsåtgärder i samband med tjänster för molninfrastruktur (GDPR, artikel 40 [2]).
- Den hjälper kunderna att förstå hur de kan behålla suveräniteten över sina data genom att se till att de stannar inom EU.
- Den främjar bästa praxis för dataskydd som stöder EU:s GAIA-X-initiativ att utveckla europeiska datatjänster för molnet.

⁶ <https://cispe.cloud/code-of-conduct/>

Molntjänstleverantörens efterlevnad av uppförandekoder för dataskydd, t.ex. CISPE-koden, försäkrar att personuppgifter kommer att behandlas i strikt överensstämmelse med GDPR.

Exempel på formuleringar i offertförfrågan: dataskydd

Molntjänstleverantören som lämnar anbud (direkt eller via en återförsäljare) ska kunna uppvisa att denna följer en uppförandekod för dataskydd, t.ex. CISPE-koden. Koden för dataskydd måste överensstämma med de krav som fastställs i dataskyddsförordningen. Koden bör som minst innehålla följande: 1) en tydlig definition av molntjänstleverantörens roller och ansvarsområden, 2) krav på att molntjänstleverantören inte kommer att använda kunduppgifter i marknadsförings- eller reklam syfte, och 3) kundernas möjlighet att välja molntjänster som gör det möjligt att behandla uppgifterna helt och hållet inom Europeiska ekonomiska samarbetsområdet. Efterlevnaden av koden måste bekräftas av externa oberoende revisorer (övervakningsorgan) som är ackrediterade av oberoende, externa revisorer som i sin tur är ackrediterade av Europeiska dataskyddsmyndigheten.

2.3.1.2 Byte av molnleverantör och dataportering

Kunderna bör ha frihet att välja vilka molntjänster de vill använda och inte vara "låsta" till en molntjänstleverantör eller PaaS/SaaS-leverantör.

Molntjänstleverantörernas tjänster är standardiserade och erbjuds på sättet "en till många", där tjänsterna konfigureras, etableras och kontrolleras av kunden. En fördel med molntjänster är att kunderna kan välja de standardiserade tjänsterna de behöver för att utveckla sina unika program och lösningar. Denna fördel innebär även att kunna byta till nya eller andra tjänster som bäst uppfyller kundernas behov vid en viss tidpunkt.

Precis som när det gäller dataskydd kan uppförandekoder bidra till att ge kunderna trygghet och förtroende när det gäller att byta till molnet från lokal infrastruktur eller när de byter mellan olika leverantörer. Tillsammans med EuroCIO (European Association of CIOs) var CISPE medordförande i utvecklingen av uppförandekoden för dataportabilitet och byte av molntjänster för IaaS-molntjänster (SWIPO:s IaaS-kod^{7,8}). Den första versionen av koden utvecklades i enlighet med EU:s förordning om fritt flöde av data. Den överlämnades till Europeiska kommissionen i november 2019 under det finska ordförandeskapet och publicerades av föreningen SWIPO AISBL maj 2020. I april 2021 förklarade SWIPO AISBL de första tjänsterna som följde koden. I maj 2021 förklarades de även de första CISPE-medlemstjänsterna som följde koden.

Exempel på formuleringar för offertförfrågan: byte av molnleverantör och dataportabilitet

Molntjänstleverantören som lämnar anbud (direkt eller via en återförsäljare) ska kunna uppvisa att denna följer en uppförandekod för "växling och dataportering", t.ex. SWIPO:s IaaS-kod. Koden måste innehålla information om hur en CISP erbjuder en säker överföring av företagsdata om de beslutar sig för att byta molntjänstleverantör.

⁷ <https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security>

⁸ <https://swipo.eu/>

2.3.2 Jämföra 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 kriterier för att jämföra molntjänstleverantörens funktioner och tjänster för säkerhet under en utvärdering med konkurrens.

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

Exempel på formuleringar 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)*
- *påvisbar bakgrund av säkerheten i molntjänstleverantörens infrastruktur 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 utformningen av sina konton, automatisera säkerheten och styrningskontrollen samt effektivisera granskningsprocessen*
- *möjligheten att skapa, tillhandahålla och hantera en samling resurser på ett malliknande sätt (innehåller säkerhetsmallar med guldstandard som skapats av en molntjänstleverantör eller dess partner)*
- *möjligheten att skapa en tillförlitlig och repeterbar drift för kontrollerna*
- *funktioner för fortlöpande granskning i realtidsrevision*
- *möjligheten att kontrollera principer 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 modell för molnstyrning i IT-miljöerna*
- *tjänster som skyddar mot de vanliga, mest förekommande distribuerade överbelastningsattackerna (DDoS) mot nätverks- och transportlager tillsammans med möjligheten att skriva anpassade regler för att minska avancerade angrepp mot programlager*
- *förvaltd 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 in, 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 uppdatera sina erbjudanden kontinuerligt eller att leverantörer tillåts lägga till produkter efter den sista inlämningsdagen, så länge de uppfyller offertförfrågans ursprungliga parametrar. Detta passar in på att funktioner och tjänster för säkerhet utvecklas snabbt och att molntjänstleverantörer lanserar ofta säkerhetsfokuserade tjänster som i många fall är kostnadsfria. Observera att det är viktigt att fastställa en lägsta säkerhetsnivå (se minimikraven ovan) så att ändringar i säkerhetserbjudanden inte leder till en försämring.

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

Ett ramavtal för molnet ska vara flexibelt nog att kunna avlägsna en leverantör om denne inte längre uppfyller de minimikraven på säkerhet och efterlevnad som anges i offertförfrågan för molntjänsterna.

2.4 Prissättning

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 värde och den totala ägandekostnaden (TCO), i stället för att bara göra en jämförelse av enhetspriserna för liknande tjänster. Den traditionella metoden av att titta på det lägsta enhetspriset fungerar inte i molnmodellen och tenderar därför att inte leda till det ekonomiskt mest fördelaktiga anbudet eller det lägsta övergripande priset.

*För att underlätta utvärderingen av molntjänstleverantörers priser kan det hjälpa att först låta molntjänstleverantörerna förkvalificera sig eller väljas ut till en slutlista via **minimikrav angående priser**, så att molntjänstleverantörer med liknande funktioner kan kvalificera sig för ramavtalet. Utvärderingsprocessen för avrop och förnyad konkurrensutsättning 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 testskript för demonstrationer av molnteknik.*

2.4.1 Minimikrav

Prisavsnittet i en offertförfrågan för molntjänster har fyra huvudsakliga 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 resursmätningar.
2. **Transparent prissättning:** molntjänstleverantörens prissättning ska vara offentligt och transparent.
3. **Dynamisk prissättning:** gör det möjligt att vara flexibel nog att låta priset skifta beroende på marknadspriset. Den här metoden drar nytta av molnprisernas dynamiska och konkurrensutsatta natur och stöder innovation och prissänkningar.
4. **Kontrollerade utgifter:** molntjänstleverantören ska erbjuda verktyg för rapportering, övervakning och förutsägelser 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 formuleringar 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 dessa beskrivningar
- dokument med villkor
- dokument med prissättning (länkar till offentliga priser accepteras, under förutsättning att ett dokument med en fullständig prislista/prissättning finns tillgänglig på begäran)

Priset är kostnaden för tjänstens vanligaste upplägg. Molntjänstleverantörer ska erbjuda alternativ för volymbaserade rabatter och verktyg för priskalkylering så att kunden kan 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, priser eller dokument med och modeller för tjänstedefinitioner. En logg med eventuella samtal med leverantörer kommer att föras.

Ytterligare krav på prissättning

- Tillhandahåll molnteknik med en dynamisk prismodell som ger största möjliga affärsflexibilitet och möjlighet till skalbarhet och tillväxt.
- Prisattributen måste innehålla följande:
 - Erbjuds prissättningen för tjänsterna på begäran, baserat på löpande betalning? Beskriv er modell för prissättning.
 - Kan man uppnå ytterligare rabatter genom att förbinda sig till att använda en mängd resurser eller genom att köpa större mängder? Beskriv hur.
 - Är prissättningen offentligt tillgänglig och transparent? Inkludera länkar till offentligt tillgänglig prissättning.
 - Är priserna dynamiska och svarar de snabbt och effektivt på konkurrensen på marknaden?
 - Erbjuder ni bästa praxis och resurser för att spåra utgifter?
 - Erbjuder ni bästa praxis och resurser för kostnadsoptimering?

Transparent prissättning

På grund av den ständigt nedåtgående pristrenden inom kommersiell molnteknik som drivs av innovation och konkurrens får molntjänstleverantörens fakturerade enhetskostnad för tjänster som betalas av **<ORGANISATION>** under ramavtalet inte överskrida de 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 samt per produkt eller produktresurs eller enligt kunddefinierade taggar. **<ORGANISATION>** godkänner 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 förutsägelse och rapportering.

- Tillhandahåll information om hur <ORGANISATION> kan se faktureringsinformation både på detaljnivå och översiktligt, visualisera mönster i utgifter för molntjänstleverantörers resurser över tid och förutsäga framtida utgifter.
- Tillhandahåll 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 de tröskelvärde/budgetar som angivits av <ORGANISATION>.
- Tillhandahåll information om hur <ORGANISATION> kan förutsäga volymen förbrukade molntjänster under en angiven tidsperiod baserat på tidigare användning. Molntjänstleverantören ska erbjuda en **uppskattning** av vad beloppet som <ORGANISATION> faktureras av molntjänstleverantören blir och göra det möjligt för <ORGANISATION> att använda larm och budgetar för den förväntade förbrukningen, så att de kan få bättre kontroll över kostnader och utgifter.

2.4.2 Jämföra leverantörer

Organisationer i den offentliga sektorn kräver ofta konkurrens mellan anbudsgivare genom att använda utvärderingskriterier som hur prisvärda de är, ekonomiskt mest fördelaktigt anbud (MEAT) eller lägsta priser. Vid planeringen av prissättningen för ramavtalets avrop eller förnyade konkurrensutsättning 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. beräkningskapacitet eller lagring) eftersom det inte tar hänsyn till funktioner som prestanda, kostnadsoptimering genom att använda tjänster och övervakningsverktyg från molntjänstleverantören som är utvecklade för molnet eller olika tjänster som molntjänstleverantörer eventuellt erbjuder kostnadsfritt. Dessutom kan en molntjänstleverantörs katalogpriser innehålla tiotusentals standardartiklar och modellerna för prissättningen kan skilja sig från en tjänst till en annan och mellan olika leverantörer.

Analysera den totala ägandekostnaden

Vi rekommenderar att lägga 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 sänka/optimera kostnader osv.).

Jämföra scenarier

Utvärderingsprocessen kan även beakta vanliga scenarier som motsvarar vanligt förekommande system eller program. Sådana scenarier (till exempel webbhotell) 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 till exempel skatteåterbäring eller nödaviseringar för att varna vid översvämningar. Scenarierna ska innehålla omfattningen av tekniken och tjänsterna som kunden kan komma att 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 jämförelser av priserna för molntjänstleverantörernas erbjudanden. En molntjänstleverantör kan till exempel göra det möjligt för kunder att skapa en topologi för haveriberedskap (DR) med aktiv redundans 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 behovet av haveriberedskap. Se alternativen nedan för en direkt jämförelse av liknande tjänster 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 ifall 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 exemplet hos 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 tekniska överväganden som spelar in vid prissättningen, i synnerhet när det gäller säkerhet och efterlevnad.

Överväganden för prisscenarier

Baspriser – dessa är generellt molntjänstleverantörernas offentliga priser. Molntjänstleverantörer ska ange dessa priser officiellt. Däremot, som beskrivs ovan, kan kunder be om att runt 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 baserat på standardartiklar/artikelnummer 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 så pass detaljerad information och sedan hantera den när det faktiska priset endast fastställs utifrån förbrukningen av tjänsten).

Det är ett måste för molnkunder som vill ha de mest prisvärda alternativen att utvärdera en molntjänstleverantörs övergripande uppsättning funktioner. Molntjänstleverantörer kan till exempel ha flera tjänster som antingen är kostnadsfria eller så gott som kostnadsfria, och en prisutvärdering bör ta hänsyn till sådana tjänster. Andra molntjänstleverantörer kan eventuellt ta betalt för liknande funktioner.

Utvärderingskriterier kan skrivas på ett sätt som gör att molntjänstleverantörerna kan visa sina funktioner av typen "inklusive x som standard" och hur sådana tjänster påverkar den övergripande kostnaden. Utvärderingskriterier kan även överväga molntjänstleverantörens prissättning baserad på volym/nivåindelning och kommersiellt tillgängliga rabatter som reserverade instanser och spot-instanser. Exempelvis:

- en besparing på x % om kunden köper reserverad beräkningskapacitet (ett år, tre år osv.)
- en rabatt på x % för nivåindelade/volymbaserade priser
- en besparing på x % för 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 med löpande betalning.

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 månaders kapacitet på begäran och 12 och 36 månaders reserverad kapacitet.

Ange:

- Namnen på de föreslagna lösningarna:
- Anbudsgivarens bästa pris:
- Tider för tjänsten: dygnet och året runt
- Tjänstens tillgänglighet: 99,95 %

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

2.5 Utformning av/villkor för avtalets fullgörande

Teknik och drift 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-upphandlingar innehåller ofta strikta regler om att sökanden måste uppfylla många eller alla krav i upphandlingen, annars blir de avvisade. Eller så innehåller de en del helt 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 upphandlingarna misslyckas.

2.5.1 Villkor

Det första steget för att upphandla om en offertförfrågan för molntjänster är att granska och förstå molntjänstleverantörens befintliga kommersiella villkor, som ofta går att hitta på dennes 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 fördjupa sig mer i deras tillvägagångssätt. Den viktiga frågan är exakt varför molntjänstleverantörerna 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 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 ramavtalet via offertförfrågan för molntjänster. Molntjänstleverantörer lägger ständigt till nya tjänster och 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.

Diskutera offertförfrågan 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 exakt varför de relevanta villkoren fungerar som de gör. Villkor för moln skiljer sig till exempel från villkor för traditionella datacenter, förvaldade tjänster, maskinvara, paket med licensierad programvara 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 kunna få förtydliganden genom förhandlingar och diskussioner.

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 egentligen kan tillgodose organisationens behov. En vanlig process är att organisationen fastställer vissa villkor i förväg som den är villig att diskutera och förhandla innan avtalet tilldelas. 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 avisades. 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 kunna 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 distribueras 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 (givetvis förutom de klausuler som är obligatoriska enligt lag).

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 villkor** i avtalet för varje område i ett ramavtal för molnet. Ett tillvägagångssätt där samma lösning används för alla i upphandlingen för alla områden leder till problem med teknisk genomförbarhet och kompatibilitet.*

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 obligatoriska. 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. Mer information om återförsäljare till molntjänstleverantörer finns i avsnitt 2.1.3 ovan.

Exempel på formuleringar för offertförfrågan: villkor

Molntjänstleverantörer eller representerande leverantörer måste tillhandahålla sina offentliga villkor och ge feedback på huvudsakliga 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 uppsägning
 - ramverkets omfattning
 - beställningsprocess
 - sekretessbestämmelser
 - kategorispecifik IP och information
 - minska tekniska krav som molntjänstleverantörerna ska uppfylla, till exempel kvalitetsstandarder, 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, skraddarsydda servicenivåavtal som skiljer sig från molntjänstleverantörernas leveransmodeller för standardtjänster. Genom att tillåta de servicenivåavtal som molntjänstleverantörerna använder som standard kan molntjänstleverantörerna hålla nere kostnaderna och föra vidare besparingarna till 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 "test" 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 Villkor för programvara

Även om den här handboken fokuserar på inköp av molnteknik för IaaS och PaaS som tillhandahålls av en molntjänstleverantör, är det viktigt att belysa villkor för programvara som organisationer inom den offentliga sektorn kan beakta när de köper programvara från leverantörer. Se figur 1 (sida 5) för att se hur programvara köps in som en del av en välstrukturerad offertförfrågan för molntjänster.

Programvara spelar en avgörande roll i nästan alla företag, även inom den offentliga sektorn. Att inkludera skyldigheter som villkor för programvarulicenser i en offertförfrågan för molntjänster bidrar till att säkerställa att enheter inom den offentliga sektorn får erbjudanden som är så prisvärda som möjligt och har frihet att välja leverantör när de köper programvara.

Mer information finns i Ten Principles of Fair Software Licensing for Cloud Customers⁹. Principerna har tagits fram av Cigref¹⁰, en sammanslutning av stora franska företag och offentliga organ som företräder användarna av digital teknik, i samarbete med CISPE och med stöd av andra europeiska branschorganisationer för CIO:er och leverantörer, för att ta itu med de metoder som de båda sammanslutningarna anser skadar den digitala transformationen av organisationer av alla storlekar i samband med att de går över till molnet.

Exempel på formuleringar för offertförfrågan: programvara

<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. Programvaruleverantörer och **<ORGANISATION>** kan diskutera båda villkorsuppsättningarna under fasen för **<DISKUSSION/FÖRHANDLING>**.

⁹ <https://www.fairsoftware.cloud/principles/>

¹⁰ <https://www.cigref.fr/>

Krav 1.0. Programvaruleverantörer <u>måste</u> tillhandahålla tydliga licensvillkor, inklusive en uppdelning av kostnaderna på sammanfattande och detaljerad nivå. Krav 1.1. Alla avgifter i relation till bristande efterlevnad av licensvillkoren <u>måste</u> anges på sammanfattande och detaljerad nivå.
Krav 2.0. Programvarulicenserna <u>måste</u> ge <ORGANISATION> möjlighet att migrera den licensierade programvaran från lokal verksamhet till valfritt moln, utan att behöva köpa separata, dubbla licenser för samma programvara. Krav 2.1. Programvarulicenser <u>måste</u> vara fria från licensbegränsningar och ökade kostnader som begränsar möjligheten för <ORGANISATION> att köra den licensierade programvaran i valfritt moln.
Krav 3.0. Programvarulicenser <u>måste</u> göra det möjligt för <ORGANISATION> att köra den licensierade programvaran på sin egen maskinvara (vanligtvis kallad "lokal" programvara eller programvara "på plats") samt i valfritt moln.
Krav 4.0. Programvarulicenser <u>får inte</u> kräva att den licensierade programvaran endast får köras på maskinvara som enbart är dedikerad till <ORGANISATION>.
Krav 5.0. Programvaruleverantörer <u>får inte</u> bestraffa <ORGANISATION> om leverantörens licensierade programvara används i en annan leverantörs molnerbjudande, till exempel genom att inkludera rättigheter att genomföra ökade eller påträngande programvarubedömningar eller införa högre licensavgifter för programvara.
Krav 6.0. Programvara för kataloger <u>måste</u> stödja öppna standarder för synkronisering och autentisering av användaridentiteter på ett icke-diskriminerande sätt i förhållande till andra identitetstjänster.
Krav 7.0. Programvaruleverantörer <u>får inte</u> ta ut olika priser för samma programvara enbart beroende på vem som äger den maskinvara som den installeras på. Krav 7.1. Priserna för programvara <u>får inte</u> diskriminera mellan programvara som installeras i <ORGANISATIONS> eget datacenter, ett datacenter som förvaltas av en tredje part, på datorer som hyrs av en tredje part eller hos en molnleverantör som <ORGANISATION> väljer.
Krav 8.0. Under avtalstiden <u>får</u> programvaruleverantörerna <u>inte</u> göra väsentliga ändringar i licensvillkoren som begränsar <ORGANISATION> från tidigare tillåtna användningsområden, såvida det inte krävs enligt lag eller på grund av säkerhetsproblem.
Krav 9.0. Programvaruleverantörer <u>får inte</u> vilseleda <ORGANISATION> genom att hävda att programvarulicenser kommer att täcka <ORGANISATIONS> avsedda programvaruanvändning enligt <ORGANISATIONS KRAV>, när det för att täcka sådan användning kan krävas inköp av ytterligare licenser.
Krav 10.0. Om <ORGANISATION> har rätt att sälja vidare och överföra programvarulicenser <u>måste</u> programvaruleverantörerna fortsätta att erbjuda support och patchar på rättvisa villkor till <ORGANISATION> som lagligen har förvärvat en licens som sålts vidare.

2.5.3 Välja mellan utvalda leverantörer per projekt

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

Om det anses nödvändigt kan en förnyad konkurrensutsättning anordnas för att fastställa den bästa leverantören för en särskild arbetsbelastning eller ett särskilt projekt. En förnyad konkurrensutsättning innebär att en kund höjer konkurrensen under ramverket genom att bjuda in alla leverantörer inom ett område till att svara på en uppsättning krav. Kunden bjuder in alla kapabla leverantörer inom området att lämna anbud. Det är därför viktigt att använda sig av minimikrav för deltagare 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 samma lösning används för 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.

2.5.4 Introduktion och utträde

Något som bör övervägas vid upprättandet av ett ramavtal för molnet är möjligheten att använda ett dynamiskt inköpssystem (DPS). Med en DPS-modell antas alla leverantörer som uppfyller minimikraven 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 kvaliteten på och försäkra sig om att tjänsterna är 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 slutänden 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 ramavtal med en välskrivna offertförfrågan för molntjänster upprättas.

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 skapa den IT-miljö de vill ha snarare än att bara hantera den de har. Molnkunder kan (1) starta med en full uppsättning av alla IT-tillgångar, (2) hantera alla dessa tillgångar centralt och (3) skapa varningar för 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 sparas (alla uppgifter om vem, vad, var och när för varje ändring sparas). 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 ändringarna i processerna och den nya kompetensen man får 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 ramavtal för molnet kan fortsätta att utvecklas så att kraven passar de nya processerna och den nya flexibiliteten.

3.2 Budgetera för molnet

När det gäller att strukturera prissättningen för molnet med betalning baserat på förbrukningen 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 (beräkningskapacitet, lagring, nätverk, databaser, IoT osv.), under **molnteknik**. Detta tillvägagångssätt ger flexibiliteten att erbjuda kunderna alla molntjänstleverantörens 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 optimerad användning och låga kostnader.

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

Det går att åstadkomma ytterligare flexibilitet i upphandlingen genom att använda valfria standardartiklar i avtalet inom lämpliga resurskategorier för att möjliggöra framtida tillväxt. Om en organisation istället vill samla molntekniker med konsulttjänster, professionella eller hanterade tjänster i en enda standardartikel går det att göra med en standardartikel som "Molnteknik och relaterat arbete".

Nedan visas ett 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 aktuell och förutsagd användning.

Tabell 3 – Exempel på prisstruktur med en standardartikel.

ARTIKELNUMMER	LEVERANSER/TJÄNSTER	KVANTITET	ENHET	ENHETSPRIS	BELOPP
1001	Molnteknik	1 000	Varje	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	3 000 €	3 000 €
1005	Molnmarknadsplats	10	Varje	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 tjänster för molnteknik som organisationen ska använda. Organisationen och leverantören enas om 10 miljoner euro på 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 verktyg för övervakning och förutsägelser används till att övervaka förbrukningen av återstående medel. Om återstående medel börjar ta slut begär organisationen ytterligare medel från finansdirektören för att använda dessa till att fortsätta använda tjänsterna.

Exempel på formuleringar för offertförfrågan: priser – upphandling

BETALNINGSVILLKOR

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

1. Månadsbetalningen baseras på den faktiska användningen/förbrukningen av tjänsterna och enligt molntjänstleverantörens offentligt tillgängliga prissättning.

MINIMIGARANTI 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 beställd standardartikel för "molnteknik".

Varje enhet av standardartikeln som beställs motsvarar <1,00 €> av den beställda molntekniken. Inkrementella beställningar läggs regelbundet via ändringar av beställningen i olika kvantiteter för att erbjuda <ORGANISATION> flexibiliteten att förbeställa flera olika mängder "eurobelopp" av molntjänstleverantörens molnteknik baserat på den uppskattade användningen för behov som kan vara olika länge. Kvantiteterna 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.

Artikelnummer	Beskrivning	Antal	Enhet	Pris
01	Molntjänstleverantörens molnteknik	1 000	Varje enhet	1 000,00 €

MINMIBESTÄLLNING/INKREMENTELL BESTÄLLNING

Beställningar läggs regelbundet för flera kvantiteter på <10 000> enheter av standardartiklar baserat på den uppskattade användningen av molnteknik hos <ORGANISATION>. Det här arrangemanget ger <ORGANISATION> flexibiliteten att förbeställa <10 000> enheter av "molnteknik" för att hantera driften i enlighet med den kommersiella principen av löpande betalning för molntjänster.

En första ökning på <100 000> enheter till ett pris på <100 000 €> beställs när avropet görs. 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> och 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.

STÖRSTA 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 behovet hos <ORGANISATION> under prestandaperioden, men kan inte garanteras.

3.3 Förstå affärsmodell med partner

Enheter i den offentliga sektorn bör försöka förstå modellerna som molntjänstleverantörer använder för att tillhandahålla sina erbjudanden, och att partners som levererar konsulttjänster, förvaldade tjänster, återförsäljning och mycket mer är mycket viktiga för processen. Många kunder behöver en molnleverantör för sin infrastruktur, och anlitar en systemintegratör eller leverantör av förvaldade 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 partner/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 så 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 (att köpa molntjänster direkt från en molntjänstleverantör) avvisar vanligtvis en molntjänstleverantör dessa "obligatoriska" klausuler som passar en vanlig underleverantör av handelsvaror på grund av att de upphandlade tjänsterna är kommersiella och det faktum att de flesta molntjänstleverantörer inte behöver underleverantörer för att leverera sina kommersiella tjänster.

3.4 Molnmäklare

Konceptet med molnmäklare som ett sätt 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.

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 inför offertförfrågan

När en enhet i den offentliga sektorn planerar en offertförfrågan för molntjänster bör den inkludera intressenterna från alla delar av organisationen – högre chefer, affärsintressenter, avdelningarna för teknik, ekonomi, upphandling, juridik och avtal – från första 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, bland annat från molntjänstleverantörer, deras partner, 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.

3.6 Hållbarhet

Hållbarhet är en naturlig del av molntjänster och att flytta till molnet ger en vinst i energieffektivitet jämfört med lokala servrar eller datacenter hos företag. Att identifiera en molntjänstleverantör som prioriterar hållbarhet och har gjort offentliga åtaganden för att uppnå hållbarhetsmålen ger ytterligare garantier för att molnet är hållbart. Europeiska molntjänstleverantörer och datacenteroperatörer (med stöd av Europeiska kommissionen) skapade Climate Neutral Data Centre Pact¹¹, ett självreglerande initiativ för att fastställa tydliga, enkla och långtgående hållbarhetskriterier för datacenterbranschen och se till att datacenteroperatörer och leverantörer av molntjänster är klimatneutrala senast 2030. Det självreglerande initiativet innehåller tydliga mål för energieffektivitet i datacenter, vattenbesparing, återanvändning och reparation av servrar samt användning av koldioxidfri energi för att driva datacenter. Molntjänstleverantörer som ansluter sig till det självreglerande initiativet samtycker till att uppfylla dessa mål och certifiera sig mot kriterierna för att betraktas som en klimatneutral operatör.

I ett förfrågningsunderlag för molntjänster bör man fråga CISP:erna om de har åtagit sig att följa sådana kriterier, och särskilt fråga om de har undertecknat självreglering och när de har åtagit sig ett sådant åtagande.

Exempel på formuleringar för offertförfrågan: hållbarhet

Har ni åtagit er att driva klimatneutrala datacenter genom att underteckna Climate Neutral Data Centre Self-Regulatory Initiative? Om så är fallet, när undertecknade ni det?

Kan du bevisa att du har tilldelats stämpeln för Climate Neutral Data Centre Pact?

¹¹ <https://www.climateneutraldatacentre.net/self-regulatory-initiative/>

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 förnyad konkurrensutsättning för ett ramavtal för molnet.

1. Molnleverantörens profil

	Krav
1.	MARKNADSERFARENHET: <i>Hur många år har molnleverantören varit verksam inom marknadssegmentet för molntjänster?</i>
2.	ÖPPENHET OCH DATASKYDD: <i>Följer molnleverantören uppförandekoderna för dataskydd och möjlighet till förändring? Följer molnleverantören principerna för utveckling av öppen källkod och öppen API?</i>

2. Global infrastruktur

	Krav
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> Ange i så fall antalet domäner eller zoner och antalet datacenter i det aktuella geografiska området.
4.	AVSTÅND MELLAN 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.	HUR DATACENTER ÄR BYGGDA: <i>Erbjuder molnleverantören datacenter som är isolerade från fel i andra datacenter, med redundant strömförsörjning, kylning och nätverk?</i>
6.	REPLIKERING MELLAN DATACENTER: <i>Erbjuder molnleverantören datareplikering mellan datacentren inom en domän eller zon med automatisk överlämning vid fel?</i>
7.	REPLIKERING MELLAN DOMÄNER/ZONER: <i>Erbjuder molnleverantören datareplikering mellan domäner eller zoner inom en region?</i>

3. Infrastruktur

3.1 Beräkningskapacitet

	Krav
1.	BERÄKNINGSKAPACITET – VANLIG INSTANS – ALLMÄNNA ÄNDAMÅL: Erbjuder molnleverantören följande instanstyper? - För allmänna ändamål – optimerad för allmänna program och balanserar resurser för databehandling, minne och nätverk. - Vilken är i så fall den största instansen?
2.	BERÄKNINGSKAPACITET – VANLIG INSTANS – MINNESOPTIMERAD: Erbjuder molnleverantören följande instanstyper? - Minnesoptimerad – optimerad för minnesintensiva program. - Vilken är i så fall den största instansen?
3.	BERÄKNINGSKAPACITET – VANLIG INSTANS – BERÄKNINGSOPTIMERAD: Erbjuder molnleverantören följande instanstyper? - Beräkningsoptimerad – optimerad för beräkningsintensiva program. - Vilken är i så fall den största instansen?
4.	BERÄKNINGSKAPACITET – VANLIG INSTANS – LAGRINGSOPTIMERAD: Erbjuder molnleverantören följande instanstyper? - Lagringsoptimerad – erbjuder stor kapacitet för lokal lagring. - Vilken är i så fall den maximala lagringskapaciteten (dvs. 5, 10, 20, 50 TB) och det maximala antalet diskar (hårddiskar/SSD-enheter) som kan etableras och kopplas till en instans?
5.	BERÄKNINGSKAPACITET – VANLIG INSTANS – GRAFIKOPTIMERAD: Erbjuder molnleverantören följande instanstyper? - Grafik till låg kostnad – erbjuder grafikaccelerering till låg kostnad för instanser med beräkningskapacitet. - Vilken är i så fall den största instansen?
6.	BERÄKNINGSKAPACITET – VANLIG INSTANS – GPU-OPTIMERAD: Erbjuder molnleverantören följande instanstyper? - GPU – erbjuder maskinvara för grafikprocessorer (GPU) för grafikintensiva program. - Hur många GPU-enheter och vilka GPU-modeller kan molnleverantören erbjuda per instans i så fall?
7.	BERÄKNINGSKAPACITET – VANLIG INSTANS – FPGA-OPTIMERAD: Erbjuder molnleverantören följande instanstyper? - FPGA – erbjuder en eller flera field programmable gate array (FPGA) för att utveckla och distribuera anpassade maskinvaruaccelereringar för program. - Hur många FPGA-enheter kan molnleverantören erbjuda per instans i så fall?
8.	BERÄKNINGSKAPACITET – UTÖKBAR INSTANS: Erbjuder molnleverantören utökbara instanser som ger en grundläggande nivå av processorprestanda (CPU) med möjligheten att utöka till en högre nivå? Vilken är den största utökbara instansen i så fall?

9.	BERÄKNINGSKAPACITET – I/O-INTENSIV INSTANS: Erbjuder molnleverantören instanser som använder sig av SSD-enheter med NVM Express (NVMe) optimerade för korta svarstider, mycket hög slumpmässig I/O-prestanda och höga sekventiell läsprestanda? Vilken är i så fall den maximala kapaciteten för I/O-åtgärder per sekund för den största instansen?
10.	BERÄKNINGSKAPACITET – TILLFÄLLIG LOKAL LAGRING: Stödjer molnleverantören att lokal lagring för beräkningsinstanser används för tillfällig lagring av information som ofta ändras?
11.	BERÄKNINGSKAPACITET – STÖD FÖR FLERA NÄTVERKSKORT: Stödjer molnleverantören att flera (primära och extra) nätverkskort (NIC) tilldelas en given instans? Vilket är i så fall det största antalet nätverkskort per instans?
12.	BERÄKNINGSKAPACITET – INSTANSTILLHÖRIGHET: Erbjuder molnleverantören möjligheten att på ett logiskt sätt gruppera instanser i samma datacenter?
13.	BERÄKNINGSKAPACITET – ANTITILLHÖRIGHET FÖR INSTANSER: Erbjuder molnleverantören användare möjligheten att på ett logiskt sätt gruppera instanser och placera dem i olika datacenter inom en region?
14.	BERÄKNINGSKAPACITET – SJÄLVBETJÄNAD ETABLERING: Erbjuder molnleverantören självbetjäning för att etablera flera instanser samtidigt, antingen via ett programmeringsgränssnitt, en hanteringskonsol eller en webbportal?
15.	BERÄKNINGSKAPACITET – ANPASSNING: Erbjuder molnleverantören anpassningsbara instanser, dvs. möjligheten att modifiera konfigurationsinställningar som virtuella processorer (vCPU) och RAM (Random Access Memory)?
16.	BERÄKNINGSKAPACITET – UPPDELNING AV INSTANSER: Erbjuder molnleverantören instanser med dedikerade miljöer som körs på maskinvara som är avsedd för en enda användare? Vilken är i så fall den största tillgängliga instansen med dedikerad miljö?
17.	BERÄKNINGSKAPACITET – VÄRDTILLHÖRIGHET: Erbjuder molntjänstleverantören möjligheten att starta en instans och specificera att denna instans alltid startar om på samma fysiska värd?
18.	BERÄKNINGSKAPACITET – ANTITILLHÖRIGHET FÖR VÄRDAR: Erbjuder molnleverantören möjligheten att dela upp och köra specifika instanser på flera olika fysiska värdar?
19.	BERÄKNINGSKAPACITET – AUTOMATISK SKALNING: Erbjuder molnleverantören möjligheten att automatiskt öka antalet instanser under behovstoppar för att bibehålla prestanda (dvs. "skala ut")?
20.	BERÄKNINGSKAPACITET – MEKANISM FÖR ATT IMPORTERA AVBILDNINGAR: 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? Vilka format stöds i så fall?
21.	BERÄKNINGSKAPACITET – MEKANISM FÖR ATT EXPORTERA AVBILDNINGAR: Stödjer molnleverantören möjligheten att ta en befintlig instans som körs eller en kopia av en instans och exportera instansen till ett format för virtuella maskiner? Vilka format stöds i så fall?

22.	BERÄKNINGSKAPACITET – STÖRNINGAR I TJÄNSTEN: <i>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?</i>
23.	BERÄKNINGSKAPACITET – INSTANSOMSTART: <i>Erbjuder molnleverantören mekanismer för att automatiskt starta om instanser på en fungerande värd om den ursprungliga fysiska värden slutar att fungera?</i>
24.	BERÄKNINGSKAPACITET – AVISERINGAR: <i>Om något inträffar som påverkar beräkningskapaciteten, 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?</i>
25.	BERÄKNINGSKAPACITET – SCHEMALÄGGNING AV HÄNDELSER: <i>Erbjuder molnleverantören möjligheten att kunna schemalägga händelser för användarens instanser, till exempel att starta om, stoppa, starta eller ta instansen ur drift?</i>
26.	BERÄKNINGSKAPACITET – MEKANISM FÖR SÄKERHETSKOPIERING OCH ÅTERSTÄLLNING: <i>Erbjuder molnleverantören en integrerad mekanism för säkerhetskopiering och återställning?</i>
27.	BERÄKNINGSKAPACITET – MEKANISM FÖR ÖGONBLICKSBILDER: <i>Erbjuder molnleverantören en manuell mekanism för ögonblicksbilder på begäran?</i>
28.	BERÄKNINGSKAPACITET – METADATA: <i>Erbjuder molnleverantören en tjänst för instansmetadata som gör att användare kan ange godtyckliga nyckelvärdepar för instansen?</i>
29.	BERÄKNINGSKAPACITET – ANROP OM METADATA: <i>Erbjuder molnleverantören en tjänst för instansmetadata med ett programmeringsgränssnitt (API) som instansen kan anropa för att få information om sig själv?</i>
30.	BERÄKNINGSKAPACITET – MEKANISM FÖR ATT LÄMNA ANBUD: <i>Erbjuder molnleverantören en mekanism för att lämna anbud på billigare instanser som omedelbart kan skapas för att köra mindre viktiga arbetsbelastningar?</i>
31.	BERÄKNINGSKAPACITET – MEKANISM FÖR SCHEMALÄGGNING: <i>Erbjuder molnleverantören ett sätt att regelbundet schemalägga och reservera extra beräkningskapacitet, dvs. varje dag, vecka eller månad?</i>
32.	BERÄKNINGSKAPACITET – MEKANISM FÖR RESERVATION: <i>Erbjuder molnleverantören ett sätt att reservera extra beräkningskapacitet för framtiden (dvs. ett år, två år, tre år osv.)?</i>
33.	BERÄKNINGSKAPACITET – LINUX-OPERATIVSYSTEM: <i>Stödjer molnleverantören de senaste två långsiktigt 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)?</i>
34.	BERÄKNINGSKAPACITET – WINDOWS-OPERATIVSYSTEM: <i>Stödjer molnleverantören de senaste två stora Windows Server-versionerna (Windows Server 2017 och Windows Server 2016)?</i>
35.	BERÄKNINGSKAPACITET – LICENS PORTABILITET: <i>Erbjuder molnleverantören portabilitet och support för licenser?</i> Ange i så fall programvaruleverantör, programvarunamn, utgåvor och dess versioner.

36.	BERÄKNINGSKAPACITET – TJÄNSTGRÄNSER: Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet om beräkningskapacitet ovan? Exempel: högsta antal instanser per konto högsta antal dedikerade värdar per konto högsta antal reserverade IP-adresser (internetprotokoll).
-----	--

3.2 Nätverk

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

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 Single Root Input/Output Virtualization (SR-IOV) för högre prestanda (dvs. paket per sekund, PPS), korta svarstider och mindre störningar?</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 spara flödesloggar med nätverkstrafiken?</i>
18.	NÄTVERK – NAT: <i>Erbjuder molnleverantörer en förvaltd lösning med en gateway för Network Address Translation (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 kontrollen 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 anslutning av flera 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 med Internet protocol security (IPsec) eller en VPN-tunnel med Secure Sockets Layer (SSL) via offentligt internet?</i>
23.	NÄTVERK – STÖD FÖR BGP: <i>Använder molnleverantören border gateway protocol (BGP) för att förbättra den automatiska överlämningen vid fel i VPN-tunnlar med Internet protocol security (IPsec)?</i>
24.	NÄTVERK – PRIVAT DEDIKERAD ANSLUTNING: <i>Erbjuder molnleverantörer en direkt, privat anslutningstjänst mellan molnleverantörens lokaler och användarens datacenter, kontor eller samlokaliseringsscenter som klarar stora och snabba dataöverföringar?</i>
25.	NÄTVERK – LASTBALANSERING FÖR FRONTEND: <i>Erbjuder molnleverantören en lastbalanseringstjänst för frontend (mot internet) som tar emot begäran från klienter över internet och fördelar dem mellan instanser som är registrerade i lastbalanseraren?</i>
26.	NÄTVERK – LASTBALANSERING FÖR BACKEND: <i>Erbjuder molnleverantören en lastbalanseringstjänst för backend (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 med 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 med 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 men tillhör en enda domän?</i>
31.	NÄTVERK – LASTBALANSERINGSLOGGAR: <i>Erbjuder molnleverantören loggar som sparar detaljrik information om alla förfrågningar som skickas till en lastbalanserare?</i>
32.	NÄTVERK – DNS: <i>Erbjuder molnleverantören en tjänst för domännamnssystemet (DNS) med mycket hög tillgänglighet och skalbarhet?</i>
33.	NÄTVERK – LATENSBASERAD DNS-ROUTNING: <i>Erbjuder molnleverantören en tjänst för domännamnssystemet (DNS) med stöd för latensbaserad routning (dvs. DNS-tjänsten svarar på DNS-frågor med de resurser som ger bästa möjliga svarstid)?</i>
34.	NÄTVERK – GEOGRAFIBASERAD DNS-ROUTNING: <i>Erbjuder molnleverantören en tjänst för domännamnssystemet (DNS) med stöd för geografibaserad routning (dvs. DNS-tjänsten svarar på DNS-frågor baserat på användarnas geografiska plats)?</i>
35.	NÄTVERK – DNS-ROUTNING BASERAD PÅ AUTOMATISKA ÖVERLÄMNINGAR VID FEL: <i>Erbjuder molnleverantören en tjänst för domännamnssystemet (DNS) med stöd för routning baserat på automatisk överlämning vid fel (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 tjänst för domännamnssystemet (DNS) som använder hälsokontroller för att övervaka resursernas tillstånd och prestanda?</i>
38.	NÄTVERK – INTEGRERING AV DNS OCH LASTBALANSERARE: <i>Erbjuder molnleverantören en tjänst för domännamnssystemet (DNS) som integreras med molnleverantörens lastbalanserare?</i>
39.	NÄTVERK – VISUELLT REDIGERINGSVERKTYG: <i>Erbjuder molnleverantören ett verktyg som gör det möjligt för användare att utforma principer för trafikhantering?</i>
40.	CONTENT DELIVERY NETWORK (CDN): <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) för att distribuera innehåll med korta svarstider och hög dataöverföringshastighet?</i>

41.	NÄTVERK – CDN OCH CACHEMINNEN SOM UPPHÖR: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) som gör det möjligt att ta bort objekt från cacheminnen på enheter i kanten innan de upphör, bland annat funktioner som att ogiltigförklara och versionshantera objekt?</i>
42.	NÄTVERK – CDN OCH EXTERNA URSPRUNG: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) med stöd för anpassade ursprung, t.ex. en Hypertext Transfer Protocol-server (HTTP)?</i>
43.	NÄTVERK – CDN OCH OPTIMERING: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) med detaljerad kontroll att konfigurera servrar med flera ursprung och cachelagringsegenskaper för olika URL-adresser?</i>
44.	NÄTVERK – CDN MED GEOGRAFISK BEGRÄNSNING: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) med stöd för geografisk begränsning, dvs. som hindrar användare i ett visst geografiskt område från att få åtkomst till innehåll?</i>
45.	NÄTVERK – CDN OCH TOKENS: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) med stöd för undertecknade URL-adresser som vanligtvis skulle innehålla ytterligare information, till exempel utgångsdatum/utgångstid, för att ge användare mer kontroll över åtkomsten till deras innehåll?</i>
46.	NÄTVERK – CDN OCH CERTIFIKAT: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) med stöd för anpassade Secure Sockets Layer-certifikat (SSL) för att på ett säkert sätt leverera innehåll via Hypertext Transfer Protocol Secure (HTTPS) från nätverkets utkant?</i>
47.	NÄTVERK – CDN OCH CACHEMINNEN MED FLERA NIVÅER: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) som tillämpar en metod för cacheminnen med flera nivåer för användningen av regionala cacheminnen i kanten för att minska svarstiderna?</i>
48.	NÄTVERK – CDN OCH KOMPRIMERING: <i>Erbjuder molnleverantören en Content Delivery Network-tjänst (CDN) med stöd för filkomprimering?</i>
49.	NÄTVERK – CDN OCH KRYPTERAD UPPLADDNING: <i>Erbjuder molnleverantören ett Content Delivery Network (CDN) 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?</i>
50.	NÄTVERK – SLUTPUNKTER: <i>Erbjuder molnleverantörens nätverkstjänst användarna slutpunkter som kan dirigera trafik via leverantörens interna nätverksanslutning (dvs. privata anslutningar) för att sänka kommunikationskostnaderna och förbättra trafiksäkerheten?</i>
51.	NÄTVERK – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller nätverksavsnittet ovan?</i> <i>Exempel:</i> <i>högsta antal virtuella nätverk per konto</i> <i>största storlek på ett virtuellt nätverk</i> <i>högsta antal undernät per konto</i> <i>högsta antal lastbalanserare per konto</i> <i>högsta antal poster i åtkomstkontrollistan (ACL)</i>

	<i>högsta antal VPN-tunnlar (virtuellt privat nätverk)</i> <i>högsta antal ursprung per distribution</i> <i>högsta antal certifikat per lastbalanserare.</i>
--	---

3.3 Lagring

	Krav
1.	BLOCKLAGRINGSTJÄNST: <i>Erbjuder molnleverantören lagringsvolymen på blocknivå som ska användas med instanser med beräkningskapacitet?</i>
2.	BLOCKLAGRING – IOPS: <i>Erbjuder molnleverantören möjligheten att köpa ett uttryckligt prestandamål eller en prestandanivå för blocklagringsvolymen, till exempel ett visst antal I/O-åtgärder per sekund eller dataflödets megabyte per sekund (MB/S)?</i>
3.	BLOCKLAGRING – SSD: <i>Stödjer molnleverantören säkerhetskopierade lagringsmedia på SSD-enheter som ger svarstider på bara några millisekunder?</i> <i>Vilket är i så fall det maximala antalet SSD-enheter som kan kopplas per instans?</i>
4.	BLOCKLAGRING – SKALNING: <i>Erbjuder molnleverantören möjligheten att öka storleken på en befintlig blocklagringsvolym utan att behöva etablera en ny volym och kopiera/flytta över data?</i>
5.	BLOCKLAGRING – ÖGONBLICKSBILDER: <i>Erbjuder molnleverantören en funktion för ögonblicksbilder för deras blocklagringstjänst?</i>
6.	BLOCKLAGRING – DATAELIMINERING: <i>Stödjer molnleverantören fullständig eliminering av data på ett sådant sätt att data inte längre kan läsas eller är tillgängliga för obehöriga användare eller tredje part?</i>
7.	BLOCKLAGRING – KRYPTERING I VILA: <i>Erbjuder molnleverantören kryptering av vilande data på serversidan för data som lagras i volymen och deras ögonblicksbilder?</i> <i>Vilken krypteringsalgoritm används i så fall?</i>
8.	OBJEKTLAGRINGSTJÄNST: <i>Erbjuder molnleverantören säker och varaktig objektlagring med hög skalbarhet för lagring och hämtning från webben oavsett datavolym?</i>
9.	OBJEKTLAGRING – OREGELBUNDEN ÅTKOMST: <i>Erbjuder molnleverantören en lagringstjänstnivå till lägre pris som är avsedd att lagra objekt och filer som används sällan?</i>
10.	OBJEKTLAGRING – KORTARE VARAKTIGHET: <i>Erbjuder molnleverantören en reducerad redundansnivå till ett lägre pris där en användare kan lagra icke-kritiska objekt som är enkla att återskapa?</i>
11.	OBJEKTLAGRING – MINDRE FREKVENT ÅTKOMST: <i>Erbjuder molnleverantören en nivå för data som används mer sällan, men som ändå kräver snabb åtkomst?</i>

12.	OBJEKTLAGRING – OBJEKTNIVÅER: <i>Erbjuder molnleverantören en funktion för objektlagringsnivåer, dvs. möjligheten att rekommendera överföring av ett objekt mellan lagringsklasser eller nivåer baserat på hur ofta det används?</i>
13.	OBJEKTLAGRING – HANTERING AV LIVSCYKELN: <i>Stödjer molnleverantören hanteringen av ett objekts livscykel genom att använda en livscykelkonfiguration som definierar hur objekt hanteras under dess livstid, från skapande till borttagning?</i>
14.	OBJEKTLAGRING – PRINCIPDRIVEN HANTERING: <i>Erbjuder molnleverantören möjligheten att skapa och använda principer för att hantera lagrade data, deras livscykel och nivåinställningar?</i>
15.	OBJEKTLAGRING – PLATS- OCH TIDSBASERADE PRINCIPER: <i>Erbjuder molnleverantören användare möjligheten att skapa principer som kan begränsa åtkomsten till data baserat på var och när användaren begär åtkomsten?</i>
16.	OBJEKTLAGRING – WEBBPLATSVÄRDAR: <i>Stödjer molnleverantören att statiska webbplatser körs från objektlagringstjänsten?</i>
17.	OBJEKTLAGRING – KRYPTERING I VILA: <i>Stödjer molnleverantören kryptering av vilande data på serversidan (SSE), där molnleverantören hanterar krypteringsnycklarna?</i> • Vilken krypteringsalgoritm används i så fall?
18.	OBJEKTLAGRING – KRYPTERING MED ANVÄNDARNYCKLAR: <i>Erbjuder molnleverantören funktioner för kryptering på serversidan (SSE) med hjälp av krypteringsnycklar som kunden tillhandahåller?</i>
19.	OBJEKTLAGRING – TJÄNST FÖR NYCKELHANTERING: <i>Stödjer molnleverantören kryptering på serversidan (SSE) genom att använda en tjänst för nyckelhantering som skapar krypteringsnycklar, definierar principer som kontrollerar hur nycklar kan användas och granskar nyckelanvändningen för att bekräfta att de används på rätt sätt?</i>
20.	OBJEKTLAGRING – PRIMÄRNYCKEL PÅ KLIENTSIDAN: <i>Erbjuder molnleverantören användare möjligheten att behålla kontrollen över krypteringsnycklarna och kryptera/dekryptera objekt på klientsidan?</i>
21.	OBJEKTLAGRING – STARK KONSISTENS: <i>Stödjer molnleverantören direkt konsistens för PUT-åtgärder för nya objekt?</i>
22.	OBJEKTLAGRING – DATAPLATS: <i>Erbjuder molnleverantören en stark regionbaserad isolering, så att objekt som lagras i en region aldrig lämnar regionen såvida inte användaren uttryckligen överför dem till en annan region?</i>
23.	OBJEKTLAGRING – REPLIKERING: <i>Erbjuder molnleverantören en funktion för replikering mellan regioner, som automatiskt replikerar objekt mellan olika regioner som användaren väljer själv?</i>
24.	OBJEKTLAGRING – VERSIONSHANTERING: <i>Stödjer molnleverantören versionshantering, dvs. möjligheten att lagra och upprätthålla flera versioner av samma objekt?</i>
25.	OBJEKTLAGRING – MÖJLIGHET ATT NEKA BORTTAGNING: <i>Erbjuder molnleverantören användarna möjligheten att markera att ett objekt inte kan tas bort?</i>

26.	OBJEKTLAGRING – MFA-BORTTAGNING: <i>Stödjer molnleverantören multifaktorautentisering (MFA) för borttagningsåtgärder som ett extra säkerhetsalternativ?</i>
27.	OBJEKTLAGRING – UPPLADDNING I FLERA DELAR: <i>Erbjuder molnleverantören möjligheten att ladda upp ett objekt som en uppsättning delar, där varje del är en sammanhängande del av objektets data och dessa objekt delar kan laddas upp oberoende av varandra och i valfri ordning?</i>
28.	OBJEKTLAGRING – TAGGAR: <i>Erbjuder molnleverantören möjligheten att skapa och koppla föränderliga, dynamiska taggar på objektnivå?</i>
29.	OBJEKTLAGRING – AVISERINGAR: <i>Erbjuder molnleverantören möjligheten att skicka aviseringar när vissa händelser inträffar på objektnivå (dvs. åtgärder som att lägga till/ta bort)?</i>
30.	OBJEKTLAGRING – LOGGAR: <i>Erbjuder molnleverantören möjligheten att generera revisionsloggar som innehåller detaljer om enskilda åtkomstförfrågningar, till exempel vem som gjorde förfrågningen, när förfrågningen gjordes, begärd åtgärd, svarsstatus och felkod?</i>
31.	OBJEKTLAGRING – INVENTERING AV OBJEKT: <i>Erbjuder molnleverantören en funktion för objektinventering för att ge användare möjligheten att snabbt visualisera objekt och deras status, så att användare snabbt kan hitta objekt med offentlig åtkomst?</i>
32.	OBJEKTLAGRING – INVENTERING AV METADATA: <i>Erbjuder molnleverantören en funktion för objektinventering för att ge användare möjligheten att snabbt visualisera objektens metadata?</i>
33.	OBJEKTLAGRING – OPTIMERING AV UPPLADDNINGAR: <i>Erbjuder molnleverantören möjligheten att dirigera data från nätverkets utkant till lagringstjänsten med hjälp av en optimerad nätverkssökväg?</i>
34.	OBJEKTLAGRING – FRÅGEFUNKTION: <i>Erbjuder molnleverantören användare möjligheten att köra frågor mot objektlagringstjänsten med hjälp av Structured Query Language-uttryck (SQL)?</i>
35.	OBJEKTLAGRING – HÄMTNING AV DELMÄNGDER: <i>Erbjuder molnleverantören användare möjligheten att hämta endast en delmängd av data från ett objekt med hjälp av enkla Structured Query Language-uttryck (SQL)?</i>
36.	FILLAGRINGSTJÄNST: <i>Erbjuder molnleverantören en enkel och skalbar fillagringstjänst som går att använda med instanser med beräkningskapacitet i molnet?</i>
37.	FILLAGRING – REDUNDANS: <i>Lagrar molnleverantören objekten i filsystemen redundant (dvs. katalog, fil och länk) i flera datacenter eller anläggningar för att få högre tillgänglighet och hållbarhet?</i>
38.	FILLAGRING – DATAELIMINERING: <i>Stödjer molnleverantören fullständig eliminering av data i fillager 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 Network File System-protokoll (NFS)?</i>
41.	FILLAGRING – SMB: <i>Stödjer molnleverantören Server Message Block-protokoll (SMB)?</i>
42.	FILLAGRING – KRYPTERING I VILA: <i>Har molnleverantörens fillagringstjänst stöd för kryptering i vila?</i>
43.	FILLAGRING – KRYPTERING VID ÖVERFÖRING: <i>Har molnleverantörens fillagringstjänst stöd för kryptering av data vid överföring?</i>
44.	FILLAGRING – VERKTYG FÖR DATAMIGRERING: <i>Erbjuder molnleverantören något verktyg för datamigrering 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 funktionen Write Once Read Many (WORM)?</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 Structured Query Language-uttryck (SQL)?</i>
50.	ARKIVLAGRING – SNABB HÄMTNING: <i>Erbjuder molnleverantören användare flera alternativ för datahämtningar med olika kostnader och hämtningstider?</i>
51.	ARKIVLAGRING – KRYPTERING I VILA: <i>Har molnleverantörens arkivlagringstjänst stöd för kryptering i vila?</i>
52.	LAGRING – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet ovan om lagring?</i> <i>Exempel:</i> <i>största volymstorlek</i> <i>högsta antal enheter kopplade till en instans</i> <i>högsta antal I/O-åtgärder per sekund</i> <i>största objektstorlek</i> <i>högsta antal objekt per lagringskonto</i> <i>högsta 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 självbetjänad återställning av lösenord?</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 AUTENTISERINGSUPPGIFTER: <i>Erbjuder molnleverantören användare möjligheten att skapa och ge betrodda användare tillfälliga autentiseringsuppgifter för säkerhetssystemen som är konfigurerade att gälla från några minuter till flera timmar?</i>
6.	ADMINISTRATION – ÅTKOMSTKONTROLL: <i>Erbjuder molnleverantören detaljerade åtkomstkontroller för resurserna i infrastrukturen?</i> • Vilka villkor kan i så fall användas med dessa kontroller (dvs. tid på dagen, ursprunglig IP-adress osv.)?
7.	ADMINISTRATION – INBYGGDA PRINCIPER: <i>Innehåller molnleverantörens infrastruktur inbyggda principer för åtkomstkontroll som kan kopplas till användare och grupper?</i>
8.	ADMINISTRATION – ANPASSADE PRINCIPER: <i>Erbjuder molnleverantörens infrastruktur möjligheten att skapa och anpassa principer för åtkomstkontroll som kan kopplas till användare och grupper?</i>
9.	ADMINISTRATION – PRINCIPSIMULATOR: <i>Erbjuder molnleverantören en mekanism för att testa åtkomstprincipernas effekter innan de läggs till i produktionen?</i>
10.	ADMINISTRATION – MFA FÖR MOLNET: <i>Stödjer molnleverantören användningen av multifaktorautentisering (MFA) som ytterligare ett lager åtkomstkontroll och autentisering i infrastrukturen?</i>
11.	ADMINISTRATION – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet ovan om administration?</i> <i>Exempel:</i> <i>högsta antal användare</i> <i>högsta antal grupper</i> <i>högsta antal hanterade principer.</i>

5. Säkerhet

	Krav
1.	SÄKERHET – BAKGRUNDSKONTROLLER: <i>Görs bakgrundskontroller på all personal hos molnleverantören som har tillgång till tjänstens infrastruktur (fysisk eller inte)?</i>
2.	SÄKERHET – FYSISK ÅTKOMST: <i>Hindrar molnleverantören de anställda från att komma åt tjänstens infrastruktur, såvida det inte föreligger ett särskilt problem, en ändringsbegäran eller någon liknande formell behörighet?</i>
3.	SÄKERHET – ÅTKOMSTLOGGAR: <i>Skapar molnleverantören loggar med de anställdas åtkomst till sin infrastruktur, där sådan åtkomst alltid loggas och lagras i minst 90 dagar?</i>
4.	SÄKERHET – INLOGGNING PÅ VÄRDAR: <i>Hindrar molnleverantören de anställda från att logga in på molntjänsternas värdar? Automatiserar leverantören istället alla uppgifter som utförs på värdarna där innehållet i dessa automatiserade jobb loggas och lagras i minst 90 dagar?</i>
5.	SÄKERHET – KRYPTERINGSNYCKLAR: <i>Erbjuder molnleverantören en tjänst för att skapa och kontrollera krypteringsnycklar som används för att kryptera användardata?</i>
6.	SÄKERHET – HANTERING AV ÅTKOMSTNYCKLAR: <i>Erbjuder molnleverantören möjligheten att identifiera när en åtkomstnyckel senast användes, rotera gamla nycklar och ta bort inaktiva användare?</i>
7.	SÄKERHET – NYCKLAR TILLHANDAHÅLLNA AV KUNDER: <i>Erbjuder molnleverantören användare möjligheten att importera nycklar från den egna infrastrukturen för nyckelhantering till molntjänstleverantörens nyckelhanteringstjänst?</i>
8.	SÄKERHET – INTEGRERING MED TJÄNSTER FÖR KRYPTERINGSNYCKLAR: <i>Kan molnleverantörens nyckelhanteringstjänst integreras med andra molntjänster för att tillhandahålla en funktion för datakryptering i vila?</i>
9.	SÄKERHET – HSM: <i>Erbjuder molnleverantören särskilda fysiska säkerhetsmoduler (HSM), dvs. maskinvaruenheter som tillhandahåller säker nyckellagring och krypteringsåtgärder i en säkerhetsmodul som kan motstå manipulering?</i>
10.	SÄKERHET – KRYPTERINGSNYCKLARNAS HÅLLBARHET: <i>Stödjer molnleverantören varaktighet för nycklar, bland annat genom att lagra flera kopior så att nycklarna finns tillgängliga när de behövs?</i>
11.	SÄKERHET – SSO: <i>Erbjuder molnleverantören en förvaltd tjänst för enkel inloggning (SSO) som ger användare centralt hanterad åtkomst till flera konton och företagsprogram?</i>
12.	SÄKERHET – CERTIFIKAT: <i>Erbjuder molnleverantören en hanterad tjänst för att tillhandahålla, hantera och distribuera certifikat för Secure Sockets Layer (SSL) och Transport Layer Security (TLS)?</i>
13.	SÄKERHET – FÖRNYELSE AV CERTIFIKAT: <i>Underlättar molnleverantörens tjänst för hantering av certifikat förnyelse av certifikat?</i>

14.	SÄKERHET – WILDCARD-CERTIFIKAT: <i>Stödjer molnleverantörens certifikatshanteringstjänst användningen av wildcard-certifikat?</i>
15.	SÄKERHET – CERTIFIKATUTFÄRDARE: <i>Fungerar molnleverantörens certifikatshanteringstjänst även som en certifikatutfärdare (CA)?</i>
16.	SÄKERHET – ACTIVE DIRECTORY: <i>Erbjuder molnleverantören en hanterad Microsoft Active Directory-tjänst (AD) i molnet?</i>
17.	SÄKERHET – LOKAL ACTIVE DIRECTORY: <i>Stödjer molnleverantörens hanterade Microsoft Active Directory-tjänst (AD) integrering med Microsoft Active Directory (AD) på plats?</i>
18.	SÄKERHET – LDAP: <i>Stödjer molnleverantörens hanterade Microsoft Active Directory-tjänst (AD) Lightweight Directory Access Protocol (LDAP)?</i>
19.	SÄKERHET – ACTIVE DIRECTORY: <i>Stödjer molnleverantörens hanterade Microsoft Active Directory-tjänst (AD) Security Assertion Markup Language (SAML)?</i>
20.	SÄKERHET – HANTERING AV AUTENTISERINGSUPPGIFTER: <i>Erbjuder molnleverantören en förvaltd tjänst som hjälper användare att enkelt rotera, hantera och hämta autentiseringsuppgifter, till exempel nycklar för programmeringsgränssnittet (API), autentiseringsuppgifter för databaser och andra hemligheter?</i>
21.	SÄKERHET – WAF: <i>Erbjuder molnleverantören en web application firewall (WAF) som hjälper till att skydda webbprogram mot vanligt förekommande hot på webben som kan påverka tillgängligheten, äventyra säkerheten eller förbruka kostsamma resurser?</i>
22.	SÄKERHET – DDOS: <i>Erbjuder molnleverantören en tjänst som skyddar mot vanliga, mest förekommande överbelastningsattacker (DDoS) mot nätverks- och transportlagren tillsammans med möjligheten att skriva anpassade regler för att minska avancerade angrepp mot programlagret?</i>
23.	SÄKERHET – SÄKERHETSREKOMMENDATIONER: <i>Erbjuder molnleverantören en tjänst för att automatiskt bedöma potentiella sårbarheter i program och resurser?</i>
24.	SÄKERHET – UPPTÄCKT AV HOT: <i>Erbjuder molnleverantören en förvaltd tjänst för upptäckt av hot?</i>
25.	SÄKERHET – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet ovan om säkerhet?</i> <i>Exempel:</i> <i>högsta antal kundhuvudnycklar</i> <i>högsta antal fysiska säkerhetsmoduler (HSM-enheter).</i>

6. Lagefterlevnad

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
☐ C5 [Tyskland]	☐ EU:s dataskyddsdirektiv	☐ CDSA
☐ CISPE:s Data Protection Code of Conduct	☐ EU:s modellklausuler	
☐ CNDP (Climate Neutral Data Centre Pact)		
☐ DIACAP	☐ FERPA	☐ CIS
☐ Nivå 2 och 4 i DoD SRG	☐ GDPR	☐ Informationstjänster om straffrätt (CJIS)
☐ FedRAMP	☐ GLBA	☐ Cybersäkerhetsakten
☐ FIPS 140-2	☐ HIPAA	☐ EU-US Privacy Shield
☐ HDS (Frankrike, sjukvård)	☐ HITECH	☐ EU Safe Harbor
☐ ISO 9001	☐ IRS 1075	☐ FISC
☐ ISO 27001	☐ ITAR	☐ FISMA
☐ ISO 27017	☐ PDPA – 2010 [Malaysia]	☐ G-Cloud [Storbritannien]
☐ ISO 27018	☐ PDPA – 2012 [Singapore]	☐ GxP (del 11 i FDA CFR 21)
☐ IRAP [Australien]	☐ PIPEDA [Kanada]	☐ ICREA
☐ Nivå 3 av MTCS [Singapore]	☐ Privacy Act [Australien]	☐ IT Grundschutz [Tyskland]
☐ Nivå 1 av PCI DSS	☐ Privacy Act [Nya Zeeland]	☐ MARS – E
☐ SEC Rule 17-a-4(f)	☐ Spansk DPA-auktorisering	☐ MITA 3.0
☐ SOC1/ISAE 3402	☐ Storbritanniens DPA – 1988	☐ MPAA
☐ SOC2/SOC3	☐ VPAT/avsnitt 508	☐ NIST
☐ SWIPO:s uppförandekod för IaaS		
		☐ Nivåer från Uptime Institute
		☐ Storbritanniens Cloud Security Principles

Genom att använda rapporterna ovan om efterlevnad 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.

- **Granskat tillträde:** molntjänstleverantören bör begränsa det fysiska tillträdet till de personer som måste befinna sig på en plats av en motiverad affärsanledning. Om tillträde tillåts bör det återkallas så snart det nödvändiga arbetet är utfört.
- **Kontrollerat och övervakat tillträde:** det bör vara en kontrollerad process att gå in i utkanten av datacenter. 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 tillträde till områden som blivit godkända i förväg.
- **Personal i molntjänstleverantörens datacenter:** molntjänstleverantörens anställda som regelbundet behöver åtkomst till ett datacenter bör få tillträde 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 datacentrens områden med hjälp av videoövervakning, intrångsdetektering och övervakningssystem med åtkomstloggar. Ingångar bör säkras med enheter som aktiverar ett larm om en dörr tvingas upp eller hålls öppen.
- **Global säkerhet för molntjänstleverantörens datacenter:** molntjänstleverantören 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 fysiskt tillträde samt 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:** tillträdet till infrastrukturlagret bör vara begränsad baserat på affärsbehov. Genom att använda en åtkomstgranskning per lager beviljas inte tillträde till alla 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 utrustning och verktyg i datacentren bör vara en del av den regelbundna verksamheten i molntjänstleverantörens datacenter.
- **Reservutrustning för nödsituationer:** reserver för vatten, ström, telekommunikation och internetanslutning bör vara utformade med redundans så att molntjänstleverantören kan upprätthålla en kontinuerlig drift i en nödsituation. Elektriska kraftsystem bör vara fullständigt redundanta så att enheter som ger en 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 ytterligare minskar risken för avbrott i tjänsterna.
- **Teknik och människor samarbetar för att ge en ökad säkerhet:** det bör finnas obligatoriska processer för att få tillträde till datalagret. Detta inkluderar att behöriga personer granskar och godkänner en persons ansökan om tillträde. Dessutom bör detekteringssystem för hot och elektroniska intrång 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.
- **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.

- **Serverar 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 kassera media genom att använda tekniken som anges i NIST 800-88. Molnleverantören fortsätter att kontrollera media som har lagrat kunddata tills de har kasserats på ett säkert sätt.
- **Tredjepartsrevisorer verifierar molntjänstleverantörens rutiner och system:** molntjänstleverantören bör granskas av externa revisorer 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 revisorer intervjua molntjänstleverantörens anställda om hur de hanterar och kasserar media. Revisorer kan även titta på video från säkerhetskamerorna och observera ingångar och korridorer i ett datacenter. De kan även undersöka utrustning, till exempel molntjänstleverantörens elektroniska enheter för åtkomstkontroll och säkerhetskameror.
- **Förberedd för det oväntade:** molntjänstleverantören bör proaktivt förbereda sig för potentiella hot från omgivningen, 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 tillgänglighetszoner:** molntjänstleverantören bör tillhandahålla flera tillgänglighetszoner för att ge en ökad feltolerans. Varje tillgänglighetszon bör bestå av ett eller flera datacenter, vara fysiskt åtskilda och ha redundant ström och nätverk. Tillgänglighetszoner bör vara anslutna till varandra via snabba, privata fiberoptiska nätverk för att göra det möjligt att utforma program som automatiskt skapar redundans mellan tillgänglighetszonerna utan avbrott.
- **Simulera avbrott och mätta 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 korrigerande 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 risker från omgivningen bör molntjänstleverantören även införa överväganden kring hållbarhet i datacentrets utformning. Molntjänstleverantören bör tillhandahålla information om sitt åtagande 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. Datacentrens utplaceringar bör väljas med omsorg för att minska risker från omgivningen, till exempel översvämningar, svåra väderförhållanden och seismisk aktivitet. Molntjänstleverantörens tillgänglighetszoner bör vara oberoende av varandra och vara fysiskt åtskilda.
- **Redundans:** datacentren bör utformas för att förebygga och tolerera fel samtidigt som de bibehåller tjänsternas nivåer. Om ett fel inträffar bör automatiska processer föra bort 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 återuppta driften om ett avbrott inträffar. Kritiska systemkomponenter bör säkerhetskopieras till flera isolerade platser. Varje plats eller tillgänglighetszon bör vara utformad för att drivas oberoende av varandra med hög tillförlitlighet. Tillgänglighetszoner bör vara anslutna så att program automatiskt kan skapa redundans mellan tillgänglighetszonerna utan avbrott. Stor motståndskraft och tillgänglighet till tjänsterna bör vara inbyggd i systemets utformning. Datacenterdesignen med tillgänglighetszoner och datareplikering bör ge molntjänstleverantörens kunder extremt korta återställningstider och mål för återställningspunkter samt högsta möjliga tillgänglighet till tjänsterna.

- **Kapacitetsplanering:** molntjänstleverantören bör övervaka tjänstanvändningen kontinuerligt för att distribuera infrastruktur som stödjer åtaganden kring 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 avbrott på grund av omgivningen. Den ska innehålla information 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 testerna bör molntjänstleverantören dokumentera personalens och processernas prestationer, korrigeringar, åtgärder och lärdomar med syftet att ständigt förbättra dem.
- **Pandemirespons:** molntjänstleverantören bör införa policyer och rutiner för pandemirespons i planeringen för haveriberedskap för att snabbt kunna reagera på hot från 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 myndigheter och föreskrifter inom sjukvården, bland annat kontaktpunkter för internationella myndigheter.

ÖVERVAKNING och LOGGNING

- **Granskning av tillgång till datacenter:** tillgången till datacenter bör granskas regelbundet. Tillgången ska återkallas automatiskt när en anställd tas bort från molntjänstleverantörens HR-system. När en anställd eller leverantörs tillgång upphör i enlighet med varaktigheten för den godkända förfrågnings ska denna åtkomst återkallas, även om personen fortfarande är anställd hos molntjänstleverantören.
- **Loggar över tillgång till datacenter:** fysisk tillgång till molntjänstleverantörens datacenter bör loggas, övervakas och lagras. Molntjänstleverantören bör använda information som hämtas från logiska och fysiska övervakningssystem för att öka säkerheten utefter behov.
- **Övervakning av tillgång 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 tillgångsaktiviteter på datacentret, utrusta lokala team och andra supportteam så att de kan reagera på säkerhetsincidenter genom att prioritera, konsultera, analysera och svara på situationen.

ÖVERVAKNING och UPPTÄCKT

- **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 tillgång 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 att få tillgång till datacenter. Ingångar till serverrum bör säkras med enheter som aktiverar ett larm för att inleda incidentrespons om en dörr tvingas upp eller hålls öppen.
- **Inträngsdetektering:** elektroniska system för inträngsdetektering 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 använder multifaktorautentisering innan inträde eller utträde beviljas. Dessa enheter aktiverar ett larm om dörren tvingas upp utan autentisering eller hålls öppen. Larmenheterna för dörrarna bör även konfigureras att upptäcka tillfällen då en person lämnar eller går in i ett datalager utan att använda multifaktorautentisering. Larm bör omedelbart skickas till molntjänstleverantörens säkerhetscenter som arbetar dygnet runt för att omedelbart logga, analysera och svara på dem.

ENHETSHANTERING

- **Hantering av tillgångar:** molntjänstleverantörens tillgångar bör hanteras centralt via ett system för inventeringshantering 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.
- **Kassering av media:** molntjänstleverantören bör klassificera medielagringsenheter 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 kasseras när de inte längre är användbara. När en lagringsenhet har nått slutet av sin livslängd ska molntjänstleverantören kassera media genom att använda tekniken som anges i NIST 800-88. Molnleverantören ska fortsätta att kontrollera media som har lagrat kunddata tills de har kasserats på ett säkert sätt.

SYSTEM FÖR DRIFTMÄSSIGT STÖD

- **Ström:** molntjänstleverantörens elektriska kraftsystem i datacentren bör vara fullständigt redundanta och kunna upprätthållas dygnet runt utan att driften påverkas. 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 värmen och hålla en lämplig driftstemperatur för servrar och annan maskinvara för att förhindra överhettning och minska risken för serviceavbrott. Både personal och system bör övervaka och reglera temperaturen och fuktigheten till lämpliga nivåer.
- **Avkänning och bekämpning av brand:** molntjänstleverantörens datacenter bör vara utrustade med automatisk avkänning och utrustning för eventuella bränder. System för brandavkänning bör använda sensorer som känner av rök i nätverks- och infrastrukturutrymmen samt i mekaniska utrymmen. Dessa områden bör dessutom skyddas med system för brandbekämpning.
- **Läckageupptäckt:** 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 ytterligare eventuella vattenskador.

UNDERHÅLL AV INFRASTRUKTUR

- **Underhåll av utrustning:** molntjänstleverantören bör övervaka och utföra förebyggande underhåll på elektrisk och mekanisk utrustning för att upprätthålla systemens kontinuerliga drift i molntjänstleverantörens datacenter. Underhållsrutinerna för utrustningen bör utföras av kvalificerade 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 system för fastighetsförvaltning och övervakning av strömtillförseln. 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 för datacentren. Pågående bedömningar och minskande av risken 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 risker kring regler och miljö.
- **Säkerhetsintyg från tredje part:** tredjepartstestning av molntjänstleverantörens datacenter, som dokumenterats i tredjeparttrapporterna, bör säkerställa att molntjänstleverantören har implementerat lämpliga säkerhetsåtgärder i enlighet med de upprättade regler som krävs för att erhålla säkerhetscertifikat. Beroende på efterlevnadsprogram och dess krav kan externa revisorer utföra tester på kassering av media, granska videor från säkerhetskameror, observera ingångar och korridorer i ett datacenter, testa elektroniska enheter för åtkomstkontroll och undersöka datacentrets utrustning.

7. Migreringar

	Krav
1.	MIGRERINGSTJÄNST: <i>Hur många olika tjänster för datamigrering erbjuder molnleverantören?</i>
2.	MIGRERINGAR – CENTRALISERAD ÖVERVAKNING: <i>Erbjuder molnleverantören organisationer en centraliserad tjänst (dvs. en översikt) som de kan använda för att spåra och övervaka statusen för migrering av servrar och program?</i>
3.	MIGRERINGAR – INSTRUMENTPANEL: <i>Erbjuder molnleverantörens migreringsverktyg en instrumentpanel som snabbt visualiserar migreringsstatus, relaterade mätningar och migreringshistorik?</i>
4.	MIGRERINGAR – VERKTYG FRÅN MOLNLEVERANTÖREN: <i>Erbjuder molnleverantörens migreringsverktyg integration med andra migreringsverktyg från molnleverantören som kan utföra migrering av servrar och program?</i>
5.	MIGRERINGAR – VERKTYG FRÅN TREDJE PART: <i>Erbjuder molnleverantörens migreringsverktyg möjligheten att använda migreringsverktyg från tredje part?</i> • Vilka migreringsverktyg från tredje part stöds i så fall?
6.	MIGRERINGAR – MIGRERINGAR I FLERA REGIONER: <i>Erbjuder molnleverantörens migreringsverktyg möjligheten att spåra och övervaka migrering av servrar och program som sker i olika regioner?</i>
7.	MIGRERINGAR – SERVERMIGRERING: <i>Erbjuder molnleverantörens migreringsverktyg ett sätt att migrera lokala, virtualiserade servrar till molnet?</i> • Vilka virtualiserade miljöer stöds i så fall för tillfället?
8.	MIGRERINGAR – SERVERUPPTÄCKT: <i>Erbjuder molnleverantörens migreringsverktyg möjligheten att automatiskt hitta lokala, virtuella servrar som ska migreras till molnet?</i>
9.	MIGRERINGAR – DATA FÖR SERVERPRESTANDA: <i>Erbjuder molnleverantörens migreringsverktyg möjligheten att samla in och visa servrars eller virtuella maskiners prestanda som användningen av CPU eller RAM?</i>
10.	MIGRERINGAR – DISCOVERY-DATABAS: <i>Kan molnleverantörens migreringsverktyg lagra alla insamlade data i en centraliserad databas?</i> • Kan organisationer exportera dessa data i så fall? Till vilka format?
11.	MIGRERINGAR – KRYPTERING I VILA: <i>Krypterar molnleverantören all information i vila och lagrar den i discovery-databasen?</i>
12.	MIGRERINGAR – INKREMENTELL SERVERREPLIKERING: <i>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?</i> • Hur länge kan denna tjänst köras i så fall?

13.	MIGRERINGAR – VMWARE: <i>Stödjer molnleverantörens migreringsverktyg migreringar av virtuella VMWare-maskiner från lokala platser till molnet?</i>
14.	MIGRERINGAR – HYPER-V: <i>Stödjer molnleverantörens migreringsverktyg migreringar av virtuella Hyper-V-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> • Ange alla källdatabaser som kan migreras till molnet i så fall.
20.	MIGRERINGAR – HETEROGENA MIGRERINGAR: <i>Kan molnleverantörens migreringsverktyg utföra heterogena migreringar av databaser, dvs. från en källdatabas till en annan måldatabas, till exempel från Oracle till SQL Server?</i> • Ange i så fall alla möjliga kombinationer för heterogen databasmigrering.
21.	MIGRERINGAR – DATAMIGRERING I PETABYTESKALA: <i>Erbjuder molnleverantören en datatransportlösning i petabyteskala som överför stora mängder data till och från molnet med säkra apparater?</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 möjligheten att lagra och hämta objekt med hjälp av filprotokoll som Network File System (NFS)?</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 Internet Small Computer Systems Interface (iSCSI)?</i>

27.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – BANDÅTKOMST: <i>Erbjuder molnleverantörens säkerhetskopieringstjänst för företag 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 data i vila och vid överföring?</i>
29.	MIGRERINGAR – SÄKERHETSKOPIERING FÖR FÖRETAG – INTEGRERING AV PROGRAMVARA FRÅN TREDJE PART: <i>Kan molnleverantörens säkerhetskopieringstjänst för företag integreras med vanlig programvara för säkerhetskopiering från tredje part?</i>
30.	MIGRERINGAR – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet ovan om migrering?</i> <i>Exempel:</i> <i>högsta antal samtidiga migreringar av virtuella datorer</i> <i>högsta 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 molnerbjödanden?</i>
2.	FAKTURERING – LARM OCH AVISERINGAR: <i>Erbjuder molnleverantören en mekanism för att ställa in 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 uppskatta kommande kostnader?</i>
5.	FAKTURERING – SAMLAD ÖVERSIKT: <i>Erbjuder molnleverantören en mekanism för samlingsfakturerings med flera konton under ett primärt betalningskonto?</i>
6.	FAKTURERING – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet ovan om fakturering?</i> <i>Exempel:</i> <i>högsta antal konton som kan grupperas tillsammans</i> <i>högsta antal larm som kan skapas</i> <i>högsta antal budgetar som kan hanteras.</i>

9. Hantering

	Krav
1.	HANTERING – ÖVERVAKNINGSTJÄNST: <i>Erbjuder molnleverantören en övervakningstjänst för att hantera resurser och program i molnet som samlar in, övervakar och rapporterar med hjälp av fördefinierade mätningar?</i>
2.	HANTERING – LARM: <i>Erbjuder molnleverantörens övervakningstjänst möjligheten att ställa in larm?</i>
3.	HANTERING – ANPASSADE MÄTNINGAR: <i>Erbjuder molnleverantörens övervakningstjänst användare möjligheten att skapa och övervaka anpassade mätningar?</i>
4.	HANTERING – ÖVERVAKNINGENS DETALJNIVÅ: <i>Erbjuder molnleverantörens övervakningstjänst flera detaljnivåer, ned till en minut?</i>
5.	HANTERING – TJÄNST FÖR API-SPÅRNING: <i>Erbjuder molnleverantören en tjänst som loggar, övervakar och lagrar aktivitet mot molnresurser både på konsolen och på programmeringsgränssnittens (API) nivå för ökad synlighet?</i> • Vilka av molnleverantörens tjänster kan i så fall integreras med denna spårningstjänst?
6.	HANTERING – AVISERINGAR: <i>Erbjuder molnleverantören möjligheten att skicka ut aviseringar baserade på programmeringsgränssnittens (API) aktivitet?</i>
7.	HANTERING – KOMPRIMERING: <i>Erbjuder molnleverantören en mekanism för att komprimera loggar som genererats av programmeringsgränssnittens (API) spårningssystem för att hjälpa användare att sänka lagringskostnaderna relaterade till denna tjänst?</i>
8.	HANTERING – REGIONSAGGREGERING: <i>Erbjuder molnleverantören möjligheten att registrera programmeringsgränssnittens (API) aktivitet för konton i alla regioner och leverera denna information på ett samlat sätt som är enkelt att använda?</i>
9.	HANTERING – RESURSinVENTERING: <i>Erbjuder molnleverantören en tjänst för att bedöma, granska och utvärdera konfigurationerna av resurser som distribuerats av en användare?</i>
10.	HANTERING – ÄNDRINGAR I KONFIGURATIONER: <i>Loggar molnleverantören automatiskt konfigurationsändringar för resurser när de sker?</i>
11.	HANTERING – KONFIGURATIONSHISTORIK: <i>Erbjuder molnleverantören möjligheten att undersöka resursers konfigurationer vid alla tidigare tillfällen?</i>
12.	HANTERING – KONFIGURATIONSGREGLER: <i>Erbjuder molnleverantören riktlinjer och rekommendationer för efterlevnad gällande etablering, konfigurerings och kontinuerlig övervakning?</i>
13.	HANTERING – RESURSMALLAR: <i>Erbjuder molnleverantören möjligheten att skapa, tillhandahålla och hantera en samling resurser i en malliknande form?</i>
14.	HANTERING – REPLIKERING AV RESURSMALLAR: <i>Erbjuder molnleverantören möjligheten att snabbt replikera dessa resursmallar i olika regioner för att potentiellt använda dem i situationer som kräver haveriberedskap (DR)?</i>

15.	HANTERING – UTFORMNING AV MALLAR: <i>Erbjuder molnleverantören ett lättanvänt grafiskt verktyg med dra och släpp-funktion som gör processen att skapa sådana resursmallar snabbare?</i>
16.	HANTERING – TJÄNSTKATALOG: <i>Erbjuder molnleverantören en tjänst för att skapa och förvalta en katalog med tjänster, dvs. servrar, virtuella maskiner, programvara, databaser osv.?</i>
17.	HANTERING – KONSOLÅTKOMST: <i>Erbjuder molnleverantören ett webbaserat användargränssnitt för att underlätta hanteringen och övervakningen av molntjänster?</i>
18.	HANTERING – ÅTKOMST VIA KOMMANDORAD: <i>Erbjuder molnleverantören ett enhetligt verktyg för att hantera och konfigurera flera molntjänster via en kommandorad (CLI) och möjliggör de automatisk hantering av uppgifter med hjälp av skript?</i>
19.	HANTERING – MOBIL ÅTKOMST: <i>Erbjuder molnleverantören en app för smartphones som gör att användare kan ansluta till molntjänsten och hantera sina resurser?</i> • Är denna app i så fall tillgänglig för både iOS och Android?
20.	HANTERING – BÄSTA PRAXIS: <i>Har molnleverantören en tjänst som hjälper användare att jämföra sin molnanvändning med bästa praxis?</i>
21.	HANTERING – TJÄNSTGRÄNSER: <i>Har molnleverantören några begränsningar (dvs. tjänstgränser) vad gäller avsnittet ovan om hantering?</i> <i>Exempel:</i> <i>högsta antal konfigurationsregler per konto</i> <i>högsta antal larm som kan skapas</i> <i>högsta 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 en 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: <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 från översikten över tjänsternas tillstånd från ett år tillbaka?</i>
8.	SUPPORT – RÅDGIVARE FÖR MOLNET: <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 Technical Account Manager (TAM) som tillhandahåller teknisk expertis för alla molntjänster?</i>
10.	SUPPORT – SUPPORT FÖR PROGRAM FRÅN TREDJE PART: <i>Erbjuder molnleverantören support för vanliga operativsystem och vanliga komponenter av en programstack?</i>
11.	SUPPORT – OFFENTLIGT API: <i>Erbjuder molnleverantören ett offentligt programmeringsgränssnitt (API) för programmatisk hantering av supportärenden för att skapa, redigera och stänga dem?</i>
12.	SUPPORT – TJÄNSTDOKUMENTATION: <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 – DOKUMENTATION OM KOMMANDORADEN: <i>Erbjuder molnleverantören offentlig teknisk dokumentation av bra kvalitet för sin kommandorad (CLI)?</i>
14.	SUPPORT – REFERENSARKITEKTURER: <i>Erbjuder molnleverantören en kostnadsfri samling av dokument med referensarkitektur 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 procedurer (bland annat bästa praxis) för att implementera vanliga lösningar (dvs. DevOps, stordata, datalager, Microsoft-arbetsbelastningar, SAP-arbetsbelastningar osv.) i sina molnerbudanden, som är detaljerade, testade, validerade och steg för steg?</i>

Bilaga B – Teknisk utvärdering i realtid

Det är viktigt att bedöma molnplattformens kapacitet "live" med hjälp av molntjänstleverantörens offentligt tillgängliga tjänster och infrastruktur när man ska välja en leverantör. Vi rekommenderar minst en hel dag för teknisk utvärdering per kortlistad molntjänstleverantör. Under utvärderingen kan du: 1) genomföra en djupgående utvärdering för att bedöma om den uppvisade kapaciteten stämmer överens med kraven i er offertbegäran och molntjänstleverantörens skriftliga svar, 2) ge era experter en plattform för att undersöka molntjänstleverantören för att säkerställa att den passar och stämmer överens med era specifika tekniska och organisatoriska behov, och 3) få förtroende för molntjänstleverantörens tjänster och förmåga att skalas upp, fungera säkert, fungera på ett motståndskraftigt sätt och fortsätta att innovera för att möta framtida behov.

När molntjänstleverantörer svarar på kraven i en offertförfrågan för molntjänster kan det hända att de anger att de uppfyller kraven baserat på en tolkning av kraven på hög nivå, vilket saknar det fullständiga sammanhanget av en organisations driftsmiljö/programbehov. Vi rekommenderar att du tillsätter en teknisk utvärderingspanel med ledande experter inom teknik, drift, säkerhet och program. Utvärderarna bör utmana leverantörerna under hela utvärderingen, och som bästa praxis bör de poängsätta leverantörerna oberoende av varandra genom att betygsätta scenarier på en fastställd skala, t.ex. 0–4 (0 = Oacceptabelt, 1 = Marginellt, 2 = Acceptabelt, 3 = Bra, 4 = Utmärkt). Efteråt kan värdena för demonstrationerna konsolideras och den genomsnittliga värderingen för varje utvärderingsscenario räknas samman till den övergripande utvärderingen av molntjänstleverantören. Scenarier med hög standardavvikelse bör diskuteras i utvärderingsgruppen innan de färdigställs. När poängen har sammanställts kan en viktning baserad på hur kritiska de olika scenarierna är tillämpas.

När det gäller demonstrationens omfattning rekommenderar vi att du ser på molntjänstleverantörens plattform som helhet och sedan går djupare för att utvärdera specifika arbetsbelastningar som körs på plattformen. Nedan följer en exempelutvärdering av en plattform och arbetsbelastning. Organisationer kan bygga vidare på denna grund eller anpassa den för att se till att den valda leverantören uppfyller deras specifika funktionella och icke-funktionella krav. Som bästa praxis kan leverantörer som får en lista över scenarier och krav få föreslå en dagordning för den direkta utvärderingen som maximerar omfånget och inkluderar 20 % av tiden för frågor och svar.

Utvärdering av plattformen: flera CISP:er har antagit termen "Well Architected" för att hänvisa till ett tillvägagångssätt för molnet som ger ett så stort värde och så små risker som möjligt. Well Architected-scenarier i en teknisk demonstration i realtid kan omfatta följande:

1. **Säkerhet:** identitet, centraliserad styrning, automatiserad upptäckt av hot, dataskydd, beredskap inför händelser.
2. **Prestandaeffektivitet:** rätt dimensionering, skalbarhet/elasticitet, serverlöshet.
3. **Tillförlitlighet:** hög tillgänglighet (motståndskraft mot fel), minskad risk för förändringar, haveriberedskap, säkerhetskopiering.
4. **Kostnadsförvaltning:** finansiell verksamhet, kommersiell optimering, budgetar och kostnadsfördelning.
5. **Operativ kompetens:** automatisering, övervakning, support, förvaltning och kapacitet som krävs för att migrera till och arbeta i molnet.

Utvärdering av arbetsbelastningen: i en vanlig uppsättning programtyper som kan demonstreras finns bland annat:

- **Webbapplikation:** att vara en offentlig värd för en dynamisk webbplats, inklusive en backend-databas och statisk objektlagring.
- **Dataanalys:** en arkitektur med en data lake eller ett lake house som möjliggör konsolidering av data från olika dataleverantörer och förmågan att hantera stora volymer (terabytes/petabytes av data), variation (strukturerad, ostrukturerad, olika format etc.) och hastighet (hastighet av datagenerering, förändring och frågemönster).

- **Plattform för data science:** en plattform som gör det möjligt att utveckla, distribuera och använda funktioner baserade på AI/ML i hela organisationen.
- **IoT-tillämpning:** en IoT-plattform/funktion som sträcker sig över molnet, en nätverksfunktion och enheterna.

För varje representativ arbetsbelastning som är viktig för din organisation kan du definiera de scenarier som molntjänstleverantören ska demonstrera. Scenarierna bör visa övergripande kapacitet som gör det möjligt att implementera arbetsbelastningen på ett sätt i enlighet med Well Architected. Följande sidor innehåller exempel på tekniska utvärderingskriterier för 1) molntjänstleverantörens plattform och 2) ett exempel på arbetsbelastningen för en webbapplikation.

Plattform – exempel på en teknisk utvärdering i realtid

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Sec.1	Identitetsfederering	4	Visa förmågan att federera från ett befintligt identitetslager till molntjänsten.	• Stöd för standardprotokoll som SAML. • Stöd för SCIM-baserad identitetsreplikering. • Möjligheten att definiera olika åtkomstnivåer i företagets identitetsarkiv och få dem tillämpade hos molnleverantören. • Möjligheten att begränsa specifika team/individer till endast vissa konton/projekt/arbetsbelastningar. • Förmåga att stödja attributbaserad åtkomstkontroll (ABAC) och använda dessa attribut i molnleverantörens system för identitets- och åtkomsthantering (IAM) för att kontrollera åtkomst till molnresurser.
Plat.Sec.2	Central styrning	4	Visa förmågan att definiera principer och krav centralt, på organisationsnivå (globala principer) och även på affärsenhets- och projektnivå.	• Principen bör omfatta följande: aktivera/avaktivera tjänster, tillämpa geografiska begränsningar (begränsa regioner). • Principen bör också hindra användare, inklusive administratörer, från att inaktivera kontroller för granskning och styrning.
Plat.Sec.3	Begränsning av användarbehörighet	3	Visa de automatiska rekommendationerna för att skärpa användarbehörigheter.	• Möjlighet att jämföra nuvarande behörigheter med nödvändiga behörigheter. • Automatisk generering av principer för att främja användning av lägsta behörighet.
Plat.Sec.4	Revisionsloggning	4	Visa revisionsloggning av molnaktivitet, inklusive både tillåtna och otillåtna åtgärder.	• Centraliserade loggar för hela organisationen. • Konto-/projektspecifika loggar för att stödja spårning och ansvarsskyldighet på låg nivå. • Verktyg för att göra det möjligt att söka i loggar. • Verktyg som gör det möjligt att utlösa åtgärder baserat på specifika händelser/loggposter. • Möjlighet att se aktiviteter för leverantörssupport. • Möjlighet att förhindra att loggar tas bort, även av administratörer.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Sec.5	Nätverksisolering	4	Visa och bevisa om möjligt isoleringen av olika instanser i molnet. Demonstrera konfigurationen av isolerade (utan anslutning), privata (utan Internet) och offentliga (med tillgång till Internet) undernät.	• Separering av instanser, även när det gäller VPN- och korskopplingstjänster. • Möjlighet att styra trafikflödet från utanför molninfrastrukturen (på plats), inom den och till internet. • Hur separationen tillämpas vid användning av delade tjänster, t.ex. containervärdar eller funktion som tjänst.
Plat.Sec.6	Kryptering i vila	4	Visa förmågan att kryptera data i vila, inklusive alternativen för BYOK och kryptering på klientsidan.	• Möjlighet att kräva kryptering av känsliga uppgifter. • Möjlighet att använda antingen leverantörsstyrda nycklar eller kundstyrda nycklar. • Överensstämmelse med FIPS 140-2. • Möjlighet att varna för och logga brist på efterlevnad av krypteringskraven. • Ytterligare kostnadseffekter. • Prestandapåverkan. • Stöd för kvantumsäkra algoritmer och nyckelstorlekar.
Plat.Sec.7	Kryptering under överföring	4	Visa förmågan att kryptera data under överföring.	• Standardkryptering för tjänsternas API:er. • Möjlighet att aktivera kryptering under överföring (TLS) på lastbalanserare och hanterade API:er. • Stöd för ömsesidig autentisering (klient och server).
Plat.Sec.8	Nyckelhantering	4	Visa er förmåga att hantera nycklar. Inkludera hela nyckelns livscykel. Inkludera integration med andra molntjänster.	• Loggning av skapande, användning, rotation och kassering av nycklar.
Plat.Sec.9	Konfigurationshantering	3	Visa möjligheterna för konfigurationshantering i molnplattformen.	• Upprätthålla en korrekt konfigurationsdatabas. • Kontrollera efterlevnad av kraven. • Utlösa åtgärder baserat på bristande efterlevnad automatiskt. • Förmåga att utvärdera konfigurationsändringar mot bästa praxis eller anpassade regler.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Sec.10	Nätverkssäkerhet	3	Visa funktionerna för brandväggar och web application firewalls, inklusive integration med regeluppsättningar/brandväggar från tredje part och skydd mot volymmässiga attacker.	• Funktioner för WAF (web application firewall): skalbarhet. • Stöd för privata och offentliga nätverk. • Möjlighet att prenumerera på flöden för regeluppsättningar från branschen/leverantören. • Automatiskt utlösa åtgärder inom infrastrukturen baserat på händelser från WAF. • Brandväggsfunktioner, skalbarhet. • Värld- och nätverksbaserade brandväggar. • Möjlighet att hänvisa till logiska grupper eller objekt utöver möjligheten att ange CIDR-IP-block. • Antal regler som stöds på varje nivå/för varje komponent. • Förmåga att stödja en distribuerad verksamhetsmodell (nätverksteam + utvecklingsteam) genom princip- och nätverkskonfiguration.
Plat.Sec.11	Nätverksanslutning	3	Visa förmågan att ansluta till lokala nätverk samt slutpunkter/klienter till privata nätverk i molnet.	• Privat anslutning (hög bandbredd > 10 GB). • Möjlighet att styra routnings- och brandväggsprinciper i hela organisationen. • VPN-anslutning (plats till plats och klientbaserad). • Stöd för IPV6.
Plat.Sec.12	Instanshantering	3	Visa funktioner för instanshantering.	• Möjlighet att övervaka och hantera patchstatus för en stor mängd instanser. • Stöd för patchhantering för Linux- och Windows-operativsystem. • Möjlighet att utföra kommandon på en flotta servrar utan behov av SSH. • Möjlighet att centralt styra och granska fjärråtkomst till virtuella maskiner. • Möjlighet att ändra en instansstorlek, ansluta ytterligare volymer, ändra nätverkskonfiguration etc. via konsolen, kommandoraden och API.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Sec.13	Tillämpning av principer	3	Visa förmåga att konfigurera tjänster för att förhindra åtkomst från offentligt internet.	• Möjlighet att isolera trafik till privata nätverk för tjänster som sannolikt innehåller kritiska/sekretessbelagda uppgifter. • Möjlighet att definiera principer som kontrollerar åtkomst till data baserat på källnätverket. • Tillämpning av dessa åtkomstrestriktioner på alla användare, inklusive användare med autentiseringsuppgifter på hög nivå.
Plat.Sec.14	Söka efter sårbarheter	2	Visa förmågan att söka efter sårbarheter i avbildningar (containrar och virtuella maskiner).	• Möjlighet att automatiskt söka igenom containrar i ett register. • Möjlighet att söka efter kända sårbarheter i virtuella maskiner. • Förmåga att söka igenom nätverk.
Plat.Sec.15	Nätverksinspektion	2	Visa förmågan att spara/spegla nätverkstrafik (NetFlow och fullständiga paket) från en kunds miljö.	• Möjlighet att spegla en del av/all trafik inom molnleverantörens infrastruktur (från kundinstansens perspektiv), inklusive att spara hela paket. • Möjlighet att helt enkelt välja vilken trafik du vill spara. • Förmåga att skala upp till mycket stora trafikvolymmer (> 50 GBps).
Plat.Sec.16	Identifiering av hot	3	Demonstrera din plattforms förmåga att upptäcka intrång, inklusive hot från ett nätverk, användning av autentiseringsuppgifter och analys av användningsmönster.	• Möjlighet att upptäcka misstänkt verksamhet som "utvinning". • Möjlighet att upptäcka uttömmande autentiseringsattacker som SSH-inloggningar. • Möjlighet att upptäcka läckage eller missbruk av autentiseringsuppgifter. • Tillämpning av ML, analys av ett stort antal händelser och framtagning av prioriterade händelser. • Arbete för att aktivera/konfigurera (enkelt är bättre). • Möjlighet att integrera med externa tjänster och utlösa aviseringar. • Möjlighet att konfigurera IDS på global nivå för alla projekt/konton.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Perf.1	Optimering av beräkningskapacitet	2	Visa automatiska rekommendationer för optimering av kostnaderna för virtuella maskiner och funktioner som tjänst.	• Rekommendationer baserade på det faktiska mönstret i användning och arbetsbelastning. • Rekommendationerna omfattar uppskattade besparingar och insikter om förväntad belastningsnivå/tekniska konsekvenser. • Optimeringarna bör omfatta både besparingar och "prestandarisker" där virtuella maskiner till exempel kan vara underdimensionerade.
Plat.Perf.2	Miljöoptimering	2	Visa automatiska rekommendationer för andra komponenter i molnet, t.ex. lastbalanserare, nätverk, databaser, lagring osv.	• Rekommendationer som identifierar besparingar och potentiella möjligheter till effektivisering av prestanda i andra komponenter än den huvudsakliga beräkningskapaciteten.
Plat.Perf.3	Automatisk skalning av beräkningskapacitet	4	Visa den automatiska skalningskapaciteten hos ett program som distribueras bakom en lastbalanserare i en virtuell beräkningsmiljö. Visa de olika alternativ/metoder som finns tillgängliga och möjligheten att utlösa andra (valfria) åtgärder före/efter skalningshändelser, t.ex. en avisering.	• Olika alternativ för skalning, utlösarbaserade, tidsbaserade, manuella eller mer intelligenta metoder som tillämpar maskininlärning för att förutsäga den nödvändiga kapaciteten. • Helt automatiserad skalning, inklusive registrering med en lastbalanserare och hälsokontroller. • Möjligheten att köra godtycklig kod vid specifika punkter i skalningens livscykel.
Plat.Perf.4	Onlineskalning för lagring	3	Visa förmågan att skala både kapacitet och dataflöde för blocklagring utan avbrott i arbetsbelastningen.	• Möjlighet att överföra blocklagring mellan olika lagringstyper utan att behöva bygga om tjänsterna helt och hållet. • Möjlighet att öka storleken på de volymer som presenteras för virtuella maskiner.
Plat.Perf.5	Automatisk skalning för förvaldade tjänster	3	Visa att Object Store, API Gateway, FaaS-plattformen och NoSQL-databasen kan skalas från ett fåtal (10-tal) till många (1000-tal) samtidiga användare.	• Sömlös automatisk skalning, helst utan ingripande av administratör. • Konsekvent prestanda under en period av uppskalning som är i linje med produktionens skalningskrav. • För vissa komponenter, t.ex. FaaS, bör du även se över alternativen för föruppvärmning och hantering av gränser för samtidiga utföranden om det behövs.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Perf.6	Containerbaserade arbetsbelastningar	3	Visa förmågan att vara värd för containerbaserade arbetsbelastningar.	• Alternativ för värdplattformar för containrar. • Integrering med andra IaaS-komponenter, t.ex. lastbalanserare. • Tillgänglighet till en lösning med servicenät. • Generiska alternativ för containervärdar, t.ex. Kubernetes. • Inbyggt stöd för hög tillgänglighet inom kontrollplanet för containrar. • Möjlighet att hantera lokala containervärdar.
Plat.Rel.1	Regional motståndskraft	4	Visa hur en instans för relationsdatabaser inom en region gör en automatisk överlämning när ett geografiskt lokalt fel (t.ex. ett strömavbrott) simuleras.	• Automatisk överlämning vid fel. • Isolerade felzoner inom en molnregion. • Tydligt avgränsad och enkel att bygga upp för hög tillgänglighet.
Plat.Rel.2	Automatisk instansåterställning	2	Visa automatisk återställning av en instans/opsättning instanser efter en misslyckad hälsokontroll.	• Konfigurerbara hälsokontroller. • Helt automatiserad återhämtning/omtablering av instanser.
Plat.Rel.3	Lastbalanserarens hälsoavkänning	3	Visa hur en lastbalanserare automatiskt upptäcker en dåligt fungerande instans och omdirigerar trafiken till fungerande värdar.	• Konfigurerbara hälsokontroller. • Automatiserad omdirigering av trafik till fungerande värdar.
Plat.Rel.4	Automatisk överlämning mellan regioner vid fel	3	Demonstration av en arkitektur med flera regioner, inklusive automatiserad trafikflyttning till en sekundär region.	• Global avkänning för hälsokontroller. • Automatiserade routningsalternativ: svarstider, vägning och automatisk överlämning vid fel. • Stöd för arbetsbelastningar för virtuella maskiner samt förvaltade tjänster som databastjänster med objektlagring/NoSQL.
Plat.Rel.5	Säkerhetskopiering och återställning	4	Visa alternativen för säkerhetskopiering och återställning för: virtuella maskiner, databaser, förvaltade tjänster.	• Automatiseringsgrad. • Möjlighet att återställa till samma eller en annan molnregion.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
				Möjlighet att kopiera säkerhetskopior till en annan molnregion.
Plat.Cost.1	Budgetar	3	Visa förmågan till budgethantering, inklusive hur den ska struktureras för underkonton och projekt.	- Överväg förmågan att tillämpa budgetkontroller och övervakning på olika nivåer i organisationen. - Kontrollera om det finns flexibilitet, t.ex. möjligheten att gruppera komponenter (med taggar), fastställa budgetar för specifika molntjänster och konfigurera tröskelvärden för varningar/övervakning.
Plat.Cost.2	Budgettilldelning	1	Visa etableringen av en ny projektmiljö (konto), inklusive processen för budgettilldelning för projektet. Etableringen bör omfatta manuella godkännandesteg för 1) teknisk granskning/IT, 2) kommersiell granskning/finans.	- Förmåga till egenetablering med lämpliga godkännanden. - Automatisering av konfigurationen av lämpliga budgetinställningar, meddelanden eller budgetprinciper som är lämpliga för din organisation.
Plat.Cost.3	Budgetrapportering	2	Visa förmågan att rapportera om budgetar inom hela organisationen. Rapportering för en specifik avdelning jämfört med hela organisationen (utefter behovet av informationen). Rapporteringen bör omfatta såväl "faktiska" som förutsagda/uppskattade utgifter.	- Förmågan att ge insyn på olika nivåer i organisationen, vilket skapar medvetenhet och transparens, men endast efter behovet av informationen. - Uppskattningar bör baseras på nuvarande och tidigare konsumtionstrender och ge tidig varning för potentiella budgetöverskridanden.
Plat.Cost.4	Budgetkontroller	1	Visa förmågan att vidta åtgärder när ett tröskelvärde i budgeten har uppnåtts. Åtgärderna kan omfatta meddelanden, tillämpning av begränsningar eller aktiva ingripanden för att förhindra budgetöverskridanden.	- Möjligheten att enkelt definiera åtgärder för olika projekt. - Möjligheten för åtgärderna att variera från ett projekt till ett annat, t.ex. med hänsyn till konsekvenserna av skillnaderna mellan utveckling och produktion. - Möjligheten att definiera flera åtgärder och tröskelvärden för samma budget/projekt. - Möjligheten att definiera anpassade åtgärder utöver standardfunktionerna.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Cost.5	Budgetperioder	1	Visa förmågan att tillämpa budgetar för olika tidsperioder, dagligen/månadsvis/årligen osv. För årliga budgetar, visa förmåga att tillämpa en föränderlig fördelning av förväntade utgifter under hela året.	- Möjlighet att definiera budgetar för olika tidsperioder. - Möjlighet att konfigurera en fördelning av utgifter över året för årliga budgetar, vilket är särskilt viktigt för säsongsmässiga/mycket elastiska arbetsbelastningar som t.ex. en årlig skattedeklaration.
Plat.Cost.6	Marknadsplats för tredje part	3	Visa förmågan att köpa och använda produkter från tredje part. Visa hur man fastställer en budget för en uppsättning produkter från tredje part som är tillgängliga via en marknadsplats och hur man begränsar de tillgängliga produkterna.	- Möjlighet att fastställa en budget för en specifik produkt, en global budget, en budget för en uppsättning projekt/konton. - Möjlighet att endast presentera en delmängd av marknaden som helhet för molnanvändare.
Plat.Cost.7	Beräkna modeller för prissättning	3	Visa de olika modellerna för prissättning och kommersiella ändamål som kan tillämpas på virtuella maskiner.	- Bland alternativen bör finnas på begäran, utan krav på långsiktigt åtagande och detaljerad prissättning (per minut/timme). - Valfria långsiktiga åtaganden i utbyte mot en rabatt. - Möjlighet att köpa instanser som kan bli avbrutna i utbyte mot en rabatt. - Det är viktigt att det ska vara möjligt att blanda dessa modeller inom samma projekt/konto och att dela fördelarna mellan olika konton.
Plat.Cost.8	Rekommendationer för kommersiell optimering	3	Visa förmågan att ta emot rekommendationer om kommersiell optimering för att optimera utgifterna (utan att behöva göra tekniska ändringar).	- Helhetsrekommendationer för flera tjänster, till exempel virtuella maskiner och förvaltade databaser. - Förmåga att enkelt genomföra rekommendationer och förstå de förväntade besparingarna/fördelarna.
Plat.Cost.9	Dedikerade värdar	4	Visa förmågan att etablera en dedikerad värd för att göra det möjligt att använda lokala licenser som är knutna till en specifik värd.	- Lätt att etablera resurser. - Förmågan att hantera utnyttjandet av värden. - Möjligheten att dela värden mellan olika projekt/instanser.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Ops.1	Migrering av virtuella maskiner	3	Visa en import av en virtuell maskin från en lokal anläggning till en molnbaserad VM-tjänst.	• Möjlighet att importera både Windows- och Linuxbaserade operativsystem. • Möjlighet att importera flera maskiner på en gång. • Möjlighet att upprätthålla en replikeringsession för att möjliggöra snabb automatisk överlämning till molnet vid fel.
Plat.Ops.2	DevOps-funktioner och automatiseringsfunktioner	4	Visa DevOps- och automatiseringsförmågorna, inklusive hur miljöer definieras som kod, stöd för helt automatiserade distributioner, automatiserad testning och återkoppling.	• Förmåga att definiera alla systemkomponenter som kod, inklusive nätverk, virtuella maskiner, lagring och databaser. • Möjlighet att skapa en pipeline. • Möjlighet att skapa en lagringsplats för koder. • Möjlighet att automatisera byggandet. • Förmåga att genomföra blå/gröna distributioner. • Möjlighet att skapa flera miljöer och ha flera steg för distribution. • Automatiserad återgång till tidigare tillstånd för misslyckade distributioner.
Plat.Ops.3	Vara värd för program	2	Visa att ni kan vara värd för ett enkelt program i två nivåer i en tjänst som kräver lite kodning eller en plattformstjänst. Inklusive en relationsdatabas och automatisk skalning för program-/webblagret.	• Enkel konfiguration via användargränssnittet. • Inkludering av hälsokontroller, skalning, hög tillgänglighet. Plattformstöd, Windows och Linux.
Plat.Ops.4	Säkerhetsintegration	2	Visa plattformens integrationsmöjligheter ur perspektivet för hantering av säkerhetsincidenter och händelser.	• Möjlighet att enkelt integrera och använda säkerhetsrelaterade loggar från molnleverantören + API:er för integration.
Plat.Ops.5	ITSM-integration	3	Visa plattformens integrationsmöjligheter ur ett IT Service Management-perspektiv (ITSM).	• Möjlighet att ta upp, övervaka och uppdatera ett supportärende via ett API. • Möjlighet att tillhandahålla tjänster eller uppsättningar av tjänster som "produkter" via ett API.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Plat.Ops.6	Support	4	Visa ditt supporterbjudande.	- Olika supportnivåer för olika typer av arbetsbelastningar. - Förmåga att även stödja operativsystemet/databasmotorn etc. i enlighet med vad som är lämpligt för en viss tjänst. - Möjlighet att erbjuda ett VIP-erbjudande med namngivna supportansvariga för kritiska arbetsbelastningar. - Möjlighet att erbjuda en strukturerad process för beredskap för evenemang och granskning av arkitektur. - Insikt i leverantörens färdplan.
Plat.Ops.7	Revisionsmöjlighet	4	Visa vilka verktyg du har för att stödja revision av efterlevnad.	- Möjlighet att få information om efterlevnadsrevisioner via konsolen. - Förmåga att hantera och automatisera miljörevisioner.
Plat.Ops.8	VM till container	1	Visa konverteringen av ett program i en virtuell maskin till en container och att lägga ut den med hjälp av molnleverantörens behållarplattform.	- Enkel användning av konverteringen. - Konverteringstid. - Plattformsstöd, .Net och Java.

Arbetsbelastning: Webbapplikation – exempel på teknisk utvärdering i realtid

I följande avsnitt finns ett exempel på ett utvärderingsblad för en specifik arbetsbelastning för en "webbapplikation". När man utarbetar ett utvärderingsformulär för ett visst program rekommenderas det starkt att involvera programmets användare, utvecklare och administratörer, eftersom de sannolikt har den bästa förståelsen för kraven, de aktuella utmaningarna och begränsningarna.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Web.Sec.1	Säkerhet – programskydd	3	Visa er förmåga att blockera skadliga försök att utnyttja programmet genom SQL-injektioner, cross-site scripting-attacker (XSS) och andra attacker.	• Möjlighet att skydda mot vanliga attacker från första början med standardregler/kapaciteter. • Möjlighet att skapa egna kontroller/regler/funktioner.
Web.Sec.2	Säkerhet – skydd baserat på hastighet	3	Visa förmågan att blockera/skydda mot attacker med stora förfrågningshastigheter eller datamängder som riktas mot ett program.	• Möjlighet att konfigurera gränser och begränsa antalet förfrågningar från en viss IP-adress eller en lista med adresser.
Web.Sec.3	Säkerhet – skydd baserat på källa	3	Visa förmågan att begränsa åtkomst baserat på nätverk/geografisk källa.	• Möjlighet att begränsa genom nätverksblock eller en lista över nätverksblock. • Möjlighet att begränsa efter ursprungsland (utan att behöva hantera IP-listor).
Web.Sec.4	Säkerhet – nätverkssegmentering	4	Visa förmågan att isolera/skydda komponenter (webbserver, app-server/dataserver) för att skydda mot både nordlig-sydlig och östlig-västlig spridning genom infrastrukturen.	• Möjlighet att placera komponenter i olika undernät och styra trafikflödet mellan olika undernät. • Förmåga att styra trafikflödet på nätverkets gränssnittsnivå. • Möjlighet att hänvisa till logiska grupper och CIDR-block.
Web.Sec.5	Säkerhet – stöd för TLS och hantering av certifikat	4	Visa förmågan att leverera en TLS-säkrad slutpunkt och automatiskt hantera de stödjande komponenterna för att leverera detta, inklusive t.ex. automatisk rotation av certifikat.	• Stöd för de senaste TLS-protokollen och möjlighet att inaktivera äldre versioner vid behov. • Enkel generering, hantering och rotation av certifikat (helst helt automatiserat).
Web.Perf.1	Prestanda – skalbarhet	4	Visa din förmåga att skala från 10 till 100 000 samtidiga användare av webbapplikationen genom dynamisk automatisk skalning.	• Möjlighet att definiera tidsbaserade och utlösarbaserade skalningsregler. • Smidig skalning för slutanvändaren och administratören. Skala automatiskt ut när belastningen ökar och skala automatiskt in när belastningen minskar. • Se till att skalbarhet finns i varje lager av webbapplikationen (lastbalanserare, webblager, datalager osv.). • Tillgänglighet till cachetjänster i olika lager av programmet, när så är lämpligt.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Web.Perf.2	Prestanda – global leverans	3	Visa din CDN-kapacitet genom att demonstrera svarstider från olika punkter runt om i världen, inklusive: Australien, Asien, Afrika, Mellanöstern, Nordamerika, Sydamerika och Europa.	• Möjlighet att skapa och konfigurera ett CDN via CISP-konsolen/API:erna. • Konfigurerbara distributionsregler för olika geografiska områden. • Konfigurerbar cache för olika användningsfall/tillämpningar.
Web.Rel.1	Tillförlitlighet – motståndskraft i en enskild region	4	Visa förmågan att tolerera en lokal händelse, t.ex. en förlust av nätverksanslutning till molntjänstleverantörens datacenter.	• Automatisk överlämning vid fel och hög tillgänglighet inom en molnregion (stad).
Web.Rel.2	Tillförlitlighet – distribution i flera regioner	3	Demonstrera en distribution av en webbapplikation i flera regioner med en globalt replikerad databas.	• Möjlighet att programmatiskt distribuera ett program i flera regioner. • Replikering mellan regionerna för datalagret. • Automatiserad routning av användare till deras optimala region.
Web.Rel.3	Tillförlitlighet – automatisk överlämning vid fel med flera regioner	3	Visa en automatisk överlämning av en webbapplikation i händelse av ett problem med regional påverkan på tjänsten.	• Automatisk överlämning vid fel och hög tillgänglighet i flera molnregioner.
Web.Cost.1	Kostnad – synlighet	2	Visa förmågan att spåra kostnader per program.	• Möjlighet att visa kostnadshistorik för ett specifikt program, inklusive när det skalas upp/ned.
Web.Cost.2	Kostnad – budgetar	2	Visa förmågan att ställa in budgetar och relaterade varningar per program.	• Budgetar som konfigureras per program och möjlighet att utlösa åtgärder/varningar baserat på konfigurerade tröskelvärden.
Web.Ops.1	Ops – underhållstider	3	Visa förmågan att konfigurera underhållstider för att anpassa dem till verksamhetens krav, särskilt när underhållet kan påverka programmets tillgänglighet.	• Konfigurerbara underhållstider för komponenter som t.ex. en tjänst för en relationsdatabas.

Scenario-ID	Namn på scenariot	Kritisk nivå (1 = Låg, 4 = Kritisk)	Demonstrationskrav	Överväganden vid poängsättning
Web.Ops.2	Ops – loggning	3	Visa förmågan att centralisera loggningen för ett program med flera komponenter, inklusive loggningar vid avslutande av/fel i virtuella maskiner.	• Möjlighet att konfigurera en centraliserad loggningstjänst som kan skalas utefter programkraven. • Möjlighet att definiera regler/filter för att utlösa varningar eller åtgärder baserat på specifika logghändelser.
Web.Ops.3	Ops – övervakning	3	Visa övervakning av programmet, inklusive prestanda, tillgänglighet, svarstider, antal fel osv. och funktionalitet för att vidta åtgärder/skicka aviseringar baserat på olika mätbara tröskelvärden.	• En samling standardmätvärden finns tillgängliga, t.ex. disk IO, CPU, databasmätvärden, nätverk, lastbalanserare osv. • Möjlighet att definiera anpassade mätvärden, tröskelvärden. • Möjlighet att skapa en anpassad instrumentpanel som representerar de viktigaste mätvärdena och dela dessa instrumentpaneler med relevanta användare.