Køb af cloud-tjenester i den offentlige sektor

Håndbog, inklusive eksempel på formulering i en anmodning om tilbud (RFP) til en cloud-rammeaftale

Version 2: februar 2022

Bemærkninger

Dette dokument er kun til orientering. Det er ikke udarbejdet i overensstemmelse med lovpligtige krav til offentlige indkøbsprocesser i noget bestemt område. Cloud-kunder er ansvarlige for at foretage deres egen uafhængige vurdering af oplysningerne i dette dokument og af enhver brug af cloud-udbyderens produkter eller tjenester. Dette dokument giver ikke anledning til nogen garantier, erklæringer, kontraktlige forpligtelser, betingelser eller løfter.

Eksempler på dokumenter og formulering skal ikke betragtes som juridisk rådgivning, vejledning eller råd. Cloud-kunder bør tale med deres egne advokater om deres ansvar i henhold til den gældende lovgivning i det land, hvor de driver forretning. CISPE frasiger sig udtrykkeligt enhver form for garanti eller ansvar for skader i forbindelse med eller som følge af oplysningerne i dette dokument.

Om CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) er en selvstændig almennyttig branchegruppe. Vi repræsenterer udbydere af cloud-infrastruktur i hele Europa, og vi samarbejder med branchen og beslutningstagere om at tilbyde rådgivning og kurser i forbindelse med cloud-tjenester og deres rolle i brancher, det offentlige liv og samfundet som helhed.

Vi får stadig flere medlemmer, blandt andet virksomheder i alle EU-lande og 16 europæiske lande med hovedkvarterer andre steder i verden. Virksomheder er velkomne i foreningen, såfremt de erklærer, at mindst én af deres tjenester overholder kravene i CISPE's adfærdskodeks for databeskyttelse. Vi:

- Taler for fordelene ved indkøbspolitikker med fokus på cloud i EU og EU's medlemslande
- Inddrager cloud-infrastruktursektoren for at opnå klimaneutralitet inden 2030
- Promoverer sammenhængende sikkerhedskrav og tekniske standarder i hele EU
- Understøtter omfattende krav til beskyttelse af personlige oplysninger med en adfærdskodeks for beskyttelse af personlige oplysninger
- Arbejder for at holde EU's cloud-infrastruktur åben, konkurrencedygtig og fri for fastlåsning
- Forebygger ubegrundede forpligtelser til overvågning af indhold i EU's juridiske rammeværk

Vores medlemmer leverer og opretholder uundværlige "byggesten til it", der giver regeringer, offentlige myndigheder og virksomheder mulighed for at lave deres egne systemer og give milliarder af borgere adgang til uundværlige tjenester. Dermed er vi med til at realisere udviklingen af revolutionerende teknologier og tjenester med kunstig intelligens (AI), forbundne objekter, selvkørende biler og 5G samt den næste generation af mobil netværksteknologi.

Adfærdskodeks for cloud-infrastruktur-tjenester

CISPE's adfærdskodeks for databeskyttelse, der blev offentligt lanceret i september 2016, gik forud for ikrafttrædelsen af den generelle EU-forordning om databeskyttelse (GDPR). Det overholder de strenge krav i GDPR, for at hjælpe cloud-infrastrukturudbydere med at operationalisere overholdelse af databeskyttelse og tilbyde en solid ramme, der hjælper kunder med at vælge cloud-udbydere og have tillid til deres tjenester. CISPE's adfærdskodeks er blevet valideret af Det Europæiske Databeskyttelsesråd (EDPB) i maj 2021, og godkendt af den franske CNIL, der fungerer som den kompetente myndighed, i juni 2021. https://www.codeofconduct.cloud/

Pagt om klimaneutrale datacentre

CISPE samarbejdede i slutningen af 2019 med Europa-Kommissionen om at udvikle et sæt målepunkter og et selvreguleringsinitiativ for at sikre klimaneutralitet for datacentre inden 2030. Dette initiativ er blevet udviklet sammen med European Data Centre Association (EUDCA) og andre brancheorganisationer og aktører i datacenterindustrien - lanceret i januar 2021 som "Pagt om klimaneutrale datacentre" https://www.climateneutraldatacentre.net/

Fair Software-initiativet

Sammen med den franske CIO-sammenslutning CIGREF og med støtte fra andre brancheorganisationer for CIO'er og udbydere i hele Europa har CISPE lanceret Ti principper om rimelige software licensvilkår for cloud-kunder, et sæt af bedste praksis for virksomheder, der søger vækst, innovation og fleksibilitet i clouden, og som udfordrer deres softwareleverandører til at sikre fair licensvilkår.
https://www.fairsoftware.cloud/

GAIA-X

CISPE var et af de 22 stiftende medlemmer af GAIA-X – det europæiske initiativ til at skabe et åbent, gennemsigtigt og sikkert digitalt økosystem. CISPE har derfor fra starten været engageret i GAIA-X-organisationens vision og principper, og CISPEs generalsekretær er i juni 2021 blevet genvalgt til at sidde i bestyrelsen. Nogle af de værktøjer, som der henvises til i håndbogen, såsom CISPE's adfærdskodeks for databeskyttelse og SWIPO IaaS adfærdskodeks, er nyttige til at påvise overholdelse af GAIA-X-principperne. https://www.gaia-x.eu

CISPE og den offentlige sektor

CISPE bidrager til den europæiske offentlige politiske debat og har til formål at sikre en bedre forståelse af den europæiske cloud-infrastrukturbranches rolle, bidrag og potentiale.

Selv om de offentlige indkøbsmodeller bør fungere som en klargøring til processen for implementering og brug af cloudcomputing, så er anskaffelsen af cloud-tjenester anderledes end de fleste traditionelle teknologianskaffelser, som er kendt i den offentlige sektor. Det er nødvendigt at gentænke indkøbsmetoder: CISPE opfordrer politikere i EU til at udvikle en mere ambitiøs og fremadrettet tilgang på EU-skala, som er baseret på politikinitiativer med "primært fokus på cloud", hvilket er med til at skabe vækst i et enkelt cloud-infrastrukturmarked i Europa og understøtte vækstmål for et digitalt indre marked (DSM).

Denne håndbog er beregnet til at give nyttige råd og fungere som en hjælp for offentlige myndigheder ved køb af cloud-tjenester.

Mere information

CISPE-medlemmer: https://cispe.cloud/members
Bestyrelse: https://cispe.cloud/board-of-directors
Cloudcomputing-tjenester som er bekendtgjort i CISPE's adfærdskodeks:
https://www.codeofconduct.cloud/public-register/

Indholdsfortegnelse

v2 2022 - februar

Oversigt og denne håndbogs formål

Formålet med denne **Håndbog i køb af cloud-tjenester** er at hjælpe de cloud-kunder, der gerne vil købe cloud-tjenester ved hjælp af en konkurrenceudsættelse **(anmodning om tilbud på cloud-tjenester – RFP)**, men som ikke har ekspertise til at lave et udkast til en cloud-rammeaftale.

Dette dokument er kun til orientering. Det er ikke udarbejdet i overensstemmelse med lovpligtige krav for offentlige indkøbsprocesser i bestemte lande eller områder.

Håndbogen ser også nærmere på en række formuleringer for yderligere evalueringskriterier for **call offs** eller **minikonkurrencer**, når der købes i forbindelse med en cloud-rammeaftale. Afsnittene i håndbogen er ordnet således, at de ligner almindelige RFP'er for it. Eksempler på formuleringer i almindelige RFP'er og evalueringskriterier er suppleret med kommentarer, der gør det lettere at forstå, hvorfor en cloud-RFP er anderledes end en almindelig RFP for it.

Efter offentliggørelsen af EU-Kommissionens cloud-strategi, der vejleder i, hvordan de europæiske institutioner og agenturer vil modernisere deres it-infrastruktur gennem en cloud-first-tilgang, overrakte CISPE i juli 2019 håndbogen til EU-Kommissionen under arrangementet '*How to transform governments through a smart cloud policy*'.

Version 2 af denne håndbog indeholder nyt indhold vedrørende databeskyttelse (afsnit 2.3.1.1), ændring af cloud-udbyder og overførsel af data (afsnit 2.3.1.2), vilkår og betingelser for software (afsnit 2.5.2), bæredygtighed i cloud (afsnit 3.6) og et opdateret bilag B - Live teknisk vurdering.

> ***'Cloud-tjenester'*** *betyder alle de cloud-teknologier og relaterede tjenester, som en slutbruger muligvis skal have adgang til. Det omfatter konsulenttjenester eller professionelle/administrerede tjenester, der er nødvendige for at understøtte og gennemføre omstillingen til cloud og til at supplere workloads i cloud foruden selve cloud-infrastrukturen og cloud-markedspladstjenester såsom Software som en tjeneste (SaaS)-produkter.*

Cloudcomputing er blevet standardvalget for it i den offentlige sektor, og det medfører muligheder for at modernisere de nuværende indkøbsstrategier. Cloud-baserede indkøbsprocesser kan give parter i den offentlige sektor mulighed for at udnytte alle fordelene ved cloud, f.eks. adgang til den nyeste innovation, øget hastighed og mere fleksibilitet samt forbedret sikkerhed og styring af compliance, samtidig med at der opnås mere effektivitet, og udgifterne nedbringes.

Almindelige it-indkøbsmetoder til køb af hardware, software og datacentre kan ikke bruges til køb af cloud-tjenester. Metoder til prissætning, kontraktstyring, vilkår og betingelser, sikkerhed, tekniske krav, serviceaftaler og meget mere ændres i en cloud-model, og brug af de nuværende indkøbsmetoder reducerer eller fjerner i sidste ende de fordele, som man opnår med cloud.

En af de bedste metoder til effektivt indkøb af cloud-tjenester i den offentlige sektor er at have en **cloud-rammeaftale**, som er en menu af cloud-systemer med flere leverandørorganisationer, hvor berettigede købere med tilknytning til den organisation, der køber, kan anskaffe cloud-teknologierne og de tilhørende tjenester, der passer til deres behov. Som fundament for cloud-kontrakter kan disse rammeaftaler gøre det muligt at købe cloud-tjenester på en effektiv måde, hvilket giver de organisationer, der køber, og slutbrugerparterne adgang til en lang række cloud-tjenester, og dermed udnytte alle fordelene ved cloud: Fleksibilitet, stordriftsfordele, skalerbarhed, der giver mere tilgængelighed til en lavere pris, større bredde med hensyn til anvendelse, innovationstempo og kapacitet til at skalere til nye geografiske områder.

Bemærk at **denne håndbog fokuserer primært på køb af Infrastruktur som en tjeneste (IaaS) og Platform som en tjeneste (PaaS)-cloudteknologier, som de leveres af en *udbyder af cloud-infrastrukturtjenester (CISP)***. Disse cloud-teknologier kan enten købes hos en CISP eller gennem en CISP-forhandler. *Flere overvejelser er nødvendige ved RFP'er for distributører af cloud-markedspladstjenester (PaaS og SaaS) og cloud-konsulenttjenester.*

Bemærk desuden, at denne håndbog ikke omhandler alle dele af oprettelsen af et komplet rammeværk for cloud-indkøb. Der findes mange andre dokumenter fra branchen og analytikere om blandt andet retningslinjer for cloud-indkøb, hvordan man laver budget til cloud, cloud-governance osv., og vi anbefaler på det kraftigste, at disse råd og dokumenter tages i betragtning, når en overordnet strategi for cloud-indkøb udarbejdes.
Tabel 1 nedenfor giver et overblik over håndbogen i RFP'er for cloud-tjenester og viser, hvor eksempler på formuleringer i RFP'er kan ses for hver enkelt del af en RFP for cloud-tjenester.

Tabel 1 – resumé over afsnittene i håndbogen om anmodning om tilbud (RFP) til cloud-tjenester

Afsnit	Oversigt og eksempel på formuleringer i anmodning om tilbud
1.0 Oversigt over en cloud-rammeaftale	En overordnet oversigt over cloud-rammeaftalemodellen (grupper, hvordan man byder, og hvordan man laver kontrakter)
2.0 Oversigt over anmodning om tilbud til cloud-tjenester	Eksempler på generiske formuleringer i anmodninger om tilbud, der omhandler følgende afsnit, samt kommentarer om filosofien bag struktur og formuleringer i anmodninger om tilbud for cloud-tjenester.
2.1 Opsætning af anmodninger om tilbud til cloud-tjenester	2.1.1 Introduktion og strategiske mål 2.1.2 Tidslinje for respons i forbindelse med anmodninger om tilbud 2.1.3 Definitioner 2.1.4 Detaljeret beskrivelse af købsmodellen og budgivning inden for rammeaftalen 2.1.5 Minimumskrav for budgiver - administrativt
2.2 Teknisk	2.2.1 Minimumskrav 2.2.2 Sammenligning af leverandører 2.2.3 Indgåelse af kontrakter
2.3 Sikkerhed	2.3.1 Minimumskrav 2.3.1.1 Databeskyttelse 2.3.1.2 Ændring af cloud-udbyder og overførsel af data 2.3.2 Sammenligning af leverandører 2.3.3 Indgåelse af kontrakter

Afsnit	Oversigt og eksempel på formuleringer i anmodning om tilbud
2.4 Priser	2.4.1 Minimumskrav 2.4.2 Sammenligning af leverandører
2.5 Opsætning af kontraktopfyldelse/vilkår og betingelser	2.5.1 Vilkår og betingelser 2.5.2 Vilkår og betingelser for software 2.5.3 Sådan vælger du mellem leverandører på rammeaftalen 2.5.4 Klargøring og afslutning
3.0 Bedste praksis/erfaringer	3.1 Cloud-governance 3.2 Budgettering til cloud 3.3 Forstå partnerforretningsmodellen 3.4 Cloud-mæglere 3.5 Sourcing før RFP/markedsundersøgelse 3.6 Bæredygtighed
Bilag A – tekniske krav til sammenligning af budgivere	En liste med generiske krav til cloud-teknologi for call offs eller minikonkurrencer
Bilag B – Live teknisk vurdering	Et eksempel på et manuskript, som demonstrerer scoring af cloud-teknologi (cloud-demoer som en del af call off eller minikonkurrence)

1.0 Oversigt over en cloud-rammeaftale

En solidt udarbejdet cloud-rammeaftale kan gøre det muligt at købe cloud-tjenester på en måde, der er til gavn for de deltagende organisationer i den offentlige sektor og cloud-udbydere. Her er nogle af fordelene ved en solid cloud-rammeaftale:

- Samarbejdsorienteret pr. definition:
    - Flere organisationer, der går sammen om at afgive ordrer efter lignende krav, betyder bekvemmelighed, effektivitet, reducerede omkostninger samt en forenklet bestillingsproces. Det medfører en effektiv metode til at samle kravene fra flere organisationer i den offentlige sektor til almindelige cloud-teknologier og tilhørende cloud-tjenester som f.eks. markedspladsløsninger og konsulentydelser.
- Fuldt udbud af cloud-tjenester:
    - Dette kan omfatte alle konsulenttjenester og professionelle/administrerede tjenester, der er nødvendige for at understøtte og udføre migreringen til cloud, og understøtter workloads i cloud, og det omfatter også cloud-teknologier og markedsplads-tjenester fra CISP'er.
    - Cloud-teknologier kan købes hos en CISP eller en særlig forhandler.
- Kontraktstyring:
    - Resultatet bliver, at forskellige organisationer/købere får de samme vilkår og betingelser, og at der er en enkelt primær kontrakttildeling i stedet for nogle forskellige for hver enkelt organisation.
    - Desuden er det en fordel for leverandører, da det giver en standard for indkøbsproces, vilkår og betingelser og bestillingsmekanismen, der skal navigeres rundt i, i stedet for nogle forskellige for hver enkelt organisation i den offentlige sektor.
    - Det giver fleksibilitet. Oprettelse, godkendelse og brug af en effektiv cloud-kontrakt i de nuværende regeringspolitikker/lovbestemmelser kræver, at du eksperimenterer og kan tilpasse dig hurtigt. Det er meget mere fordelagtigt at lave en rammeaftale, der giver den offentlige sektor og cloud-udbydere mulighed for at samarbejde om forbedring af kontrakten, både kontraktmæssigt, mekanisk og effektivitetsmæssigt. En kontrakt med flere års levetid, der ikke fungerer og ikke kan tilpasses, giver slutbrugere i den offentlige sektor, indkøbsorganisationer og cloud-udbydere en negativ oplevelse.
- Valg:
    - Det giver indkøbere mulighed for at vælge mellem flere kvalificerede CISP'er og sætter en høj standard for cloud-tjenester og tilhørende tjenester såsom en cloud-markedsplads for PaaS/SaaS og cloud-konsulentydelser.
    - Det gør det muligt at vælge, hvor mange leverandører der skal være i en rammeaftale, da det sikrer, at standarden af hver enkelt leverandør godkendes korrekt.

En rammeaftale for køb af cloud-tjenester fungerer bedst, når den indeholder primære IaaS-/PaaS-teknologier fra CISP'en samt en PaaS-/SaaS-markedsplads og de konsulenttjenester, som slutbrugere i den

offentlige sektor kan få adgang til, hvis det behøves, så de kan planlægge, skifte til, benytte og vedligeholde en workload, der køres i cloud. Derfor anbefaler vi, at en RFP for cloud-tjenester til opsætning af en cloud-rammeaftale opdeles i 3 grupper som vist nedenfor:

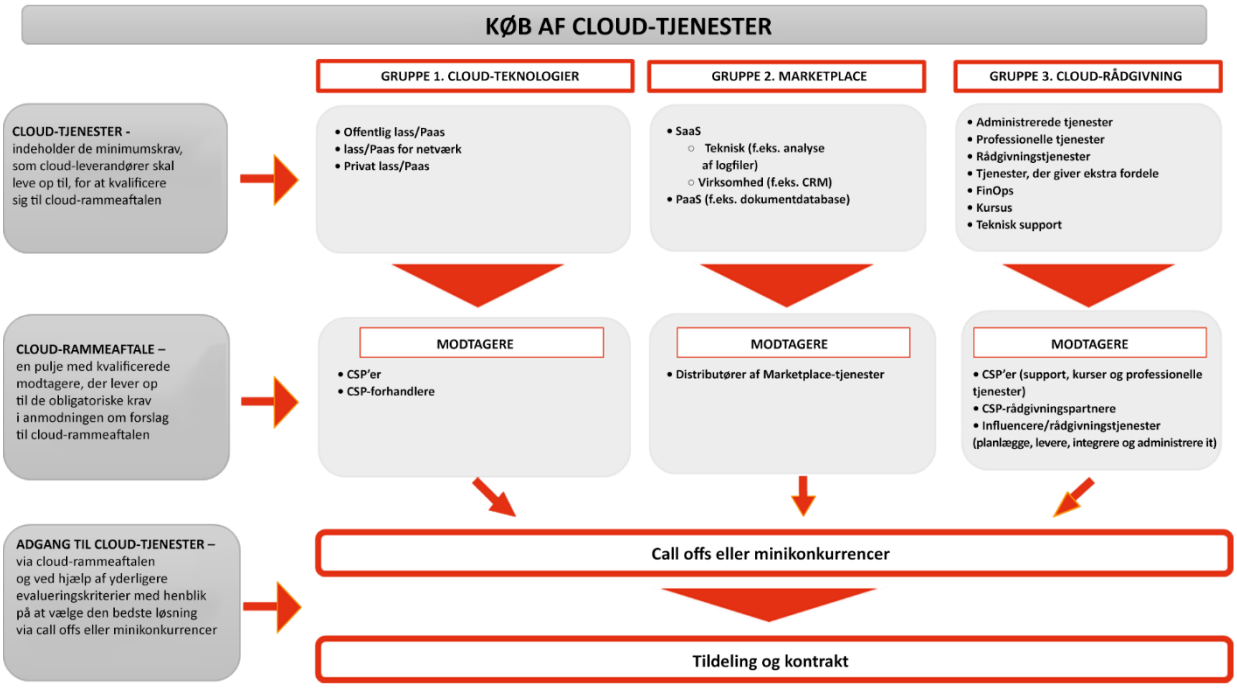
- GRUPPE 1 – CLOUD-TEKNOLOGIER
  Cloud-teknologier, der købes direkte hos en CISP eller gennem en udpeget CISP-forhandler.

- GRUPPE 2 – MARKETPLACE
  Adgang til en markedsplads med PaaS- og SaaS-tjenester.

- GRUPPE 3 – CLOUD-RÅDGIVNING
  Cloud-relaterede konsulenttjenester (kurser, professionelle og administrerede tjenester osv.) og teknisk support.

*Som tidligere nævnt handler denne håndbog primært om køb af IaaS- og PaaS-cloudteknologier (**GRUPPE 1**) fra en CISP (købt direkte hos en CISP eller gennem en CISP-forhandler). Separate krav til leverandørkvalificering er nødvendigt for leverandører i GRUPPER 2 og 3 i en RFP for cloud-tjenester.*

Figur 1 nedenfor er en overordnet oversigt over, hvordan en velorganiseret RFP for cloud-tjenester, som er opdelt i tre grupper, kan føre til en cloud-rammeaftale, der giver parter i den offentlige sektor fleksibilitet (både teknisk og kontraktmæssigt), synlighed og kontrol over udgifter samt cloud-forbrug og fleksibiliteten til at få alle de nødvendige cloud-tjenester til at opbygge og opretholde de nødvendige løsninger.



Figur 1 – en vellykket RFP for cloud-tjenester er opdelt i 3 grupper. Hver gruppe indeholder kategorier eller "tilbudstyper" under den respektive gruppe for at sikre teknisk og kontraktmæssig egnethed til at opfylde slutbrugernes krav, når der købes i henhold til cloud-rammeaftalen.

Bemærk:

- Hver gruppe har flere tildelinger.
- Gruppe 3 kan tildeles via en anden RFP eller muligvis via en nuværende kontrakt til konsulentydelser.

Gruppe 1-kategorier

Vellykkede cloud-rammeaftaler betyder, at CISP'er bliver bedt om at beskrive modellen for det cloud-system, de tilbyder, med en opdeling i kategorier under hver gruppe. Vi anbefaler, at du bruger branchens standard for cloudcomputing (National Institute of Standards and Technology (NIST) Essential Cloud Characteristics) – til definitionerne af **offentlig** cloud, **community** cloud og **privat** cloud. Når en cloud-rammeaftale struktureres på denne måde, kan det agentur, der køber, og de offentlige organer benytte rammen til at vælge en eller flere cloud-modeller, der passer til deres behov.

Se *afsnit 2.1.3 Definitioner* for NIST-definitionen af hver cloud-model under GRUPPE 1 (offentlig IaaS/PaaS, community-IaaS/PaaS og privat IaaS/PaaS).

Sådan byder du – call offs eller minikonkurrencer?

Kvalifikationskriterier for en RFP for cloud-tjenester skal omfatte vigtige elementer og minimumsstandarder og bør ikke indeholde standarder, der er "gode at have". Hvis yderligere standarder tilføjes oven på minimumsgrænsen for leverandører, der er kvalificerede til rammeaftalen, kan det medføre, at enkelte leverandører ikke kan byde, og det betyder færre valgmuligheder køberne.

Efter RFP'en og den efterfølgende opsætning af cloud-rammeaftalen kan organer i den offentlige sektor, der er en del af rammeaftalen, bestille eller lave "call off" for de cloud-tjenester, de har brug for, hvis det behøves. Afgivelse af en call-off-kontrakt i henhold til en rammeaftale giver købere mulighed for at finjustere kravene med en yderligere funktionel specifikation for en call-off, samtidig med at de har fordelene, der tilbydes i henhold til rammeaftalen.

Hvis det vurderes som nødvendigt, kan der afholdes en minikonkurrence med det formål at vælge den bedste leverandør til bestemte workloads eller projekter. En minikonkurrence er en konkurrence, hvor en kunde byder yderligere i henhold til rammeaftalen ved at invitere alle leverandører i en gruppe til at reagere på en række krav. Kunden vil invitere alle leverandører i en gruppe, der kan klare opgaven, til at byde, og derfor er minimumskravene for leverandører på rammeaftalen vigtige i en RFP for cloud-tjenester, da den medfører en høj standard for valgmuligheder under hver enkelt gruppe.

*Bemærk, at det er vigtigt, at der findes **særskilte sæt kontraktvilkår og -betingelser** for hver enkelt gruppe som anført i figur 1 ovenfor. En "universaltilgang" til kontraktindgåelser for alle grupper vil føre til spørgsmål om teknisk gennemførligheden tekniske rentabilitet og kompatibilitet.*

2.0 Oversigt over anmodning om tilbud til cloud-tjenester

Dette afsnit handler om RFP-modellen og omfanget for cloud-tjenester, deriblandt: strategiske mål, deltagere, definitioner, tidslinje og administrative minimumskrav. Vi vil som sagt understrege, at denne håndbogs primære fokus er **GRUPPE 1 – CLOUD-TEKNOLOGIER.**

2.1 Opsætning af anmodninger om tilbud til cloud-tjenester

Vi anbefaler på det kraftigste, at parter i den offentlige sektor er indforståede med deres mål og krav på højt niveau i introduktionen af RFP for cloud-tjenester.

2.1.1 Introduktion og strategiske mål

Af hensyn til forståeligheden af strategiske mål er det en god idé at formulere følgende i introduktionen til en RFP for cloud-tjenester: **(1)** virksomhedsmål og -fordele, som organisationen vil opnå ved hjælp af cloud; **(2)** rammeaftalens struktur – hvem køber, hvem får det til at fungere, hvem laver et budget osv.; **(3)**, en klar forståelse af modellen for ansvarsdeling mellem den offentlige sektor og cloud-udbyderne, hvilket er selve essensen af et vellykket køb og brug af cloud, og **(4)** den type forhold, der etableres mellem cloud-udbydere (CISP'er), distributører af markedsplads-tjenester, konsulentpartnere, myndigheder, der køber/laver kontrakter, og slutbrugere hos myndighederne. En formulering af disse fire punkter hjælper organisationer med at udvikle en RFP, der passer bedst til deres krav, og desuden er det med til at sikre, at både kunder og leverandører forstår RFP-resultaterne.

Der er en grund til, at en cloud-RFP er anderledes en almindelige RFP'er for it. Cloud-teknologi er ikke bare en identisk erstatning for almindelige beregningsmetoder. Det introducerer helt nye måder at benytte teknologi på. Solidt designede RFP'er for cloud-tjenester kan hjælpe parter i den offentlige sektor med at udnytte fordelene ved cloud hurtigt.

Vi betegner flere aspekter ved køb af cloud som retningslinjer, men en tydelig forståelse af modellen for ansvarsdeling er muligvis det bedste udgangspunkt. Modellen for ansvarsdeling[1] bruges primært i drøftelsen af sikkerhed og compliance i en cloud, men denne afgrænsning af ansvar gælder i alle aspekter af cloud-teknologier. En RFP for cloud-tjenester bør tydeligt vise, hvad der ligger inden for en CISP's ansvarsområde i et cloud-miljø, og hvad der stadig vil være en kundes ansvar. En CISP gør det for eksempel muligt at holde øje med ressourcer og programmer, der kører i en cloud, ***men*** det er faktisk kundens ansvar at benytte disse muligheder, som en CISP tilbyder, da en CISP, der fungerer på en enorm skala, ikke er beregnet til at gøre dette for millioner af kunder.

Desuden skal cloud-kunder vide, hvordan en CISP's partnernetværk gør det lettere for kunder at benytte cloud og administrere deres ansvar. En cloud-MSP (Managed Service Provider) kan f.eks. hjælpe en kunde med at konfigurere og bruge en CISP's overvågningsfunktioner, så deres unikke krav til compliance og revision opfyldes.

Kort sagt er ansvarsområderne i cloud-modellen:

EN CISP sørger for cloud-teknologien

[1] Se afsnit 5 i CISPE-adfærdskodeksen for udbydere af cloud-infrastruktur-tjenester: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

En kunde benytter cloud-teknologien

Konsulentfirmaer (hvis dette er relevant) hjælper en kunde med at få adgang til og benytte cloud-teknologi

***'Konsulentfirmaer'** er firmaer, der tilbyder konsulenttjenester og administrerede/professionelle tjenester, der gør det lettere for kunderne at designe, lave arkitektur, migrere og administrere deres workloads og programmer i cloud. Disse firmaer kan f.eks. være systemintegratorer, strategiske konsulentbureauer, agenturer, udbydere af administrerede tjenester og værditilvækstforhandlere.*

Når man 'køber' cloud-tjenester, er det ligesom at købe varer i et byggemarked. I et byggemarked kan du finde et enormt udvalg af materialer og værktøj til at bygge det, du har brug for. Du kan bygge et skab eller en swimmingpool eller et helt hus, det er dit valg. Når du køber materialer og værktøjer, kan medarbejderne i byggemarkedet give vejledning og ekspertise, men de kommer ikke hjem og bygger noget for dig. Derfor har du et par muligheder:

1. Du kan købe materialerne og værktøjet og bygge noget selv.
2. Du kan købe materialerne og værktøjet selv og få en anden til at bygge og/eller betjene noget for dig.
3. Du kan få en anden til at bygge/betjene noget for dig og få vedkommende til at sørge for materialerne og værktøjet som en del af deres generelle tilbud.

Hvis en organisation selv har personale med kompetencer til at opbygge og administrere virksomhedens cloud-miljø og løsninger, skal den kun have adgang til de standardiserede cloud-teknologier og -værktøjer fra CISP'en (direkte hos en CISP eller ved hjælp af en CISP-forhandler – se **GRUPPE 1**). Den nødvendige SaaS- og PaaS-software skal være tilgængelig på en cloud-markedsplads (**GRUPPE 2**). Hvis der er brug for yderligere konsulenthjælp, migrering, implementering og/eller hjælp til styring, er det her, at CISP'ens partnernetværk kommer ind i billedet (**GRUPPE 3**).

Eksempel på formulering i RFP: Introduktion og strategiske mål

Cloudcomputing giver organisationer i den offentlige sektor hurtig adgang til en lang række fleksible og billige it-ressourcer med betaling baseret på brug. Organisationer kan stille den rigtige type og størrelse af ressourcer til rådighed, som de har brug for til at drive deres nyeste smarte idéer eller deres it-afdelinger, hvilket fjerner behovet for store investeringer i hardware og/eller langvarige licenskontrakter til software.

***<ORGANIZATION>** har et behov om adgang til disse typer cloud-teknologier til virksomhedsbrug, før de kan opfylde deres virksomhedsbehov i en lang række associerede organisationer.*

*Det primære mål med denne RFP er at give en ikke-eksklusiv og parallel **<RAMMEAFTALE>** med op til **<x>** udbyderer, der tilbyder forskellige cloud-teknologier og cloud-relaterede tjenester.*

1. ***GRUPPE 1**. Cloud-udbydere (CISP'er) eller CISP-forhandlere til køb af cloud-teknologier.*
2. ***GRUPPE 2.** Leverandører af markedsplads-tjenester.*
3. ***GRUPPE 3.** Leverandører af konsulenttjenester, der sørger for yderligere eksperthjælp til migrering og benyttelse af disse CISP-tilbud.*

*Hvad angår **GRUPPE 1**, skal organisationer, der byder (CISP'er eller CISP-forhandlere), vise, hvordan deres tilbud opfylder disse mål:*

- ***Fleksibilitet –** it-ressourcer gøres tilgængelige for slutbrugerne på få minutter i stedet for de traditionelle uger og måneder.*
- ***Innovation –** man har øjeblikkelig adgang til den nyeste og mest innovative teknologi på markedet.*
- ***Omkostninger** – muligheden for at erstatte faste omkostninger med variable omkostninger (f.eks. kapitalomkostninger til driftsomkostninger). At der kun betales for, hvor meget der bruges.*
- ***Budgettering** – mulighed for at se fakturerings- og brugsoplysninger på både detaljerede og overordnede niveauer og en visualisering af forbrug i en periode foruden prognoser til fremtidige udgifter.*
- ***Elasticitet –** mulighed for at opnå lavere variable omkostninger fra de større stordriftsfordele, som cloud giver.*
- ***Kapacitet –** slip for gætterier, når det gælder behov for infrastrukturkapacitet.*
- ***Fjernelse af behovet for datacentre –** fokus på borgernes virksomheder i stedet for besværet med at organisere og drive servere.*
- ***Sikkerhed –** formalisering af kontodesign med mere synlighed og mulighed for revision af ressourcer og reduktion af udgifter til beskyttelse af anlæg og fysisk hardware.*
- ***Fælles ansvar -** Aflastning af den operationelle byrde, da CISP'en driver, administrerer og kontrollerer komponenterne fra værtsoperativsystemet og virtualiseringslaget, helt ned til den fysiske sikkerhed i de faciliteter, hvor tjenesten er i drift.*
- ***Automatisering –** Indbyg automatisering i cloud-arkitekturen for at forbedre muligheden for at skalere sikkert, hurtigere og mere omkostningseffektivt.*
- ***Cloud-governance –** (1) start med at gøre status over alle it-aktiver, (2) administrer alle disse aktiver på ét sted, og (3) opret påmindelser vedrørende brug/fakturering/sikkerhed osv. med mulighed for at holde øje med aktiver, lagerstyring, ændringsstyring, logfils-styring og analyse samt få overordnet synlighed og cloud-governance.*
- ***Kontrol** – få fuld synlighed over, hvor meget it-tjenester bruges, og hvor de kan finjusteres med henblik på sikkerhed, pålidelighed, effektivitet og omkostninger.*
- ***Reversibilitet** – portabilitetsværktøjer og -tjenester gør det lettere at migrere til og fra CISP-infrastrukturen, minimere afhængighed af leverandører og overholde branchens adfærdskodeks(er).*
- ***Databeskyttelse –** mulighed for at demonstrere overholdelse af den generelle databeskyttelsesforordning (GDPR) gennem en særlig brancheadfærdskodeks for Cloud Infrastructure-tjenester: CISPE's adfærdskodeks for databeskyttelse.*
- ***Transparens** – kunderne har ret til at vide, hvor de infrastrukturer, der behandler og gemmer deres data, er placeret (byområde).*
- ***Klimaneutralitet –** kunderne bør arbejde sammen med CISP'er, der tager dokumenterede, specifikke skridt til at opfylde målene for klimaneutralitet inden 2030 og har underskrevet pagten om klimaneutrale datacentre. Dette vil hjælpe kunderne med at opfylde deres egne mål for klimaneutralitet.*

2.1.2 Tidslinje for respons i forbindelse med anmodninger om tilbud

Det er en god idé at sørge for, at budgivere kan se en tidslinje med forventet budaktivitet, når en cloud-rammeaftale oprettes, og den tilknyttede RFP for cloud-tjenester. Jo mere engagement der er med branchen, desto bedre, da dette er med til at sikre, at alle parter er indforstået med kravene i RFP'en og især ved, hvordan alle leverandører passer ind i modellen for cloud-tjenester.

Bemærk: RFP-tidslinjen er underlagt lokal lovgivning og juridiske forpligtelser, og listen nedenfor er beregnet som en vejledning med retningslinjer og ikke en liste med aktiviteter og tidsfrister som forebyggelse.

Eksempel på formulering i RFP: tidslinje for svar

Se følgende RFP-tidslinje for cloud-tjenesternes RFP:

Tidslinje for RFP for cloud-tjenester
• *Udsendelse af anmodning om oplysninger (RFI):* • *RFI-svar:* • *Udkast til udgivelse af anmodning om tilbud (RFP):* • *Udkast til svar på RFP forfalder:* • *Branche-konsultationsfase: <timelines>* • *Udgivelse af prækvalifikations-RFP:* • *Svar på prækvalifikations-RFP:* • *Udgivelse af anmodning om tilbud (RFP):* • *Spørgsmål i runde 1 forfalder:* • *Runde 1-svar:* • *Spørgsmål i runde 2 forfalder:* • *Runde 2-svar:* • *RFP-svar forfalder:* • *Tilbuddets afklaringsperiode:* • *Forhandlingsperiode:* • *Dato for planlagt tildeling:* • *Kontrakttildeling:* • *Kontraktens varighed (muligheder for forlængelse):*

Bemærk: RFP-tidslinjen er underlagt lokal lovgivning og juridiske forpligtelser, og listen nedenfor er beregnet som en vejledning med retningslinjer og ikke en liste med aktiviteter og tidsfrister som forebyggelse.

2.1.3 Definitioner

En RFP for cloud-tjenester bør indeholde en detaljeret liste med definitioner. Denne liste indeholder leverandørroller (f.eks. cloud-udbyder, cloud-forhandler eller leverandørpartner), generelle teknologikoncepter (beregning, lager, IaaS/PaaS, SaaS) og andre vigtige dele af aftalen. Følgende er et eksempel på en liste med definitioner:

Eksempel på formulering i RFP: definitioner

Følgende definitioner er NIST's definitioner (National Institute of Standards and Technology) af cloudcomputing.[2]

- ***Infrastruktur som en tjeneste (IaaS).*** *Kunden har mulighed for at klargøre behandling, lager, netværk og andre fundamentale beregningsressourcer, hvor kunden kan udrulle og køre påkrævet software, som kan omfatte operativsystemer og programmer. Kunden administrerer og styrer ikke den underliggende cloud-infrastruktur, men har kontrol over operativsystemer, lager og udrullede programmer og muligvis begrænset kontrol over udvalgte netværkskomponenter, (f.eks. værts-firewalls).*

- ***Platform som en tjeneste (PaaS).*** *Kunden har mulighed for at udrulle programmer, som vedkommende selv har udviklet eller købt, og som er udviklet ved hjælp af programmeringssprog, biblioteker, tjenester og værktøjer, der understøttes af udbyderen, i cloud-infrastrukturen. Kunden administrerer eller styrer ikke den underliggende cloud-infrastruktur, herunder netværk, servere, operativsystemer eller lager, men har kontrol over de udrullede programmer og muligvis konfigurationsindstillingerne for miljøer til hosting af programmer.*

- ***Software som en tjeneste (SaaS).*** *Kunden har mulighed for at bruge udbyderens programmer, der kører i en cloud-infrastruktur. Programmerne kan åbnes med diverse klienter via enten en grafisk brugergrænseflade, f.eks. en webbrowser (f.eks. webbaseret e-mail) eller en programgrænseflade. Kunden administrerer eller styrer ikke den underliggende cloud-infrastruktur, deriblandt netværk, servere, operativsystemer, lager eller endda individuelle programfunktioner, dog muligvis med undtagelse af begrænsede brugerspecifikke programkonfigurationsindstillinger.*

- ***Offentlig cloud.*** *Cloud-infrastrukturen klargøres til fri benyttelse af offentligheden. Den kan ejes, administreres og drives af en virksomhed, uddannelsesinstitution eller en offentlig organisation eller en kombination af disse. Den er placeret fysisk hos cloud-udbyderen.*

- ***Community cloud.*** *Cloud-infrastrukturen klargøres til kun at blive brugt af en bestemt gruppe brugere fra organisationer med de samme mål (f.eks. mission, sikkerhedskrav, politik og betragtninger i forbindelse med compliance). Den kan ejes, administreres og deles af en eller flere organisationer i gruppen, en tredjepart eller en kombination af disse, og den kan være placeret både i eller uden for organisationen.*

- ***Hybrid cloud.*** *Cloud-infrastrukturen består af to eller flere tydelige cloud-infrastrukturer (privat, community eller offentlig), der altid vil være unikke parter, men er knyttet sammen af standardiseret eller patenteret teknologi, der gør det muligt at overføre data og programmer, (f.eks. cloudbursting til fordeling af opgaver mellem cloud-systemer).*

- ***Privat cloud.*** *Cloud-infrastrukturen klargøres til kun at blive brugt af en enkelt organisation, der består af flere kunder (f.eks. afdelinger). Den kan ejes, administreres og deles af organisationen, en tredjepart eller en kombination af disse, og den kan være placeret både i eller uden for organisationen.*

2.1.4 Detaljeret beskrivelse af købsmodellen og budgivning inden for rammeaftalen

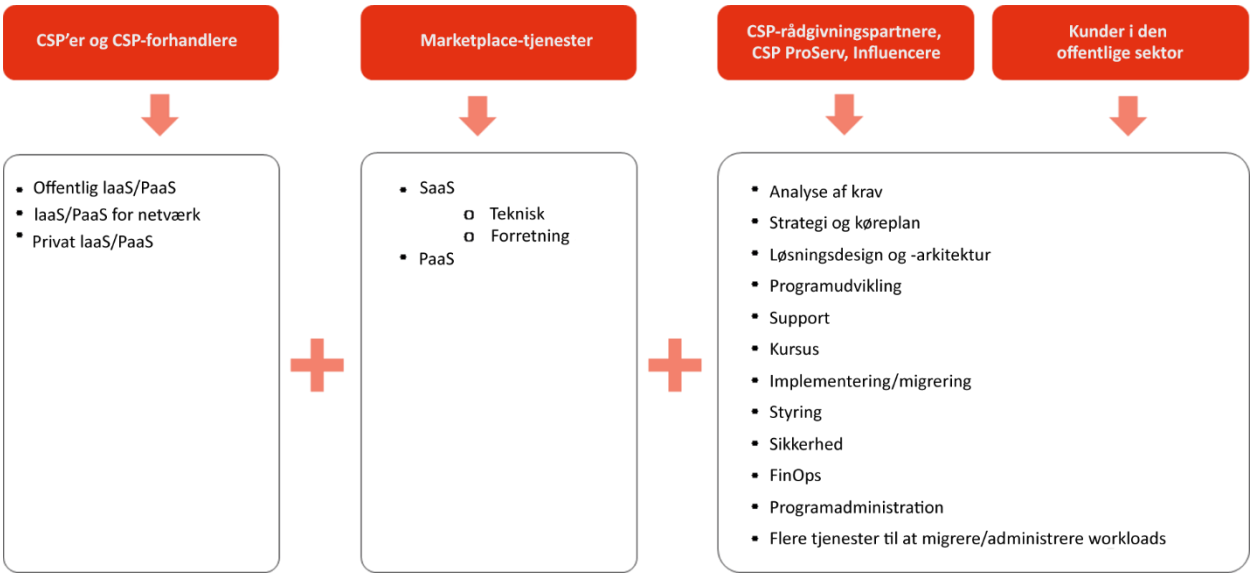
Som tidligere nævnt bør organisationer i den offentlige sektor finde en model for, hvordan rammeaftalen skal fungere som en mekanisme til køb af cloud-teknologier samt relaterede implementerings- og administrationstjenester. Dette bør formuleres i RFP'en for cloud-tjenester, så cloud-teknologileverandørerne, de relaterede organisationer, der tilbyder konsulenttjenester, markedsplads-distributører og parter, der køber, kender deres respektive roller.

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Organisationer bør overveje følgende angående omfanget af rammeaftalen og de følgende call offs eller minikonkurrencer:

- Hvem er ansvarlig for integration og administrerede tjenester vedrørende brugen af cloud-teknologier i henhold til kontrakten?
- Er der et krav til en CISP-forhandler/partner om at levere andre værdifulde tillægstjenester end at opretholde et kontraktligt forhold til CISP'en, levere konsoliderede faktureringstjenester og rettidig og direkte adgang til brugs- og faktureringsdata i forbindelse med brugen af cloud-udbyderens tjenester?
- Er der et krav om en forhandler, der tilbyder komplette tjenester, en systemintegrator eller en udbyder af administrerede tjenester eller nogen form for it-arbejdstjenester?

Det er vigtigt at nævne, at CISP ikke er en systemintegrator (SI) eller en MSP (Managed Service Provider). Mange kunder i den offentlige sektor har brug for en CISP til deres IaaS/PaaS og hyrer en SI eller MSP til konsulenttjenester og "personlig" planlægning, migrering og administrationsarbejde. En beskrivelse af afgrænsningen af roller og ansvarsområder i en model for cloud-tjenester findes nedenfor i **figur 2.**



Figur 2 – en RFP for cloud-tjenester bør give slutbrugerne en menu med alle de cloud-tjenester, de har brug for. Kunder i den offentlige sektor får brug for en CISP til cloud-tjenester, en markedsplads til PaaS og SaaS-produkter, hvis det er nødvendigt. Herefter kan kunden finde ud af, hvor stor en rolle vedkommende får i forbindelse med leveringen af cloud-tjenesterne, og hvor meget vedkommende vil overlade til konsulentfirmaer/systemintegratorer/udbydere af administrerede tjenester osv.

Eksemplet på formulering nedenfor er baseret på de roller og ansvarsområder, som er vist i figur 2 ovenfor. En cloud-rammeaftale og en RFP for tilknyttet cloud-tjenester bør sikre, at køberne får mulighed for på passende vis at vurdere hver leverandørs tilbud, så de kan vælge mellem de tjenester, der er nødvendige til et workload/projektet. Dette opnås bedst ved at dele tjenesterne op i grupper som tidligere nævnt og ved at redegøre for, hvordan call offs og minikonkurrencer udføres i henhold til rammeaftalen.

Eksempel på formulering i RFP: købsmodel

*Denne kontrakt vil fungere som en **ramme** for indkøb. Denne cloud-rammeaftale vil indeholde flere **grupper**, som er defineret af **<ORGANIZATION>**, for cloud-teknologier og tilhørende markedsplads-tjenester/produkter, konsulentydelser, professionelle tjenester/systemintegration/administrerede tjenester/migrering, kurser og support, som er defineret af **<ORGANIZATION>**, og skal bruges af flere kvalificerede købere med tilknytning til **<ORGANIZATION>**. Dette vil forenkle indkøbsprocessen og samtidig optimere stordriftsfordelene.*

Når denne rammeaftale er etableret, kan en organisation købe netop de cloud-teknologier og cloud-relaterede tjenester, de har behov for, når det er nødvendigt, i stedet for at købe dem via separate indkøb. Denne metode reducerer antallet af administrative krav og gør i høj grad indkøbene mindre komplekse og tidskrævende.

*Denne rammeaftale gælder i maks. **<X>** år, herunder med eventuelle fornyelser. Den maksimale varighed af en call-off rammeaftale er normalt **<x>** måneder; denne kan forlænges med **<x>** måneder og derefter med yderligere **<x>** måneder med de relevante interne godkendelser, hvis det er nødvendigt for kontraktforlængelsen. Dette skal angives i hver enkelt specifikke **call off.***

*RAMMEAFTALEN er delt op i **3 (tre) grupper.***

1. ***GRUPPE 1: CLOUD-TEKNOLOGIER** -det fulde omfang af cloud-udbyderens teknologier (direkte fra CISP'en til forhandleren eller fra forhandleren med tjenester/support).*
    i. ***IaaS- og PaaS-tjenester** – en menu med cloud-teknologier, f.eks. beregnings-, lager-, netværks-, database-, analyse- og programtjenester, udrulning, administration, udvikler, IoT (Tingenes internet) osv. Indeholder samlede cloud-teknologiløsninger som DR/COOP, Arkiv, Big Data & Analytics, DevOps osv.*
2. ***GRUPPE 2: MARKETPLACE** – det fulde omfang af PaaS- og SaaS-tjenester/-produkter såsom regnskab, CRM, design, HR, GIS og tilknytning, HPC, BI, indholdsstyring, analyse af logfiler osv.*
3. ***GRUPPE 3: CLOUD-KONSULENTYDELSER** – det fulde omfang af konsulenttjenesterne (administrerede og professionelle tjenester, rådgivnings-/konsulenttjenester, tjenester, FinOps, teknisk support) i forbindelse med cloud-migrering og brug. Disse tjenester kan omfatte: planlægning, design, migrering, administration, support, kvalitetskontrol, sikkerhed, kurser osv.*

Leverandørerne kan indsende deres tilbud i flere grupper.

Leverandørerne sender deres tilbud og relaterede priser i et valgfrit format.

BUDGIVNING INDEN FOR RAMMEAFTALEN OG TILDELING AF KONTRAKTER

CALL OFFS

Organer i den offentlige sektor, der er part i rammeaftalen, kan bestille eller "call-off" de tjenester, de har brug for, når det er nødvendigt. Afgivelse af en call off-kontrakt i henhold til rammeaftalen giver købere mulighed for at finjustere kravene med en yderligere funktionel specifikation for en call off, samtidig med at de har fordelene, der tilbydes i henhold til rammeaftalen.

Kontrakter, der tildeles via rammeaftalen, kan vise et tydeligt revisionsspor med hensyn til de krav, der bruges til at vælge leverandøren i hver enkelt gruppe. De endelige aftagere laver fortegnelser over kommunikationen med leverandører, herunder tidligt markedsengagement, uddybende spørgsmål, e-mails og personlige samtaler.

1. UDARBEJDELSE AF CALL OFF-KRAV OG ANMODNING OM INTERN GODKENDELSE AF KØB

Alle slutkøbere, der er berettiget til at anvende rammeaftalen, vil oprette fælles teams af slutbrugere, indkøbsspecialister og tekniske eksperter, der skal udarbejde en liste over "skal have" og "ønsker". Disse krav gør det lettere at vælge, hvilken gruppe eller grupper, der er relevante, og hvilken leverandør, der er mest kvalificeret til at opfylde disse krav. Køberne skal overveje følgende, når de laver en kladde med krav:

- *Hvor mange penge der er til benyttelse af tjenesten*
- *Projekt tekniske krav og krav i forbindelse med køb*
- *De kriterier, valget er baseret på*

2. SØGNING EFTER TJENESTER

Købere, som er omfattet af rammeaftalen, benytter et online-rammekatalog (en portal, hvor kvalificerede leverandører i rammeaftalen og deres tjenester angives), så det er muligt at finde produkter/tjenester, der opfylder deres behov. De vælger de relevante grupper og søger derefter efter tjenesterne.

3. GENNEMGÅ OG EVALUER TJENESTER

Købere, som er omfattet af rammeaftalen, gennemgår beskrivelserne af tjenesterne og finder de tjenester, der passer bedst til deres behov, med udgangspunkt i både krav og budget. Hver enkelt beskrivelse af tjeneste skal indeholde:

- *Et dokument med en beskrivelse af tjenesten eller links til definitioner af tjenesterne*
- *Et dokument med vilkår og betingelser*
- *Dokumenter med priser (links til offentlige priser er acceptable med formodningen om, at det er muligt at anmode om et komplet dokument med prislister og prissætning)*

Prisen skal være omkostningen for tjenestens mest almindelige konfiguration. Prissætningen er dog normalt volumenbaseret, så køberne bør altid se på leverandørens prissætningsdokument eller offentlig prissætning og prisberegningsværktøjer for at finde ud af den faktiske pris på det, der købes, og den samlede værdi, der leveres til køberen (for eksempel tjenester til optimering og deraf følgende omkostningsreduktion).

Købere, som er omfattet af rammeaftalen, kan bede leverandørerne om at uddybe deres beskrivelse af tjenesten, vilkår og betingelser, priser eller dokumenter med tjenestedefinition/model. Der skal føres en fortegnelse over kommunikationen med leverandørerne.

4. VÆLG EN TJENESTE, OG TILDEL EN KONTRAKT

Enkelt leverandør

Hvis det kun er én leverandør, der lever op til kravene, kan vedkommende få tildelt en kontrakt.

Flere leverandører

Hvis der er flere tjenester på en shortliste, vælger køberen den tjenesteydelse med det økonomisk mest fordelagtige tilbud (Most Economically Advantageous Tender (MEAT)). Se kriterierne i følgende tabel for den MEAT-baserede bedømmelse. Købere kan vælge, hvilke detaljerede karakteristika der skal bruges, og hvordan de skal vægtes.

Bemærk, at køberen muligvis skal:

- *overveje kombinationen af forskellige leverandører*
- *få specifikke oplysninger om mængde eller virksomhedskonti og tjenester til optimering af leverandøromkostninger*

Vurderingen af leverandører bør altid være retfærdig og gennemsigtig. Valget skal ske med udgangspunkt i, hvem der er bedst egnet, og leverandører/tjenester skal ikke udelukkes uden henvisning til projektets krav.

Tabel 2 - MEAT-baseret bedømmelse

Tildelingskriterier
Samlede levetidsomkostninger: *omkostningseffektivitet, pris og driftsomkostninger*
Teknisk fordel og funktionel egnethed: *dækning, netværkskapacitet og ydeevne som angivet i relevante tjenesteniveauer*
Administration af tjenester efter salg: *helpdesk, dokumentation, funktion til kontostyring og garanti for levering af en række tjenester*
Ikke-funktionelle karakteristika

MINIKONKURRENCER

Hvis det vurderes som nødvendigt, kan der afholdes en minikonkurrence med det formål at vælge den bedste leverandør til bestemte workloads eller projekter. En minikonkurrence er en konkurrence, hvor en kunde byder yderligere i henhold til rammeaftalen ved at invitere alle leverandører i en gruppe til at reagere på en række krav. Kunden inviterer alle kvalificerede leverandører i den pågældende gruppe til at byde. Se de yderligere sammenligningsoplysninger i afsnittene nedenfor vedrørende teknik, sikkerhed og prissætning/værdi.

KONTRAKT

Både køberen og leverandøren skal underskrive kontrakten, før tjenesten kan benyttes. En rammekontrakts maksimale varighed er typisk <x> måneder. Den kan forlænges med <x> måneder og derefter i yderligere <x> måneder med de relevante interne godkendelser, hvis det er nødvendigt i forbindelse med kontraktforlængelse.

Alle interesserede parter (køberen og leverandøren) skal underskrive en kopi af kontrakten, før tjenesten kan bruges.

2.1.5 Minimumskrav for budgiver - administrativt

En enkel og klar formulering af kvalifikationskriterierne for rammeaftalen vil være med til at sikre, at der ikke kommer forslag fra traditionelle datacentre eller hardwareudbydere, der pakker en traditionel løsning ind som en 'cloud.' RFP-deltagere skal vise, hvordan de opfylder nedenstående administrative minimumskrav til tilbudsgiverne.

Som tidligere nævnt omhandler dette dokument GRUPPE 1 - CLOUD-TEKNOLOGIER. Men vi har tilføjet yderligere oplysninger om GRUPPE 2 - MARKETPLACE og GRUPPE 3 - CLOUD-RÅDGIVNING, hvis det er med til at klarlægge den generelle sammenhæng med hensyn til krav og RFP'ens omfang. Det er for eksempel vigtigt at inkludere minimums-kvalifikationskriterier for CISP-forhandler/MSP/SI/konsulentfirma osv., og det er med til at sikre, at de (1) har direkte tilknytning til CISP'en som en forhandler eller kanalpartner, (2) er certificerede til at sælge direkte adgang til CISP-produkterne til tredjeparter og (3) har certificeringer fra disse CISP'er, der viser deres kompetencer og ekspertise.

Eksempel på formulering i RFP: minimumskrav for budgiver – administrativt

Denne rammeaftale tildeler kontrakter til flere leverandører i flere kategorier. Leverandører skal være en kommerciel CISP, en tredjepartsforhandler for en CISP, en distributør af markedsplads-tjenester og/eller udbyder af tjenester til brug af en CISP (f.eks. konsulentydelser, migreringstjenester, administrerede tjenester, FinOps osv.). Angiv de roller, du byder på:

GRUPPE 1

____ - Direkte udbyder (CISP) af offentlige cloud-tjenester (IaaS OG PaaS)

____ - Direkte udbyder (CISP) af community cloud-tjenester (IaaS OG PaaS)

____ - Direkte udbyder (CISP) af private cloud-tjenester (IaaS OG PaaS)

____ - CISP-tredjepartsforhandler (mulighed for at give direkte adgang til en CISP's online-cloud-tilbud).

- *Angiv det CISP-tilbud, hvor du kan sælge direkte adgang til deres tjeneste: _____*
- *Fremlæg et brev fra CISP'en om, at du er en autoriseret forhandler af deres tilbud: _____*

GRUPPE 2

____ - Direkte leverandør af markedsplads-tjenester, der kører på en CISP (PaaS og/eller SaaS)

____ - Distributør af markedsplads-tjenester, der kører på en CISP (PaaS og/eller SaaS)

GRUPPE 3

____ - CISP, der leverer professionelle tjenester

____ - Udbyder af CISP teknisk support

____ - CISP-partner, der leverer tjenester til benyttelse eller drift på en CISP

____ - Influencer/rådgiver, der leverer tjenester til benyttelse eller drift på en CISP

Angiv typen af tilbud:

- *Administrerede tjenester til workloads på en CISP (J/N): _____*
  - *Angiv ekspertområder, hvis det er relevant: _____*
- *Professionelle tjenester (J/N): _____*
- *Konsulentydelser – kurser (J/N): _____*
- *Konsulentydelser – strategi (J/N): _____*
- *Konsulentydelser – migrering (J/N): _____*
- *Konsulentydelser – cloud-governance (J/N): _____*
- *Konsulentydelser – FinOps (J/N): _____*
- *Konsulentydelser – andet (angiv venligst): _____*

Angiv CISP/CISP'er, som du leverer tjenester for: _____
Send et brev fra CISP'en, der bekræfter din rolle som partner i henhold til CISP'ens model: _____

ADMINISTRATIVE MINIMUMSKRAV FOR GRUPPE 1

Cloud-tjenesteudbydere (CISP'er)

For at kunne blive kvalificeret som CISP skal følgende krav opfyldes.

Foreslåede kvalifikationskriterier for CISP	*Årsag*
Oplysninger om organisationen, f.eks. navn, juridisk struktur, registrering/DUNS-nummer, moms osv.	
Virksomhedens størrelse og økonomiske status.[3]	*Kunden kan vurdere, om CISP'en vil være i stand til at gennemføre kontrakten.*
Årsager til udelukkelse, f.eks. kriminalitet/bedrageri osv.	
Casestudier/kundehenvisninger (angiv nødvendigt antal/type).	*Kunden har mulighed for at vurdere CISP'ens erfaring i leveringen af de påkrævede tjenester.*
Virksomhedens sociale ansvar.	*Disse bør være offentligt tilgængelige versioner, som CISP'en stiller til rådighed.*
Offentligt tilgængelige oplysninger om indsats og retningslinjer for bæredygtighed.	*Kunden kan se, at en CISP er forpligtet til at drive sin virksomhed på den mest miljøvenlige måde.*
CISP'en skal kunne bevise innovation og lancering af nye nyttige tjenester og funktioner i løbet af de seneste fem år, især med hensyn til PaaS, maskinlæring og analyse, big data, administrerede tjenester og funktioner til optimering af cloud-brug. Offentligt tilgængelige logfiler om ændringer eller opdateringsfeeds kan bruges til at bevise dette.	*Viser, at CISP arbejder på at få nye produkter hurtigt ud til kunderne og derefter hurtigt gentager og forbedrer produkterne. Dette hjælper kunderne med at opretholde en topmoderne it-infrastruktur uden at skulle foretage investeringer i kapitaltilførsler.*

Forhandlers/partners samarbejde med CISP

<ORGANIZATION> *kræver, at den primære leverandør har direkte tilknytning til CISP'en som en forhandler eller kanalpartner og er godkendt af en CISP til at sælge adgang til dennes produkter til tredjeparter, og disse CISP'ers certificering angiver deres evner og ekspertise. Dette eliminerer kravet om, at* ***<ORGANIZATION>*** *skal gennemgå de vilkår og tjenester, der er forbundet med et yderligere lag af underleverance mellem den primære leverandør i* ***rammeaftalen*** *og CISP. Dette krav fjerner også den kompleksitet, som yderligere forhandlerlag skaber, når (1)* ***<ORGANIZATION>*** *udfører sin due diligence for at sikre en tydelig tildeling af ansvar med hensyn til de tjenester, der skal leveres, og (2)* ***<ORGANIZATION>*** *udfører de daglige aktiviteter vedrørende brugen af cloud-tjenesterne.*

2.2 Teknisk

En RFP for cloud-tjenester skal hæve standarden for CISP'er ved at kræve, at de angiver de standardiserede cloud-teknologier, som en kunde skal bruge til at lave sin egen tilpassede løsning. Som tidligere nævnt er denne forskel på, hvad der er standardiseret, og hvad der er tilpasset, meget vigtig, når man skal udarbejde en RFP for cloud-tjenester. CISP'er tilbyder standardiserede tjenester til millioner af kunder. Derfor fokuserer tilpasninger i en RFP for cloud-tjenester på løsninger højere oppe i stakken og resultater i modsætning til de underliggende metoder, infrastruktur eller hardware, der bruges til at levere de cloud-tjenester, som bruges for at opnå løsningens resultater.

[3] Bemærk: En RFP for cloud-tjenester ser på virksomhedsoplysninger på højt niveau i stedet for antallet af medarbejdere i virksomheden og afdelingsstrukturen for interne medarbejdere. Med cloud-teknologi er der ingen sammenhæng mellem garantier for tjenestens effektivitet og antallet af medarbejdere. I stedet ser RFP'er på virksomhedens overordnede størrelse i afgørelsen af, om kravene overholdes (tilstrækkelig skala), og dokumenterede erfaring/effektivitet.

2.2.1 Minimumskrav

Typiske it-køb omfatter som regel virksomhedskrav, som er udarbejdet i en række arbejdsmøder, der dokumenterer, hvordan organisationen fungerer på nuværende tidspunkt. Selv under de bedste omstændigheder er det svært at opstille disse krav perfekt. Hvis det lykkedes, dokumenterer disse møder om krav de historiske virksomhedsprocesser, der i sig selv kan være umoderne og virkningsløse. Hvis disse krav derefter gøres til en del af RFP'en og skal udføres af CISP'en, kan en skræddersyet løsning være den eneste udvej. Denne model kan ikke bruges til cloud-indkøb.

Organisationer i den offentlige sektor skal være klar over deres virksomhedsmål og effektivitetsbehov, men skal ikke binde nogen i en RFP og diktere systemets design og funktionalitet. I stedet bør organisationen forsøge at finde den bedste løsning til virksomheden. I stedet for at evaluere tilbud efter hundredvis eller endda tusindvis af bindende krav, der muligvis ikke gør tjenesterne bedre, bør organisationer inkludere evalueringskriterier, som er baserede på, hvor godt teknologien og de tilhørende tjenester opfylder eller forbedrer virksomhedsmål, uanset om det opfylder deres effektivitetsbehov, og muligheden for at finjustere virksomhedsregler ved hjælp af konfiguration.

Cloud-RFP'er bør stille de rigtige spørgsmål for at opnå de bedste løsninger. Da der i en cloud-model ikke købes fysiske aktiver, er mange af de traditionelle krav til indkøb af datacentre ikke gældende. ***Genbrug af spørgsmål om datacentre vil uundgåeligt føre til svar fra datacentre,*** *hvilket resulterer i, at CISP'er ikke kan byde, eller fører til dårligt udformede kontrakter, der forhindrer kunder i den offentlige sektor i at udnytte alle funktionerne og fordele ved cloud.*

En RFP for cloud-tjenester fokuserer på de vigtigste krav, som en CISP og cloud-tjenester skal leve op til, så leverandører, der opfylder kravene til GRUPPE 1, lever op til en høj standard. Kravene må heller ikke være for restriktive, så de ikke begrænser den offentlige sektors adgang til en bred vifte af kvalificerede CISP'er.

Eksempel på formulering i RFP: cloud-udbyderens muligheder

Se også de administrative minimumskrav for CISP'er for GRUPPE 1

Foreslåede kvalifikationskriterier for CISP	*Årsag*
Infrastruktur	
CISP-infrastrukturen bør tilbyde mindst to klynger med datacentre. Hver klynge skal bestå af mindst to datacentre, som har en forbindelse med lav forsinkelse, så Highly Available Active-Active-udrulninger og implementeringer af DR-BC-scenarier er mulige. Datacentrene i hver klynge skal være fysisk isolerede og i stand til arbejde selvstændigt i tilfælde af nedbrud.	*CISP'en skal kunne tilbyde en infrastruktur, der er egnet til at opbygge yderst tilgængelige programmer, hvor enkelte fejlpunkter kan undgås.*
CISP'en bør sørge for logisk og geografisk isolerede områder. Kundedata må ikke kopieres uden for disse områder af CISP'en.	*Ifølge kravene til dataplacering skal kunderne have fuld kontrol over, hvor deres data gemmes.*
CISP'en skal have mulighed for at levere en direkte, dedikeret og privat forbindelse mellem CISP-datacentrene.	*En privat forbindelse er et afgørende krav, hvis en hybrid-infrastruktur skal være sikker.*

CISP'en skal sørge for tilstrækkelige mekanismer, deriblandt kryptering af data i transit.	*Kunden kan kræve, at der en funktion, som sørger for, at data ikke kan sendes uden kryptering.*
Minimumscertificeringer for CISP	
CISP'en skal have en ISO 27001-certificering.	*Tredjepartsrevision, certificering og kreditering sikrer, at kunder kan lave benchmark for tjenester (og især platformen) med hensyn til kvalitet, sikkerhed og pålidelighed. Det er vigtigt, at et minimum af certificeringer kan påvises.*
CISP'en skal overholde CISPE's adfærdskodeks for databeskyttelse for at kunne levere funktioner og tjenester, der kan anvendes i overensstemmelse med GDPR, og som giver kunderne mulighed for at opbygge programmer, der er i overensstemmelse med GDPR.	*Kunden skal være i stand til at bygge eller køre programmer i overensstemmelse med GDPR.*
CISP'en skal sørge for rapporter, der gennemgås af tredjeparter, såsom SOC 1- og 2-rapporter (der beskriver de placeringer og tjenester, som benyttes af EC), så der opnås transparens med hensyn til CISP'ens kontrolforanstaltninger og procedurer.	*CISP'en skal være gennemsigtig med hensyn til, hvordan programmet drives og administreres. SOC-rapporter er afgørende for at sikre tillid og gennemsigtighed.*
CISP'en skal overholde pagten om klimaneutrale datacentre.	*Pagten om klimaneutrale datacentre forpligter CISP'en til at opnå klimaneutralitet inden 2030 og dermed gøre det muligt for brugeren, at støtte sine egne bæredygtighedsmål. Tredjepartsrevisorer er obligatoriske for udbydere > 250 FTE (ikke SMV'er).*
CISP'en skal overholde SWIPO IaaS adfærdskodeks for portabilitet.	*SWIPO IaaS adfærdskodeks for portabilitet sikrer, at tjenesterne opfylder kravene i art. 6 "Dataportering" i forordningen om fri udveksling af ikke-personlige data.*
Tjenestekarakteristika	
CISP-infrastrukturen skal være tilgængelig via programmatiske grænseflader (API'er) og en webbaseret administrationskonsol.	*Selvbetjeningsadgang og programmatiske grænseflader er en påkrævet standard hos CISP-udbydere, så formidlere fjernes mellem brugeradgang og selve leverandøren.*
CISP'en skal tilbyde en fundamental række tjenester, deriblandt: objektlagring, administreret relationsdatabase, administreret ikke-relationsdatabase, administrerede belastningsudlignere, overvågning og integreret automatisk skalering.	*Muligheden for virtuelle maskiner er ikke nok til, at en udbyder kan kvalificeres som cloud-udbyder. Cloud-udbydere skal tilbyde en række PaaS- og IaaS-tjenester, der forbedrer kundernes programmer og får dem til at fungere hurtigere.*
CISP'en skal give kunden frihed til at ændre brugen og konfigurationen af sine tjenester eller flytte data inden for eller uden for CISP'en (mulighed for selvbetjening).	*Selvbetjeningsadgang til tjenester og data er et ufravigeligt krav, som gør det muligt for kunden at være helt uafhængig.*
CISP'en skal give mulighed for "betaling pr. brug"-fakturering af deres tjenester.	*Betaling pr. brug gør det muligt for kunden at optimere sine workloads på en omkostningseffektiv måde, minimere risikoen og udnytte CISP'en til kortvarige programmer og PoC'er.*

Data- og systemsikkerhed	
CISP'en skal give kunden mulighed for at bevare den fulde kontrol over sine data, give kunden frihed til at vælge, hvor dataene opbevares (by- og byområde), og garantere, at ingen kundedata flyttes, medmindre kunden selv tager initiativ til en sådan flytning.	*Kunden skal have kontrol over, hvor dataene gemmes, hvordan adgangen til indholdet administreres og brugeradgang til tjenester og ressourcer.*
CISP'ens karakteristika skal give kunden fuld kontrol over sine sikkerhedspolitikker, blandt andet fortrolighed, integritet og tilgængelighed i forbindelse med kundedata og systemer.	*Kunden skal have mulighed for at definere og implementere sine sikkerhedsstandarder i alle workloads. Det er ikke nok at stole på, at udbyderen "gør det rigtige" med kundernes data.*
Omkostningskontrol	
CISP'en skal have mekanismer og værktøjer, der giver kunden mulighed for at holde øje med udgifter i en periode. Værktøjerne skal give mulighed for grundlæggende opdeling af udgifter med udgangspunkt i workload, tjeneste og konto.	
CISP'en skal tilbyde værktøjer, der giver kunderne påmindelser, når grænsen for udgifter er nået.	
CISP'en skal give kunden detaljerede regninger. Det skal være muligt at strukturere regningen efter workload, miljø og konto.	

CISP'erne bør også give svar på nedenstående spørgsmål om de tekniske krav.

LØSNINGER

CISP'en skal vise, hvordan de kan levere færdigbyggede skabeloner, og softwareløsninger, der enten hostes på eller er integreret hos CISP'en, til følgende løsninger:

- *Lager*
- *DevOps*
- *Sikkerhed/compliance*
- *Big data/analyse*
- *Virksomhedsprogrammer*
- *Telekommunikation og netværk*
- *Geospatial*
- *IoT*
- *[Andet]*

Give en oversigt over, hvordan CISP'en er blevet brugt til følgende workloads:

- *Gendannelse efter nedbrud*
- *Udvikling og test*
- *Arkivering*
- *Sikkerhedskopiering og gendannelse*
- *Big data*
- *Højtydende databehandling (High Performance Computing eller HPC)*
- *Tingenes internet (IoT)*
- *Websteder*
- *Serveruafhængig beregning*
- *DevOps*
- *Indholdslevering*
- *[Andet]*

2.2.2 Sammenligning af leverandører

Foruden minimumskravene i en RFP for cloud-tjenester er det vigtigt at udarbejde kriterier for, hvordan CISP-teknologier kan sammenlignes ved evaluering i forbindelse med budgivning på kontrakter.

RFP'er til cloud-tjenester bør spørge efter de cloud-funktioner, som en organisation har brug for, med en forståelse af, at kunden har ret til at bruge sådanne funktioner til at opbygge deres løsning. Funktionalitet ud over den standard, som en CISP kan levere (f.eks. færdigbyggede løsninger via CISP'en eller automatiseringsfunktioner) kan bruges til en mere meningsfuld analyse af "værdiskabende muligheder" eller "den bedste værdi" i en RFP for cloud-tjenester.

Den offentlige sektor har ofte brug for konkurrence mellem budgivere ved hjælp af evalueringskriterier såsom det økonomisk mest fordelagtige tilbud (MEAT) eller den laveste pris. Når parter i den offentlige sektor planlægger denne del af en RFP for cloud-tjenester, er det vigtigt at bruge en tilgang, hvor der tages højde for de unikke funktioner i en cloud. Det er for eksempel vigtigt at forstå, at når man skal sammenligne tilbud, så er det ikke nok, at man bare sammenligner regnskabsposter mellem cloud-udbyderens tilbud (f.eks. computerkraft eller lager). I stedet anbefaler vi på det kraftigste, at der fokuseres på løsninger på et højere niveau, f.eks. dem der er angivet ovenfor i afsnit *2.2.1*. Parter i den offentligt sektor kan derefter se på cloud-specifikke krav, som f.eks. dem, der er anført i *Bilag A – tekniske krav til sammenligning af budgivere*.

RFP'er bør angive de vigtigste cloud-karakteristika, der er nødvendige for, at dens cloud-løsning kan laves. For at gøre dette skal organisationer i den offentlige sektor benytte NIST-karakteristika (National Institute of Standards and Technology) og bruge tredjepartsanalytikeres rapporter til at sikre, at CISP'en har det bedste 'rigtige cloud'-tilbud, der fungerer i stor skala.

Eksempel på formulering i RFP: sammenligning af leverandører

*CISP'er skal besvare ALLE spørgsmålene til tekniske krav i **bilag A**.*

Respondenterne skal have følgende kendetegn og beskrive, hvordan de cloud-tjenester, de tilbyder, overholder de fem vigtige karakteristika for cloudcomputing[4].

1) ***Selvbetjening efter behov:** Respondenter skal give mulighed for ensidig klargøring af computerfunktioner, f.eks. servertid og netværkslager, som det behøves, automatisk uden krav om menneskelig indgriben for hver enkelt tjenesteudbyder. Respondenten skal angive muligheden for bestillingsaktivitet, så tjenester kan klargøres ensidigt (dvs. uden leverandørens kontrol eller godkendelse). Forklar, hvordan dette fungerer med dit produkt eller det tilbud, du formidler.*

2) ***Total netværksadgang**: Respondenten skal tilbyde flere muligheder for netværksforbindelse, hvoraf en af disse skal være internetbaseret. Forklar, hvordan dette fungerer med dit produkt eller det tilbud, du formidler.*

3) ***Sammenlægning af ressourcer**: Respondentens CISP skal tilbyde samlede computerressourcer, der betjener flere kunder ved hjælp af en model med flere lejere med virtuelle ressourcer, der tildeles dynamisk og tildeles igen i henhold til kundens behov. Brugeren kan vælge placeringen på et højere abstraktionsniveau (f.eks. land, område eller datacenterplacering). Respondenten skal give mulighed for skalering af disse ressourcer på få minutter eller timer efter en anmodning om klargøring. Forklar, hvordan dette fungerer med dit produkt eller det tilbud, du formidler.*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

*4) **Hurtig elasticitet**: Respondentens CISP skal gøre det muligt at klargøre og annullere klargøringen af tjenester (skalere op og ned), så tjenesten kan gøres tilgængelig inden for de foreskrevne minimumstider (maks. 'x' timer) i anmodningen om klargøring. Respondenten skal gøre det muligt at tilpasse faktureringen som følge af disse anmodninger om klargøring på time- eller dagsbasis.*

*5) **Målt tjeneste**: Respondenten skal gøre tjenesten synlig ved hjælp af et online-dashboard eller lignende elektroniske metoder.*

Desuden skal CISP'en:

- *Være en anerkendt førende leverandør af cloud-tjenester ifølge Gartner Magic Quadrant for IaaS[5]*
- *Levere brancheanerkendte tredjepartsanalytikerrapporter, der viser CISP'ernes dokumenterede kapacitet og pålidelighed.*

Som en sidste ting skal CISP'er sammenlignes ved hjælp af scenarierne i bilag B.

2.2.2.1 SLA'er (Service Level Agreements)

CISP'er leverer standardiserede kommercielle SLA'er til millioner af kunder og er derfor ikke i stand til at tilbyde tilpassede SLA'er, som det er tilfældet i en model med et lokalt datacenter. CISP-kunder (ofte med hjælp fra CISP-partnere) kan imidlertid tilrettelægge deres cloud-anvendelse for at udnytte en CISP's kommercielle SLA'er til at opfylde og overgå kundespecifikke krav og unikke SLA'er.

RFP'er for cloud-tjenester skal sikre, at CISP'er tilbyder de muligheder og den hjælp, der er nødvendig for at udnytte deres tjenester og kommercielle SLA'er, så de enkelte slutbrugere kan opfylde krav til ydeevnen og tilgængeligheden.

Eksempel på formulering i RFP: serviceniveauaftaler (SLA'er)

Angiv oplysninger om og links til CISP'ernes tilgang til serviceniveauaftaler (SLA'er).

***<ORGANIZATION>** skal altid være opmærksom på CISP'ers SLA'er og udrulle vigtige workloads og programmer på en sådan måde, at de fortsætter med at fungere i tilfælde af, at en SLA ikke opfyldes.*

***<ORGANIZATION>** er ansvarlig for at opretholde passende SLA'er i forbindelse med alt udstyr ejet af **<ORGANIZATION>** eller tjenester der leveres af **<ORGANIZATION>** og der anvendes sammen med CISP'en.*

*CISP'en skal give **<ORGANIZATION>** mulighed for at have løbende synlighed og rapporter om sin driftsmæssige SLA's effektivitet og dokumenterede retningslinjer for udnyttelse af CISP-infrastrukturen til at udforme tjenester med henblik på ydeevne, holdbarhed og pålidelighed.*

2.2.3 Indgåelse af kontrakter

CISP'ens vilkår og betingelser er beregnet til at vise, hvordan en model for cloud-tjenester fungerer (fysiske aktiver købes ikke, og CISP'er fungerer på enorm skala og tilbyder ensartede tjenester). Derfor er det vigtigt, at en CISP's vilkår og betingelser indarbejdes og benyttes i videst muligt omfang. Se afsnit *2.5* nedenfor for yderligere oplysninger om vilkår og betingelser og indgåelse af kontrakter.

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

2.2.3.1 Nye og ændrede tjenester

CISP'er sørger for ydeevnen ved hjælp af en tjeneste. I modsætning til almindelige lokale løsninger, der kræver opgraderinger og kontrakter til opretholdelse af tjenesten, tilbyder cloud-udbydere blot en ensartet tjeneste. For at en cloud-model kan opnå stordriftsfordele, udrulles opgraderinger og ændringer i den underliggende infrastruktur til alle brugere, ikke de enkelte brugere, og kunderne kan herefter vælge de tjenester, de skal bruge. Tjenesten er lettere at bruge end lokale systemer, som er blevet brugt hidtil, og cloud-udbydere tilbyder hele tiden nye og forbedrede tjenester, som kunderne kan bruge, som de vil.

Hvis de nye eller forbedrede CISP-tjenester ikke kan tilføjes efter tidsfristen for indsendelse af en RFP, begrænser organisationerne i den offentlige sektor sig fra at kunne benytte nye tjenester og forbedrede funktioner indtil udgivelsen af den næste rammeaftale. Derfor anbefaler vi på det kraftigste, at klargøringen af de tjenester, der er beskrevet i rammeaftalen, er omfattende, så det er muligt at tilføje nye CISP-tjenester efter tidsfristen for indsendelse. EU's indkøbslov begrænser muligvis introduktionen af betydelige, nye CISP-tjenester, som skal tilføjes i rammeaftalen, men opdateringer og nye versioner af tjenester, der ikke betragtes som materielle ændringer, kan tilføjes uden udfordring i forbindelse med køb.

Eksempel på formulering i RFP: nye og ændrede tjenester

CISP'en skal levere en omkostningseffektiv løsning, der benytter både dokumenterede og stabile virtualiseringsteknologier og revolutionerende teknologier, der hele tiden opdateres. ***<ORGANIZATION>*** *bekræfter og accepterer, at cloud-teknologier kan klargøres som delte tjenester til* ***<ORGANIZATION>*** *og CISP'ens øvrige kunder ud fra et almindeligt kodefundament og/eller fælles miljø, og CISP'en kan fra tid til anden: ændre, tilføje eller slette funktioner, ydeevne eller andre kendetegn ved cloud-tjenesterne, og hvis denne ændring, tilføjelse eller sletning udføres, skal cloud-tjenestens specifikationer ændres i overensstemmelse med dette.*

Denne leveringsordre omfatter alle de nuværende, nye eller forbedrede CISP-tjenester ***INDEN FOR RAMMEAFTALENS OMFANG****. CISP'ens cloud-tjenester, som kan benyttes af alle erhvervskunder, skal stilles til rådighed til* ***<ORGANIZATION>****.*

2.2.3.2 Leverandørfastlåsning/-reversibilitet

Cloud-teknologi betyder, at man er mindre afhængig af leverandører, fordi de fysiske aktiver ikke købes, og kunderne kan altid flytte deres data fra den ene cloud-udbyder til den anden.

Det er dog uundgåeligt med en vis grad af leverandørbinding, når man køber cloud-tjenester - da ikke alle clouds er ens, og derfor kan en CISP tilbyde tjenester og funktioner, som en anden ikke kan tilbyde – hvilket reducerer muligheden for at bruge sådanne tjenester hos en anden leverandør. En fornuftig tilgang er at kræve, at CISP'er leverer de nødvendige funktioner og tjenester til at forlade deres cloud, med dokumentation for, hvordan man bruger disse tjenester som en rimelig "exitstrategi" - da det er umuligt for en CISP at kende den unikke konfiguration af en kundes brug af deres standardiserede tjenester, og som sådan levere en skræddersyet exitplan.

Se afsnit 2.3.1.2 for oplysninger om branchens adfærdskodekser vedrørende “dataportering” og “ændring af cloududbyder” for at opfylde kravene i artikel 6 i EU's “forordning om fri udveksling af ikke-personlige data”.

Eksempel på formulering i RFP: klargøring og afslutning

<ORGANIZATION> søger tilbud med en fornuftig exitstrategi, der forhindrer afhængighed. <ORGANIZATION> køber ikke fysiske aktiver, og CISP'en skal gøre det muligt at flytte it-stakken op og flytte den ned igen. CISP'en skal sørge for portabilitetsværktøjer og -tjenester, der gør det muligt at migrere til og fra CISP-platformen, hvilket reducerer afhængigheden. Detaljeret dokumentation om, hvordan CISP'ens portabilitetsværktøjer og -tjenester bruges, skal fungere som en rimelig exitplan.

*CISP'en må ikke have **påkrævede** minimums bindingsperioder eller **påkrævede** langfristede kontrakter.*

Data, der gemmes hos en udbyder, kan altid eksporteres af kunden. CISP'en skal give <ORGANIZATION> lov til at flytte data efter behov både til og fra CISP'ens lager. CISP'en skal desuden gøre det muligt af downloade afbildninger af virtuelle maskiner og portere dem til en ny cloud-udbyder. <ORGANIZATION> kan eksportere sine maskinafbildninger og bruge dem lokalt eller hos en anden udbyder (afhængigt af begrænsninger for softwarelicensering).

2.3 Sikkerhed

Både CISP'en og cloud-kunderne er ansvarlige for sikkerhed og overholdelse af angivne standarder. I denne model bestemmer cloud-kunder, hvordan de laver en arkitektur og sikrer deres programmer og data i infrastrukturen, mens CISP'er er ansvarlige for at levere tjenester på en yderst sikker og styret platform og for at levere en lang række yderligere sikkerhedsfunktioner. Niveauet af CISP- og kundeansvar i denne model afhænger af cloud-udrulningsmodellen (IaaS/PaaS/SaaS), og kunderne skal være indforståede med deres ansvar i hver enkelt model.

Det er vigtigt at forstå denne model for ansvarsdeling, hvis man skal udarbejde en vellykket RFP for cloud-tjenester. Organisationer i den offentlige sektor bør sikre, at de ved, hvad en CISP har ansvar for, hvad de selv har ansvar for, og hvordan konsulentfirmaer, ISV'er og partnere og deres løsninger kan være nyttige.

2.3.1 Minimumskrav

Muligheder er nøgleordet, når det gælder sikkerhed i clouden. Organisationer i den offentlige sektor bør stille krav til CISP'er og forlange, at de kan sørge for de nødvendige sikkerhedsmuligheder, så kunderne kan leve op til deres ansvar i modellen for ansvarsdeling. Som det fremgår af listen med repræsentative krav nedenfor, så skal CISP'en sørge for en ensartet mulighed, så kunden kan udnytte deres unikke cloud-miljø sikkert.

- ***Sørg for** netværksfirewalls og firewall**muligheder** til webprogrammer, så kunderne kan oprette private netværk og vælge, hvem der har adgang til forekomster og programmer.*
- ***Sørg for** netværks**muligheder** for private eller dedikerede forbindelser fra dit kontor eller lokale miljø.*
- ***Sørg** for **mulighed for** at implementere en strategi med forsvar i dybden og forhindring af DDoS-angreb.*
- ***Mulighed** for data-kryptering i lager- og databasetjenester.*
- ***Sørg for** fleksible **valgmuligheder** for nøglestyring, så du kan vælge, om CISP'en skal administrere krypteringsnøglerne, eller om kunden skal have fuld kontrol over nøglerne.*
- ***Sørg for API'er** til kunder, så de kan integrere kryptering og databeskyttelse i enhver tjeneste, der udvikles eller udrulles i et CISP-miljø.*
- ***Sørg for** udrulnings**værktøjer** til at administrere oprettelsen og udfasningen af CISP-ressourcer i henhold til organisationens standard.*
- ***Sørg for værktøjer** til lager- og konfigurationsstyring, der identificerer CISP-ressourcer og derefter holder øje med og administrerer ændringer i disse værktøjer med tiden.*
- ***Sørg for værktøjer og funktioner**, der giver kunder mulighed for at se, præcis hvad der sker i deres CISP-miljø.*
- ***Sørg** for dyb **synlighed** i API-kald, herunder hvem, hvad, hvornår, og hvorfra opkald blev foretaget.*

- ***Sørg for muligheder*** *for samling af logfiler, så undersøgelser og rapportering af overholdelse af angivne standarder strømlines.*
- ***Sørg for muligheder*** *for konfiguration af påmindelser, når bestemte hændelser finder sted, eller når grænseværdier overskrides.*
- ***Sørg for muligheder*** *for at definere, håndhæve og administrere brugeradgangspolitikker i alle CISP-tjenester.*
- ***Sørg for mulighed for*** *at definere enkelte brugerkonti med tilladelser i alle CISP-ressourcer.*
- ***Sørg for mulighed for*** *at integrere og samordne med virksomhedsbiblioteker for at nedbringe administrative udgifter og give slutbrugere en bedre oplevelse.*

Flere af disse krav findes i*Bilag A – tekniske krav til sammenligning af budgivere*.

Funktionalitet ud over minimumsstandarden for sikkerhed kan bruges og give en mere betydningsfuld analyse af "værdiskabende muligheder" eller "den bedste værdi" i en RFP. Og jo flere funktioner, der er indbyggede eller automatiske, når det gælder sikkerheden, desto bedre. Igen henvises til*Bilag A – tekniske krav til sammenligning af budgivere* for kravene til sammenligning af budgivere.

Organisationer i den offentlige sektor bør ser på cloud-akkrediteringscertificeringer og -evalueringer for at sikre, at den påkrævede CISP-sikkerhedskontrol er på plads. Eksempel: Overvej en CISP, som er blevet valideret og certificeret af en uafhængig kontrollant for at bekræfte overholdelse af ISO 27001-certificeringsstandarden. ISO 27001 Anneks A, domæne 14 omhandler de specifikke kontrolforanstaltninger, som CISP overholder ifølge ISO-kravene vedrørende indkøb, udvikling og vedligeholdelse af systemer. Disse kontrolforanstaltninger vil formentlig dække de fleste kontrolforanstaltninger i forbindelse med indkøb, udvikling og vedligeholdelse af systemer (hvis ikke dem alle), der typisk er påkrævet af en organisation i it-relateret RFP. Derfor giver det mening, at en organisation simpelthen kræver, at en CISP er ISO 27001-certificeret, i stedet for at lave det samme arbejde igen og igen og angive kontrolkrav i forbindelse med indkøb, udvikling og vedligeholdelse af systemer i en RFP for cloud-tjenester.

Metoden med at udnytte tredjepartsrapporter om overholdelse kan f.eks. anvendes på de fleste sikkerheds- og overensstemmelseskontroller: CISPE GDPR adfærdskodeks, ISO, SOC osv.

Eksempel på formulering i RFP: Sikkerhed

CISP'en skal afsløre sine ikke-patenterede sikkerhedsprocesser og tekniske begrænsninger til ***<ORGANIZATION>****, så der opnås tilstrækkelig beskyttelse og fleksibilitet mellem* ***<ORGANIZATION>*** *og tjenesteudbyderen.*

CISP'en skal angive sine roller og ansvarsområder i forbindelse med sikkerhed og compliance:

- *Beskrive CISP'ens og* ***<ORGANIZATION>****s sikkerhedsrelaterede roller og ansvarsområder i tilbuddet. Vær klar med hensyn til afgrænsningen af ansvarsområder og beskriv de CISP-tjenester, der skal hjælpe* ***<ORGANIZATION>*** *med at opbygge og automatisere sikkerhedsfunktioner i sit cloud-miljø.*
- *Besvare de tekniske spørgsmål i* ***BILAG A*** *vedrørende* ***<ORGANIZATION'S>*** sikkerhedskrav.

EJERSKAB OG KONTROL AF <ORGANIZATION>S INDHOLD

Beskriv, hvordan CISP'ens muligheder kan beskytte ***<ORGANIZATION'S>*** *datasikkerhed. Medtag de kontroller, der er indført for at sikre beskyttelsen af* ***<ORGANIZATIONS>*** *indhold. CISP'en skal sørge for avanceret områdeisolation, så objekter, der er lagret i et område, aldrig forlader området, medmindre* ***<ORGANIZATION>*** *udtrykkeligt overfører dem til et andet område.*

- *<ORGANIZATION> skal administrere adgangen til sit indhold, sine tjenester og sine ressourcer. CISP'en skal sørge for en række avancerede funktioner til adgang, kryptering og logføring, der hjælper <ORGANIZATION> med at gøre dette effektivt. CISP'en vil hverken tilgå eller bruge <ORGANIZATION'S> indhold til andre formål end dem, der er lovpligtige, og med henblik på vedligeholdelse af CISP's tjenester og levere dem til <ORGANIZATION> og deres slutbrugere.*

- *<ORGANIZATION> vælger de områder, hvor indholdet lagres. CISP'en vil hverken flytte eller kopiere <ORGANIZATION'S> indhold uden for sine valgte områder, medmindre det er lovpligtigt og nødvendigt for vedligeholdelsen af CISP's tjenester, og levere dem til <ORGANIZATION> og dennes slutbrugere.*

- *<ORGANIZATION> vælger selv, hvordan dens indhold skal sikres. CISP'en skal sørge for avanceret kryptering til <ORGANIZATION'S> indhold, når det sendes eller ikke bruges, og give <ORGANIZATION> mulighed for at administrere sine egne krypteringsnøgler.*

- *CISP'en skal have et program til sikring af sikkerheden ved hjælp af global bedste praksis for beskyttelse af privatlivets fred og databeskyttelse for at <ORGANIZATION> kan etablere, drive og udnytte CISP's sikkerhedskontrolmiljø. Sikkerhedsbeskyttelser og kontrolprocesser skal valideres uafhængigt af flere uafhængige vurderinger fra tredjeparter.*

Certificeringer og evalueringer af cloud-akkreditering giver organisationer i den offentlige sektor sikkerhed for, at CISP'er har effektive fysiske og logiske sikkerhedskontroller på plads. Når disse akkrediteringer benyttes i RFP'er, strømlines indkøbsprocessen, så man undgår dobbeltarbejde og alt for krævende processer eller godkendelsesprocedurer, der muligvis ikke er påkrævede for et cloud-miljø.

Cloud-RFP'er bør give CISP'er mulighed for at bevise, at de opfylder compliance-akkrediteringerne og -evalueringerne. Som tidligere nævnt er der en betragtelig overlapning i risikoscenarierne og retningslinjerne for risikostyring i disse akkrediteringsordninger, og fordi kontrolforanstaltninger og krav kombineres i disse akkrediteringer, klares overholdelsen i en RFP hurtigere med krav om, at CISP'er overholder akkrediteringerne, end med dobbeltarbejde i angivelsen, f.eks. individuelle kontrolforanstaltninger (hvoraf mange kan være fra tidligere RFP'er, der er direkte på lokale datacentre og derfor muligvis ikke gælder for cloudcomputing).

BEMÆRK: Det er også meget vigtigt at vide, hvordan man får adgang til de rapporter, der er angivet nedenfor. Et eksempel er SOC 1- og SOC 2-rapporter, der typisk er følsomme dokumenter. Det er nødvendigt at forstå de aftaler, der er nødvendige for at få adgang til dem (f.eks. en fortrolighedsaftale (NDA)), og det er ikke nok bare at bede om, at dokumenterne sendes som en del af RFP-svaret (disse dokumenter kan offentliggøres via Open Records-lovgivningen eller lignende, hvilket kan kompromittere cloud-sikkerheden).

Eksempel på formulering i RFP: Compliance

Brugen af disse anerkendte standarder for compliance og drift, der er inspireret af retningslinjerne for drift af cloud-tjenester, deriblandt datahåndtering, datasikkerhed, fortrolighed, tilgængelighed osv., strømliner indkøb af cloud-teknologi.

<ORGANIZATION> skal evaluere unikke tilbud i forhold til de accepterede standarder for sikkerhed, compliance og drift, som er beskrevet nedenfor og i bilag A. Når man ser på leverandørens certificering for compliance i forhold til hver enkelt standard, kan <ORGANIZATION> benytte et minimum af overholdelse i forhold til standarden som udgangspunkt, når tilbuddet evalueres.

Hvis man kræver, at CISP'en fortsætte med at overholde minimumstandarden i kontraktens løbetid, giver det en fordel, fordi overholdelsen af tjenesten altid er aktuel.

*CISP'en, som der bydes på (direkte eller via en forhandler), skal kunne dokumentere sin evne til at opfylde følgende uafhængige tredjepartsattester, rapporter og certificeringer (Bemærk - hvis nogle af disse attester, rapporter og certificeringer er underlagt begrænsninger for offentliggørelse på grund af sikkerhedsspørgsmål, vil **<Organization>** samarbejde med CISP'en for at opnå adgang efter fælles aftale):*

Certificeringer/bekræftelser	*Love, bestemmelser og privatliv*	*Tilpasninger/rammer*
☐ C5 (Tyskland)		*☐ CDSA*
☐ CISPE-adfærdskodeks for databeskyttelse (GDPR)		
☐ CNDCP (Pagt om klimaneutrale datacentre)		
☐ DIACAP	*☐ EU forordningen om databeskyttelse*	*☐ CIS*
☐ DoD SRG niveau 2 og 4	*☐ EU-modelklausuler*	*☐ Info om strafferetspleje Service (CJIS)*
☐ HDS (Frankrig, sundhedspleje)		
☐ FedRAMP	*☐ FERPA*	*☐ CSA*
☐ FIPS 140-2	*☐ GDPR*	*☐ EU's og USA's værn om privatlivets fred*
☐ ISO 9001	*☐ GLBA*	*☐ EU's Safe Harbor*
☐ ISO 27001	*☐ HIPAA*	*☐ FISC*
☐ ISO 27017	*☐ HITECH*	*☐ FISMA*
☐ ISO 27018	*☐ IRS 1075*	*☐ G-Cloud [Storbritannien]*
☐ IRAP [Australien]	*☐ ITAR*	*☐ GxP (FDA CFR 21 del 11)*
☐ MTCS Tier 3 [Singapore]	*☐ PDPA – 2010 [Malaysia]*	*☐ ICREA*
☐ PCI DSS Niveau 1	*☐ PDPA – 2012 [Singapore]*	*☐ IT Grundschutz [Tyskland]*
☐ SEC-regel 17-a-4(f)	*☐ PIPEDA [Canada]*	*☐ MARS – E*
☐ SecNumCloud (Frankrig)		
☐ SOC1 / ISAE 3402	*☐ Privacy Act [Australien]*	*☐ MITA 3.0*
☐ SOC2 / SOC3	*☐ Privacy Act [New Zealand]*	*☐ MPAA*
☐ SWIPO IaaS-kode		
	☐ Spansk DPA-godkendelse	*☐ NIST*
	☐ U.K. DPA - 1988	*☐ Uptime Institute Tiers*
	☐ VPAT/afsnit 508	*☐ Principperne for cloudsikkerhed i Storbritannien*

Ovenstående liste er kun til illustrationsformål og skal ikke betragtes som en udførlig liste over alle de certificeringer og standarder, der kan gælde for cloud-tjenester.

2.3.1.1 Databeskyttelse

En vigtig overvejelse ved brug af cloud-tjenester er, at behandlingen af personoplysninger sker i overensstemmelse med gældende EU-lovgivning om databeskyttelse, herunder den generelle forordning om databeskyttelse (GDPR). GDPR er en principbaseret forordning og indeholder derfor ikke sektorspecifik vejledning, der kan hjælpe med at sikre overholdelse. GDPR tilskynder imidlertid til at indføre complianceværktøjer som f.eks. adfærdskodekser for at give en sådan vejledning. CISPE har i samarbejde med den franske databeskyttelsesmyndighed (CNIL) udarbejdet en adfærdskodeks for databeskyttelse (CISPE-kodeks[6]), der er godkendt af Det Europæiske Databeskyttelsesråd og har generel gyldighed i Europa. Formålet med kodeksen er at hjælpe CISP'er med at overholde GDPR og vejlede kunderne i vurderingen af, om CISP'er er egnede til den behandling af personoplysninger, som kunden ønsker at udføre.

- Kodeksen fokuserer udelukkende på IaaS-sektoren og omhandler IaaS-udbyderens specifikke roller og ansvar.
- Den bidrager til at tydeliggøre aspekterne af fair og gennemsigtig behandling og passende sikkerhedsforanstaltninger i forbindelse med cloud-infrastrukturtjenester (GDPR, artikel 40 [2]).
- Den hjælper kunderne med at forstå, hvordan de kan bevare ejerskabet over deres data ved at sikre, at de forbliver inden for EU.
- Den fremmer bedste praksis for databeskyttelse, der støtter EU's GAIA-X-initiativ til udvikling af europæiske clouddata-tjenester.

CISP's overholdelse af adfærskodeksen on databeskyttelse som CISPE-kodeksen giver sikkerhed for, at personoplysninger vil blive behandlet i nøje overensstemmelse med GDPR.

Eksempel på formulering i RFP: Databeskyttelse

CISP'en, som der bydes på (direkte eller gennem en forhandler), skal kunne dokumentere sin evne til at overholde en adfærdskodeks for databeskyttelse som f.eks. CISPE-koden. Kodeksen for databeskyttelse skal være i overensstemmelse med de krav, der er fastsat i GDPR-rammen. Kodeksen bør som minimum omfatte: (1) en klar definition af CISP'ens roller og ansvarsområder, (2) et krav om, at CISP'en ikke må anvende kundedata til markedsførings- eller reklameformål, og (3) kundernes mulighed for at vælge CISP-tjenester, der gør det muligt at behandle data udelukkende inden for Det Europæiske Økonomiske Samarbejdsområde. Overholdelse af kodeksen skal kontrolleres af eksterne uafhængige revisorer (overvågningsorganer), der er akkrediteret af uafhængige, eksterne revisorer, som er akkrediteret af Den Europæiske Tilsynsmyndighed for Databeskyttelse.

2.3.1.2 Ændring af cloud-udbyder og overførsel af data

Kunderne bør have frihed til at vælge de cloud-tjenester, de ønsker at bruge, og ikke være "låst fast" af en CISP- eller PaaS/SaaS-udbyder.

CISP-leverede cloud-tjenester er standardiserede og tilbydes på et "en til mange"-grundlag, hvor tjenesterne konfigureres, tilvejebringes og kontrolleres af kunden. En af fordelene ved cloudcomputing er, at kunderne har mulighed for at vælge de standardiserede tjenester, de har brug for til at udvikle deres

[6] https://cispe.cloud/code-of-conduct/

unikke programmer og løsninger. Denne fordel omfatter også muligheden for at skifte til nye eller andre tjenester, der bedst opfylder kundernes behov på et hvilket som helst tidspunkt.

Ligesom med databeskyttelse kan adfærdskodekser være med til at give kunderne sikkerhed og tillid, når de skal skifte til cloud fra en lokal infrastruktur, eller når de skifter mellem CISP'er. Sammen med EuroCIO (den europæiske sammenslutning af CIO'er) var CISPE medansvarlig for udviklingen af adfærdskodeksen for dataportabilitet og ændring af cloud-tjenester for IaaS cloud-tjenester (SWIPO IaaS-kode[7,8]). Den første version af kodeksen blev udviklet i overensstemmelse med EU's forordning om fri udveksling af data, overdraget til Europa-Kommissionen i november 2019 under det finske EU-formandskab og offentliggjort af foreningen SWIPO AISBL i maj 2020. I april 2021 blev det erklæret af SWIPO AISBL, at de første tjenester overholder kodeksen, og i maj 2021 blev det erklæret at de første CISPE-medlemstjenester overholder kodeksen.

Eksempel på formulering i RFP: Ændring af cloud-udbyder og overførsel af data

CISP'en, som der bydes på (direkte eller gennem en forhandler), skal kunne dokumentere sin evne til at overholde en adfærdskodeks for "ændring og dataoverførsel" som f.eks. SWIPO IaaS-koden. Kodeksen skal indeholde detaljerede oplysninger om, hvordan en CISP tilbyder kunderne en sikker overførsel af forretningsdata, hvis de beslutter sig for at skifte fra en CISP.

2.3.2 Sammenligning af leverandører

Ligesom med de tekniske kriterier i afsnittene ovenfor (foruden minimumskravene til sikkerhed i en RFP for cloud-tjenester) er det vigtigt at udarbejde kriterier for, hvordan CISP'ers sikkerhedsmuligheder og tjenester kan sammenlignes i en evaluering i forbindelse med budgivning.

Se *Bilag A – tekniske krav til sammenligning af budgivere* for eksempler på CISP-sikkerhedskrav. Vi anbefaler på det kraftigste, at nedenstående muligheder er afgørende for parter i den offentlige sektor, der evaluerer CISP'er:

Eksempel på formulering i RFP: vigtige sikkerhedsovervejelser

- *CISP'en skal være indforstået med modellen for ansvarsdeling og sørge for dokumentation, der hjælper kunder med at forstå afgrænsningen mellem sikkerhedsansvar for CISP'ens funktioner og tjenester (f.eks. i forbindelse med GDPR)*
- *Dokumenteret CISP-infrastruktursikkerhed med offentlig, ikke-navnebeskyttet dokumentation af CISP'ens sikkerhedsstatus og fysiske/logiske kontrolforanstaltninger*
- *CISP-support, der er specifik for cloud-sikkerhed*
- *Tjenester, der giver kunder mulighed for at formalisere design af konti, automatisering af sikkerhed og cloud-governance, implementering af kontrolforanstaltninger og strømlining af revision*
- *Muligheden for at oprette, klargøre og administrere en række ressourcer på en skabelonlignende måde (omfatter førsteklasses sikkerhedsskabeloner, som udvikles af en CISP eller dennes partner)*
- *Muligheden for at etablere pålidelig og gentagelig betjening af kontrolfunktioner*
- *Funktioner til vedvarende revision i realtid*
- *Muligheden for at lave tekniske scripts til politikker for cloud-governance*
- *Muligheden for at oprette tvingende funktioner, der ikke kan tilsidesættes af brugere, der ikke har tilladelse til at ændre disse funktioner*

[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/

- *Muligheden for at udføre pålidelig implementering af det, der tidligere stod i politikker, standarder og bestemmelser, samt muligheden for at oprette sikkerhed, der kan håndhæves, og compliance, hvilket til gengæld giver en pålidelig cloud-governancemodel cloud til it-miljøer*
- *Tjenester til at beskytte mod de mest almindelige og hyppige gentagne DDoS-angreb (distributed denial of service) mod netværk og transportlag samt mulighed for at skrive brugerdefinerede regler mod sofistikerede angreb på programlag*
- *Administreret trusselregistreringsservice*

2.3.3 Indgåelse af kontrakter

Som tidligere nævnt, er CISP'ens vilkår og betingelser er beregnet til at vise, hvordan en model for cloud-tjenester fungerer (fysiske aktiver købes ikke, og CISP'er fungerer på enorm skala og tilbyder ensartede tjenester). Derfor er det vigtigt, at en CISP's vilkår og betingelser indarbejdes og benyttes i videst muligt omfang. Se afsnit *2.5* nedenfor for yderligere oplysninger om vilkår og betingelser og indgåelse af kontrakter.

Med hensyn til sikkerheden anbefaler vi som sagt på det kraftigste, at CISP'er hele tiden har mulighed for at opdatere tilbud, eller at leverandører kan tilføje produkter efter indsendelsesdatoen, så længe de overholder RFP'ens oprindelige parametre. Dette beviser, at sikkerhedsfunktioner og -tjenester udvikler sig hurtigt, og CISP'er udgiver tit tjenester med fokus på sikkerhed, som i mange tilfælde er gratis at benytte. Bemærk: Det er vigtigt at have et grundlæggende sikkerhedsniveau (se minimumskravene ovenfor) som en garanti for, at ændringer ikke forringer sikkerhedsprodukterne.

Modellen for ansvarsdeling er naturligvis kernen i sikkerheden i en RFP for cloud-tjenester. Alle parter skal være indforståede med deres sikkerhedsansvar, og CISP'er skal dokumentere CISP-/kundesikkerhedsansvar for CISP'ers cloud-teknologier og sørge for dokumentation, der hjælper kunder med at indbygge og automatisere retningslinjer for sikkerhed.

En cloud-rammeaftale bør give fleksibiliteten til at fjerne en leverandør, hvis vedkommende ikke længere overholder minimumskravene til sikkerhed og compliance som fastsat i RFP'en for cloud-tjenester.

2.4 Priser

For at indgå kontrakter til cloud-teknologi på en måde, der tager højde for skiftende efterspørgsel, har organisationer i den offentlige sektor brug for en kontrakt, hvor de kan betale for tjenester efter forbrug, og hvor der er den påkrævede cloud-governance og synlighed i forbindelse med brug og udgifter.

Først og fremmest bør RFP'er for cloud-tjenester se på værdien og de samlede omkostninger ved ejerskab (TCO) i stedet for en simpel sammenligning af produktpriser. Denne almindelige metode, hvor man ser på den laveste produktpris, passer ikke til cloud-modellen, og derfor fører den som regel ikke til det mest økonomisk fordelagtige tilbud eller den laveste samlede pris.

For at CISP'en bedre kan evaluere prisen, er det nyttigt, hvis man først har forhåndskvalificering eller mulighed for at lave en shortliste med CISP'er med ***minimumskrav for priser****, så CISP'er med lignende muligheder er kvalificerede til rammeaftalen. Derefter kan man i evalueringsprocessen for call-offs og minikonkurrencer se på et udvalg af typiske eksempler på cloud-arkitekturer og* ***prisscenarier****, der passer til nogle af de typiske workloads i den offentlige sektor, og lade CISP'er prissætte dem. Live-testdemoer anbefales også, så det er muligt at sammenligne CISP'ernes cloud-teknologitjenesters ydeevne og elasticitet. Se bilag B for et eksempel på et test-script til en demonstration af cloud-teknologier.*

2.4.1 Minimumskrav

Afsnittet om priser i en RFP for cloud-tjenester består af fire vigtige elementer:

1. **Brugspris**: Cloud-kunder benytter en brugsmodel med betaling efter forbrug, hvor de i slutningen af hver måned blot betaler for deres forbrug, hvilket er optimalt, når de skal måle udnyttelses- og ressourcemålinger.
2. **Gennemsigtig prissætning:** CISP-priserne bør være offentligt tilgængelige og gennemsigtige.
3. **Dynamiske priser**: Giv mulighed for fleksibiliteten til, at cloud-priser kan følge udviklingen i markedspriserne. Med denne metode udnytter man cloud-prisernes dynamiske og konkurrencedygtige tendens og giver mulighed for innovation og rabatter.
4. **Kontrollerede udgifter**: CISP'er skal give kunderne værktøjer til rapportering, overvågning og prognoser, (1) så de kan overvåge forbrug og udgifter på både overordnede og detaljerede niveauer, (2) så de får påmindelser om, at forbruget når tilpassede grænseværdier, (3) og så de kan lave et estimat for forbrug og udgifter og lægge fremtidige cloud-budgetter.

Eksempel på formulering i RFP: priser

<ORGANIZATION> anmoder om at de CISP'er, der henvender sig, medtager deres foreslåede metode og prismodel for levering af alle deres tjenester til slutbrugere som en kommerciel cloud-mulighed.

CISP'en skal sørge for følgende:

- *Et dokument med en beskrivelse af tjenesten eller links til definitioner af tjenesterne*
- *Et dokument med vilkår og betingelser*
- *Dokumenter med priser (links til offentlige priser er acceptable med formodningen om, at det er muligt at anmode om et komplet dokument med prislister og prissætning)*

Prisen skal være omkostningen for tjenestens mest almindelige konfiguration. CISP'er skal give muligheder for mængdebaseret rabat og værktøjer til beregning af priser med henblik på at finde ud af den faktiske pris på det, der købes, og den samlede værdi, der leveres til køberen (f.eks. tjenester til optimering og den deraf følgende reduktion af udgifter).

Købere, som er omfattet af rammeaftalen, kan bede leverandørerne om at uddybe deres beskrivelse af tjenesten, vilkår og betingelser, priser eller dokumenter med tjenestedefinition/model. Der skal føres en fortegnelse over kommunikationen med leverandørerne.

Yderligere krav til priser

- *Der skal sørges for cloud-teknologier med en dynamisk prismodel, som giver mest mulig virksomhedsfleksibilitet samt mulighed for skalerbarhed og vækst.*
- *Prisattributter skal omfatte følgende:*
  - *Er priserne en behovsbaseret tjeneste, som er baseret på forbrug? Uddyb din prismodel.*
  - *Kan du opnå yderligere rabatter, hvis du forpligter dig til at bruge og/eller købe i store mængder? Uddyb hvordan.*
  - *Er priserne offentligt tilgængelige og gennemsigtige? Angiv links til offentligt tilgængelige priser.*
  - *Er priserne dynamiske, og tilpasses de hurtigt og effektivt til markedskonkurrencen?*
  - *Tilbyder du bedste praksis og ressourcer til at spore udgifter?*
  - *Sørger du for retningslinjer og ressourcer til optimering af omkostninger?*

Gennemsigtighed af priser
*Da priserne på kommercielle cloud-teknologier hele tiden falder på grund af innovation og konkurrence, må den målte pris pr. produkt for CISP-tjenesten, der betales af **<ORGANIZATION>** i henhold til rammeaftalen, aldrig overskride cloud-udbyderens pris pr. produkt, som er offentliggjort på udbyderens websted og er gældende på det pågældende tidspunkt, hvor kunden bruger tjenesten.*

Budget- og faktureringspåmindelser/-rapporter
*For at CISP'er kan vise, at cloud-teknologierne kan leveres og bruges, skal de give **<ORGANIZATION>** værktøjer til oprettelse af detaljerede faktureringsrapporter med oplysninger om udgifter pr. time, dag eller måned, hver enkelt konto i en organisation efter produkt eller produktressourcer eller efter kundedefinerede tags. **<ORGANIZATION>** anerkender, at som en del af modellen for ansvarsdeling i cloud-systemet er **<ORGANIZATION>** ansvarlige for brug af CISP'ens budget- og faktureringsfunktioner og -værktøjer, så de kan overholde unikke prognose- og rapporteringskrav.*

- *Sørg for oplysninger om, hvordan **<ORGANIZATION>** kan se faktureringsoplysninger på både detaljerede og overordnede niveauer, se visualisering af udgiftsmønstre i forbindelse med CISP-ressourcer i en periode og lave prognoser om fremtidige udgifter.*
- *Sørg for oplysninger om, hvordan **<ORGANIZATION>** kan filtrere i visningen af brug/fakturering efter tjeneste, efter tilknyttet konto eller efter tilpassede tags, der anvendes i ressourcer, og oprette faktureringspåmindelser, der sendes, når brugen af tjenester nærmer sig eller overskrider de grænseværdier/budgetter, som er fastsat af **<ORGANIZATION>**.*
- *Sørg for oplysninger om, hvordan **<ORGANIZATION>** kan lave prognoser for, hvor mange cloud-tjenester der skal bruges i en defineret prognoseperiode baseret på tidligere brug. CISP skal tilbyde et **estimat** for, hvad **<ORGANIZATION'S>** CISP-faktura bliver, og give **<ORGANIZATION>** mulighed for at bruge påmindelser og budgetter for beløb, der forventes at bruge, for at få mere kontrol over omkostninger og udgifter.*

2.4.2 Sammenligning af leverandører

Organisationer i den offentlige sektor har ofte brug for konkurrence mellem budgivere ved hjælp af evalueringskriterier såsom den bedste værdi, MEAT (det mest rentable tilbud) eller den laveste pris. Når priser planlægges i rammeaftalens call-offs eller minikonkurrencer, er det vigtigt at bruge en tilgang, der tager cloud-teknologiens unikke træk i betragtning. F.eks. er det ikke er en effektiv måde at sammenligne linjeelementer mellem cloud-udbyderes tilbud (f.eks. beregning eller lagring), da det ikke tager højde for funktioner som ydeevne, omkostningsoptimering ved hjælp af tjenester der er udviklet til skyen og CISP-overvågningsværktøjer eller differentiering af tjenester, som CISP'er kan tilbyde gratis. Desuden kan katalogprisen for en CISP være på titusindvis af poster, og prismodellerne varierer fra tjeneste til tjeneste og fra udbyder til udbyder.

Analysér de samlede ejerudgifter

Vi anbefaler, at du fokuserer på de samlede omkostninger ved ejerskab (TCO) blandt de definerede brugstilfælde, der tager højde for alle aspekter af en cloud-løsning (deriblandt partnertjenester, standardrabat hos CISP'er, tekniske funktioner, der kan forbedre ydeevnen og reducere/optimere udgifter osv.)

Sammenlign efter scenarier

Evalueringen kan også være en overvejelse af de typiske scenarier, der svarer til almindelige systemer eller programmer. Disse scenarier (f.eks. webhosting eller implementeringen af et HR-system med x antal brugere osv.) kan omfatte variabler som f.eks. ressourcernes hastighed og omfang, programmets eller løsningens ydeevne, hvor hurtigt man kan få adgang til lageret, en lille mængde komplekse data sammenlignet med enkle beregningsopgaver med en stor mængde osv. Programmerne eller systemerne

kan også have typiske scenarier som f.eks. behandling af en stor mængde som ved selvangivelse eller beskeder i nødstilfælde som f.eks. stormflodsvarsel. Scenarierne skal være omfattende og inkludere både omfanget af teknologier og tjenester, som kunden muligvis skal bruge i løbet af projektet. På den måde kan kunden sammenligne projektets anslåede samlede omkostninger.

Sammenlign scenarier økonomisk og teknisk

Det er også vigtigt at tage højde for tekniske fordele, når priserne i CISP'ernes tilbud sammenlignes. Den ene CISP kan f.eks. muligvis give kunderne mulighed for at oprette en aktiv-aktiv-topologi for gendannelse efter nedbrud, fordi den har en model med datacentre i klynger i et geografisk område. En CISP, der ikke har denne form for redundans og datacenterkonfiguration, kan være x % dyrere, når man tager højde for omkostningerne ved at indregne behovene for gendannelse efter nedbrud. Et eksempel på, hvorfor en holistisk tilgang til priser, der omfatter yderligere tekniske funktioner, er vigtig, når CISP'er skal evalueres. Overvej nedenstående alternativ, som er en direkte sammenligning.

Eksempel: En kunde vil sammenligne prisen på et objektlagring fra kvalificerede CISP'er i en rammeaftale. Prisen for lager-'enhed' fra CISP 1 er 0,023 EUR/GB. Prisen på samme 'enhed' CISP 2 er 0,01 EUR/GB. Ved en enkel sammenligning af enheder vil kunden stille kritiske spørgsmål såsom:

1. Hvor mange kopier af objektet er tilgængelige i tilfælde af nedbrud? I ovenstående eksempel er CISP 1 beregnet til at klare det samtidige tab af data i to anlæg og beholder flere kopier af dataene. Med CISP 2 bliver der ikke taget kopier.
2. Hvad er de gemte objekters holdbarhedsniveau? Hos CISP 1 er det 99,999999999 %, og hos CISP 2 er det 99 %.
3. Overvej omkostningerne i forhold til ejerskabslevetiden for det overordnede projekt eller den overordnede workload, og overvej, hvordan funktioner til omkostningsoptimering kan nedbringe udgifter til, hvordan data gemmes og bruges (hvis der f.eks. bruges serveruafhængige-funktioner hos en CISP, kan udgifterne nedbringes med x %.

Dette er kun nogle af mange øvrige tekniske overvejelser i forbindelse med priser, især når det gælder sikkerhed og compliance.

Her er nogle eksempler på overvejelser i forbindelse med prisscenarier

Basispriser – dette er CISP'ens offentlige priser. CISP'er skal offentliggøre disse priser. Men som tidligere nævnt kan kunder anmode om måske 3-5 specifikke scenarier (eller hvor mange, der nu giver mening for kunden), som prissættes af alle leverandører, så CISP'er kan sammenlignes effektivt. Scenarierne bør være omfattende og inkludere et udvalg af tjenester og teknologier, som kunden formentlig vil bruge i løbet af projektet. På den måde kan kunden sammenligne projektets anslåede samlede omkostninger. Sammenligninger på enkeltpost-/SKU-niveau kan være mere problematisk end nyttigt for kunderne og leverandørerne (kunder skal sammenligne titusindvis af poster hos alle CISP'er, og leverandører skal sørge for dette niveau af detaljer og administrere det, selvom den reelle pris faktisk kun fastsættes med udgangspunkt i tjenesteforbrug).

Evaluering af en CISP's overordnede kapacitetssæt er et must for cloud-kunder, der ønsker at få den bedste værdi. CISP'er kan f.eks. have en række tjenester, der enten er gratis eller stort set gratis, og en prisvurdering bør tage hensyn til sådanne tjenester og til, at andre CISP'er muligvis tager penge for lignende funktioner.

Evalueringskriterier kan formuleres på en måde, der giver CISP'er mulighed for at fremhæve deres "inkluderet x standard"-funktioner, og hvordan disse tjenester påvirker den overordnede effektomkostning. Evalueringskriterier kan også se på CISP-volumenbaseret/differentieret prissætning og kommercielt tilgængelige rabatter såsom reserverede instanser/spotinstanser. Eksempel:

- x % besparelse, hvis kunderne køber reserveret databehandlingskapacitet (1 år, 3 år osv.)
- x % rabat på differentierede priser/volumenpriser
- x % besparelse baseret på arkitekturgennemgang og optimering af infrastrukturen, f.eks. ved at skifte til den bedst egnede beregningsmulighed
- Som tidligere nævnt skal man overveje omkostningen i den samlede levetid, og hvordan omkostningsoptimering kan nedbringe udgifter

PRISSÆTNINGSSCENARIE
Budgivere må kun angive priserne for nedenstående scenarie med henblik på evaluering. Den faktiske pris vil være baseret på forbrug af tjenester med en model med betaling efter forbrug og efter behov.

Nedenfor ses de repræsentative krav, som bruges til prisfastsættelse og oplyses med udtrykkelige forståelse, at disse nominelle krav kan ændre sig i løbet af kontraktens løbetid. Oplys priser for både 12 og 36 måneder efter behov samt 12 og 36 måneders reserveret kapacitet.

Angiv:

- *Navn på foreslåede løsning(er):*
- *Budgivers bedste priser:*

- *Tjenestetider: døgnet rundt hele året*
- *Tjenestetilgængelighed: 99,95 %*

Prisscenarier kan også omfatte eksempler fra nuværende kunder med lignende workloads, som har optimeret deres forbrug i løbet af 1/2/3 år ved hjælp af CISP'ens overvågnings- og optimeringsværktøjer, ved at benytte løsninger, der er udviklet til cloud, og ved hjælp af CISP-rabatter.

2.5 Opsætning af kontraktopfyldelse/vilkår og betingelser

CISP'ens cloud-teknologier og drift er standardiseret efter design, og derfor er betingelserne i kontrakten også standardiserede. Men det er muligt at tilpasse disse kontrakter marginalt, så det er muligt at tilpasse sig efter lokale love og betingelser.

De typiske metoder til indkøb af it omfatter tit strenge regler, der kræver, at ansøgerne overholder mange eller alle krav til indkøbet. Ellers bliver de afvist. Eller også omfatter de en række strenge, obligatoriske delkrav. Indkøb mislykkes som regel, når denne type indkøbsmetode bruges med cloud-teknologier, som i virkeligheden er en række standardiserede komponenter og værktøjer, der gør det lettere at lave en arkitektur med en tilpasset løsning.

2.5.1 Vilkår og betingelser

Det første trin, når det gælder kontrahering i en RFP for cloud-tjenester, er at gennemgå og forstå de nuværende CISP-virksomhedsbetingelser, som i de fleste tilfælde kan ses af alle på CISP'ens websites. Parter i den offentlige sektor bliver stadig mere trygge ved at acceptere kommercielle vilkår fra CISP'er. Når de forsøger at forstå vilkårene, besøger de blandt andet CISP'er og deres partnere for at gennemgå deres tilgange. Det centrale spørgsmål, der skal stilles, er, 'hvorfor' CISP'er opererer med specifikke vilkår.

Nogle af disse vilkår kan virke anderledes end traditionelle it-vilkår, men der er meget specifikke grunde til, at de er en del af en cloud-kontrakt. Hvis de offentligt tilgængelige vilkår ikke er acceptable, har CISP'er ofte aftaler for erhvervskunder, der kan ændres en smule, og som kan undersøges.

Sammen med gennemgangen af CISP'ens vilkår og betingelser er det vigtigt at forstå eksisterende politikker, bestemmelser og/eller love (f.eks. dem, der involverer teknologi, dataklassifikation, privatliv, personale osv.). Ofte findes der eksisterende politikker/bestemmelser/love, der er designet til at købe og udnytte traditionelle it-tilbud, og de kan være i strid med en CISP's model. Det kan f.eks. være, at det kun er tilladt at bruge cloud-teknologier, der var inkluderet i det oprindelige rammeaftalebud via RFP'en for cloud-tjenester. CISP'er tilføjer hele tiden nye tjenester og nye funktioner. Det giver ikke mening for slutbrugeren, hvis du begrænser adgangen til disse nye tjenester, bare fordi du benytter en almindelig metode til opdatering af it-produkter. Hvis dette er tilfældet, så er det vigtigt at tage en grundig samtale med CISP'erne, hvor I blandt andet ser på disse politikker/bestemmelser og/eller love.

Drag fordel af diskussioner forud for RFP

Som tidligere nævnt skal du bruge tid på at mødes med CISP'er og relaterede leverandører, inden du udarbejder en RFP, så du kan forstå deres vilkår og betingelser og fortælle dem om din organisations tilgang, politikker, bestemmelser og love. Den vigtigste del af disse drøftelser er, at begge parter lærer, 'hvorfor' de relevante begreber fungerer, som de gør. Cloud-vilkår og -betingelser er f.eks. anderledes end almindelige vilkår for datacentre, administrerede tjenester, ikke-tilpasset software og systemintegration. Da de er enkelte modeller og hele tiden kræver nyskabelser, kræver deres virksomhedsmodeller, at RFP-processen er fleksibel nok til, at der er plads til forhandlinger eller samtaler med henblik på at få en afklaring.

Ved at inkludere muligheden for at præcisere vilkår og betingelser under samtaler eller forhandlinger opnår offentlige organisationer større forståelse af cloud-modeller og undgår problemet med at afvise udbydere, der rent faktisk kan opfylde organisationens behov. En typisk proces er, at organisationen identificerer bestemte vilkår på forhånd, som de er villige til at drøfte og forhandle om inden tildelingen. Ved at forhandle med budgiver(e) på forhånd om acceptable vilkår sikrer organisationen, at den får den bedste kandidat til tildelingen og klarer uenigheder, der ellers ville have medført afvisning af et effektivt tilbud. Parter i den offentlige sektor kan også gennemgå deres politikker, bestemmelser og love, og begge sider kan lære, hvordan brugen af cloud-systemet passer til disse modeller. Det er som regel muligt at benytte de nuværende klausuler. Men hvis et område er problematisk, kan begge parter samarbejde om at finde en løsning (det er bedre at tale om dette i god tid før en eventuel RFP og efterfølgende kontraktforhandlinger).

Forhandlingsfleksibilitet

For at kunne underskrive kontrakter i overensstemmelse med den lokale lovgivning og samtidig stole på CISP'ens standardiserede kontraktvilkår anbefales det (1) at anmode ansøgerne om deres standardkontrakt, (2) ikke at indføre uhensigtsmæssige kontraktvilkår ved udarbejdelsen af rammeaftalen for RFP'en til cloud-tjenester og (3) at give mulighed for at forhandle om alle bestemmelser i den konsultation og de tilbud, der vil resultere i rammeaftalen (medmindre de obligatoriske klausuler, er påbudt ved lov).

NB: omfanget af det fælles ansvar er en del af cloud-modellen og bør fremgå af kontraktens vilkår (f.eks. bekræfter CISP'en, at kunder ejer deres data, bestemmer, hvor de gemmes, og sørger for værktøjer, der sikrer, at antallet af mulige dataplaceringer begrænses, MEN det er kundens eller partnerens ansvar at bruge disse værktøjer.

*Bemærk at det er vigtigt, at der **findes særskilte sæt vilkår og betingelser** i kontrakter for hver enkelt gruppe i en cloud-rammeaftale. En "universaltilgang" til kontraktindgåelser for alle GRUPPER vil føre til spørgsmål om teknisk gennemførligheden tekniske rentabilitet og kompatibilitet.*

Som allerede nævnt er RFP'er, der indeholder obligatoriske vilkår, som ikke kan forhandles, i bund og grund et "take it or leave it"-tilbud for udbyderne, som kan medføre, at et ellers acceptabelt tilbud afvises. Organisationer i den offentlige sektor bør tænke nøje over konsekvenserne ved brug af obligatoriske vilkår, medmindre de er lovpligtige. Organisationer skal være sikre på behovet for obligatoriske krav eller vilkår, da fremtidige forhandlinger vil blive påvirket, fordi de klassificeres som obligatoriske. Brugen af obligatoriske krav eller vilkår skal begrænses så meget som muligt, så organisationen får den nødvendige fleksibilitet til at købe de bedste teknologier og løsninger.

Husk, at CISP-cloud-teknologier er fuldstændig standardiserede og leveres på en fuldstændig automatiseret måde. Derfor kan en CISP ikke ændre vilkår og betingelser, der ellers ville kræve en tilpasning af den underliggende tjeneste. Desuden er tjenesternes priser typisk offentlige og standardiserede for alle brugere, hvilket betyder, at en CISP ikke kan hæve eller sænke priser for at imødekomme flere risici på vegne af en bestemt kunde.

Indirekte køb

I stedet for at købe cloud-teknologier direkte hos en CISP kan man købe dem hos en CISP-forhandler. Du kan læse mere om CISP-forhandlere i afsnit *2.1.3* ovenfor.

Eksempel på formulering i RFP: vilkår og betingelser

*CISP'er eller repræsentative leverandører skal oplyse deres offentlige vilkår og betingelser og give feedback om vigtige vilkår og betingelser hos <**ORGANIZATION**>.*

*<**ORGANIZATION**> har til hensigt at indgå en skriftlig kontrakt med den budgiver, der vinder, på grundlag af dennes kontraktmæssige vilkår. Budgiveren skal sørge for en række foreslåede kontraktvilkår, som <**ORGANIZATION**> kan gennemgå, og som udgør det bedste kommercielle og juridiske tilbud. Tilbudsgiveren og <ORGANIZATION> kan drøfte begge sæt af vilkår og betingelser i <DISCUSSION/NEGOTIATION>-fasen.*

- *Primære rammevilkår på højt niveau vil højst bestå af følgende komponenter:*
  - *Rammevarighed*
  - *Styring af rammer*
  - *Rammepræstation*
  - *Rammeophør*
  - *Rammens omfang*
  - *Bestillingsproces*
  - *Fortrolighedsbetingelser*
  - *Kategorispecifik IP og oplysninger*
  - *Tekniske minimumskrav, som CISP'er skal opfylde – f.eks. kvalitetsstandarder, akkreditering, sikkerhed og databeskyttelse*
- ***Der vil være forskellige vilkår for hvert enkelt gruppe i rammeaftalen***
- *Detaljerne ved CISP-tjenesterne kan evalueres og vil blive håndteret i call-off-fasen.*
- *Tillad kontraktændringer – vilkårene bør ikke begrænse kunder og leverandører fra at aftale kontraktændringer og tilføje nye tjenester eller forbedringer. Cloud-tjenesterne ændrer sig på en måde, der gør, at forbedringer af tjenester bliver tilgængelige løbende, og dette kan være med til at give kunderne effektivitet.*

- *Serviceniveauaftaler (SLA'er) bør ikke angives af kunden. Kundens vilkår skal ikke definere provisionsspecifikke, skræddersyede SLA'er, der er anderledes end CISP'ers standard-leverancemodeller for tjenester. Hvis CISP'er har mulighed for standard-SLA'er, kan de holde udgifterne nede og sende dem videre til kunderne, samtidig med at kunderne er sikre på, at CISP'en kan overholde SLA'en.*
- *Ansvarsdækninger skal være proportionale. Ansvaret skal være proportionalt med tjenesterne, der købes, og ansvarsgrænserne skal ikke være urimeligt høje. Hvis grænserne er urimeligt høje, kan det få CISP'er til at sige nej til projekter med lav værdi. Disse projekter fungerer ofte som en nyttig introduktion og "test"-sag, hvor kunderne kan afgøre, om visse cloud-løsninger er effektive for deres organisation.*
- *Kunderne skal eje deres egne data. Kunderne skal have kontrol over deres data og eje dem og have mulighed for at vælge, hvor de skal gemmes. Dette vil gøre det muligt for kunderne at undgå leverandørbinding og frit flytte data til nye udbydere.*

2.5.2 Vilkår og betingelser for software

Selv om denne håndbog fokuserer på køb af IaaS- og PaaS-cloud-teknologier, som leveres af en CISP, er det vigtigt at fremhæve de vilkår og betingelser for software, som organisationer i den offentlige sektor kan overveje, når de køber software fra leverandører. Se figur 1 (side 5) for at se, hvordan software købes som en del af et velstruktureret RFP for cloud-tjenester.

Software spiller en afgørende rolle i næsten alle virksomheder, også i den offentlige sektor. Ved at inkludere forpligtelser som f.eks. vilkår og betingelser for softwarelicensering i et RFP til af cloud-tjenester kan man sikre, at parter i den offentlige sektor får den bedste værdi og frit kan vælge leverandør, når de køber software.

Se de ti principper om rimelige software licensvilkår for cloud-kunder[9] for mere information. Principperne er udviklet af Cigref, [10] en sammenslutning af større franske virksomheder og offentlige myndigheder, der repræsenterer brugerne af digital teknologi, i samarbejde med CISPE og med støtte fra andre europæiske brancheforeninger af CIO'er og udbydere, for at behandle praksis, som begge sammenslutninger mener skader den digitale transformation af organisationer af alle størrelser, når de går over til cloud.

Eksempel på formulering i RFP: Software

*<**ORGANIZATION**> har til hensigt at indgå en skriftlig kontrakt med den budgiver, der vinder, på grundlag af dennes kontraktmæssige vilkår. Budgiveren skal sørge for en række foreslåede kontraktvilkår, som <**ORGANIZATION**> kan gennemgå, og som udgør det bedste kommercielle og juridiske tilbud. Softwareleverandører og <ORGANIZATION> kan drøfte begge sæt vilkår og betingelser i <DISKUSSION/NEGOTIATION>-fasen.*

***Krav 1.0.** Softwareleverandører skal give klare licensbetingelser, herunder en opdeling af omkostningerne på overordnet og detaljeret niveau.*

***Krav 1.1.** Alle anklager i forbindelse med manglende overholdelse af licensbetingelserne skal angives på overordnet og detaljeret niveau.*

***Krav 2.0.** Softwarelicenser skal give <Organization> mulighed for at migrere den licenserede software fra det lokale miljø til en cloud efter eget valg, uden at det kræver køb af separate, dobbelte licenser for den samme software.*

***Krav 2.1.** Softwarelicenser skal være fri for licensbegrænsninger og øgede omkostninger, der begrænser <Organization's> mulighed for at køre den licenserede software i den cloud, som de ønsker.*

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Krav 3.0. *Softwarelicenser skal give <Organization> mulighed for at køre den licenserede software på deres egen hardware (typisk benævnt "lokalt" software) såvel som i den cloud, de selv vælger.*
Krav 4.0. *Softwarelicenser må ikke kræve, at den licenserede software kun må køre på hardware, der udelukkende er dedikeret til <Organization>.*
Krav 5.0. *Softwareleverandører må ikke straffe <Organization>, hvis leverandørens licenserede software anvendes på en anden leverandørs cloud-tilbud, f.eks. ved at inkludere rettigheder til at foretage øgede eller indgribende softwarerevisioner eller pålægge højere gebyrer for softwarelicenser.*
Krav 6.0. *Katalogsoftware skal understøtte åbne standarder for synkronisering og autentificering af brugeridentiteter på en ikke-diskriminerende måde i forhold til andre identitetstjenester.*
Krav 7.0. *Softwareleverandører må ikke opkræve forskellige priser for den samme software udelukkende på grundlag af, hvem der ejer den hardware, som den er installeret på.* ***Krav 7.1.*** *Priserne for software må ikke skelne mellem software, der er installeret i <Organization's> eget datacenter, et datacenter, der forvaltes af en tredjepart, på computere, der er leaset af en tredjepart, eller hos den cloud-udbyder, som <Organization's> vælger.*
Krav 8.0. *I kontraktens løbetid må softwareleverandørerne ikke foretage væsentlige ændringer af licensbetingelserne, der begrænser <Organization> fra tidligere tilladte anvendelser, medmindre det er påkrævet ved lov eller af sikkerhedshensyn.*
Krav 9.0. *Softwareleverandører må ikke vildlede <Organization> ved at påstå, at softwarelicenser vil dække <Organization's> planlagte softwareanvendelse som beskrevet i <Organization's Requirements>, når det kan kræve køb af yderligere licenser at dække en sådan anvendelse.*
Krav 10.0. *Hvis <Organization> har ret til at videresælge og overdrage softwarelicenser, skal softwareleverandørerne fortsat tilbyde support og opdateringer på rimelige vilkår til <Organization>, som lovligt har erhvervet en videresolgt licens.*

2.5.3 Sådan vælger du mellem leverandører på rammeaftalen for hvert projekt

Parter i den offentlige sektor, som er en del af rammen, kan bestille eller udføre 'call off' med de tjenester, de har brug for, hvis det er nødvendigt. Afgivelse af en call-off-kontrakt i henhold til en rammeaftale giver købere mulighed for at finjustere kravene med en yderligere funktionel specifikation for en call-off, samtidig med at de har fordelene, der tilbydes i henhold til rammeaftalen.

Hvis det vurderes som nødvendigt, kan der afholdes en minikonkurrence med det formål at vælge den bedste leverandør til bestemte workloads eller projekter. En minikonkurrence er en konkurrence, hvor en kunde byder yderligere i henhold til rammen, ved at invitere alle leverandører i en gruppe til at reagere på en række krav. Kunden vil invitere alle leverandører i en gruppe, der kan klare opgaven, til at byde, og derfor er minimumskravene for leverandører på rammeaftalen vigtige i en RFP for cloud-tjenester, da den medfører en høj standard for valgmuligheder under hver enkelt gruppe.

Som sagt er det vigtigt, at der er forskellige sæt vilkår og betingelser til kontrakter for alle gruppekategorierne i typen af tilbud (f.eks. offentlig IaaS/PaaS, community IaaS/PaaS, privat IaaS/PaaS), da

en "universaltilgang" for kontraktindgåelse for hver enkelt gruppe vil forringe den tekniske rentabilitet og kompatibilitet.

Se afsnit *2.1.4* for eksempler på RFP-formuleringer angående valget mellem leverandører.

2.5.4 Klargøring og afslutning

Én vigtig ting, du bør overveje, når du udarbejder en cloud-rammeaftale, er muligheden for et dynamisk indkøbssystem (DPS). Med en DPS-model kan alle leverandører, der overholder minimumskravene i rammeaftalen, blive en del af rammen. Der er ingen hård grænse for antallet af leverandører, der kan deltage i rammen, og i modsætning til den traditionelle rammemodel kan leverandører også ansøge om at deltage i "DPS-rammen" på et hvilket som helst tidspunkt i løbet af dens levetid.

Vi anbefaler på det kraftigste, at parter i den offentlige sektor laver strenge standarder, der sikrer kvalitet og tillid til tjenesten fra kvalificerede leverandører, men de må ikke være for specifikke med afvisningen af CISP'er på en måde, der forhindrer rimelig konkurrence. Målet er at undgå, at slutbrugeren overvældes med for mange muligheder, samtidig med at standarden for tilgængelige cloud-teknologier altid er høj.

3.0 Bedste praksis/erfaringer

Nedenfor fremhæver vi nogle erfaringer med, hvordan man laver en vellykket cloud-rammeaftale med en vellykket RFP for cloud-tjenester.

3.1 Cloud-Governance

Styring i et cloud-system er et fælles ansvar. CISP leverer funktioner og tjenester til indbygget governance i alle dele af cloud-miljøet, mens kunderne bruger deres nuværende standarder for cloud-governance og lærer, hvordan cloud-systemet giver mulighed for cloud-governance.

I cloud-systemet har kunderne en chance for at lave de it-miljøer, de vil have, i stedet for bare at administrere det, de har nu. Med cloud kan kunderne: (1) Starte med en komplet oversigt over alle it-aktiver, (2) administrere alle aktiverne fra centralt hold og (3) oprette advarsler om forbrug/fakturering/sikkerhed m.m. Alle disse vigtige fordele ved cloud hjælper kunderne med at få en optimeret – og automatiseret (i det omfang, det er muligt) – arkitektur, uden at der løbende er brug for at købe og installere ny hardware. Det klarer CISP'en ved at lade kunderne flytte fokus fra en unuanceret administration af infrastrukturen til det missionskritiske driftsniveau.

Du kan se på en CISP-cloud som en meget omfattende API. Uanset om du er ved at tage en ny server i brug eller vil ændre sikkerhedsindstillinger, foretager du blot API-kald. Alle ændringer i miljøet logføres og registreres (hvem, hvad, hvor og hvornår registreres for alle ændringer). Dette giver en cloud-governance, kontrol og synlighed, som kun er mulig med et cloud-miljø. Det giver kunder mulighed for at genoverveje deres nuværende modeller til it-styring og finde ud af, hvordan de kan strømlines og forbedres med de fordele, som cloud-teknologi giver.

Cloud-governance kan også betyde meddelelser om og benyttelse af de positive procesændringer samt nye kompetencer, som cloud-teknologi medfører. Projektledere er f.eks. vant til at vente i månedsvis på, at et it-miljø bliver bygget. Derfor kan de risikere at tro, at det vil tage endnu længere tid, end det rent faktisk vil, at lave et miljø eller testmiljø i et cloud-system (og med cloud vil det kun tage et par minutter). Benyttelsen af denne nye fleksibilitet vil blive en udviklingsproces og blive udført fra program til program.

Disse erfaringer skal deles, således at rammeaftalen fortsat kan udvikle sig på en måde, der gør, at kravene passer til de nye processer og den nye fleksibilitet.

3.2 Budgettering til cloud

Når det gælder om at strukturere cloud-priser med betaling efter forbrug i forbindelse med indkøb og krav til budgettering i den offentlige sektor, så har vi fundet ud af, at det er nyttigt at kombinere CISP-tjenester i en enkelt post (beregning, lager, netværk, database, IoT osv.), som alt sammen er en del af det samme post for **cloud-teknologier.** Denne metode giver fleksibiliteten til at give brugerne adgang til alle de nuværende og nye CISP-teknologier i realtid, så de får hurtig adgang til de ressourcer, de skal bruge, når det er nødvendigt. Den tager også højde for skiftende behov, hvilket fører til bedre udnyttelse og lavere udgifter.

Organisationer i den offentlige sektor kan tilføje yderligere poster til ordrer fra andre grupper i en cloud-ramme, hvis de kræver konsulent/professionelle eller administrerede tjenester, software fra en markedsplads, cloud-support-tjenester og undervisning om CISP'ers tilbud.

Der opnås en mere fleksibel kontrahering ved benyttelse af valgfri kontraktpunkter i relevante ressourcekategorier af hensyn til fremtidig vækst. Hvis en organisation derimod vil kombinere cloud-teknologier med konsulenttjenester eller professionelle/administrerede tjenester i ét punkt, kan dette gøres med et punkt som f.eks. "cloud-teknologier og accessorisk arbejdskraft".

Nedenfor er et repræsentativt eksempel på denne tilgang. I nedenstående eksempel er hver enhed af punkt '#1001 – cloud-teknologier lig med 1,00 EUR "cloud-teknologier" brugt. Hver måned kan trinvise bestillinger finansieres med udgangspunkt i det nuværende og det forventede forbrug.

Tabel 3 – eksempel på prisstruktur for enkelte punkter

ARTIKEL NR.	FORBRUGSVARER/TJENESTER	ANTAL	ENHED	ENHEDSPRIS	BELØB
1001	Cloud-teknologier	1.000	Hver	1 EUR	1.000 EUR
1002	Konsulenttjenester	1	pr. uge	3.000 EUR	3.000 EUR
1003	Cloud-support	1	pr. måned	1.000 EUR	1.000 EUR
1004	Cloud-kurser	1	pr. dag	3,00 EUR	3.000 EUR
1005	Cloud-markedsplads	10	Hver	10 EUR	100 EUR

Her er et eksempel på, hvordan denne struktur kan fungere: En organisation i den offentlige sektor henvender sig til en CISP for at få et estimat for, hvor meget organisationen vil bruge cloud-tjenester. Organisationen accepterer leverandørens vilkår, f.eks. 10 millioner EUR i en periode på 5 år, hvilket svarer til 2 millioner EUR pr. år. Organisationen betaler det første årlige beløb på 2 millioner EUR. Hver måned modtager de en faktura, og pengene overføres fra puljen, der skal bruges som betaling. Der udføres en udbetaling mod den pågældende konto. Forbruget af de sidste midler overvåges ved hjælp af CISP'ens overvågnings- og prognoseværktøjer. Hvis de sidste midler er ved at være brugt, beder organisationen CFO'en om flere midler til betaling for, at tjenesterne kan køre videre.

Eksempel på formulering i RFP: priser – kontraktindgåelse

BETALINGSVILKÅR
Betalingsvilkårene skal struktureres således, så der kun betales for ressourcer, som benyttes af <ORGANIZATION>, som beskrevet nedenfor:

1. *Den månedlige betaling skal baseres på det reelle forbrug af tjenester og i henhold til CISP'ens offentlige priser.*

MINIMUMSGARANTI OG MAKSIMALT FORBRUG
<ORGANIZATION> har ikke mulighed for at se, hvor meget af en bestemt cloud-udbyders ressourcer, der bruges i en periode, og derfor skal ordrer angives med en fast pris pr. antal enheder for et enkelt bestillingspunkt for "cloud-teknologier.

Hver enhed i punktet, der bestilles, svarer til bestilling af cloud-teknologier for <€1,00>. Trinvise ordrer afgives periodisk via ændringen af denne ordrer i flere antal, således at <ORGANIZATION> får fleksibiliteten til at bestille flere antal CISP-cloud-teknologier på forhånd i "eurobeløb" med udgangspunkt i dennes estimerede forbrug til behov med forskellig varighed. <ORGANIZATION> vil med jævne mellemrum forudbestille tilstrækkelige mængder til at dække de anslåede omkostninger til cloud-teknologier, der vil blive anvendt til at opfylde en række forskellige krav.

Artikelnr.	Beskrivelse	Antal	Enhed	Pris
01	CISP-cloud-teknologier	1.000	EA	1.000,00 EUR

MINIMUMORDRE/TRINVIS ORDRE
Der vil med jævne mellemrum blive afgivet ordrer på forskellige mængder af <10,000> enheder baseret på <ORGANIZATION'S> anslåede brug af cloud-teknologier. Dette arrangement giver <ORGANIZATION> fleksibiliteten til at forudbestille <10.000> enheder af "cloud-teknologier" efter behov for at understøtte operationer og forblive i overensstemmelse med cloudcomputing-baseret "betal efter forbrug" handelspraksis".

Et indledende trin på <100.000> enheder til <€100.000> bestilles ved afgivelsen af en call off. Minimumsantallet af samlede punktenheder, der kan afgives i en enkelt trinvis ordre ved hjælp af et eller flere punkter, er <x>. Det maksimale antal enheder, der kan afgives i leveringsordren, må ikke overskride <x>, men må aldrig være større end call off-værdien, når det kombineres med alle de tidligere bestilte enheder. <ORGANIZATION> er ansvarlig for at sikre, at alle ordrer er inden for de angivne begrænsninger i dette afsnit.

ORDREMAKSIMUM
Den samlede maksimumsværdi for en ordre er op til <x> og består af op til <x> enheder i et enkelt punkt til en pris, som er <x> pr. enhed. Værdien er baseret på et estimat af <ORGANIZATION'S> krav i løbet af effektivitetsperioden, men den er ikke garanteret.

3.3 Forstå partnerforretningsmodellen

Parter i den offentlige sektor skal prøve at forstå de modeller, som CISP'er bruger til at levere deres produkter, og være opmærksomme på, at partnere, der leverer konsulenttjenester, administrerede tjenester, videresalg og meget mere, er kritiske for denne proces. Mange kunder har brug for en cloud-udbyder til deres infrastruktur og outsource "personlig" planlægnings-, migrerings- og administrationsarbejde til en Systems Integrator (SI) eller udbydere af administrerede tjenester. På grund

af denne blanding af 'tjenester' er nogle af kravene muligvis ikke relevante for cloud-udbydere, f.eks. "flow-down"-klausuler til underleverandører.

Disse flow-down-klausuler viser, hvorfor det er vigtigt at vide, hvordan partnere og forhandlere fungerer i forbindelse med CISP'er. I visse typer indkøb er der klausuler, der kræver, at den primære kontrahent har flow-down for visse påkrævede klausuler til alle sine partnere/underleverandører. Som regel vil CISP'er ikke sørge for eller byde som formelle underleverandørpartnere, da de tilbyder en standardiseret tjeneste på en enorm skala, som ikke er skræddersyet til en bestemt slutkundes unikke krav (deriblandt krav hos en kunde i den offentlige sektor, som er omfattet af en kontrakt for den offentlige sektor). I en indirekte indkøbsmodel (indkøb af cloud-tjenester gennem en CISP-forhandler) kan en CISP afvise disse klausuler fra sin forhandler, da de ikke finder anvendelse på en leverandør af kommercielle tjenester på "2. niveau". I dette tilfælde er det ikke CISP'en, der udfører omfanget af arbejdet i henhold til kontrakten. I stedet vil en CISP-partner gøre dette ved hjælp af CISP-infrastrukturen. CISP'en er derfor en kommerciel leverandør (ikke en underleverandør) til en partners aktiviteter. I en direkte indkøbsmodel (køb af cloud-tjenester direkte hos en CISP) vil en CISP typisk afvise disse "obligatoriske" klausuler, som er relevante for en typisk underleverandør, der sælger produkter, på grund af disse kontraherede tjenesters kommercielle natur, og fordi de fleste CISP'er ikke har brug for underleverandører til at levere deres kommercielle tjenester.

3.4 Cloud-mæglere

Konceptet med at bruge en cloud-mægler til at reducere muligheden for afhængighed af leverandører kan være problematisk. Selv om en cloud-mægler kan være en god idé i teorien, så vil det i praksis medføre mere kompleksitet og forvirring end reel værdi.

Forsøg på at udvikle programmer, der kan fungere på tværs af flere clouds samtidig eller på kryds og tværs af hinanden, fører uundgåeligt til kompromiser med hensyn til kapacitet (**der findes ikke en opskrift på alt til clouds**). Denne metode kan i sidste ende medføre et unødvendigt, kompliceret lag mellem kunder i den offentlige sektor og deres cloud-tjenester, hvilket kan forringe effektiviteten og de sikkerhedsfordele, der er formålet. Resultatet er mindre skalerbarhed, flere udgifter og en nedgang i innovationen.

3.5 Sourcing før RFP/markedsundersøgelse

Når en part i den offentlige sektor planlægger en RFP for cloud-tjenester, skal den også medregne interessenter fra hele organisationen, dvs. både ledelsen, virksomhedsinteressenter, teknologiafdelingen, regnskabsafdelingen, indkøbsafdelingen, den juridiske afdeling og kontrakter, så snart processen påbegyndes. Denne metode sikrer, at alle interessenter kan forstå cloud-modellen og derefter benytte en fornuftig metode til genovervejelsen af traditionelle metoder til it-indkøb.

Når det gælder dialog med branchen, anbefaler vi, at parter i den offentlige sektor bruger tid på grundige samtaler for at få feedback fra branchen, dvs. CISP'er, CISP-partnere, PaaS/SaaS markedsplads-leverandører og brancheeksperter. En sådan dialog kan f.eks. finde sted i form af branchedage eller workshops om sikkerhed og indkøb. En anden effektiv metode til at få en bedre forståelse af cloud-indkøb er at udsende en RFI eller helst en kladde af et RFP-dokument. De omfatter tit mulige problemer, der kan identificeres, drøftes og forbedres, inden den endelige udgave af RFP'en til cloud-tjenester udsendes.

3.6 Bæredygtighed

Bæredygtighed er indbygget i cloudcomputing, og flytning til cloud giver en energieffektivitetsgevinst sammenlignet med lokale servere eller i virksomhedens datacentre. Identificering af en CISP, der prioriterer

bæredygtighed og har afgivet offentlige løfter om at nå målene for bæredygtighed, giver yderligere sikkerhed for, at clouden er bæredygtig. Europæiske CISP'er og datacenteroperatører har (med støtte fra Europa-Kommissionen) oprettet pagten om klimaneutrale datacentre[11], et selvreguleringsinitiativ, der skal fastsætte klare, enkle og vidtrækkende bæredygtighedskriterier for datacenterbranchen og sikre, at datacenteroperatører og cloud-tjenesteudbydere er klimaneutrale inden 2030. Selvreguleringsinitiativet omfatter klare mål for datacentrenes energieffektivitet, vandbesparelse, genbrug og reparation af servere og brug af kulstoffri energi til at drive datacentre. CISP'er, der tilmelder sig selvreguleringsinitiativet, accepterer at opfylde disse mål og certificere i forhold til kriterierne for at blive betragtet som en klimaneutral operatør.

En RFP for cloud-tjenester bør spørge CISP'er, om de har forpligtet sig til at overholde sådanne kriterier, og der bør specifikt spørges, om de har tilmeldt sig selvregulering, og hvornår de har påtaget sig en sådan forpligtelse.

Eksempel på formulering i RFP: bæredygtighed

Har du forpligtet dig til at drive klimaneutrale datacentre ved at underskrive det selvregulerende initiativ for klimaneutrale datacentre? Hvis ja, hvornår skrev du under?

Kan du fremlægge dokumentation for, at du har fået tildelt stemplet for pagten for klimaneutrale datacentre til brug?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

Bilag A – tekniske krav til sammenligning af budgivere

Nedenfor viser vi nogle af de typiske krav til cloud-teknologi, der kan bruges til at sammenligne CISP'er i løbet af call-offs eller minikonkurrencer i en cloud-rammeaftale.

1. Profil af cloud-udbyder

	Krav
1.	***MARKEDSERFARING:*** *Hvor mange år har cloud-udbyderen været aktiv inden for cloud-markedssegmentet?*
2.	***ÅBENHED OG DATABESKYTTELSE:*** *Overholder cloud-udbyderen branchens adfærdskodekser for databeskyttelse eller reversibilitet? Overholder cloud-udbyderen principperne for open source og fri API-udvikling?*

2. Global infrastruktur

	Krav
1.	***GLOBAL RÆKKEVIDDE:*** *Tilbyder cloud-udbyderen en global infrastruktur, der kan hjælpe brugerne med at opnå lav latenstid og høj gennemløb?*
2.	***OMRÅDER:*** *Har cloud-udbyderen en tilstedeværelse i de nødvendige geografiske områder?*
3.	***DOMÆNER/ZONER:*** *Implementerer cloud-udbyderen koncepter med domæner eller zoner, hvor flere datacentre grupperes i et netværk med lav latenstid, hvilket giver mere tilgængelighed og større fejltolerance?* • *Hvis svaret er ja, så angiv antallet af domæner eller zoner og antallet af datacentre i det nødvendige geografiske område*
4.	***DOMÆNER/ZONERS AFSTAND:*** *Laver cloud-udbyderen sine domæner eller zoner med datacentre, der ikke befinder sig de samme steder, med henblik på reserveforanstaltninger, høj tilgængelighed og lav latenstid?*
5.	***BYGGEDE DATACENTRE:*** *Har cloud-udbyderen datacentre, der er fremstillet til at blive isoleret fra fejl i andre datacentre med reservestrøm, -nedkøling og -netværksteknologi?*
6.	***REPLIKERING AF DATACENTER:*** *Har cloud-udbyderen datareplikering hos flere datacentre i et domæne eller en zone med automatisk failover?*
7.	***DOMÆNE-/ZONEREPLIKERING:*** *Har cloud-udbyderen datareplikering i flere zoner eller domæner i et område?*

3. Infrastruktur

3.1 Beregning

	Krav
1.	***BEREGNING – ALMINDELIG INSTANS – GENERELT FORMÅL:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *Generelle formål – optimeret til generiske programmer og giver en balance mellem databehandlings-, hukommelses- og netværksressourcer.* ○ *Hvis ja, hvilken instans er så den største?*
2.	***BEREGNING – ALMINDELIG INSTANS – HUKOMMELSESOPTIMERET:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *Hukommelsesoptimeret – optimeret til hukommelseskrævende programmer* ○ *Hvis ja, hvilken instans er så den største?*
3.	***BEREGNING – ALMINDELIG INSTANS – BEREGNINGSOPTIMERET:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *Beregningsoptimeret – optimeret til beregningskrævende programmer* ○ *Hvis ja, hvilken instans er så den største?*
4.	***BEREGNING – ALMINDELIG INSTANS – LAGRINGSOPTIMERET:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *Lagringsoptimeret – tilbyder en stor mængde lokal lagringskapacitet* ○ *Hvis ja, hvad er så den maksimale lagerkapacitet (dvs. 5, 10, 20 eller 50 TB) og det maksimale antal harddiske (HDD'er/SSD'er), der kan klargøres og tilknyttes en instans?*
5.	***BEREGNING – ALMINDELIG INSTANS – GRAFIKOPTIMERET:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *Lavpris-grafik – tilbyder billig grafikacceleration til beregningsinstanser?* ○ *Hvis ja, hvilken instans er så den største?*
6.	***BEREGNING – ALMINDELIG INSTANS – GPU-OPTIMERET:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *GPU – tilbyder hardware-grafikprocessorer (GPU'er) til grafiktunge programmer* ○ *Hvis ja, hvor mange GPU'er og hvilke GPU-modeller kan cloud-udbyderen så tilbyde for hver instans?*
7.	***BEREGNING – ALMINDELIG INSTANS – FPGA-OPTIMERET:*** *Tilbyder cloud-udbyderen følgende instanstyper?* • *FPGA - tilbyder FPGA'er (field programmable gate arrays) til udvikling og implementering af brugerdefineret hardwareacceleration til programmer.* ○ *Hvis ja, hvor mange FPGA'er kan cloud-udbyderen så tilbyde for hver instans?*

8.	***BEREGNING – KONTINUERLIG INSTANS:*** *Tilbyder cloud-udbyderen kontinuerlige instanser, der giver et basisniveau for CPU'ens ydeevne med mulighed for kontinuerlig aktivitet over basislinjen?* • *Hvis ja, hvilken kontinuerlig instans er så størst?*
9.	***BEREGNING – IO-KRÆVENDE INSTANS:*** *Tilbyder cloud-udbyderen instanser med solid state-harddiske af typen NVMe (non-volatile memory express), som er optimerede til lav latenstid, meget kraftig, tilfældig I/O-ydeevne og højt sekventielt læsningsgennemløb?* • *Hvis ja, hvad er så den maksimale IOPS-kapacitet (input/output operationer pr. sekund) for den største instans?*
10.	***BEREGNING – MIDLERTIDIGT LOKALT LAGER:*** *Tilbyder cloud-udbyderen lokalt lager til beregningsinstanser, der kan bruges til midlertidigt at gemme oplysninger, der ændres regelmæssigt?*
11.	***BEREGNING – MULIGHED FOR FLERE NIC'ER:*** *Understøtter cloud-udbyderen flere primære og yderligere NIC'er (network interface cards), som kan allokeres til en given instans?* • *Hvis ja, hvad er så det maksimale antal NIC'er pr. instans?*
12.	***BEREGNING – TILHØRSFORHOLD FOR INSTANSER:*** *Giver cloud-udbyderen brugere mulighed for at gruppere instanser sammen logisk i det samme datacenter?*
13.	***BEREGNING – ANTI-TILHØRSFORHOLD FOR INSTANSER:*** *Giver cloud-udbyderen brugere mulighed for at gruppere instanser sammen logisk og anbringe dem i forskellige datacentre i et område?*
14.	***BEREGNING – KLARGØRING MED SELVBETJENING:*** *Tilbyder cloud-udbyderen klargøring med selvbetjening af flere instanser på samme måde ved hjælp af enten en programmatisk grænseflade, en administrationskonsol eller en webportal?*
15.	***BEREGNING – TILPASNING:*** *Tilbyder cloud-udbyderen instanser, der kan tilpasses, dvs. muligheden for at ændre konfigurationsindstillinger såsom vCPU'er (virtual central processing units) og RAM (random access memory)?*
16.	***BEREGNING – LEJEMÅL:*** *Tilbyder cloud-udbyderen enkeltlejerinstanser, der kører på hardware, der er dedikeret til en enkelt bruger?* • *Hvis ja, hvad er den største tilgængelige enkeltlejerinstans?*
17.	***BEREGNING – VÆRTSTILHØRSFORHOLD:*** *Gør cloud-udbyderen det muligt at starte en instans og angive, at denne instans altid genstartes på den samme fysiske vært?*
18.	***BEREGNING – VÆRTS-ANTI-TILHØRSFORHOLD:*** *Gør cloud-udbyderen det muligt at opdele og hoste bestemte instanser på flere forskellige fysiske værter?*
19.	***BEREGNING – AUTOMATISK SKALERING:*** *Gør cloud-udbyderen det muligt at forøge antallet af instanser automatisk ved stigende efterspørgsel for at opretholde ydeevnen (dvs. "skalere ud")?*

20.	***BEREGNING – MEKANISME TIL IMPORT AF AFBILDNING:*** *Giver cloud-udbyderen brugere mulighed for at importere deres nuværende afbildninger og gemme dem som nye og privat tilgængelige, der kan bruges til klargøring af fremtidige afbildninger?* • *Hvis ja, hvilke formater understøttes?*
21.	***BEREGNING – MEKANISME TIL EKSPORT AF AFBILDNING:*** *Giver cloud-udbyderen mulighed for at eksportere en nuværende instans, der kører, eller en kopi af en instans og eksportere den i et virtuelt maskinformat?* • *Hvis ja, hvilke formater understøttes?*
22.	***BEREGNING – DRIFTSAFBRYDELSER:*** *Tilbyder cloud-udbyderen mekanismer, der gør det muligt at undgå instans-nedbrud eller nedetid, når udbyderen vedligeholder hardware eller tjenester på værtsniveau?*
23.	***BEREGNING – GENSTART AF INSTANSER:*** *Tilbyder cloud-udbyderen mekanismer, der gør det muligt at genstarte instanser automatisk på en aktiv vært, hvis den originale vært ikke virker?*
24.	***BEREGNING – NOTIFIKATIONER:*** *Gør cloud-udbyderen det muligt at underrette brugeren om, at en beregningstolerant begivenhed har fundet sted, og kan brugeren vælge eller fravælge at modtage disse meddelelser ved hjælp af selvbetjening?*
25.	***BEREGNING – PLANLÆGNING AF BEGIVENHED:*** *Gør cloud-udbyderen det muligt at planlægge begivenheder for brugerens instanser, f.eks. genstart, stop, start eller udfasning af instansen?*
26.	***BEREGNING – MEKANISME TIL SIKKERHEDSKOPIERING OG GENDANNELSE:*** *Har cloud-udbyderen en integreret mekanisme til sikkerhedskopiering og gendannelse?*
27.	***BEREGNING – SNAPSHOT-MEKANISME:*** *Har cloud-udbyderen en manuel mekanisme til at tage snapshots efter behov?*
28.	***BEREGNING – METADATA:*** *Har cloud-udbyderen en metadatatjeneste for instanser, der giver brugere mulighed for at vælge vilkårlige par til instansen med nøgleværdi?*
29.	***BEREGNING – METADATAKALD:*** *Har cloud-udbyderen en metadatatjeneste for instanser med en Application Programming Interface (API), som instansen kan kalde for at få oplysninger om sig selv?*
30.	***BEREGNING – BUDGIVNINGSMEKANISME:*** *Tilbyder cloud-udbyderen en budmekanisme til at byde på omkostningsinstanser, der umiddelbart kan instantieres til at hoste ikke-missionskritiske workloads?*
31.	***BEREGNING – PLANLÆGNINGSMEKANISME:*** *Gør cloud-udbyderen det muligt at planlægge og reservere yderligere beregningskapacitet på faste tidspunkter, f.eks. hver dag, uge eller måned?*
32.	***BEREGNING – RESERVATIONSMEKANISME:*** *Gør cloud-udbyderen det muligt at reservere yderligere beregningskapacitet til fremtidige datoer (f.eks. om 1, 2 eller 3 år osv.)?*

33.	***BEREGNING – LINUX-OPERATIVSYSTEM:*** *Har cloud-udbyderen support til de sidste to versioner med langsigtet understøttelse af mindst én distribution af Linux til virksomheder (f.eks. Red Hat eller SUSE) og en almindelig, gratis distribution (f.eks. Ubuntu, CentOS og Debian)?*
34.	***BEREGNING – WINDOWS-OPERATIVSYSTEM:*** *Understøtter cloud-udbyderen de sidste to store versioner af Windows Server (Windows Server 2017 og Windows Server 2016)?*
35.	***BEREGNING – LICENSPORTABILITET:*** *Giver cloud-udbyderen mulighed for licensmobilitet og -support?* • *Hvis ja, så angiv softwareleverandør, softwarenavne, udgaver og deres versioner.*
36.	***BEREGNING – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte beregningssektion?* *Eksempel:* *Maks. antal instanser pr. konto* *Maks. antal dedikerede værter pr. konto* *Maks. antal reserverede IP-adresser (internetprotokol)*

3.2 Netværksmuligheder

	Krav
1.	***NETVÆRKSMULIGHEDER – VIRTUELLE NETVÆRK:*** *Gør cloud-udbyderen det muligt at oprette et logisk, isoleret og virtuelt netværk, som repræsenterer virksomhedens eget netværk i en cloud?*
2.	***NETVÆRKSMULIGHEDER – FORBINDELSER I SAMME OMRÅDE:*** *Gør cloud-udbyderen det muligt at oprette forbindelse med to virtuelle netværk i det samme område til trafik mellem disse netværk ved hjælp af en privat IP-adresse?*
3.	***NETVÆRKSMULIGHEDER – FORBINDELSER I FORSKELLIGE OMRÅDER:*** *Gør cloud-udbyderen det muligt at oprette forbindelse med to virtuelle netværk i forskellige områder til trafik mellem disse netværk ved hjælp af en privat IP-adresse?*
4.	***NETVÆRKSMULIGHEDER – PRIVAT UNDERNET:*** *Gør cloud-udbyderen det muligt at oprette fuldt isolerede (private), virtuelle netværk og undernet, hvor instanser kan klargøres uden offentlige IP-adresser eller internet-routing?*
5.	***NETVÆRKSMULIGHEDER – VIRTUELLE NETVÆRKSADRESSEOMRÅDER:*** *Understøtter cloud-udbyderen IP-adresseområder, der er angivet i anmodningen om RFC 1918 (request for comments) samt CIDR-blokke (classless inter-domain routing), der kan routes offentligt?*
6.	***NETVÆRKSMULIGHEDER – FLERE PROTOKOLLER:*** *Understøtter cloud-udbyderen flere protokoller, deriblandt TCP (transmission control protocol), UDP (user datagram protocol) og ICMP (Internet control message protocol)?*

7.	*NETVÆRKSMULIGHEDER – AUTOMATISK TILDELING FOR IP-ADRESSER:* *Gør cloud-udbyderen det muligt at tildele offentlige IP-adresser automatisk til instanser?*
8.	*NETVÆRKSMULIGHEDER – RESERVEREDE STATISKE IP-ADRESSER:* *Understøtter cloud-udbyderen IP-adresser, der er knyttet til en brugerkonto i stedet for en bestemt instans? IP-adresserne skal altid knyttes til kontoen, indtil de udtrykkeligt frigives.*
9.	*NETVÆRKSMULIGHEDER – IPV6-SUPPORT:* *Understøtter cloud-udbyderen IPv6 (Internet protocol version 6) på enten gateway- eller instansniveau, og er denne funktion synlig for brugere?*
10.	*NETVÆRKSMULIGHEDER – FLERE IP-ADRESSER PR. NIC:* *Gør cloud-udbyderen det muligt at tildele primære og sekundære IP-adresser til et NIC (network interface card), som er knyttet til en bestemt instans?*
11.	*NETVÆRKSMULIGHEDER – FLERE NIC'ER:* *Gør cloud-udbyderen det muligt at tildele flere NIC'er til en bestemt instans?*
12.	*NETVÆRKSMULIGHEDER – NIC- OG IP-MOBILITET:* *Gør cloud-udbyderen det muligt at flytte netværkskort (NIC) samt IP-adresser (Internet Protocol) mellem instanser?*
13.	*NETVÆRKSMULIGHEDER – MULIGHED FOR SR-IOV:* *Giver cloud-udbyderen muligheder for f.eks. SR-IOV (single root input/out virtualization), der giver bedre ydeevne (dvs. PPS eller pakker pr. sekund), kortere ventetid og færre udsving?*
14.	*NETVÆRKSMULIGHEDER – FILTRERING AF INDGÅENDE TRAFIK:* *Gør cloud-udbyderen det muligt at tilføje eller fjerne regler for indgående trafik til instanser?*
15.	*NETVÆRKSMULIGHEDER – FILTRERING AF UDGÅENDE TRAFIK:* *Gør cloud-udbyderen det muligt at tilføje eller fjerne regler for udgående trafik fra instanser?*
16.	*NETVÆRKSMULIGHEDER – ACL:* *Gør cloud-udbyderen det muligt at styre ind- og udgående trafik til undernet ved hjælp af ACL'er (adgangskontrollister)?*
17.	*NETVÆRKSMULIGHEDER – MULIGHED FOR FLOW-LOGFIL:* *Gør cloud-udbyderen det muligt at registrere flow-logfiler for netværkstrafik?*
18.	*NETVÆRKSMULIGHEDER – NAT:* *Har cloud-udbyderen en tjeneste, der administreres ved hjælp af en NAT-gateway (oversættelse af netværksadresser), der giver mulighed for instanser i et privat netværk, så der kan oprettes forbindelse til internettet eller andre cloud-tjenester, men forhindrer oprettelse af internetforbindelse til disse instanser?*
19.	*NETVÆRKSMULIGHEDER – KILDE-/DESTINATIONSKONTROL:* *Gør cloud-udbyderen det muligt at deaktivere kilde-/destinationskontrol på NIC'er?*
20.	*NETVÆRKSMULIGHEDER – VPN-SUPPORT:* *Gør cloud-udbyderen det muligt at oprette VPN-forbindelser (virtual private network) mellem cloud-udbyderen og brugerens datacenter?*
21.	*NETVÆRKSMULIGHEDER – VPN-TUNNELLER:* *Gør cloud-udbyderen det muligt at oprette flere VPN-forbindelser for hvert virtuelt netværk?*

22.	***NETVÆRKSMULIGHEDER – IPSEC VPN-SUPPORT:*** *Giver cloud-udbyderen brugere mulighed for at få adgang til cloud-tjenester ved hjælp af enten en privat VPN-tunnel med IPsec (Internet protocol security) eller en VPN-tunnel med SSL (secure socket layer) via det offentlige internet?*
23.	***NETVÆRKSMULIGHEDER – BGP-SUPPORT:*** *Benytter cloud-udbyderen BGP (border gateway-protokollen), der forbedrer failover i VPN-tunneller med IPsec?*
24.	***NETVÆRKSMULIGHEDER – MULIGHED FOR PRIVAT, DEDIKERET FORBINDELSE:*** *Har cloud-udbyderen en tjeneste, der giver mulighed for en direkte, privat forbindelse mellem cloud-udbyderens placeringer og en brugers datacenter, kontor eller samhusningsmiljø, der giver mulighed for store og hurtige dataoverførsler?*
25.	***NETVÆRKSMULIGHDER – FRONT-END-BELASTNINGSUDLIGNER:*** *Har cloud-udbyderen en tjeneste til front-end-belastningsudligning (internetbaseret), der accepterer anmodninger fra kunder via internettet og sender disse anmodninger på tværs af instanser, der er registreret i belastningsudligneren?*
26.	***NETVÆRKSMULIGHDER – BACK-END-BELASTNINGSUDLIGNER:*** *Har cloud-udbyderen en tjeneste med privat back-end-belastningsudligning, der sender trafik til instanser, som hostes i private undernet?*
27.	***NETVÆRKSMULIGHEDER – BELASTNINGSUDLIGNER TIL LAG 7:*** *Har cloud-udbyderen en tjeneste med belastningsudligning til lag 7 (HTTP eller hypertext transfer protocol), der kan udføre belastningsudligning af netværkstrafik mellem flere instanser?*
28.	***NETVÆRKSMULIGHEDER – BELASTNINGSUDLIGNER TIL LAG 4:*** *Har cloud-udbyderen en tjeneste med belastningsudligning til lag 4 (TCP eller transmission control protocol), der kan udføre belastningsudligning af netværkstrafik mellem flere instanser?*
29.	***NETVÆRKSMULIGHEDER – SESSIONSTILKNYTNING TIL BELASTNINGSUDLIGNERE:*** *Har cloud-udbyderen en belastningsudlignings-tjeneste med mulighed for sessionstilknytning?*
30.	***NETVÆRKSMULIGHEDER – DNS-BASERET BELASTNINGSUDLIGNING:*** *Har cloud-udbyderen en belastningsudligningstjeneste, der gør det muligt at belastningsudligne trafik til instanser, der hostes hos flere værter med tilknytning til et enkelt domæne?*
31.	***NETVÆRKSMULIGHEDER – LOGFILER TIL BELASTNINGSUDLIGNER:*** *Gør cloud-udbyderen det muligt at lave logfiler med detaljerede oplysninger om alle forespørgsler, der sendes til en belastningsudligner?*
32.	***NETVÆRKSMULIGHEDER – DNS:*** *Har cloud-udbyderen en DNS-tjeneste (Domain Name System) med høj tilgængelighed og skalerbarhed?*
33.	***NETVÆRKSMULIGHEDER – FORSINKELSESBASERET DNS-ROUTING:*** *Har cloud-udbyderen en DNS-tjeneste med mulighed for forsinkelsesbaseret routing (dvs. at DNS-tjenesten reagerer på DNS-forespørgsler med de ressourcer, der giver den bedste forsinkelse)?*
34.	***NETVÆRKSMULIGHEDER – GEOBASERET DNS-ROUTING:*** *Har cloud-udbyderen en DNS-tjeneste (Domain Name System) med mulighed for geobaseret routing (dvs. at DNS-tjenesten reagerer på DNS-forespørgsler med udgangspunkt i brugerens geografiske placering)?*
35.	***NETVÆRKSMULIGHEDER – FAILOVER-BASERET DNS-ROUTING:*** *Har cloud-udbyderen en DNS-tjeneste med mulighed for failover-baseret routing (dvs. at DNS-tjenesten sender DNS-forespørgsler til den aktive ressource, mens en anden ressource venter og kun bliver aktiv i tilfælde af en fejl i den primære ressource)?*

36.	***NETVÆRKSMULIGHEDER – TJENESTE TIL REGISTRERING AF DOMÆNER:*** *Har cloud-udbyderen tjenester til registrering af domænenavne (dvs. at brugere kan søge efter og registrere tilgængelige domænenavne)?*
37.	***NETVÆRKSMULIGHEDER – DNS-TILSTANDSKONTROL:*** *Har cloud-udbyderen en DNS-tjeneste, der overvåger ressourcernes status og ydeevne ved hjælp af tilstandskontrol?*
38.	***NETVÆRKSMULIGHEDER – INTEGRATION AF DNS OG BELASTNINGSUDLIGNER:*** *Har cloud-udbyderen en DNS-tjeneste, der kan integreres med cloud-udbyderens belastningsudligner?*
39.	***NETVÆRKSMULIGHEDER – VISUEL EDITOR:*** *Har cloud-udbyderen et værktøj, der giver brugere mulighed for at lave politikker for trafikstyring?*
40.	***INDHOLDSLEVERINGSNETVÆRK (CDN):*** *Har cloud-udbyderen en CDN-tjeneste, der gør det muligt at distribuere indhold med lav latenstid og hurtig dataoverførsel?*
41.	***NETVÆRKSMULIGHEDER – UDLØB AF CDN-CACHE:*** *Har cloud-udbyderen en indholdsleveringsnetværk (CDN)-tjeneste, der gør det muligt at fjerne et objekt fra edge-cachelagre, før det udløber, blandt andet funktioner såsom ugyldiggørelse af objekter og versionering?*
42.	***NETVÆRKSMULIGHEDER – EKSTERNE CDN-UDGANGSPUNKTER:*** *Har cloud-udbyderen en CDN-tjeneste, der understøtter et tilpasset udgangspunkt (dvs. en HTTP-server)?*
43.	***NETVÆRKSMULIGHEDER – CDN-OPTIMERING:*** *Har cloud-udbyderen en CDN-tjeneste med granulær kontrol til konfiguration af flere oprindelsesservere og cachelagringsegenskaber til forskellige URL'er (uniform ressource locators)?*
44.	***NETVÆRKSMULIGHEDER – CDN MED GEOBEGRÆNSNING:*** *Har cloud-udbyderen en CDN-tjeneste med mulighed for geobegrænsning, dvs. mulighed for at forhindre, at brugere i bestemte områder kan få adgang til indhold?*
45.	***NETVÆRKSMULIGHEDER – CDN-TOKENS:*** *Har cloud-udbyderen en CDN-tjeneste med mulighed for signerede URL'er, der typisk indeholder yderligere oplysninger såsom udløbsdato/-tidspunkt, så brugere bedre kan bestemme, hvem der har adgang til deres indhold?*
46.	***NETVÆRKSMULIGHEDER – CDN-CERTIFIKATER:*** *Har cloud-udbyderen en CDN-tjeneste med mulighed for tilpassede SSL-certifikater, der gør det muligt at sende indhold sikkert via en HTTPS fra edge-placeringer?*
47.	***NETVÆRKSMULIGHEDER – CDN-CACHE MED FLERE NIVEAUER:*** *Har cloud-udbyderen en CDN-tjeneste, der benytter en tilgang med cache på flere niveauer og regionale edge-cachelagre, der reducerer lav latenstid?*
48.	***NETVÆRKSMULIGHEDER – CDN-KOMPRIMERING:*** *Har cloud-udbyderen en CDN-tjeneste med mulighed for filkomprimering?*
49.	***NETVÆRKSMULIGHEDER – CDN-KRYPTEREDE OVERFØRSLER:*** *Har cloud-udbyderen en CDN-tjeneste, der giver brugere mulighed for at overføre deres følsomme data sikkert, således at disse oplysninger kun kan ses af bestemte komponenter og tjenester i brugerens oprindelsesinfrastruktur?*
50.	***NETVÆRKSMULIGHEDER – SLUTPUNKTER:*** *Giver cloud-udbyderens netværkstjenester brugerne slutpunkter, der kan sende trafik via udbyderens interne netværksforbindelse (dvs. private forbindelse), hvilket gør kommunikationen billigere og trafikken mere sikker?*

51.	***NETVÆRKSMULIGHEDER – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte netværksafsnit?* *Eksempel:* *Maks. antal virtuelle netværk pr. konto* *Maks. størrelse på et virtuelt netværk* *Maks. antal undernet pr. konto* *Maks. antal belastningsudlignere pr. konto* *Maks. antal poster på adgangskontrolliste (ACL)* *Maks. antal VPN-tunneller* *Maks. antal oprindelser pr. distribution* *Maks. antal certifikater pr. belastningsudligner*

3.3 Lager

	Krav
1.	***BLOKLAGRINGSTJENESTE:*** *Har cloud-udbyderen lagermængder på blokniveau, der kan bruges med beregningsinstanser?*
2.	***BLOKLAGRING – IOPS:*** *Gør cloud-udbyderen det muligt at købe et udtrykkeligt ydeevnemål eller -niveau på bloklagermængder såsom en gennemløb på et bestemt antal input/output operationer pr. sekund (IOPS) eller megabyte pr. sekund (MB/S)?*
3.	***BLOKLAGRING – SOLID STATE-HARDDISKE:*** *Understøtter cloud-udbyderen lagermedier med SSD (solid state drive), der giver mulighed for lave latenstider på etcifrede millisekunder?* • *Hvis ja, hvad er så det maksimale antal SSD'er, der kan vedhæftes pr. instans?*
4.	***BLOKLAGRING – SKALERING:*** *Gør cloud-udbyderen det muligt at gøre en nuværende bloklagermængde større uden behov for at klargøre en ny mængde og kopiere/flytte dataene?*
5.	***BLOKLAGRING – SNAPSHOTS:*** *Har cloud-udbyderen en bloklagringstjeneste, der gør det muligt at tage snapshots?*
6.	***BLOKLAGRING – DATADESTRUKTION:*** *Gør cloud-udbyderen det muligt at destruere data således, at uautoriserede brugere og/eller tredjeparter ikke længere kan læse eller få adgang til dem?*
7.	***BLOKLAGRING – KRYPTERING VED INAKTIVITET:*** *Tilbyder cloud-udbyderen kryptering på serversiden af inaktive data der er lagret på diskenheder, og dens snapshots?* • *Hvis ja, hvilken kryptografisk algoritme anvendes så?*
8.	***OBJEKTLAGRINGSTJENESTE:*** *Har cloud-udbyderen et sikkert, holdbart og yderst skalerbart objektlager til at gemme og hente en vilkårlig mængde data fra internettet?*

9.	***OBJEKTLAGRING – UREGELMÆSSIG ADGANG:*** *Har cloud-udbyderen et billigt niveau for lagringstjeneste, der er beregnet til at gemme objekter og filer, som sjældent åbnes?*
10.	***OBJEKTLAGRING – LAVERE HOLDBARHED:*** *Har cloud-udbyderen et niveau med lavere redundans, hvor en bruger kan gemme ikke-kritiske objekter, der let kan genskabes, som er billigere?*
11.	***OBJEKTLAGRING – MINDRE REGELMÆSSIG ADGANG:*** *Har cloud-udbyderen et niveau til data, som åbnes mindre regelmæssigt, men stadig kræver hurtig adgang?*
12.	***OBJEKTLAGRING – OBJEKTNIVEAUER:*** *Har cloud-udbyderen et objektlager med niveauer, dvs. muligheden for at flytte et objekt mellem objektlagerklasser eller -niveauer med udgangspunkt i, hvor regelmæssigt andre skal have adgang?*
13.	***OBJEKTLAGRING – STYRING AF LIVSCYKLUS:*** *Gør cloud-udbyderen det muligt at styre et objekts livscyklus ved hjælp af en livscykluskonfiguration, der definerer, hvordan objekter styres i deres levetid fra oprettelsen til sletningen?*
14.	***OBJEKTLAGRING – POLITIKBASERET STYRING:*** *Gør cloud-udbyderen det muligt at oprette og bruge politikker til styring af gemte data, deres livscyklus og deres niveauindstillinger?*
15.	***OBJEKTLAGRING – PLACERINGS- OG TIDSBASEREDE POLITIKKER:*** *Giver cloud-udbyderen brugerne mulighed for at oprette politikker, der kan begrænse adgangen til dataene med udgangspunkt i brugerens placering og tidspunktet for anmodningen?*
16.	***OBJEKTLAGRING – WEBSITE-HOSTING:*** *Gør cloud-udbyderen det muligt at hoste statiske websites i sin objektlagringstjeneste?*
17.	***OBJEKTLAGRING – KRYPTERING VED INAKTIVITET:*** *Giver cloud-udbyderen mulighed for server-side-kryptering (SSE) af data i hvile, hvor cloud-udbyderen sørger for krypteringsnøglerne?* • *Hvis ja, hvilken kryptografisk algoritme anvendes så?*
18.	***OBJEKTLAGRING – KRYPTERING MED BRUGERNØGLER:*** *Giver cloud-udbyderen mulighed for server-side-kryptering (SSE) ved hjælp af kryptografiske nøgler, der sendes til kunden?*
19.	***OBJEKTLAGRING – NØGLESTYRET TJENESTE:*** *Giver cloud-udbyderen mulighed for server-side-kryptering (SSE) ved hjælp af en tjeneste til nøglestyring, der opretter krypteringsnøgler, definerer politikker for, hvordan nøglerne kan bruges, og overvåger brugen af nøgler for at bevise, at de bruges korrekt?*
20.	***OBJEKTLAGRING – HOVEDNØGLE PÅ KUNDESIDE:*** *Giver cloud-udbyderen brugere mulighed for at beholde kontrollen over krypteringsnøglerne og fuldføre krypteringen/dekrypteringen af objekter på kundesiden?*
21.	***OBJEKTLAGRING – STÆRK ENSARTETHED:*** *Giver cloud-udbyderen mulighed for ensartet læsning efter skrivning for PUT-drift med nye objekter?*
22.	***OBJEKTLAGRING – DATALOKALITET:*** *Giver cloud-udbyderen mulighed for avanceret områdeisolation, så objekter, der gemmes i et område, aldrig forlader området, medmindre brugeren udtrykkeligt overfører dem til et andet område?*

23.	***OBJEKTLAGRING – REPLIKERING:*** *Gør cloud-udbyderen det muligt at replikere mellem områder, så objekter automatisk replikeres mellem brugervalgte områder?*
24.	***OBJEKTLAGRING – VERSIONERING:*** *Giver cloud-udbyderen mulighed for versionering, dvs. mulighed for at gemme og beholde flere versioner af et objekt?*
25.	***OBJEKTLAGRING – MARKÉR SOM MÅ IKKE SLETTES:*** *Gør cloud-udbyderen det muligt at markere et element som et, der ikke må slettes?*
26.	***OBJEKTLAGRING – MFA-SLETNING:*** *Giver cloud-udbyderen mulighed for multifaktorautentificering (MFA) til sletninger med henblik på yderligere sikkerhed?*
27.	***OBJEKTLAGRING – OVERFØRSEL I FLERE DELE:*** *Gør cloud-udbyderen det muligt at overføre et objekt i flere dele, hvor hver del hænger sammen med objektets data, og disse objektdele kan overføres selvstændigt i vilkårligt rækkefølge?*
28.	***OBJEKTLAGRING – TAGS:*** *Gør cloud-udbyderen det muligt at oprette og tilknytte dynamiske tags, der kan ændres, på objektniveau?*
29.	***OBJEKTLAGRING – NOTIFIKATIONER:*** *Gør cloud-udbyderen det muligt at sende notifikationer i tilfælde af visse begivenheder på objektniveau (dvs. tilføjelser/sletninger)?*
30.	***OBJEKTLAGRING – LOGFILER:*** *Gør cloud-udbyderen det muligt at oprette revisionslogfiler med oplysninger om en enkelt anmodning om adgang, f.eks. personen, der sender anmodningen, anmodningstidspunktet, anmodningshandlingen, svarstatus og fejlkoden?*
31.	***OBJEKTLAGRING – LAGER TIL OBJEKTER:*** *Har cloud-udbyderen et objektlager, der giver brugere mulighed for hurtig visualisering af objekter og deres status, så de hurtigt kan se objekter med offentlig adgang?*
32.	***OBJEKTLAGRING – LAGER TIL METADATA:*** *Giver cloud-udbyderen brugerne mulighed for at visualisere objekternes metadata hurtigt?*
33.	***OBJEKTLAGRING – OPTIMERING AF OVERFØRSLER:*** *Har cloud-udbyderen mulighed for at sende data fra Edge-placeringer til lagringstjenesten ved hjælp af en optimeret netværkssti?*
34.	***OBJEKTLAGRING – FORESPØRGSELSKAPACITET:*** *Giver cloud-udbyderen brugerne mulighed for at sende forespørgsler til sin objektlagringtjeneste ved hjælp af SQL-udtryk (structured query language)?*
35.	***OBJEKTLAGRING – HENTNING AF DELMÆNGDE:*** *Giver cloud-udbyderen brugerne mulighed for kun at hente en delmængde af data fra et objekt ved hjælp af SQL-udtryk (structured query language)?*
36.	***FILLAGRINGSTJENESTE:*** *Har cloud-udbyderen en enkel og skalerbar fillagringstjeneste, der kan bruges sammen med beregningsinstanser i cloud-systemet?*
37.	***FILLAGRING – REDUNDANS:*** *Gemmer cloud-udbyderen filsystemobjekter redundant (dvs. bibliotek, fil og link) i flere datacentre og anlæg med henblik på bedre tilgængelighed og holdbarhed?*

38.	***FILLAGRING – DATADESTRUKTION:*** *Gør cloud-udbyderen det muligt at destruere fillagringsdata således, at uautoriserede brugere eller tredjeparter ikke længere kan læse eller få adgang til dem?*
39.	***FILLAGRING – HØJ TILGÆNGELIGHED:*** *Giver cloud-udbyderens administrerede filsystem en høj grad af tilgængelighed?*
40.	***FILLAGRING – NFS:*** *Understøtter cloud-udbyderen NFS-protokol (network file system)?*
41.	***FILLAGRING – SMB:*** *Understøtter cloud-udbyderen SMB-protokol (server message block)?*
42.	***FILLAGRING – KRYPTERING VED INAKTIVITET:*** *Understøtter cloud-udbyderens fillagringstjeneste kryptering ved inaktivitet?*
43.	***FILLAGRING – KRYPTERING VED OVERFØRSEL:*** *Understøtter cloud-udbyderens fillagringstjeneste kryptering af data, der overføres?*
44.	***FILLAGRING – VÆRKTØJ TIL MIGRERING AF DATA:*** *Tilbyder cloud-udbyderen et værktøj til migrering af data, der giver brugere mulighed for at flytte data fra lokale systemer til det cloud-baserede filsystem?*
45.	***ARKIVLAGERTJENESTE:*** *Har cloud-udbyderen en meget billig lagringstjeneste, der er beregnet til arkivering af objekter og filer, der sjældent kræver adgang og næsten ikke ændres?*
46.	***ARKIVLAGER – FEJLTOLERANCE:*** *Har cloud-udbyderens arkitektur en fejltolerance til sin arkivlagertjeneste?*
47.	***ARKIVLAGER – INGEN MULIGHED FOR ÆNDRING:*** *Giver cloud-udbyderen mulighed for arkiverede objekter og filer, der ikke kan ændres?*
48.	***ARKIVLAGER – WORM:*** *Giver cloud-udbyderen mulighed for WORM (write once read many)?*
49.	***ARKIVLAGER – HENTNING AF DELMÆNGDE:*** *Giver cloud-udbyderen brugerne mulighed for kun at hente en delmængde af data fra et arkiveret objekt ved hjælp af SQL-udtryk?*
50.	***ARKIVLAGER – HURTIG HENTNING:*** *Giver cloud-udbyderen brugene flere muligheder for at hente data til forskellige priser med forskellige hentningstider?*
51.	***ARKIVLAGER – KRYPTERING VED INAKTIVITET:*** *Understøtter cloud-udbyderens arkivlagertjeneste kryptering ved inaktivitet?*

52.	***LAGRING – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte lagersektion?* *Eksempel:* *Maks. diskenhedsstørrelse* *Maks. antal drev, der er vedhæftet en instans* *Maks. antal IOPS (input/output operationer pr. sekund)* *Maks. objektstørrelse* *Maks. antal objekter pr. lagerkonto* *Maks. antal snapshots*

4. Administration

	Krav
1.	***ADMINISTRATION – BRUGERE OG GRUPPER:*** *Har cloud-udbyderen en tjeneste til administration og oprettelse af brugere og grupper af brugere af sin infrastruktur og dens ressourcer?*
2.	***ADMINISTRATION – NULSTILLING AF ADGANGSKODE:*** *Giver cloud-udbyderen brugerne mulighed for at nulstille deres egen adgangskode med selvbetjening?*
3.	***ADMINISTRATION – TILLADELSER:*** *Gør cloud-udbyderen det muligt at give brugere og grupper tilladelser på ressourceniveau?*
4.	***ADMINISTRATION – MIDLERTIDIGE TILLADELSER:*** *Gør cloud-udbyderen det muligt at oprette tilladelser, der er gyldige i et bestemt tidsinterval?*
5.	***ADMINISTRATION – MIDLERTIDIGE LEGITIMATIONSOPLYSNINGER:*** *Giver cloud-udbyderen brugerne mulighed for at oprette og sørge for midlertidige legitimationsoplysninger til brugere, der er tillid til, som er konfigureret til at holde i et par minutter eller flere timer?*
6.	***ADMINISTRATION – ADGANGSKONTROL:*** *Giver cloud-udbyderen detaljeret adgangskontrolforanstaltninger til sine infrastrukturs ressourcer?* • *Hvis ja, hvilke betingelser kan så bruges af disse kontrolforanstaltninger (f.eks. klokkeslæt, oprindelig IP-adresse osv.)?*
7.	***ADMINISTRATION – INDBYGGEDE POLITIKKER:*** *Indeholder cloud-udbyderens infrastruktur indbyggede politikker for adgangskontrol, der kan knyttes til brugere og grupper?*
8.	***ADMINISTRATION – TILPASSEDE POLITIKKER:*** *Giver cloud-udbyderens infrastruktur mulighed for oprettelse og tilpasning af politikker for adgangskontrol, der kan knyttes til brugere og grupper?*
9.	***ADMINISTRATION – POLITIKSIMULATOR:*** *Tilbyder cloud-udbyderen en mekanisme til at teste virkningerne af politikker for adgangskontrol, før sådanne politikker indgår i produktionen?*

10.	***ADMINISTRATION – CLOUD MFA:*** *Gør cloud-udbyderen det muligt at bruge multifaktorautentificering (MFA) som en ekstra adgangskontrol og godkendelse i sin infrastruktur?*
11.	***ADMINISTRATION – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte administrationssektion?* *Eksempel:* *Maks. antal brugere* *Maks. antal grupper* *Maks. antal administrerede politikker*

5. Sikkerhed

	Krav
1.	***SIKKERHED – PERSONUNDERSØGELSE:*** *Får alle cloud-udbyderens personale med adgang til tjenestens infrastruktur (både fysisk eller ikke-fysisk) deres baggrund undersøgt?*
2.	***SIKKERHED – FYSISK ADGANG:*** *Begrænser cloud-udbyderen personalets adgang til tjenestens infrastruktur, medmindre der er tale om en bestemt fejlsag, anmodning om ændring eller lignende formel godkendelse?*
3.	***SIKKERHED – ADGANGSLOGFILER:*** *Opretter cloud-udbyderen logfiler med personalets adgang til sin infrastruktur, således at adgang altid logføres, og logfilerne gemmes i minimum 90 dage?*
4.	***SIKKERHED – VÆRTSLOGINS:*** *Begrænser cloud-udbyderen udbyderens personales mulighed for at logge ind på beregningsværter i stedet for at automatisere alle opgaver, der udføres på beregningsværter, således at indholdet i disse automatiserede jobs logføres, og logfilerne gemmes i mindst 90 dage?*
5.	***SIKKERHED – KRYPTOGRAFISKE NØGLER:*** *Har cloud-udbyderen en tjeneste, der gør det muligt at oprette og styre de kryptografiske nøgler, der bruges til at kryptere brugerdata?*
6.	***SIKKERHED – STYRING AF ADGANGSNØGLER:*** *Gør cloud-udbyderen det muligt at se, hvornår en adgangsnøgle sidst blev brugt, udskifte gamle nøgler og fjerne inaktive brugere?*
7.	***SIKKERHED – NØGLER TIL KUNDER:*** *Giver cloud-udbyderen brugere mulighed for at importere nøgler fra deres egen infrastruktur til nøglestyring til cloud-udbyderens nøglestyringstjeneste?*
8.	***SIKKERHED – INTEGRATION AF TJENESTE MED KRYPTOGRAFISKE NØGLER:*** *Kan cloud-udbyderens nøglestyringstjeneste integreres med andre cloud-tjenester, så inaktive data kan krypteres?*
9.	***SIKKERHED – HSM:*** *Har cloud-udbyderen dedikerede HSM'er (hardware security modules), dvs. hardware, der giver sikker lagring af nøgler og gør det muligt at udføre kryptografiske handlinger i et hardwaremodul, som ikke kan saboteres?*

10.	***SIKKERHED – KRYPTOGRAFISKE NØGLERS HOLDBARHED:*** *Understøtter cloud-udbyderen nøglers holdbarhed, blandt andet med mulighed for at gemme flere kopier, så nøgler kan hentes, hvis det er nødvendigt?*
11.	***SIKKERHED – SSO:*** *Har cloud-udbyderen en SSO-tjeneste (single sign-on), der giver brugere mulighed for central styring af adgangen til flere konti og virksomhedsprogrammer?*
12.	***SIKKERHED – CERTIFIKATER:*** *Har cloud-udbyderen en administreret tjeneste til at klargøre, administrere og udrulle SSL- eller TLS-certifikater (transportlagssikkerhed)?*
13.	***SIKKERHED – FORNYELSE AF CERTIFIKATER:*** *Gør cloud-udbyderens tjeneste til styring af certifikater det muligt at forny certifikater?*
14.	***SIKKERHED – WILDCARD-CERTIFIKATER:*** *Gør cloud-udbyderens tjeneste til styring af certifikater det muligt at bruge wildcard-certifikater?*
15.	***SIKKERHED – CERTIFICATE AUTHORITY (NØGLECENTER):*** *Fungerer cloud-udbyderens tjeneste til styring af certifikater også som en CA (certificate authority)?*
16.	***SIKKERHED – ACTIVE DIRECTORY:*** *Har cloud-udbyderen en administreret Microsoft Active Directory-tjeneste (AD) i cloud-systemet?*
17.	***SIKKERHED – LOKALT ACTIVE DIRECTORY:*** *Understøtter cloud-udbyderens administrerede Microsoft Active Directory-tjeneste (AD) integration med lokalt Microsoft Active Directory (AD)?*
18.	***SIKKERHED – LDAP:*** *Understøtter cloud-udbyderens administrerede Microsoft Active Directory-tjeneste (AD) lightweight directory access protocol (LDAP)?*
19.	***SIKKERHED – ACTIVE DIRECTORY:*** *Understøtter cloud-udbyderens administrerede Microsoft Active Directory-tjeneste (AD) security assertion markup language (SAML)?*
20.	***SIKKERHED – STYRING AF LEGITIMATIONSOPLYSNINGER:*** *Har cloud-udbyderen en administreret tjeneste, der gør det let for brugerne at udskifte, styre og hente legitimationsoplysninger, f.eks. API-nøgler, legitimationsoplysninger til databaser og andre hemmeligheder?*
21.	***SIKKERHED – WAF:*** *Har cloud-udbyderen en firewall til webapplikationer (WAF), som beskytter mod almindelig udnyttelse af nettet, der kan påvirke tilgængeligheden, kompromittere sikkerheden eller bruge kostbare ressourcer?*
22.	***SIKKERHED – DDOS:*** *Har cloud-udbyderen en tjeneste til at beskytte mod de mest almindelige og hyppige gentagne DDoS-angreb (distributed denial of service) mod netværk og transportlag samt mulighed for at skrive brugerdefinerede regler mod sofistikerede angreb på programlag?*
23.	***SIKKERHED – SIKKERHEDSANBEFALINGER:*** *Har cloud-udbyderen en tjeneste, der gør det muligt at vurdere sårbarheder i programmer og ressourcer?*
24.	***SIKKERHED – TRUSSELREGISTRERING:*** *Har cloud-udbyderen en administreret tjeneste til trusselregistrering?*

25.	***SIKKERHED – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte sikkerhedssektion?* *Eksempel:* *Maks. antal kundehovednøgler* *Maks. antal HSM'er (hardware-sikkerhedsmoduler)*

6. Compliance

Nedenstående liste er kun til illustrationsformål og skal ikke betragtes som en udførlig liste over alle de certificeringer og standarder, der kan gælde for cloud-tjenester.

Angiv, hvilke internationale og branchespecifikke compliancestandarder cloud-udbyderen opfylder:

Certificeringer/bekræftelser	***Love, bestemmelser og privatliv***	***Tilpasninger/rammer***
☐ C5 [Tyskland]	*☐ EU forordningen om databeskyttelse*	*☐ CDSA*
☐ CISPE-adfærdskodeks for databeskyttelse	*☐ EU-modelklausuler*	
☐ CNDCP (Pagt om klimaneutrale datacentre)		
☐ DIACAP	*☐ FERPA*	*☐ CIS*
☐ DoD SRG niveau 2 og 4	*☐ GDPR*	*☐ Info om strafferetspleje Service (CJIS)*
☐ FedRAMP	*☐ GLBA*	*☐ CSA*
☐ FIPS 140-2	*☐ HIPAA*	*☐ EU's og USA's værn om privatlivets fred*
☐ HDS (Frankrig, sundhedspleje)	*☐ HITECH*	*☐EU's 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 (FDA CFR 21 del 11)*
☐ IRAP [Australien]	*☐ PIPEDA [Canada]*	*☐ ICREA*
☐ MTCS Tier 3 [Singapore]	*☐ Privacy Act [Australien]*	*☐ IT Grundschutz [Tyskland]*
☐ PCI DSS Niveau 1	*☐ Privacy Act [New Zealand]*	*☐ MARS – E*
☐ SEC-regel 17-a-4(f)	*☐ Spansk DPA-godkendelse*	*☐ MITA 3.0*

☐ *SOC1 / ISAE 3402*	☐ *U.K. DPA - 1988*	☐ *MPAA*
☐ *SOC2 / SOC3*	☐ *VPAT/afsnit 508*	☐ *NIST*
☐ *SWIPO IaaS-kode*		
		☐ *Uptime Institute Tiers*
		☐ *Principperne for cloudsikkerhed i Storbritannien*

Ved at benytte ovenstående compliance-rapporter kan organisationer i den offentlige sektor vurdere unikke tilbud med hensyn til sikkerhed, compliance og driftsmæssig standard. Disse rapporter kan vise, at CISP'en ved at overholde disse krav opfylder kravene i de nedenstående kontrolforanstaltninger for drift af datacentre, der er obligatoriske for den offentlige cloud-udbyder. Krav til compliance i forbindelse med disse rapporter forvisser parter i den offentlige sektor om, at nedenstående kontrolforanstaltninger er på plads.

- ***Kontrolleret adgang:*** *CISP'en skal begrænse fysisk adgang til kun at omfatte personer, som skal være på en placering af gode virksomhedsmæssige grunde. Hvis de får adgang, skal den annulleres, så snart det nødvendige arbejde er udført.*
- ***Adgang kontrolleres og overvåges:*** *Adgang til det yderste datacenterlag skal være en kontrolleret proces. CISP'en bør bevogte indgange med sikkerhedsvagter og have tilsynsførende, der holder øje med vagtpersonalet og besøgende ved hjælp af overvågningskameraer. Når godkendte personer er til stede på adressen, skal de have et badge, der kræver MFA og begrænser deres adgang til områder, hvor de er godkendt på forhånd.*
- ***CISP-datacentermedarbejdere:*** *CISP'ens medarbejdere, der regelmæssigt skal have adgang til et datacenter, skal have tilladelser til relevante dele af centeret, alt efter hvilken stilling de har, og deres adgang skal undersøges regelmæssigt. Personalelister skal gennemgås regelmæssigt af en person med ansvar for adgang til områder for at sikre, hver medarbejders tilladelse stadig er nødvendig. Hvis en medarbejder ikke har et fast arbejdsrelateret behov for at være på datacentret, skal vedkommende gennemgå processen for besøgende.*
- ***Overvågning som foranstaltning mod uautoriseret adgang:*** *CISP'er skal hele tiden holde øje med, om personer får uautoriseret adgang til datacenteret, ved hjælp af videoovervågning, adgangslogfiler og overvågningssystemer med logføring af adgang. Indgange skal beskyttes med alarmer, der aktiveres, hvis en dør tvinges åben eller holdes åben.*
- ***CISP'ens sikkerhedscenter overvåger global sikkerhed:*** *CISP'ens sikkerhedscentre skal være placeret over hele verden og være ansvarlige for overvågning, afhjælpning og udførelse af sikkerhedsprogrammer for CISP-datacentre. De skal være ansvarlige for administration af fysisk adgang og reagere i tilfælde af uvedkommende adgang og samtidig hjælpe lokale datacentres sikkerhedsmedarbejdere døgnet rundt. De skal sørge for kontinuerlig overvågning såsom at holde øje med adgangsaktiviteter, annullere adgangstilladelser og være i stand til at reagere og analysere i tilfælde af et muligt brud på sikkerheden.*
- ***Gennemgang af lag-til-lag-adgang:*** *Adgangen til infrastrukturlaget bør begrænses på baggrund af virksomhedens behov. Implementering af en adgangskontrol fra lag til lag sikrer, at der ikke gives adgang til hvert enkelt lag som standard. Adgang til et bestemt lag skal kun gives, hvis der er et specifikt behov for adgang til det pågældende lag.*
- ***Vedligeholdelse af udstyr er en del af den daglige drift:*** *CISP'ens personale skal diagnosticere maskiner, netværk og backupudstyr for at sikre, at det fungerer både nu og i nødstilfælde. Regelmæssig vedligeholdelse af datacentrets udstyr og værktøjer skal være en del af den daglige drift på CISP'ens datacentre.*
- ***Beredskabsklart backup-udstyr:*** *Vand, strøm, telekommunikation og internetforbindelse skal udformes med redundans, så CISP'en kan opretholde kontinuerlig drift i en nødsituation. Elsystemer skal designes til at være fuldstændig redundante, således at strømforsyninger, i tilfælde af nedbrud, kan aktiveres, så bestemte funktioner kan udføres, og generatorer kan forsyne hele centeret med reservestrøm. Personale og systemer skal overvåge og kontrollere temperaturen og luftfugtigheden, så overophedning undgås, og antallet af mulige nedbrud reduceres yderligere.*

- ***Teknologi og personale sørger for endnu mere sikkerhed:*** *Der skal være obligatoriske procedurer for at adgang til datalaget. Dette omfatter gennemgang og godkendelse af en persons ansøgning om adgang af autoriserede personer. Imens bør systemer til registrering af trusler og elektronisk indtrængen overvåge og automatisk aktivere alarmer i tilfælde af angreb eller mistænkelig aktivitet. Hvis en dør for eksempel holdes åben eller brydes op, udløses en alarm. CISP'en bør bruge sikkerhedskameraer og gemme optagelserne i henhold til lovpligtige krav og krav til compliance.*

- ***Forebyggelse af fysisk og teknologisk indtrængen:*** *Adgangspunkter til serverrum bør forstærkes med elektroniske styreenheder, der kræver multifaktorgodkendelse. CISP bør også være forberedt på at forhindre teknologisk indtrængen. CISP-servere bør kunne advare medarbejderne om ethvert forsøg på at fjerne data. I tilfælde af et brud på sikkerheden skal serveren deaktiveres automatisk.*

- ***Servere og medier får ekstra opmærksomhed:*** *Medielagerenheder, der bruges til at gemme kundedata, skal klassificeres af CISP'en som kritiske og behandles sådan i løbet af deres livstidscyklus. CISP'en skal have strenge standarder for, hvordan enhederne installeres, vedligeholdes og destrueres, når de ikke længere skal bruges. Når en harddisk ikke længere kan bruges, udfaser CISP'en medierne ved hjælp af teknikker som er angivet i NIST 800-88. Medier, der blev brugt til at gemme kundedata, fjernes ikke fra CISP'ens kontrol, før de er blevet udfaset sikkert.*

- ***Tredjepartskontrollanter bekræfter CISP'ens procedurer og systemer:*** *CISP'en skal kontrolleres af eksterne parter, der inspicerer datacentre grundigt for at bekræfte, at CISP'en overholder de nødvendige regler, så de kan få deres sikkerhedscertifikater. Alt efter hvilket program, der er til compliance, og hvad kravene til det er, kan eksterne kontrollører tale med CISP'ens medarbejdere om, hvordan de håndterer og destruerer medier. Kontrollanterne kan også overvåge datacenterets indgange og korridorer ved hjælp af overvågningskameraer. De kan også undersøge udstyr, såsom CISP'ens elektroniske adgangskontrolenheder og sikkerhedskameraer.*

- ***Forberedt på det uventede:*** *CISP'en skal proaktivt forberede sig på mulige miljøtrusler, såsom naturkatastrofer og brand. CISP'en kan beskytte datacentre ved enten at installere automatiske sensorer og udstyr, der reagerer. Sensorer, der registrerer vand, skal installeres, så medarbejderne advares om problemer, mens automatiske pumper fjerner væske og forhindrer skader. På samme måde kan automatiske brandalarmer og slukningssystemer reducere risikoen og advare CISP'ens medarbejdere og brandfolk, hvis der er problemer.*

- ***Høj tilgængelighed takket være flere tilgængelighedszoner:*** *CISP'en skal sørge for flere tilgængelighedszoner med henblik på højere fejltolerance. Hver tilgængelighedszone skal bestå af et eller flere datacentre, være fysisk adskilt fra hinanden og have mulighed for reservestrøm og netværksforbindelse i tilfælde af nedbrud. Tilgængelighedszoner bør forbindes med hinanden med hurtige, private fiberoptiske netværk for at kunne skabe programmer, der automatisk fejler mellem tilgængelighedszoner uden afbrydelse.*

- ***Simulation af afbrydelser og vurdering af vores respons:*** *CISP'en skal have en plan for driftskontinuitet som en driftsvejledning, der beskriver, hvordan de undgår og mindsker afbrydelser som følge af naturkatastrofer, med en detaljeret vejledning i, hvad der skal gøres før, under og efter en begivenhed. For at mindske risikoen og forberede sig på det uventede skal CISP'en afprøve planen for driftskontinuitet regelmæssigt med øvelser, der simulerer forskellige scenarier. CISP'en skal dokumentere, hvordan medarbejderne og processerne fungerer og derefter drøfte erfaringer med dem samt eventuelle ting, de skal gøre bedre for at reagere hurtigere. CISP'ens medarbejdere skal uddannes og gøre klar til at kunne gendanne hurtigt efter nedbrud med en grundig gendannelsesproces, så yderligere afbrydelser undgås pga. fejl.*

- ***Hjælp med at opfylde effektivitetsmålene:*** *Ud over at tage fat på miljørisici bør CISP også indarbejde bæredygtighedshensyn i datacenterets udformning. CISP'en skal gøre rede for sin forpligtelse til brug af vedvarende energi i sine datacentre og oplyse kunderne om, hvordan de kan reducere CO2-udledningen mere end med deres egne datacentre.*

- ***Valg af placeringer:*** *Før der vælges en placering, skal CISP'en vurdere omgivelserne og det geografiske område. Datacentres placeringer skal vælges nøjagtigt af hensyn til risici i omgivelserne såsom oversvømmelser, voldsomt vejr og jordskælvsfare. CISP'ens tilgængelighedszoner skal bygges, således at de er selvstændige og fysisk adskilt fra hinanden.*

- ***Redundans:*** *Datacentrene bør udformes således, at de kan forudse og tolerere fejl, samtidig med at tjenesteniveauet opretholdes. I tilfælde af fejl skal automatiserede processer flytte trafik væk fra det berørte område. Kerneprogrammer skal udrulles i en N+1-standard, så hvis der opstår fejl i et datacenter, er der tilstrækkelig kapacitet til at sørge for, at trafikken belastningsjusteres til de øvrige steder.*

- ***Tilgængelighed:*** *CISP'en skal identificere kritiske systemkomponenter, som er nødvendige for at sikre systemets tilgængelighed, og have en gendannelsestjeneste, der kan bruges i tilfælde af nedbrud. Kritiske systemkomponenter skal være sikkerhedskopieret på flere isolerede steder. Hver placering eller tilgængelighedszone skal kunne fungere*

selvstændigt og være yderst pålidelig. Tilgængelighedszoner skal være forbundet, så programmer automatisk har fail-over mellem tilgængelighedszoner uden afbrydelse. Systemet skal designes således, at systemerne er yderst modstandsdygtige, og tjenesterne derfor kan benyttes. Datacenterdesign med tilgængelighedszoner og datareplikering skal give CISP-kunder mulighed for at gendanne ekstremt hurtigt og nå deres mål for gendannelsespunkter samt den bedst mulige tjenestetilgængelighed.

- ***Kapacitetsplanlægning:*** *CISP'er skal hele tiden holde øje med tjenesteforbruget for at udrulle en infrastruktur, der giver mulighed for forpligtelser og krav til tilgængelighed. CISP'en skal have en model til planlægning af kapacitet, der vurderer brugen og kravene i forbindelse med CISP'ens infrastruktur mindst en gang om måneden. Denne model skal gøre det muligt at planlægge fremtidige behov og omfatte overvejelser såsom behandling af oplysninger, telekommunikation og mulighed for at gemme revisionslogfiler.*

PLAN FOR DRIFTSKONTINUITET og GENDANNELSE EFTER NEDBRUD

- ***Plan for driftskontinuitet:*** *CISP'ens plan for driftskontinuitet skal omfatte foranstaltninger, der gør det muligt at undgå og reducere afbrydelser på grund af miljømæssige risici. Den bør omfatte driftsmæssige detaljer om, hvad der skal gøres før, under og efter et nedbrud. Planen for driftskontinuitet bør omfatte test med blandt andet simulationer af forskellige scenarier. Både under og efter testen skal CISP'en dokumentere personalets og processens effektivitet, korrigerende handlinger og erfaringer med henblik på løbende forbedring.*

- ***Respons i tilfælde af pandemi:*** *CISP'en skal have politikker for respons i tilfælde af pandemi og procedurer til sin planlægning af gendannelse efter nedbrud, så det er muligt at forberede hurtig respons i tilfælde af smitsomme sygdomme. Migreringsstrategierne omfatter alternative personalemodeller, der gør det muligt at overdrage kritiske processer til eksterne ressourcer og aktivere en krisehåndteringsplan, så den kritiske drift kan fortsætte. Pandemiplaner bør henvise til internationale sundhedsorganisationer og bestemmelser, deriblandt kontaktpersoner hos internationale agenturer.*

OVERVÅGNING og LOGFØRING

- ***Kontrol af adgang til datacentre:*** *Adgangen til datacentre skal kontrolleres regelmæssigt. Adgangen skal tilbagekaldes automatisk, når en medarbejders journal slettes i CISP'ens HR-system. Og hvis en medarbejders eller leverandørs adgang udløber i henhold til den godkendte anmodningsvarighed, skal vedkommendes adgang tilbagekaldes, også selv om vedkommende stadig er ansat hos CISP'en.*

- ***Adgangslogfiler til datacentre:*** *Fysisk adgang til CISP'ens datacentre skal registreres i logfiler, overvåges og beholdes. CISP'en skal analysere oplysninger fra logiske og fysiske overvågningssystemer, så sikkerheden kan forbedres efter behov.*

- ***Overvågning af adgang til datacentre:*** *CISP'en skal overvåge datacentre ved hjælp af globale sikkerhedscentre med ansvar for overvågning, afhjælpning og udførelse af sikkerhedsprogrammer. De skal assistere globalt døgnet rundt ved at administrere og overvåge adgangen til datacentre, levere udstyr til lokale teams og andre supportteams, så de kan reagere på sikkerhedshændelser med afhjælpning, konsulentydelser, analyse og respons.*

OVERVÅGNING og OPDAGELSE

- ***Videoovervågning:*** *Fysiske indgange til serverrum skal optages af videoovervågningssystemer. Optagelserne skal beholdes i henhold til bestemmelser og krav til compliance.*

- ***Indgange til datacentre:*** *Fysisk adgang skal kontrolleres ved bygningens indgange af uddannet sikkerhedspersonale ved hjælp af overvågning, registreringssystemer og andre elektroniske metoder. Autoriseret personale skal benytte MFA for at få adgang til datacentre. Indgange til serverrum skal sikres med enheder, der slår alarm, så det er muligt at reagere, hvis nogen bryder en dør op eller holder den åben.*

- ***Opdagelse af indtrængen:*** *Elektroniske systemer til opdagelse af indtrængen skal installeres i datalaget, så det er muligt at overvåge og automatisk alarmere personalet i tilfælde af sikkerhedsbrud. Ind- og udgange til serverrum skal sikres med enheder, der kræver, at hver enkelt person skal udføre en MFA for at komme ind eller ud. Disse enheder slår alarm, hvis døren tvinges op uden tilladelse eller holdes åben. Døralarmer skal også konfigureres til at registrere tilfælde, hvor en person forlader eller går ind i et datalag uden at angive multifaktorgodkendelse. Alarmer skal øjeblikkeligt sendes til CISP'ens sikkerhedscenter der har ansvar for overvågning døgnet rundt, så de øjeblikkeligt kan logføre, analysere og reagere.*

ENHEDSSTYRING

- ***Håndtering af aktiver:*** *CISP'ens aktiver skal styres centralt ved hjælp af et lagerstyringssystem, der gemmer og sporer ejer, placering, status, vedligeholdelse og viser detaljerede oplysninger om CISP'ens aktiver. Når aktiver er købt, skal de scannes og spores, og aktiver, der vedligeholdes, skal kontrolleres, og deres ejerskab, status og afhjælpning skal overvåges.*

- ***Destruktion af medier:*** *Medielagringsenheder, der bruges til at gemme kundedata, skal klassificeres af CISP'en som kritiske og behandles sådan i hele deres livstidscyklus. CISP'en skal have strenge standarder for, hvordan enhederne installeres, vedligeholdes og destrueres, når de ikke længere skal bruges. Når en harddisk ikke længere kan bruges, skal CISP'en udfase medierne ved hjælp af teknikker, som er angivet i NIST 800-88. Medier, der blev brugt til at gemme kundedata, skal ikke fjernes fra CISP'ens kontrol, før de er blevet udfaset sikkert.*

DRIFTSMÆSSIGE SUPPORTSYSTEMER

- ***Strøm:*** *CISP'ens datacenters elektriske systemer skal designes til at kunne fungere og vedligeholdes uden driftsafbrydelser 24 timer i døgnet. CISP'en skal sikre, at datacentre er udstyret med en nødstrømforsyning, der sørger for strøm til driften i tilfælde af en afbrydelse af strømmen til kritiske og uundværlige arbejdsopgaver i centeret.*

- ***Klima og temperatur:*** *CISP-datacentre skal benytte mekanismer til at kontrollere klimaet og opretholde den korrekte driftstemperatur til servere og andet hardware for at undgå overophedning og mindske risikoen for afbrydelser. Personalet og systemerne skal sørge for, at temperaturen og luftfugtigheden altid er på de korrekte niveauer.*

- ***Brandalarmer og -slukning:*** *CISP'ens datacentre skal udstyres med automatiske brandalarmer og -slukningssystemer. Brandalarmer skal have røgalarmer, i netværks-, mekaniske og infrastrukturelle rum. Disse områder skal også beskyttes med slukningssystemer.*

- ***Opdagelse af lækager:*** *For at CISP'en kan opdage vandlækager, skal datacentre udstyres med systemer, der kan registrere vand. Hvis systemerne registrerer vand, skal der være mekanismer, som kan fjerne vandet og forhindre yderligere vandskader.*

VEDLIGEHOLDELSE AF INFRASTRUKTUR

- ***Vedligeholdelse af udstyr:*** *CISP'en skal overvåge og præventivt vedligeholde elektrisk og mekanisk udstyr for at sikre, at systemerne i CISP'ens datacentre hele tiden fungerer. Procedurerne til vedligeholdelse af udstyr skal udføres af kvalificeret personale og afsluttes i henhold til en dokumenteret tidsplan for vedligeholdelse.*

- ***Overvågning af omgivelser:*** *CISP'en skal overvåge elektriske og mekaniske systemer samt udstyr, så problemer kan opdages med det samme. Dette skal gøres ved hjælp af værktøjer til vedvarende kontrol og visning af oplysninger ved hjælp af CISP'ens systemer til styring af bygningen og overvågning af elektriske systemer. Præventiv vedligeholdelse skal udføres, så udstyret hele tiden kan fungere.*

STYRING OG RISIKO

- ***Løbende risikostyring for datacentre:*** *CISP'ens sikkerhedscenter skal udføre regelmæssig gennemgang af trusler og sårbarheder for datacentre. Løbende vurdering og afhjælpning af mulige sårbarheder skal udføres ved hjælp af risikovurdering i datacentre. Denne vurdering skal udføres foruden processerne til risikovurdering på virksomhedsniveau, der bruges til at opdage og håndtere risiko for virksomheden som helhed. Denne process skal også tage højde for regionale bestemmelser og miljømæssige risici.*

- ***Sikkerhedsgodkendelse fra tredjeparter:*** *Tredjeparter, der tester CISP'ens datacentre, hvilket dokumenteres i dennes tredjepartsrapporter, skal sikre, at CISP'en har implementeret tilstrækkelige sikkerhedsforanstaltninger i overensstemmelse med reglerne for opnåelse af sikkerhedscertificeringer. Alt efter hvilket program for compliance og krav der er tale om, kan eksterne kontrollanter udføre test i forbindelse med bortskaffelse af medier, gennemgå overvågningsvideoer, holde øje med et datacenters indgange og korridorer, teste elektroniske adgangskontrolenheder og undersøge datacentrets udstyr.*

7. Migreringer

	Krav
1.	***MIGRATIONSTJENESTE:*** *Hvor mange forskellige data-migreringstjenester tilbyder cloud-udbyderen?*
2.	***MIGRERINGER – CENTRALISERET OVERVÅGNING:*** *Tilbyder cloud-udbyderen organisationer en centraliseret tjeneste (der kan åbnes i et enkelt vindue), hvor de kan holde øje med deres serveres og programmers migrering?*
3.	***MIGRERINGER – BETJENINGSPANEL:*** *Har cloud-udbyderens migreringsværktøj et dashboard, hvor man hurtigt kan se migreringsstatussen, relaterede metrik- og migreringshistorik?*
4.	***MIGRERINGER – CLOUD-UDBYDERENS VÆRKTØJER:*** *Kan cloud-udbyderens migreringsværktøj integreres med andre migreringsværktøjer fra cloud-udbyderen, der kan migrere servere og programmer?*
5.	***MIGRERINGER – TREDJEPARTSVÆRKTØJER:*** *Tillader cloud-udbyderens migreringsværktøj at indarbejde tredjeparts migreringsværktøjer?* • *Hvis ja, hvilke migreringsværktøjer fra tredjeparter understøttes så?*
6.	***MIGRERINGER – MIGRERINGER I FLERE OMRÅDER:*** *Gør cloud-udbyderens migreringsværktøj det muligt at holde øje med server- og programmigreringer, der finder sted i flere områder?*
7.	***MIGRERINGER – SERVERMIGRERING:*** *Giver cloud-udbyderens migreringsværktøj mulighed for at overføre virtualiserede servere i det lokale miljø til cloud-miljøet?* • *Hvis ja, hvilke virtualiserede miljøer understøttes i øjeblikket?*
8.	***MIGRERINGER – SERVERREGISTRERING:*** *Gør cloud-udbyderens migreringstøj det muligt, automatisk at finde lokale virtuelle servere, der skal migreres til en cloud?*
9.	***MIGRERINGER – DATA OM SERVERYDEEVNE:*** *Gør cloud-udbyderens migreringstøj det muligt at indsamle oplysninger om og vise serverens og/eller den virtuelle maskines ydeevne, f.eks. processor- og hukommelsesudnyttelse?*
10.	***MIGRERINGER – REGISTRERINGSDATABASE:*** *Gør cloud-udbyderens migreringsværktøj det muligt at gemme alle indsamlede data i en centraliseret database?* • *Hvis ja, har organisationer så mulighed for at eksportere disse data? Til hvilke formater?*
11.	***MIGRERINGER – KRYPTERING AF INAKTIVE DATA:*** *Krypterer cloud-udbyderen inaktivt alle oplysninger, der indsamles og gemmes i registreringsdatabasen?*
12.	***MIGRERINGER – TRINVIS SERVERREPLIKERING:*** *Tilbyder cloud-udbyderens migreringsværktøj automatiseret, live trinvis serverreplikering under overførslen af serveren eller den virtuelle maskine som en måde at understøtte alle ændringer, der er foretaget på serveren, eller den virtuelle maskine er inkluderet i det endelige migrerede billede?* • *Hvis ja, hvor længe kan denne tjeneste så køre?*

13.	***MIGRERINGER – VMWARE:*** *Understøtter cloud-udbyderens migreringsværktøj migreringer af virtuelle VMWare-maskiner fra lokale systemer til cloud-systemet?*
14.	***MIGRERINGER – HYPER-V:*** *Understøtter cloud-udbyderens migreringsværktøj migreringer af virtuelle Hyper-V-maskiner fra lokale systemer til cloud-systemet?*
15.	***MIGRERINGER – PROGRAMREGISTRERING:*** *Gør cloud-udbyderens migreringsværktøj det muligt at registrere og gruppere programmer, før de migreres?*
16.	***MIGRERINGER – TILKNYTNING AF AFHÆNGIGHEDER:*** *Gør cloud-udbyderens migreringsværktøj det muligt at opdage afhængigheder mellem servere og programmer, før de migreres?*
17.	***MIGRERINGER – DATABASEMIGRERING:*** *Gør cloud-udbyderens migreringsværktøj det muligt at migrere lokale databaser til cloud-systemet?*
18.	***MIGRERINGER – NEDETID FOR DATABASEMIGRERING:*** *Gør cloud-udbyderens migreringsværktøj det muligt at migrere en database til et cloud-system med minimal afbrydelse, dvs. at kildedatabasen fungerer, mens migreringen er i gang?*
19.	***MIGRERINGER – KILDEDATABASE:*** *Understøtter cloud-udbyderens migreringsværktøj migrering af forskellige databasekilder som Oracle, SQL Server osv...?* • *Hvis ja, så angiv alle kildedatabaser, der kan migreres til et cloud-system.*
20.	***MIGRERINGER – ENSARTEDE MIGRERINGER:*** *Gør cloud-udbyderens migreringsværktøj det muligt at migrere databaser ensartet, dvs. fra én kildedatabase til en anden destinationsdatabase, f.eks. fra Oracle til SQL Server?* • *Hvis ja, så angiv alle mulige kombinationer af ensartet databasemigrering.*
21.	***MIGRERINGER – DATAMIGRERING PÅ PETABYTESKALA:*** *Har cloud-udbyderen en løsning til transport af data på petabyteskala, som bruger sikre apparater til at overføre store mængder data til og fra cloud-systemet?*
22.	***MIGRERINGER – DATAMIGRERING PÅ EXABYTESKALA:*** *Har cloud-udbyderen en transportløsning på exabyteskala, der gør det muligt at flytte ekstremt store mængder data til et cloud-system?*
23.	***MIGRERINGER – VIRKSOMHEDSBACKUP:*** *Har cloud-udbyderen en tjeneste, der gør det muligt at integrere kundens datacenter med cloud-lagertjenester uden problemer, så data kan overføres til cloud-udbyderens lagertjeneste og gemmes?*
24.	***MIGRERINGER – VIRKSOMHEDSBACKUP – OBJEKTLAGRING:*** *Kan cloud-udbyderens tjeneste til virksomhedsbackup integreres med udbyderens cloud-objektlagringstjeneste?*
25.	***MIGRERINGER – VIRKSOMHEDSBACKUP – FILADGANG:*** *Giver cloud-udbyderens tjeneste til virksomhedsbackup brugerne mulighed for at gemme og hente objekter ved hjælp af filprotokoller som f.eks. NFS (network file system)?*
26.	***MIGRERINGER – VIRKSOMHEDSBACKUP – BLOKADGANG:*** *Giver cloud-udbyderens tjeneste til virksomhedsbackup brugerne mulighed for at gemme og hente objekter ved hjælp af blokprotokoller som f.eks. iSCSI (Internet small computer systems interface)?*

27.	***MIGRERINGER – VIRKSOMHEDSBACKUP – BÅNDADGANG:*** *Giver cloud-udbyderens tjeneste til virksomhedsbackup brugerne mulighed for at sikkerhedskopiere deres data ved hjælp af et virtuelt båndbibliotek og gemme disse backupbånd i udbyderens cloud-system?*
28.	***MIGRERINGER – VIRKSOMHEDSBACKUP – KRYPTERING:*** *Gør cloud-udbyderens tjeneste til virksomhedsbackup det muligt at kryptere data, der er inaktive og under forsendelse?*
29.	***MIGRERINGER – VIRKSOMHEDSBACKUP – INTEGRATION AF TREDJEPARTSSOFTWARE:*** *Kan cloud-udbyderens tjeneste til virksomhedsbackup integreres med almindelig sikkerhedskopieringssoftware fra tredjeparter?*
30.	***MIGRERINGER – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte afsnit om migrering?* *Eksempel:* *Maksimalt antal samtidige overførsler af virtuelle maskiner* *Maksimalt antal datatransportløsninger, der kan bestilles*

8. Fakturering

	Krav
1.	***FAKTURERING – SPORING OG RAPPORTERING:*** *Har cloud-udbyderen en faktureringstjeneste med sporing og rapportering, der gør det lettere for brugerne at administrere og holde øje med deres brug af cloud-tilbud?*
2.	***FAKTURERING – ALARMER OG NOTIFIKATIONER:*** *Giver cloud-udbyderen brugerne en metode til opsætning af alarmer og notifikationer, der underretter brugerne om, at deres forbrug har overskredet en bestemt grænse?*
3.	***FAKTURERING – OMKOSTNINGSSTYRING:*** *Gør cloud-udbyderen det muligt at oprette og vise grafiske oversigter over udgifter og forbrug?*
4.	***FAKTURERING – BUDGETTER:*** *Gør cloud-udbyderen det muligt at vise og administrere budgetter og prognoser med estimerede udgifter?*
5.	***FAKTURERING – SAMLET OVERSIGT:*** *Gør cloud-udbyderen det muligt at samle faktureringen fra flere konti på en enkelt, primær betalingskonto?*
6.	***FAKTURERING – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte afsnit om fakturering?* *Eksempel:* *Maksimalt antal konti, der kan grupperes sammen* *Maks. antal alarmer, der kan oprettes* *Maksimalt antal budgetter, der kan administreres*

9. Administration

	Krav
1.	***ADMINISTRATION – OVERVÅGNINGSTJENESTE:*** *Har cloud-udbyderen en overvågningstjeneste, der gør det muligt at administrere cloud-ressourcer og -programmer, og som indsamler, overvåger og rapporterer ved hjælp af metrics, der er defineret på forhånd?*
2.	***ADMINISTRATION – ALARMER:*** *Giver cloud-udbyderens overvågningstjeneste brugerne mulighed for at konfigurere alarmer?*
3.	***ADMINISTRATION – BRUGERDEFINEREDE METRICS:*** *Giver cloud-udbyderens overvågningstjeneste brugerne mulighed for at oprette og overvåge brugerdefinerede metrics?*
4.	***ADMINISTRATION – OVERVÅGNINGSGRANULARITET:*** *Har cloud-udbyderens overvågningstjeneste forskellige niveauer for detaljer af overvågningen ned til 1-minut niveauet?*
5.	***ADMINISTRATION – API-SPORINGSTJENESTE:*** *Har cloud-udbyderen en tjeneste, der logfører, overvåger og gemmer aktivitet i sammenligning med cloud-ressourcer på både konsol- og API-niveau (application programming interface), så synligheden bliver bedre?* • *Hvis ja, hvilke af cloud-udbyderens tjenester kan så integreres med sporingstjenesten?*
6.	***ADMINISTRATION – NOTIFIKATION:*** *Gør cloud-udbyderen det muligt at sende notifikationer, som er baseret på API-aktivitetsniveauer?*
7.	***ADMINISTRATION – KOMPRIMERING:*** *Gør cloud-udbyderen det muligt at komprimere logfiler, som er oprettet af API-sporingssystemet, så brugerne lettere kan nedbringe lagerudgifterne i forbindelse med denne tjeneste?*
8.	***ADMINISTRATION – OMRÅDESAMLING:*** *Gør cloud-udbyderen det muligt at optage API-aktivitet på kontoen i alle områder og sende disse oplysninger samlet, så de er lettere at bruge?*
9.	***ADMINISTRATION – RESSOURCELAGER:*** *Har cloud-udbyderen en tjeneste, der gør det muligt at vurdere, gennemse og evaluere konfigurationerne af de ressourcer, som brugeren udruller?*
10.	***ADMINISTRATION – KONFIGURATIONSÆNDRINGER:*** *Optager cloud-udbyderen automatisk en ændring i ressourcekonfigurationen, når den finder sted?*
11.	***ADMINISTRATION – KONFIGURATIONSHISTORIK:*** *Gør cloud-udbyderen det muligt at undersøge ressourcekonfigurationen på et hvilket som helst tidligere tidspunkt?*
12.	***ADMINISTRATION – KONFIGURATIONSREGLER:*** *Har cloud-udbyderen retningslinjer og anbefalinger til klargøring, konfiguration og vedvarende overvågning af compliance?*
13.	***ADMINISTRATION – RESSOURCESKABELONER:*** *Giver cloud-udbyderen brugerne mulighed for at oprette, klargøre og administrere en samling med ressourcer ligesom med en skabelon?*

14.	***ADMINISTRATION – REPLIKERING AF RESSOURCESKABELONER:*** *Gør cloud-udbyderen det muligt at replikere disse ressourceskabeloner hurtigt i forskellige områder, så de kan bruges til gendannelse efter nedbrud?*
15.	***ADMINISTRATION – SKABELONSDESIGNER:*** *Har cloud-udbyderen et brugervenligt, grafisk værktøj, hvor elementer kan trækkes og slippes, så disse ressourceskabeloner kan oprettes hurtigere?*
16.	***ADMINISTRATION – TJENESTEKATALOG:*** *Har cloud-udbyderen en tjeneste, der gør det muligt at oprette og administrere et katalog med tjenester, dvs. servere, virtuelle maskiner, software, databaser osv.?*
17.	***ADMINISTRATION – KONSOLADGANG:*** *Har cloud-udbyderen en webbaseret grænseflade, der gør det lettere at styre og overvåge cloud-tjenester?*
18.	***ADMINISTRATION – CLI-ADGANG:*** *Har cloud-udbyderen ét værktøj, der gør det muligt at styre og konfigurere flere cloud-tjenester via en CLI (command line interface), så styringsopgaver kan automatiseres ved hjælp af scripts?*
19.	***ADMINISTRATION – MOBILADGANG:*** *Har cloud-udbyderen et smartphone-program, der giver brugere mulighed for at oprette forbindelse til cloud-tjenesten og administrere deres ressourcer?* • *Hvis ja, fås dette program så til både iOS og Android?*
20.	***ADMINISTRATION – RETNINGSLINJER:*** *Har cloud-udbyderen en tjeneste, der gør det lettere for brugerne at sammenligne vedkommendes cloud-brug i forhold til retningslinjer?*
21.	***ADMINISTRATION – TJENESTEGRÆNSER:*** *Har cloud-udbyderen begrænsninger (f.eks. tjenestegrænser) med hensyn til førnævnte afsnit om styring?* *Eksempel:* *Maks. antal konfigurationsregler pr. konto* *Maks. antal alarmer, der kan oprettes* *Maks. antal logfiler, der kan gemmes*

10. Support

	Krav
1.	***SUPPORT – TJENESTE:*** *Tilbyder cloud-udbyderen support når som helst døgnet rundt, hele ugen og hele året rundt via telefon, chat og e-mail?*
2.	***SUPPORT – SUPPORTNIVEAUER:*** *Har cloud-udbyderen support på forskellige niveauer?*
3.	***SUPPORT – NIVEAUALLOKERING:*** *Giver cloud-udbyderen brugerne mulighed for selv at tildele ressourcer/tjenester, der bruges til forskellige supportniveauer med udgangspunkt i granuleret klassificering og ikke ved at tvinge brugerne til at have separate cloud-konti, så de kan kvalificere sig til og benytte support på forskellige niveauer?*

4.	***SUPPORT – FORA:*** *Har cloud-udbyderen et offentlige supportfora, hvor kunder kan tale om deres problemer?*
5.	***SUPPORT – DASHBOARD TIL TJENESTETILSTAND:*** *Har cloud-udbyderen et dashboard til oversigt over tjenestetilstand, der viser de seneste oplysninger om tjenestens tilgængelighed i flere områder?*
6.	***SUPPORT – TILPASSET DASHBOARD:*** *Har cloud-udbyderen et dashboard, der viser en tilpasset visning af ydeevnen og tilgængeligheden for tjenesterne, der understøtter brugerens specifikke ressourcer?*
7.	***SUPPORT – DASHBOARD-HISTORIK:*** *Gør cloud-udbyderen det muligt at se 365 dages overblik over tilstanden af tjenesten?*
8.	***SUPPORT – CLOUD-RÅDGIVER:*** *Har cloud-udbyderen en tjeneste, der fungerer ligesom en tilpasset cloud-ekspert og gør det lettere at sammenligne ressourceforbruget i forhold til retningslinjerne?*
9.	***SUPPORT - TAM:*** *Har cloud-udbyderen en TAM (technical account manager) med teknisk ekspertise i alle cloud-tjenesterne?*
10.	***SUPPORT – SUPPORT TIL TREDJEPARTSPROGRAMMER:*** *Har cloud-udbyderen support til almindelige operativsystemer og almindelig programstakkomponenter?*
11.	***SUPPORT – OFFENTLIG API:*** *Har cloud-udbyderen en offentlig API (public application programming), der programmatisk interagerer med supportsager, så disse sager kan oprettes, redigeres og lukkes?*
12.	***SUPPORT – TJENESTEDOKUMENTATION:*** *Har cloud-udbyderen tekniske og offentligt tilgængelige dokumenter i professionel kvalitet til alle sine tjenester, herunder, men ikke begrænset til, brugervejledninger, selvstudier, ofte stillede spørgsmål og udgivelsesnoter?*
13.	***SUPPORT – CLI-DOKUMENTATION:*** *Har cloud-udbyderen tekniske og offentligt tilgængelige dokumenter i professionel kvalitet til sin CLI (command line interface)?*
14.	***SUPPORT – REFERENCEARKITEKTURER:*** *Har cloud-udbyderen et gratis onlinebibliotek med reference-arkitekturdokumenter, der gør det lettere for kunderne at lave specifikke løsninger og kombinere mange af cloud-udbyderens cloud-tjenester?*
15.	***SUPPORT – REFERENCEUDRULNINGER:*** *Har cloud-udbyderen et gratis onlinebibliotek med dokumenter, som indeholder detaljerede, gennemprøvede og godkendte, trinvise procedurer, herunder retningslinjer, til implementering af typiske løsninger (dvs. DevOps, Big Data, Data Warehouse, Microsoft-workloads, SAP-workloads osv.) i sine cloud-produkter?*

Bilag B – Live teknisk vurdering

Ved valget af en CISP, er det vigtigt at vurdere cloud-platformens kapacitet "live" ved hjælp af CISP'ens offentligt tilgængelige tjenester og infrastruktur. Vi anbefaler mindst 1 hel dag pr. udvalgt CISP til teknisk vurdering. Under vurderingen kan du: 1) foretage en grundig vurdering for at vurdere, om de demonstrerede kapaciteter stemmer overens med dine RFP-krav og CISP'ens skriftlige svar, 2) give dine eksperter en platform til at undersøge CISP'en for at sikre, at den passer til og stemmer overens med dine specifikke tekniske og organisatoriske behov, og 3) få tillid til CISP-tjenesterne og CISP'ens evne til at skalere, fungere sikkert, fungere robust og fortsætte med at innovere for at opfylde fremtidige behov.

Når CISP'er svarer på kravene i en RFP for cloud-tjenester, kan de erklære compliance baseret på en fortolkning af kravene på højt niveau, som ikke har den fulde kontekst af en organisations driftsmiljø/applikationsbehov. Vi anbefaler, at der nedsættes et teknisk vurderingspanel med førende eksperter inden for teknik, drift, sikkerhed og programmer. Dem, der vurderer bør udfordre CISP'en under hele vurderingen, og som bedste praksis bør de bedømme CISP'erne uafhængigt, idet de vurderer scenarierne på en fastsat skala, f.eks. 0-4 (0=Uacceptabelt, 1=Marginalt, 2=Acceptabelt, 3=Godt, 4=Fremragende). Herefter kan demoscorerne konsolideres, og den gennemsnitlige score for hvert evalueringsscenarie kan sammenfattes til den samlede CISP-vurdering. Scenarier med en høj standardafvigelse bør drøftes i vurderingsgruppen, inden de færdiggøres. Når scorerne er konsolideret, kan der anvendes en vægtning baseret på hvor kritisk scenariet er.

Med hensyn til omfanget af demonstrationen anbefaler vi, at der tages et holistisk syn på CISP's platform og derefter dykkes dybere ned for at vurdere specifikke arbejdsbelastninger, der kører på platformen. Nedenfor er et eksempel på en oversigt til en vurdering af platformen og workload. Organisationer kan bygge videre på denne baseline eller tilpasse den for at sikre, at den valgte CISP opfylder deres specifikke funktionelle og ikke-funktionelle krav. Som bedste praksis kan leverandører, der vises listen over scenarier og krav, få lov til at foreslå en dagsorden for live vurderingen, der maksimerer dækningen og sørger for, at der er 20 % tid til spørgsmål og svar.

Platformsvurdering: Flere CISP'er har indført udtrykket "Well Architected" for at henvise til en tilgang til cloud, der giver optimal værdi og minimerer risikoen. Well Architected-scenarier i en live teknisk demonstration kan omfatte:

1. **Sikkerhed:** Identitet, centraliseret styring, automatiseret trusselsregistrering, databeskyttelse, beredskab til hændelser
2. **Præstationseffektivitet:** Korrekt dimensionering, skalerbarhed/elasticitet, serveruafhængighed
3. **Pålidelighed:** Høj tilgængelighed (modstandsdygtighed over for fejl), mindsket risiko for ændringer, gendannelse efter nedbrud, backup
4. **Omkostningsstyring:** Finansielle operationer, kommerciel optimering, budgetter og omkostningsallokering
5. **Operativ ekspertise:** Automatisering, overvågning, support, administration og kapacitet, der kræves for at migrere til og operere i cloud

Vurdering af workload: Et fælles sæt af programtyper, der kan demonstreres, omfatter:

- **Webapplikation:** Offentlig hosting af et dynamisk websted, herunder backend-database og statisk objektlagring.
- **Dataanalyse:** En Data Lake eller Lake House-arkitektur, der muliggør konsolidering af data fra forskellige dataleverandører og evnen til at håndtere store mængder (TB'er / PB'er af data), variation (struktureret, ustruktureret, forskellige formater osv.) og hastighed (hastighed af datagenerering, ændringer og forespørgselsmønstre).
- **Platform til datavidenskab:** En platform, der muliggør udvikling, udrulning og brug af AI/ML-baserede funktioner i hele din organisation.
- **IoT-program:** En IoT-platform/-funktion, der dækker cloud, netværksfunktion og enhederne.

For hver repræsentativ workload, der er vigtig for din organisation, kan du definere de scenarier, der skal demonstreres af CISP'en. Scenarierne skal demonstrere de overordnede muligheder, der gør det muligt at udrulle workload på en Well Architected måde. De følgende sider indeholder eksempler på tekniske vurderingsskriterier for 1) CISP's platform og 2) et eksempel på en workload for en webapplikation.

Platform – Eksempel på live teknisk vurdering

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Sec.1	Identitetsforbund	4	Demonstrere evnen til at forbinde et eksisterende identitetslager til cloud-tjenesten.	• Understøttelse af standardprotokoller som f.eks. SAML. • Understøttelse af SCIM-baseret identitetsreplikation. • Muligheden for at definere forskellige adgangsniveauer i virksomhedens identitetslager og få dem anvendt hos cloud-udbyderen. • Muligheden for at begrænse bestemte teams/personer til kun at have adgang til bestemte konti/projekter/workloads. • Mulighed for at understøtte ABAC (Attribute-Based Access Control) og bruge disse attributter i cloud-udbyderens IAM-system (Identity and Access Management) til at kontrollere adgangen til cloud-ressourcer.
Plat.Sec.2	Central styring	4	Demonstrere evnen til at definere politikker og krav centralt, på organisatorisk niveau (globale politikker) og også på forretningsenheds- og projektniveau.	• Politikken bør omfatte: Aktivere/deaktivere tjenester, anvende geografiske begrænsninger (begrænse områder). • Politikkerne bør også forhindre brugere, herunder administratorer, i at deaktivere revisions-/styringskontroller.
Plat.Sec.3	Begrænsning af brugertilladelser	3	Demonstrere de automatiske anbefalinger til begrænsning af brugertilladelser.	• Mulighed for at sammenligne de nuværende tilladelser med de krævede tilladelser. • Automatisk generering af politikker til at fremme mindste privilegier.
Plat.Sec.4	Revisionslogføring	4	Demonstrere revisionslogføring af cloud-aktivitet, herunder både tilladte og ikke tilladte handlinger.	• Centraliserede logfiler for hele organisationen. • Konto-/projektspecifikke logfiler til støtte for sporing og ansvarlighed på lavt niveau. • Værktøjer, der gør det muligt at søge i logfiler. • Værktøjer, der gør det muligt at udløse handlinger baseret på specifikke hændelser/logfiler. • Mulighed for at se supportaktivitet af leverandører. • Mulighed for at forhindre sletning af logfiler, selv af administratorer.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Sec.5	Netværksisolering	4	Demonstrere og bevise, hvor det er muligt, at de forskellige lejere i en cloud er isoleret. Demonstration af konfigurationen af isolerede (uden forbindelse), private (uden internet) og offentlige (med internetadgang) undernet.	• Adskillelse af lejere, herunder i forbindelse med VPN- og krydsforbindelses-tjenester. • Mulighed for at styre trafikstrømmen fra uden for cloud-infrastrukturen (lokalt), i den og til internettet. • Hvordan adskillelsen gælder ved brug af delte tjenester som f.eks. beholderhosting eller funktion som en tjeneste.
Plat.Sec.6	Kryptering af inaktive data	4	Demonstrere evnen til at kryptere data i hvile, herunder mulighederne for BYOK-kryptering og kryptering fra klientsiden.	• Mulighed for at kræve kryptering af følsomme data. • Mulighed for at bruge enten leverandørstyrede nøgler eller kundestyrede nøgler. • Overholdelse af FIPS 140-2. • Mulighed for at advare om og logføre manglende overholdelse af krypteringskrav. • Yderligere omkostningspåvirkning. • Virkning på ydeevnen. • Understøttelse af kvantebevisalgoritmer og nøglestørrelser.
Plat.Sec.7	Kryptering under Overførsel	4	Demonstrere evnen til at kryptere data i transit.	• Standardkryptering for tjeneste-API'er. • Mulighed for at aktivere kryptering under overførsel (TLS) på belastningsudligner og administrerede API'er. • Understøttelse af gensidig autentificering (klient og server).
Plat.Sec.8	Nøglestyring	4	Demonstrer din evne til nøglestyring. Medtag hele nøglens livscyklus. Medtag integration med andre cloud-tjenester.	• Logføring af oprettelse, brug, rotation og destruering af nøgler.
Plat.Sec.9	Konfigurationsstyring	3	Demonstrer dine muligheder for konfigurationsstyring for cloud-platformen.	• Opretholdelse af præcis CMDB. • Kontrollér for compliance. • Automatisk udløsning af handlinger baseret på manglende overholdelse af reglerne. • Evne til at vurdere konfigurationsændringer i forhold til bedste praksis eller brugerdefinerede regler.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Sec.10	Netværkssikkerhed	3	Demonstration af firewall til webapplikationer og firewall-funktionen, herunder integration med regelsæt/firewalls fra tredjepart og beskyttelse mod volumetriske angreb.	• WAF-funktioner (firewall til webapplikationer): Skalerbarhed. • Understøttelse af private såvel som offentlige netværk. • Mulighed for at abonnere på feeds fra branchen/leverandøren for regelsæt. • Automatisk udløsning af handlinger i infrastrukturen baseret på hændelser fra WAF'en. • Firewall-funktioner, skalerbarhed. • Værtsbaserede og netværksbaserede firewalls. • Mulighed for at henvise til logiske grupper eller objekter ud over muligheden for at angive CIDR-IP-blokke. • Antal regler, der understøttes på hvert niveau/komponent. • Evne til at understøtte en distribueret driftsmodel (netværksteam + udviklingsteam) gennem politik og netværkskonfiguration.
Plat.Sec.11	Netværksforbindelse	3	Demonstrer evnen til at oprette forbindelse til lokale netværk samt slutpunkter/klienter til private netværk i cloud.	• Privat forbindelse (høj båndbredde > 10 GBs). • Mulighed for at styre routing- og firewall-politikker på tværs af organisationen. • VPN-forbindelse (sted-til-sted og klientbaseret). • IPV6-understøttelse.
Plat.Sec.12	Instansstyring	3	Demonstrere mulighederne for instansstyring.	• Mulighed for at overvåge og administrere patchtilstand for en stor mængde instanser. • Understøttelse af patchstyring af Linux- og Windows-operativsystemer. • Mulighed for at udføre kommandoer på tværs af en flåde af servere uden brug af SSH. • Mulighed for at kontrollere og overvåge fjernadgang til virtuelle maskiner centralt. • Mulighed for at ændre en instansstørrelse, tilknytte yderligere volumener, ændre netværkskonfiguration osv. via konsol, CLI og API.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Sec.13	Anvendelse af politikker	3	Demonstrere evnen til at konfigurere tjenester for at forhindre adgang fra det offentlige internet.	• Mulighed for at isolere trafik til private netværk for tjenester, der sandsynligvis indeholder kritiske/fortrolige data. • Mulighed for at definere politikker, der styrer adgangen til data baseret på kilde-netværket. • Anvendelse af disse adgangsbegrænsninger på alle brugere, herunder brugere med legitimationsoplysninger på højt niveau.
Plat.Sec.14	Sårbarhedsscanning	2	Demonstrere evnen til at scanne afbildninger (beholdere og VM) for sårbarheder.	• Mulighed for automatisk at scanne beholdere i et register. • Mulighed for at scanne virtuelle maskiner for kendte sårbarheder. • Mulighed for at udføre netværksskanning.
Plat.Sec.15	Inspektion af netværket	2	Demonstrere evnen til at optage/spejle netværkstrafik (NetFlow og fulde pakker) fra et kundemiljø.	• Mulighed for at spejle noget af/alt trafikken i cloud-udbyderens infrastruktur (fra en kundes lejers perspektiv), herunder fuld pakkeoptagning. • Mulighed for blot at vælge, hvilken trafik du ønsker at optage. • Mulighed for at skalere til meget store trafikmængder (> 50 GBps).
Plat.Sec.16	Registrering af trusler	3	Demonstrer din platforms evne til at registrere indbrud, herunder f.eks. trusler fra et netværk, brug af legitimationsoplysninger og analyse af brugsmønstre.	• Mulighed for at opdage mistænkelige aktiviteter som f.eks. "minedrift". • Mulighed for at opdage brute for authentication attacks som SSH-logins. • Mulighed for at opdage lækage eller misbrug af legitimationsoplysninger. • Anvendelse af ML, analyse af et stort antal hændelser og fremlæggelse af prioriterede hændelser. • Mulighed for at aktivere/konfigurere (simpelt er bedre). • Mulighed for at integrere med eksterne tjenester og udløse notifikationer. • Mulighed for at konfigurere IDS på et globalt niveau for alle projekter/konti.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Perf.1	Beregningsoptimering	2	Demonstration af automatiske anbefalinger til optimering af omkostningerne ved virtuelle maskiner og funktioner som en tjeneste.	• Anbefalinger baseret på den faktiske udnyttelse og workloadmønstre. • Anbefalingerne omfatter anslåede besparelser og indsigt i det forventede belastningsniveau/tekniske konsekvenser. • Optimeringer bør omfatte både besparelser og "præstationsrisici", hvor virtuelle maskiner f.eks. kan være for små.
Plat.Perf.2	Miljøoptimering	2	Demonstration af automatiske anbefalinger til andre cloud-komponenter såsom belastningsudlignere, netværk, databaser, lagring osv.	• Anbefalinger identificerer besparelser og potentielle muligheder for effektivisering af ydeevnen i andre komponenter end kerneberegninger.
Plat.Perf.3	Automatisk skalering af beregninger	4	Demonstration af muligheder for automatiske skalering for et program, der er installeret bag en belastningsudligner i et virtuelt beregningsmiljø. Demonstration af de forskellige muligheder/tilgange, der er tilgængelige, og muligheden for at udløse andre (valgfrie) handlinger før/efter skaleringshændelser, f.eks. en meddelelse.	• Forskellige muligheder for skalering, hændelsesbaseret, tidsbaseret, manuelt eller mere intelligente metoder, der anvender maskinlæring til at forudsige den nødvendige kapacitet. • Fuldt automatiseret skalering, herunder registrering med en belastningsudligner og tilstandskontrol. • Mulighed for at køre et vilkårligt stykke kode på bestemte tidspunkter i skaleringens livscyklus.
Plat.Perf.4	Online skalering til lagring	3	Demonstration af evnen til at skalere både kapacitet og gennemløb af bloklagring uden afbrydelse af workload.	• Mulighed for at skifte bloklagring mellem forskellige lagringstyper uden at det er nødvendigt at genopbygge tjenesterne fuldstændigt. • Mulighed for at øge størrelsen af de mængder, der frigøres til VM'er.
Plat.Perf.5	Automatisk skalering for administrerede tjenester	3	Demonstration af muligheden for at Object Store, API Gateway, FaaS-platformen og NoSQL-databasen kan skaleres fra få (10-vis) til mange (1000-vis) af samtidige brugere.	• Problemfri automatisk skalering, ideelt set uden indgreb af administratoren. • Konsekvent ydeevne i en opskaleringsperiode, der stemmer overens med kravene til opskalering af produktionen. • For nogle komponenter, f.eks. FaaS, skal du også se på mulighederne for forvarmning og styring af grænser for samtidig udførelse, hvis det er nødvendigt.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Perf.6	Beholderbaserede workloads	3	Demonstrere evnen til at være host for beholderbaserede workloads.	• Muligheder for beholderhosting-platforme. • Integration med andre IaaS-komponenter som f.eks. belastningsudlignere. • Tilgængelighed af en tjeneste-mesh-løsning. • Ikke-proprietære muligheder for beholderhosting, f.eks. Kubernetes. • Indbygget understøttelse af høj tilgængelighed inden for beholder-kontrolplanet. • Mulighed for lokalt at administrere beholderværter.
Plat.Rel.1	Områdebaseret modstandsdygtighed	4	Demonstration af automatiseret failover af en relationsdatabase-instans inden for et område, når der simuleres en geografisk lokaliseret fejl (f.eks. strømafbrydelse).	• Automatiseret failover. • Isolerede fejlzoner i et cloudområde. • Klart afgrænset og enkelt at bygge til høj tilgængelighed.
Plat.Rel.2	Automatisk gendannelse af instans	2	Demonstrer den automatiske gendannelse af en instans / sæt af instanser efter en tilstandskontrol, der ikke er bestået.	• Konfigurerbare tilstandskontroller. • Fuldt automatiseret gendannelse/genoprettelse af instanser.
Plat.Rel.3	Bevidsthed om belastningsudligneres tilstand	3	Demonstrere hvordan en belastningsudligner automatisk registrerer en instans der har fejl og omdirigerer trafikken til andre sunde værter.	• Konfigurerbare tilstandskontroller. • Automatiseret videresendelse af trafik til sunde hosts.
Plat.Rel.4	Område failover	3	Demonstration af en arkitektur med flere områder, herunder automatiseret trafikoverførsel til et sekundært område.	• Globalt bevidste tilstandskontroller. • Automatiserede routing-muligheder: ventetid, vejning og failover. • Understøttelse af workloads på virtuelle maskiner samt administrerede tjenester som en Object Store / NoSQL-database-tjeneste.
Plat.Rel.5	Sikkerhedskopiering og gendannelse	4	Demonstrere muligheder for backup og gendannelse for: Virtuelle maskiner, databaser, administrerede tjenester.	• Niveau af automatisering. • Mulighed for at gendanne til den samme/et andet cloud-område. • Mulighed for at kopiere sikkerhedskopier til et andet cloud-område.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Cost.1	Budgetter	3	Demonstrere en evne til budgetforvaltning, herunder hvordan det skal struktureres for underkonti og projekter.	• Overvej muligheden for at anvende budgetkontrol og overvågning på de forskellige niveauer i din organisation. • Tjek for fleksibilitet, f.eks. muligheden for at gruppere komponenter (ved hjælp af tagging), fastlægge budgetter for specifikke cloud-tjenester og konfigurere grænseværdier for advarsler/overvågning.
Plat.Cost.2	Allokering af budget	1	Demonstration af klargøringen af et nyt projektmiljø (konto), herunder processen for budgettildeling for projektet. Klargøringen bør omfatte manuelle godkendelsestrin for 1) teknisk gennemgang/IT og 2) kommerciel gennemgang/finans.	• Muligheden for selv at klargøre med de relevante godkendelser. • Automatisering af konfigurationen af de relevante budgetindstillinger, meddelelser eller budgetpolitikker, alt efter hvad der passer til din organisation.
Plat.Cost.3	Budgetrapportering	2	Demonstrere evnen til at rapportere om budgetter på tværs af organisationen. Rapportering for en specifik afdeling vs. hele organisationen (need to know). Rapporteringen bør omfatte både "faktiske" og forventede/estimerede udgiftsværdier.	• Muligheden for at skabe synlighed på forskellige niveauer i organisationen, hvilket skaber opmærksomhed og gennemsigtighed, men på et need-to-know-basis. • Prognoser bør være baseret på nuværende og tidligere forbrugstendenser og give tidlig advarsel om potentielle budgetoverskridelser.
Plat.Cost.4	Budgetkontrol	1	Demonstrere evnen til at træffe foranstaltninger, når grænsen for et budget er nået. Foranstaltningerne kan omfatte notifikationer, anvendelse af begrænsninger eller aktiv indgriben for at forhindre budgetoverskridelser.	• Muligheden for at definere handlinger til forskellige projekter. • Muligheden for at handlingerne kan variere fra et projekt til et andet, for eksempel - under hensyntagen til Dev vs. Prod. konsekvenser. • Muligheden for at definere flere handlinger og tærskler for det samme budget/projekt. • Muligheden for at definere brugerdefinerede handlinger ud over standardfunktionerne.
Plat.Cost.5	Budgetperioden	1	Demonstrere evnen til at anvende budgetter for forskellige tidsperioder, dagligt/månedligt/årligt osv. For årlige	• Mulighed for at definere budgetter for forskellige tidsperioder.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
			budgetter skal du vise, at du er i stand til at anvende en variabel fordeling af de forventede udgifter i løbet af året.	• Mulighed for at konfigurere en fordeling af udgifterne på tværs af året for årlige budgetter, hvilket især er vigtigt for sæsonbestemte/højt elastiske workloads som f.eks. en årlig selvangivelse.
Plat.Cost.6	Tredjeparts markedsplads	3	Demonstrere evnen til at købe og implementere tredjepartsprodukter. Demonstrere, hvordan et budget fastsættes for et sæt af tredjepartsprodukter, der er tilgængelige via en markedsplads, og hvordan de tilgængelige produkter begrænses.	• Mulighed for at fastlægge et budget for et specifikt produkt, et globalt budget eller et budget for et sæt projekter/konti. • Mulighed for kun at præsentere en delmængde af den bredere markedsplads for cloud-brugere.
Plat.Cost.7	Beregning af prismodeller	3	Demonstration af de forskellige prismodeller/kommercielle modeller, der kan anvendes på virtuelle maskiner.	• Mulighederne bør omfatte detaljeret prisfastsættelse (pr. minut/time) efter behov, uden langtidsforpligtelser. • Valgfri langsigtede forpligtelser til gengæld for en rabat. • Mulighed for at købe instanser med en forståelse for at blive afbrudt til gengæld for en rabat. • Det er vigtigt, at det skal være muligt at blande disse modeller inden for samme projekt/konti og også at dele fordelene på tværs af forskellige konti.
Plat.Cost.8	Anbefalinger til kommerciel optimering	3	Demonstrere evnen til at modtage anbefalinger til kommerciel optimering for at optimere udgifterne (uden at skulle foretage tekniske ændringer).	• Holistiske anbefalinger for flere tjenester, herunder f.eks. virtuelle maskiner og administrerede databaser. • Evne til at gennemføre anbefalinger på en enkel måde og forstå de forventede besparelser/fordele.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Cost.9	Dedikerede værter	4	Demonstrer evnen til at klargøre en dedikeret vært for at muliggøre brugen af lokale licenser, der er bundet til en bestemt vært.	• Nemhed ved klargøring. • Mulighed for at styre udnyttelsen af hosten. • Muligheden for at dele hosten på tværs af forskellige projekter/lejemål.
Plat.Ops.1	Migrering af virtuelle maskiner	3	Demonstration af import af en virtuel maskine fra et lokalt miljø til en cloud-baseret VM-tjeneste.	• Mulighed for at importere både Windows- og Linux-baserede operativsystemer. • Mulighed for at importere flere maskiner på én gang. • Mulighed for at opretholde en replikeringssession for at muliggøre hurtig "failover" til cloud.
Plat.Ops.2	DevOps- og automatiseringsfærdigheder	4	Demonstrer dine DevOps/automatiseringsfærdigheder, herunder hvordan miljøer defineres som kode, støtte fra fuldt automatiserede udrulninger, automatiseret test og tilbagerulninger.	• Mulighed for at definere alle systemkomponenter som kode, herunder netværk, virtuelle maskiner, lagring og databaser. • Mulighed for at oprette en pipeline. • Mulighed for at oprette et kodelager. • Mulighed for at automatisere builds. • Evne til at udføre blå/grønne udrulninger. • Mulighed for at oprette flere miljøer og have flere faser for udrulninger. • Automatiseret tilbagerulninger ved fejlslagne udrulninger.
Plat.Ops.3	Hosting af programmer	2	Demonstration af hosting af et simpelt 2-trins program i en plaforms-tjeneste med små kodebehov. Herunder en relationsdatabase og automatisk skalering for program-/webniveauet.	• Enkel konfiguration via brugergrænsefladen. • Inddragelse af tilstandskontroller, skalering, høj tilgængelighed. Platformsunderstøttelse, Windows og Linux.
Plat.Ops.4	Integration af sikkerhed	2	Demonstrer din platforms integrationsmuligheder ud fra et perspektiv af sikkerhedshændelser og hændelsesstyring.	• Mulighed for let at integrere og forbruge sikkerhedsrelaterede logfiler fra cloud-udbyderen + API'er til integration.
Plat.Ops.5	ITSM-integration	3	Demonstrer din platforms integrationsmuligheder ud fra et ITSM-perspektiv (It-tjenestestyring).	• Mulighed for at oprette, overvåge og opdatere en supportsag via en API. • Mulighed for at klargøre tjenester eller sæt af tjenester som "produkter" via en API.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Plat.Ops.6	Support	4	Demonstrer dit tilbud af support.	• Forskellige niveauer af support til forskellige typer workloads. • Mulighed for også at understøtte operativsystemet/databasemotor osv., alt efter hvad der er relevant for en given tjeneste. • Mulighed for at tilbyde et white glove-tilbud med navngivne supportansvarlige for kritiske workloads. • Mulighed for at tilbyde en struktureret proces til forberedelse af begivenheder og gennemgang af arkitekturen. • Indsigt i leverandørens køreplan.
Plat.Ops.7	Mulighed for revision	4	Demonstrer de værktøjer, du har til at understøtte revisioner af compliance.	• Mulighed for at få oplysninger om revision af compliance via konsollen. • Mulighed for at administrere og automatisere miljørevisioner.
Plat.Ops.8	VM til beholder	1	Demonstration af konverteringen af et program på en virtuel maskine til en beholder og servering af det ved hjælp af cloud-udbyderens beholderplatform.	• Brugervenlighed i forbindelse med konverteringen. • Den tid konverteringen tager. • Platformsunderstøttelse, .Net og Java.

Workload: Webapplikation - Eksempel på live teknisk vurdering

Det følgende afsnit indeholder et eksempel på et evalueringsark for workload for en specifik workload for en "web application". Når der udarbejdes et evalueringsark for et program, anbefales det kraftigt at inddrage programmets brugere, udviklere og administratorer, da de sandsynligvis har den bedste forståelse af kravene, de aktuelle udfordringer og begrænsninger.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Web.Sec.1	Sikkerhed - beskyttelse af programmer	3	Demonstrere din evne til at blokere ondsindede forsøg på at udnytte programmet via SQL-injektion, XSS Scripting-angreb og andre angreb.	• Mulighed for at beskytte mod almindelige angreb "out of the box" med standardregler/funktioner. • Mulighed for at oprette brugerdefinerede kontroller/regler/funktioner.
Web.Sec.2	Sikkerhed - Vurderingsbaseret beskyttelse	3	Demonstrer din evne til at blokere/beskytte mod angreb med store forespørgselshastigheder eller datamængder rettet mod et program.	• Mulighed for at konfigurere grænser og begrænse forespørgselshastigheder fra en given IP-adresse eller liste af adresser.
Web.Sec.3	Sikkerhed - Kildebaseret beskyttelse	3	Demonstrere evnen til at begrænse adgangen baseret på netværk / geografisk kilde.	• Mulighed for at begrænse efter netværksblok eller en liste over netværksblokke. • Mulighed for at begrænse efter oprindelsesland (uden at det er nødvendigt at administrere IP-lister).
Web.Sec.4	Sikkerhed - segmentering af netværk	4	Demonstrere evnen til at isolere/beskytte komponenter (Web Server, App Server / DB Server) for at beskytte mod både nord-syd- og øst-vest spredning gennem infrastrukturen.	• Mulighed for at placere komponenter i forskellige undernet og styre trafikstrømmen mellem forskellige undernet. • Mulighed for at styre trafikstrømmen på grænsefladeniveau på netværket. • Mulighed for at henvise til logiske grupper samt CIDR-blokke.
Web.Sec.5	Sikkerhed - TLS-understøttelse og certifikatstyring	4	Demonstrere evnen til at levere et TLS-sikret slutpunkt og automatisk administrere de understøttende komponenter til at levere dette, herunder f.eks. automatisk rotation af certifikater.	• Understøttelse af de nyeste TLS-protokoller og mulighed for at deaktivere ældre versioner, hvis det er nødvendigt. • Enkel generering, forvaltning og rotation af certifikater (ideelt set fuldt automatiseret).

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Web.Perf.1	Ydeevne - skalerbarhed	4	Demonstrere din evne til at skalere fra 10 til 100.000 samtidige brugere af webapplikationen ved hjælp af dynamisk automatisk skalering.	• Mulighed for at definere tidsbaserede såvel som udløsningsbaserede skaleringsregler. • Problemfri skalering for slutbrugeren og administratoren. Automatisk udskalering, når belastningen stiger, og indskalering, når belastningen falder. • Sikre, at der er skalerbarhed i hvert lag af webapplikationen (Belastningsudligner, weblag, datalag osv.). • Adgang til caching-tjenester i forskellige lag af programmet efter behov.
Web.Perf.2	Ydeevne - global levering	3	Demonstrer din CDN-kapacitet, herunder demonstration af ventetid fra forskellige punkter rundt om i verden, herunder: Australien, Asien, Afrika, Mellemøsten, Nordamerika, Sydamerika og Europa.	• Mulighed for at oprette og konfigurere et CDN via CISP-konsollen/API'erne. • Konfigurerbare distributionsregler for forskellige geografiske områder. • Konfigurerbar caching til forskellige brugssituationer/anvendelser.
Web.Rel.1	Pålidelighed - Modstandsdygtighed i et enkelt område	4	Demonstrere evnen til at tolerere en lokaliseret hændelse som f.eks. tab af netværksforbindelse til CISP-datacenteret.	• Automatiseret failover og høj tilgængelighed inden for et cloud-område (by).
Web.Rel.2	Pålidelighed - udrulning i flere områder	3	Demonstrere en udrulning af en webapplikation i flere områder, herunder en globalt replikeret database.	• Mulighed for at udrulle et program programmatisk i flere områder. • Replikering mellem områderne for datalageret. • Automatisk videresendelse af brugere til deres optimale område.
Web.Rel.3	Pålidelighed - Failover i flere områder	3	Demonstration af automatisk failover af en webapplikation i tilfælde af et regionalt problem, der påvirker tjenesten.	• Automatiseret failover og høj tilgængelighed på tværs af flere cloud-områder.
Web.Cost.1	Omkostninger - synlighed	2	Demonstrere evnen til at spore omkostningerne pr. program.	• Mulighed for at se historiske omkostninger for et specifikt program, herunder når den skaleres op/ned.

Scenarie-id	Navn på scenarie	Hvor kritisk det er (1=Lav, 4=Kritisk)	Demonstrationskrav	Overvejelser vedrørende bedømmelser
Web.Cost.2	Omkostninger - budgetter	2	Demonstrere evnen til at fastlægge budgetter og relaterede advarsler pr. program.	• Budgetter konfigureret pr. program og mulighed for at udløse handlinger/advarsler baseret på konfigurerede grænseværdier.
Web.Ops.1	Ops - vedligeholdelsestider	3	Demonstrere evnen til at konfigurere vedligeholdelsestider for at tilpasse dem til forretningskravene, især hvor vedligeholdelse kan påvirke programmernes tilgængelighed.	• Konfigurerbare vedligeholdelsestider for komponenter som f.eks. en relationsdatabase-tjeneste.
Web.Ops.2	Ops – Logføring	3	Demonstrere evnen til at centralisere logføring for et program med flere komponenter, herunder opretholdelse af logfiler ved afslutning/fejl af virtuelle maskiner.	• Mulighed for at konfigurere en centraliseret logførings-tjeneste, der kan skaleres i takt med applikationskravene. • Mulighed for at definere regler/filtre til at udløse advarsler eller handlinger baseret på specifikke logfilsbegivenheder.
Web.Ops.3	Ops - Overvågning	3	Demonstration af overvågning af programmet, herunder ydeevne, tilgængelighed, svartider, fejltællinger osv. og funktionalitet til at træffe foranstaltninger/udløse meddelelser baseret på forskellige metriske tærskelværdier.	• En samling af tilgængelige standardmetrikker som f.eks. disk IO, CPU, databasemetrikker, netværk, belastningsudligner osv. • Evne til at definere brugerdefinerede målinger og tærskler. • Mulighed for at oprette et brugerdefineret dashboard til at repræsentere de vigtigste målepunkter og dele disse dashboards med relevante brugere.