



Kjøp av skytjenester i offentlig sektor

Håndbok – inkludert eksempel på RFP-språk
for en rammeavtale for skytjenester

Versjon 2: februar 2022

Meldinger

Dette dokumentet er bare til informasjon. Det er ikke utviklet i samsvar med lovkrav for offentlige anskaffelsesprosesser i en bestemt region. Skykunder har ansvaret for å foreta sin egen vurdering av opplysningene i dette dokumentet og for eventuell bruk av produkter eller tjenester til en skyleverandør. Dette dokumentet medfører ingen garantier, kontraktsmessige opplysninger, kontraktsmessige forpliktelser, betingelser eller forsikringer.

Eksempeldokumenter og -språk skal ikke tolkes som juridisk rådgivning eller veiledning. Skykunder bør konsultere sine egne juridiske rådgivere om sitt ansvar i henhold til gjeldende lov i sitt eget land. CISPE fraskriver seg uttrykkelig garantier, ansvar eller skader knyttet til eller som følge av informasjon gitt i dette dokumentet.

Om CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, <https://cispe.cloud>) er en ideell, uavhengig bransjegruppe. Vi representerer leverandører av skyinfrastruktur tjenester i Europa. I arbeider med bransjen og beslutningstakere, for å gi veiledning og utdanning om skytjenester og deres rolle i bransjen, det offentlige liv og i samfunnet generelt.

Vårt økende antall medlemmer inkluderer selskaper som opererer i alle EU-land og har hovedkontor i 16 europeiske land. Foreningen er åpen for selskaper, forutsatt at de erklærer at minst én av tjenestene deres oppfyller kravene til CISPEs etiske retningslinjer for databeskyttelse. Vi gjør følgende:

- Fremhever fordelene med retningslinjer for skybaserte offentlige anskaffelser i EU og EU-land
- Arbeider med skyinfrastruktursektoren for å oppnå klimanøytralitet innen 2030
- Fremmer sammenhengende sikkerhetskrav og tekniske standarder i hele EU
- Støtter omfattende personvernkrav med etiske retningslinjer for databeskyttelse
- Jobber for å holde EUs skyinfrastrukturmarked åpent, konkurransedyktig og fritt for bindinger
- Forhindrer uberettigede innholdsovervåkingsforpliktelser i EUs juridiske rammeverk

Medlemmene våre leverer og vedlikeholder de grunnleggende «byggeklossene for IT», som gjør det mulig for offentlige myndigheter og bedrifter å bygge sine egne systemer og levere viktige tjenester til milliarder av innbyggere. I denne rollen bidrar vi til å muliggjøre utvikling av ledende teknologi og tjenester som inkluderer Kunstig intelligens (AI), tilkoblede objekter, autonome kjøretøyer, 5G og neste generasjon av mobil tilkoblingsteknologi.

Etiske retningslinjer for skyinfrastruktur tjenester

CISPEs etiske retningslinjer for databeskyttelse, som ble lansert offentlig i september 2016, gikk forut for håndhevelsen av EUs personvernforordning (GDPR). De samsvarer med strenge GDPR-krav for å hjelpe leverandører av skyinfrastruktur med å operasjonalisere overholdelsen av databeskyttelse, og tilby et sterkt rammeverk for å hjelpe kunder med å velge skyleverandører og ha tillit til tjenestene deres. CISPE-retningslinjene ble [validert av det europeiske Personvernrådet](#) (EDPB, European Data Protection Board) i mai 2021, og [godkjent av franske CNIL](#) som kompetent instans i juni 2021. <https://www.codeofconduct.cloud/>

Pakten for klimanøytrale datasentre

CISPE arbeidet på slutten av 2019 med EU-kommisjonen for å utvikle et sett med målinger og et initiativ for selvregulering for å sikre klimanøytrale datasentre innen 2030. Dette initiativet ble utviklet sammen med den europeiske datasenterforeningen (EUDCA, European Data Centre Association) og andre bransjeforeninger og markedsaktører innen datasentre. Det ble lansert i januar 2021 som «pakten for klimanøytrale datasentre» <https://www.climateneutraldatacentre.net/>

Initiativet for rettferdig programvare

Sammen med den franske organisasjonen CIGREF og andre bransjeforeninger for IT-ledere og leverandører over hele Europa, har CISPE lansert [10 prinsipper for rettferdige programvarelisenser for skykunder](#). Dette er et sett med anbefalte fremgangsmåter for bedrifter som velger skyen for vekst, innovasjon og fleksibilitet, og utfordrer programvareleverandørene sine til å sikre at det benyttes rettferdige lisensvilkår. <https://www.fairsoftware.cloud/>

GAIA-X

CISPE var blant de tjueto stifterne av GAIA-X, det europeiske initiativet for å levere et åpent, transparent og sikkert digitalt økosystem. I den forbindelse har CISPE støttet visjonen og prinsippene til GAIA-X-organisasjonen fra starten. CISPEs generalsekretær ble gjenvalgt til å sitte i styret i juni 2021. Noen av verktøyene det vises til i håndboken, blant annet [CISPEs etiske retningslinjer for databeskyttelse](#) og de [etiske retningslinjene til SWIPO IaaS](#), er nyttige når det gjelder å bevise overholdelse av GAIA-X-prinsippene. <https://www.gaia-x.eu>

CISPE og offentlig sektor

CISPE bidrar til den europeiske debatten om offentlige retningslinjer, og arbeider for å sikre en bedre forståelse av rollen, bidraget og potensialet til Europas skyinfrastrukturbransje.

Selv om modeller for offentlige innkjøp bør styre prosessen med å ta i bruk og bruke databehandling i nettskyen, er anskaffelse av skytjenester forskjellig fra de fleste tradisjonelle teknologiinnkjøp som offentlig sektor kjenner til. Innkjøpsordninger må vurderes på nytt: CISPE oppmuntrer EUs beslutningstakere til å utvikle en mer ambisiøs og fremtidsrettet tilnærming i EU-skala basert på politiske initiativer som setter skyen først, og som dermed bidrar til å drive veksten i det indre skyinfrastrukturmarkedet i Europa og underbygge vekstmålene knyttet til det digitale indre markedet (DSM, Digital Single Market).

Denne håndboken er utformet for å gi nyttig veiledning og støtte til offentlige myndigheter ved anskaffelse av skytjenester.

Mer informasjon

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

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

Databehandling i nettskyen erklært i henhold til CISPEs etiske retningslinjer: <https://www.codeofconduct.cloud/public-register/>

Innholdsfortegnelse

Meldinger	2
Om CISPE	3
Innholdsfortegnelse	5
Sammendrag og formålet med denne håndboken	1
1.0 Oversikt over en rammeavtale for skytjenester	4
2.0 Oversikt over RFP for skytjenester	7
2.1 Oppsett av RFP for skytjenester	7
2.1.1 Innføring og strategiske mål	7
2.1.2 Tidslinje for respons på RFP	9
2.1.3 Definisjoner	10
2.1.4 Detaljert beskrivelse av kjøpsmodell og konkurranse innenfor rammeavtalen	11
2.1.5 Minstekrav til budgivere – administrativt	15
2.2 Teknisk	17
2.2.1 Minimumskrav	17
2.2.2 Sammenligning mellom leverandører	20
2.2.3 Kontrahering	21
2.3 Sikkerhet	23
2.3.1 Minimumskrav	23
2.3.2 Sammenligning mellom leverandører	27
2.3.3 Kontrahering	28
2.4 Priser	28
2.4.1 Minimumskrav	29
2.4.2 Sammenligning mellom leverandører	30
2.5 Oppsett og vilkår og betingelser for kontraktutførelse	32
2.5.1 Vilkår og betingelser	33
2.5.2 Vilkår og betingelser for programvare	35
2.5.3 Hvordan velge mellom tildelte per prosjekt	36
2.5.4 Påmønstring og avmønstring	37
3.0 Anbefalte fremgangsmåter og nyttig lærdom	38
3.1 Skyadministrasjon	38
3.2 Budsjetter for skyen	38
3.3 Forstå partnerens forretningsmodell	40
3.4 Skymeglere	40
3.5 Markedsundersøkelser før RFP	41
3.6 Bærekraft	41
Tillegg A: tekniske krav for sammenligning mellom budgivere	42
1. Skyleverandørprofil	42
2. Global infrastruktur	42
3. Infrastruktur	43
3.1 Databehandling	43

3.2 Nettverk.....	46
3.3 Lagring	49
4. Administrasjon	53
5. Sikkerhet.....	54
6. Samsvar	56
7. Migreringer.....	60
8. Fakturering	62
9. Administrasjon	63
10. Support.....	64
Tillegg B: direkte teknisk evaluering	66
Plattform – eksempel på direkte teknisk evaluering	67
Arbeidsbelastning: Nettopplikasjon – eksempel på direkte teknisk evaluering	75

Sammendrag og formålet med denne håndboken

Hensikten med denne **håndboken om kjøp av skytjenester** er å gi veiledning til skykunder som ønsker å kjøpe skytjenester gjennom en konkurransebasert anskaffelsesprosess (**invitasjon til anbudskonkurranse for skytjenester – RFP, Request for Proposal**), men mangler kompetanse til å utarbeide en rammeavtale for skytjenester.

Dette dokumentet er bare til informasjon. Det er ikke utviklet i samsvar med juridiske krav til offentlige anskaffelsesprosesser i noe bestemt land eller region.

Håndboken omhandler også ekstra formuleringer av utvalgsriterier for **løpende ordre** eller **minikonkurranser** når man kjøper fra en rammeavtale for skytjenester. Delene av håndboken er organisert slik at de ligner en generell IT-RFP. Eksempler på generiske formuleringer av RFP og utvalgsriterier er ledsaget av kommentarer som bidrar til å forstå hvorfor en skybasert RFP skiller seg fra en tradisjonell IT-RFP.

Etter at EU-kommisjonen publiserte skystrategien sin, som legger føringer for modernisering av IT-infrastrukturen til EUs institusjoner og organer gjennom en tilnærming som setter skyen først, overrakte CISPE håndboken til EU-kommisjonen i juli 2019 under arrangementet «*How to transform governments through a smart cloud policy*».



Versjon 2 av denne håndboken inneholder nye veiledninger om databeskyttelse (avsnitt 2.3.1.1), skifte av skyleverandører og dataoverføring (avsnitt 2.3.1.2), vilkår og betingelser for programvare (avsnitt 2.5.2), bærekraft i skyen (avsnitt 3.6), og et fornyet Tillegg B om direkte teknisk evaluering.

«Skytjenester» refererer til skyteknologi og relaterte tjenester som en sluttbruker kan trenge tilgang til. Det inkluderer rådgivning eller profesjonelle/administrerte tjenester som trengs for å støtte og utføre migrering til og arbeidsbelastninger i skyen, i tillegg til selve skyinfrastrukturen samt skymarkedstjenester, herunder produkter for Software as a Service (SaaS).

Fremveksten av databehandling i nettskyen som standardvalg for IT i offentlig sektor gir mulighet til å modernisere eksisterende innkjøpsstrategier. Skysentriske anskaffelsesprosesser kan gjøre det mulig for offentlige virksomheter å utnytte fordeler med skyen, for eksempel tilgang til ledende innovasjon, økt hastighet og smidighet, forbedret sikkerhetsstilling og styring av samsvar – samtidig som man realiserer effektivitet og kostnadsbesparelser.

Tradisjonelle IT-anskaffelsesmetoder for kjøp av maskinvare, programvare og datasentre tilsvarer ikke kjøp av skytjenester. Tilnærminger til priser, kontraktstyring, vilkår og betingelser, sikkerhet, tekniske krav, tjenestenivåavtaler og mer endres i en skymodell, og bruk av eksisterende anskaffelsesmetoder reduserer eller eliminerer til slutt fordelene som skyen gir.

En av de beste måtene for å effektivt implementere skytjenester i offentlig sektor, er med en **rammeavtale for skytjenester** – en multiorganisatorisk tildeling av en skymeny der kvalifiserte kjøpere tilknyttet innkjøpsorganisasjonen kan anskaffe skyteknologi og tilknyttede tjenester som oppfyller behovene deres. Slike rammeavtaler for skytjenester muliggjør kjøp av skytjenester på en effektiv måte – noe som resulterer i at innkjøpsorganisasjoner og sluttbrukerenheter har tilgang til et bredt spekter av skytjenester. Dermed kan de dra nytte av alle fordelene med skyen: smidighet, stordriftsfordeler, skalerbarhet for å oppnå bedre tilgjengelighet til lavere pris, bredde i funksjonalitet, rask innovasjon og kapasitet til å skalere til nye geografiske områder.

Merk at **denne artikkelen fokuserer på kjøp av skyteknologier for Infrastructure as a Service (IaaS) og Platform as a Service (PaaS) som leveres av en leverandør av skyinfrastruktur tjenester (CISP, Cloud Infrastructure Service Provider)**. Slike skyteknologier kan kjøpes direkte fra en CISP, eller gjennom en CISP-forhandler. Ytterligere RFP-hensyn vil være påkrevd for distributører av skymarkedstjenester (PaaS og SaaS) og skyrådgivningstjenester.

Merk at denne artikkelen ikke dekker alle aspekter ved å lage et helhetlig rammeverk for skyanskaffelse. Det finnes mange andre dokumenter fra bransjen og analytikere som dekker problemstillinger som anbefalte fremgangsmåter for innkjøp i skyen, budsjettering for skyen, skyadministrasjon osv. Vi anbefaler på det sterkeste å ta slike råd og dokumenter i betraktning når man utvikler en overordnet strategi for skyinnkjøp.

Tabell 1 nedenfor gir en oversikt over RFP-håndboken for skytjenester og over hvor det finnes eksempler på RFP-formuleringer for hver komponent i en RFP for skytjenester.

Tabell 1 – Sammendrag av avsnittene i RFP-håndboken for skytjenester

Avsnitt	Oversikt og eksempel på RFP-formulering
1.0 Oversikt over en rammeavtale for skytjenester	En oversikt over en rammeavtale for skytjenester (tjenester, hvordan man kan konkurrere og kontrahering)
2.0 Oversikt over RFP for skytjenester	Eksempel på generiske RFP-formuleringer som dekker avsnittene nedenfor, sammen med kommentarer som forklarer begrunnelsen bak RFP-strukturen for skytjenester og formuleringene som brukes
2.1 Oppsett av RFP for skytjenester	2.1.1 Innføring og strategiske mål 2.1.2 Tidslinje for respons på RFP 2.1.3 Definisjoner 2.1.4 Detaljert beskrivelse av kjøpsmodell og konkurranse innenfor rammeavtalen 2.1.5 Minstekrav til budgivere – administrativt
2.2 Teknisk	2.2.1 Minimumskrav 2.2.2 Sammenligning mellom leverandører 2.2.3 Kontrahering
2.3 Sikkerhet	2.3.1 Minimumskrav 2.3.1.1 Databeskyttelse 2.3.1.2 Skifte av skyleverandør og overføring av data 2.3.2 Sammenligning mellom leverandører 2.3.3 Kontrahering
2.4 Priser	2.4.1 Minimumskrav 2.4.2 Sammenligning mellom leverandører

Avsnitt	Oversikt og eksempel på RFP-formulering
2.5 Oppsett og vilkår og betingelser for kontraktutførelse	2.5.1 Vilkår og betingelser 2.5.2 Vilkår og betingelser for programvare 2.5.3 Hvordan velge mellom tildelte 2.5.4 Påmønstring og avmønstring
3.0 Anbefalte fremgangsmåter og nyttig lærdom	3.1 Skyadministrasjon 3.2 Budsjetter for skyen 3.3 Forstå partnerens forretningsmodell 3.4 Skymeglere 3.5 Markedsundersøkelser før RFP 3.6 Bærekraft
Tillegg A: tekniske krav for sammenligning mellom budgivere	En liste over generiske skyteknologikrav for løpende ordrer og minikonkurranser
Tillegg B: direkte teknisk evaluering	Et eksempelskript for produkt demonstrasjon av skyteknologi som viser poengsum (skydemoer som en del av en løpende ordre eller minikonkurranse)

1.0 Oversikt over en rammeavtale for skytjenester

En godt utformet rammeavtale for skytjenester kan muliggjøre innkjøp av skytjenester, på en måte som gagnar både deltakende organisasjoner i offentlig sektor og skyleverandører. Fordelene med en godt utformet rammeavtale for skytjenester omfatter følgende:

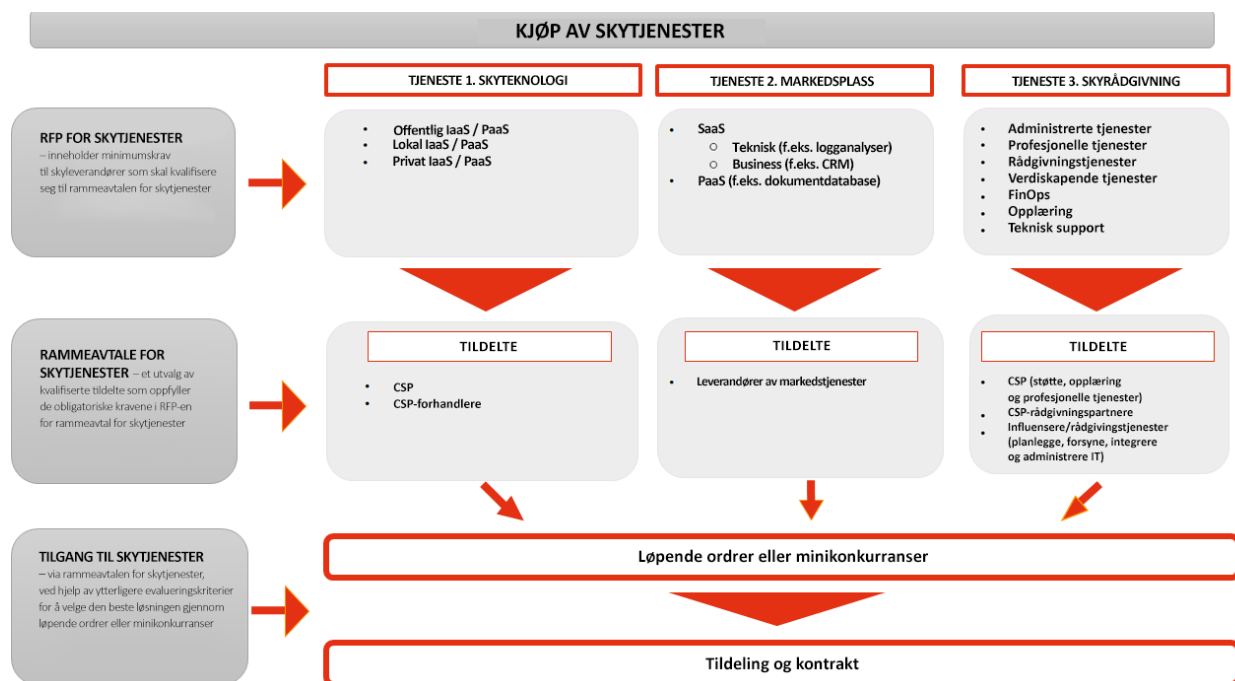
- **Samarbeidsrettet:**
 - Når flere organisasjoner slår seg sammen om å gjøre bestillinger, blir bestillingsprosessen mer bekvem, mer effektiv, billigere og enklere. Den etablerer en effektiv måte for å samle flere offentlige organisasjoners etterspørsel, både etter vanlige skyteknologier og tilknyttede skytjenester, som markedsløsninger og rådgivning.
- **Komplett utvalg av skytjenester:**
 - Det kan omfatte alle rådgivende/profesjonelle/administrerte tjenester som er nødvendige for å støtte og utføre migreringen til skyen og støtte arbeidsbelastninger i skyen, i tillegg til CISP-leverte skyteknologier og markestetjenester.
 - Slike skyteknologier kan kjøpes direkte fra en CISP, eller gjennom en utpekt forhandler.
- **Kontraktsstyring:**
 - Ulike organisasjoner/innkjøpere samles rundt et felles sett med vilkår og betingelser og en enkelt hovedkontrakt, fremfor forskjellige for hver organisasjon.
 - Det er også en fordel for leverandører, da det gir en standard anskaffelsesprosess, vilkår og betingelser og bestillingsmekanisme for å navigere, fremfor forskjellige for hver offentlige organisasjon.
 - Det gir fleksibilitet. Det å lage, godkjenne og implementere en effektiv skykontrakt innenfor eksisterende offentlige retningslinjer/forskrifter, krever eksperimentering og evne til å tilpasse seg raskt. Det er langt mer fordelaktig å opprette en rammeavtale som gjør det mulig for offentlig sektor og skyleverandører å samarbeide for å forbedre kontrakten – kontraktuelt, mekanisk og effektivt. En flerårig kontrakt som ikke fungerer og som ikke kan justeres, fører til en dårlig opplevelse for sluttbrukere i offentlig sektor, innkjøpsorganisasjoner og skyleverandører.
- **Valgfrihet:**
 - Det gjør det mulig for kjøpere å velge mellom flere kvalifiserte CISP-er. Det setter listen høyt for alle skytjenester og tilknyttede tjenester, for eksempel en skybasert PaaS/SaaS markeds plass og skyrådgivning.
 - Det gir mulighet for kontroll over antall leverandører i et rammeverk ved å sikre at standarden til hver tildelt blir riktig kontrollert.

En rammeavtale for kjøp av skytjenester fungerer best når den inkluderer CISP-leverte IaaS-/PaaS-kjerneteknologier, sammen med en PaaS-/SaaS-markeds plass og konsulent tjenester som sluttbrukere i offentlig sektor kan få tilgang til, ved behov, til hjelp med å planlegge, overføre, bruke og vedlikeholde en arbeidsbelastning som kjører i skyen. Vi foreslår derfor at en RFP for å sette opp en rammeavtale for skytjenester deles inn i følgende 3 partier med tjenester:

- **TJENESTE 1 – SKYTEKNOLOGIER**
Skyteknologier som kjøpes direkte fra en CISP eller gjennom en utpekt CISP-forhandler.
- **TJENESTE 2 – MARKEDSPASS**
Tilgang til en markeds plass for PaaS- og SaaS-tjenester.
- **TJENESTE 3 – SKYRÅDGIVNING**
Skyrelaterte konsulenttjenester (opplæring, profesjonelle tjenester, administrerte tjenester osv.) og teknisk støtte.

Som tidligere nevnt fokuserer denne artikkelen på kjøp av IaaS- og PaaS-skyteknologier (TJENESTE 1) levert av en CISP (kjøpt direkte fra en CISP, eller gjennom en CISP-forhandler). Det trengs separate krav til leverandørkvalifikasjoner for leverandører innen TJENESTE 2 og 3 i en RFP for skytjenester.

Figur 1 nedenfor gir en oversikt over hvordan en godt strukturert skybasert RFP, delt inn i disse tre tjenestene, kan føre til en rammeavtale for skytjenester som gir offentlige virksomheter smidighet (både teknisk og kontraktuelt), innsyn i og kontroll over forbruk og skybruk samt muligheten til å ha alle skytjenestene som er nødvendige for å bygge og vedlikeholde løsningene de trenger.



Figur 1: En vellykket skybasert RFP er delt inn i tre tjenester. Hver tjeneste inneholder kategorier eller «tilbudstyper» under det respektive partiet, for å sikre teknisk og kontraktsmessig tilpasning til sluttbrukerens krav ved kjøp innen rammeavtalen for skytjenester.

Merk at:

- Hver tjeneste er flertildelt.
- TJENESTE 3 kan tildeles via en annen RFP, eller muligens via en eksisterende kontrakt for konsulenttjenester.

Tjeneste 1 Kategorier

Vellykkede rammeavtaler for skytjenester ber CISP-er om å beskrive skymodellen de tilbyr, delt inn i kategorier under hver tjeneste. Vi anbefaler å bruke bransjestandarden for databehandling i nettskyen ([National Institute of Standards and Technology \(NIST\) Essential Cloud Characteristics](#)) – for definisjonene av **offentlig** sky, **lokal** sky og **privat** sky. Ved å strukturere en skyrammeavtale på denne måten kan innkjøpsbyrået og offentlige organer som bruker rammeverket, velge mellom en rekke skymodeller som passer til deres behov.

Se *avsnitt 2.1.3 Definisjoner* for NIST-definisjonen av hver skymodell under TJENESTE 1 (offentlig IaaS/PaaS, lokal IaaS/PaaS og privat IaaS/PaaS).

Hvordan konkurrere – løpende ordrer eller minikonkurranser?

Kvalifikasjonskriterier for en RFP for skytjenester skal dekke kritiske elementer og minimumsstandards, og bør ikke inneholde standarder som er «fine å ha». Ytterligere standarder for leverandører som kvalifiserer for rammeverket, kan føre til at noen leverandører ikke kan gi anbud, noe som betyr færre valg for kjøpere.

Etter RFP og påfølgende implementering av rammeavtalen for skytjenester kan offentlige organer i rammeverket bestille eller legge inn løpende ordrer på skytjenestene de trenger når det er nødvendig. En kontrakt med løpende ordrer i rammeavtalen gjør det mulig for kjøpere å forbedre kravene med ytterligere funksjonell spesifisering for en løpende ordre, samtidig som de beholder fordelene som tilbys under rammeavtalen.

Hvis det anses nødvendig, kan det avholdes en minikonkurranse for å identifisere den beste leverandøren for en bestemt arbeidsbelastning eller et bestemt prosjekt. En minikonkurranse er når en kunde øker konkurransen i rammeavtalen, ved å invitere alle leverandører av en tjeneste til å svare på et sett med krav. Kunden vil invitere alle aktuelle leverandører av tjenesten til å gi anbud, derav viktigheten av minimumskrav for tildelte på en skybasert RFP. Dermed sikres det høy standard på alternativene innen hver tjeneste.

*Merk at det er viktig at det er **forskjellige sett med vilkår og betingelser** for kontrakter for hver av tjenestene som er oppført i figur 1 ovenfor. En ensartet tilnærming til kontrahering for alle tjenester medfører problemer med teknisk gjennomførbarhet og kompatibilitet.*

2.0 Oversikt over RFP for skytjenester

Denne delen beskriver modellen for og omfanget av RFP for skytjenester, herunder: strategiske mål, deltakere, definisjoner, tidslinje og administrative minimumskrav. Merk at fokuset i denne håndboken er **TJENESTE 1 – SKYTEKNOLOGI**.

2.1 Oppsett av RFP for skytjenester

Vi anbefaler på det sterkeste at offentlige virksomheter gjør tydelig rede for sine overordnede mål og krav i innledningen til en RFP for skytjenester.

2.1.1 Innføring og strategiske mål

For å oppnå klarhet når det gjelder strategiske mål, er den anbefalte fremgangsmåten at innledningen til en RFP for skytjenester uttrykker **(1)** forretningsmålene og fordelene organisasjonen søker å oppnå ved å bruke skyen; **(2)** strukturen i rammeavtalen – hvem kjøper, hvem driver, hvem budsjetterer osv.; **(3)** en klar forståelse av modellen for delt ansvar mellom offentlig sektor og skyleverandører, som er kjernen i vellykket skyinnkjøp og -bruk, og **(4)** typen forhold som skapes mellom skytjenesteleverandører (CISP-er), distributører av markedstjenester, konsulentpartnere, offentlige organer for innkjøp/kontrahering og offentlige sluttbrukere. Disse fire punktene hjelper organisasjoner med å utvikle en RFP som best oppfyller deres behov, i tillegg til å sikre at både kunder og leverandører har en klar forståelse av hva som skal leveres i henhold til RFP-en.

En skybasert RFP er forskjellig fra tradisjonelle IT-RFP-er. Skyteknologi er ikke bare en likeverdig erstatning for tradisjonelle databehandlingsmetoder – den introduserer en helt ny måte å bruke teknologi på. Godt utformede RFP-er for skytjenester, kan hjelpe offentlige virksomheter med å hive seg rundt for å dra nytte av skyen.

Av alle de anbefalte fremgangsmåtene for å skyinnkjøp som vi nevner, er en klar forståelse av modellen for delt ansvar muligens det beste utgangspunktet. Modellen for delt ansvar¹ blir for det meste brukt når man snakker om sikkerhet og ettergivenhet i skyen, men denne avgrensningen av ansvar gjelder alle aspekter av skyteknologi. En RFP for skytjenester bør være tydelig på hva som ligger innenfor ansvarsområdet til en CISP i et skymiljø, og hva som forblir kundens ansvar. For eksempel gir en CISP muligheter til å overvåke ressurser og programmer som kjører i skyen, **men** det er kundens ansvar å faktisk bruke slike CISP-tilførte evner – ettersom en CISP som opererer i massiv skala ikke er designet for å gjøre dette for millioner av kunder.

Videre bør skykunder forstå hvordan et CISP-partnernettverk hjelper kunder med å bruke skyen og administrere ansvaret sitt. For eksempel kan en skybasert administrert tjenesteleverandør (MSP) hjelpe en kunde med å konfigurere og bruke CISP-tilførte overvåkingsfunksjoner for å oppfylle kundens unike krav til samsvar og revisjon.

¹ Se avsnitt 5 i CISPEs etiske retningslinjer for leverandører av skyinfrastruktur tjenester: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Enkelt sagt er ansvarsfordelingen i skymodellen som følger:

En CISP leverer skyteknologi.

En kunde bruker skyteknologi.

Konsulentfirmaer (hvis aktuelt) hjelper en kunde med å få tilgang til og bruke skyteknologi.

«Konsulentfirmaer» er bedrifter som tilbyr rådgivende og administrerte/profesjonelle tjenester for å hjelpe kunder med å utforme, bygge, migrere og administrere arbeidsbelastning og programmer i skyen. Slike selskaper omfatter systemintegratorer, strategiske rådgivere, byråer, leverandører av administrerte tjenester og verdiskapende forhandlere.

Tenk på å «handle» skytjenester som om du skal handle i en jernvarehandel. En jernvarehandel byr på et stort utvalg materialer og verktøy til å bygge det du trenger. Du kan bygge et skap, et svømmebasseng eller et helt hus, etter eget valg. Når du kjøper materialer og verktøy kan de ansatte i jernvarehandelen bidra med veiledning og ekspertise, men de kommer ikke hjem og bygger noe for deg. Derfor har du noen alternativer:

1. Kjøp materialene og verktøyene selv, og bygg noe selv.
2. Kjøp materialene og verktøyene selv, og betal noen for å bygge og/eller drive noe for deg.
3. Betal noen for å bygge/drive noe for deg, og få dem til å levere materialer og verktøy som en del av deres samlede tilbud.

Hvis en organisasjon har interne ferdigheter til å bygge og administrere sitt skymiljø og løsninger selv, trenger den egentlig bare å få tilgang til standardiserte skyteknologier og verktøy fra CISP-en (direkte med en CISP eller gjennom en CISP-forhandler – se **TJENESTE 1**). SaaS- og PaaS-programvare som trengs, bør være tilgjengelig på et skymarked (**TJENESTE 2**). Hvis det er behov for ytterligere rådgivning, migrering, implementering og/eller administrasjonshjelp, er det her et CISP-partnernettverk kommer inn i bildet (**TJENESTE 3**).

Eksempel på RFP-formuleringer: Innledning og strategiske mål

Databehandling i nettskyen gir offentlige organisasjoner rask tilgang til et bredt utvalg av fleksible og rimelige IT-ressurser med forbruksbasert betaling. Organisasjoner kan sørge for riktig type og størrelse på ressursene de trenger for å drive sine nyeste ideer eller betjene IT-avdelingene, noe som fjerner behovet for store investeringer i maskinvare og/eller langsiktige programvarelisensieringskontrakter.

<ORGANISASJONEN> har behov for tilgang til disse typene kommersielt tilgjengelige skyteknologier for å dekke sine forretningsbehov i et bredt spekter av tilknyttede organisasjoner.

Hovedmålet med denne RFP-en er å tildele en ikke-eksklusiv parallell <RAMMEAVTALE> med opptil <x> leverandører som representerer ulike skyteknologier og skyrelaterte tjenester.

1. **TJENESTE 1.** Skytjenesteleverandører (CISP-er) eller CISP-forhandlere for kjøp av skyteknologier.
2. **TJENESTE 2.** Leverandører av markedstjenester.
3. **TJENESTE 3.** Leverandører av konsulent tjenester for ytterligere ekspertise i å migrere til bruk av disse CISP-tilbudene.

Når det gjelder **Tjeneste 1**, må organisasjoner som gir anbud (CISP-er eller CISP-forhandlere) demonstrere hvordan tilbudet deres oppfyller disse målene:

- **Smidighet** – gjøre IT-ressurser tilgjengelig for sluttbrukere på få minutter i fremfor de tradisjonelle ukene og månedene.
- **Innovasjon** – ha øyeblikkelig tilgang til den nyeste og mest innovative teknologien på markedet.
- **Kostnad** – handelskapitalutgift for variable utgifter (f.eks. CapEx til OpEx). Betale kun for den mengden som forbrukes.
- **Budsjettering** – se fakturerings- og bruksinformasjon på både detaljert nivå og sammendragsnivå, visualisere mønstre i forbruk over tid, samt lage prognoser for fremtidige utgifter.
- **Elastisitet** – oppnå lavere variable kostnader med de større stordriftsfordelene som skyen gir.
- **Kapasitet** – eliminere gjettverk når det gjelder behov for infrastrukturkapasitet.
- **Slutte å stole på datasentre** – fokusere på virksomheten for innbyggerne våre, ikke på grovarbeidet med å sette opp og drifte servere.
- **Sikkerhet** – formalisere kontodesign med større innsyn i og mulighet for revisjon av ressurser, og eliminere kostnadene ved å beskytte anlegg og fysisk maskinvare.
- **Delt ansvar** – frigjøre operasjonell belastning når CISP opererer, administrerer og kontrollerer komponentene fra vertsoverativsystemet og laget for virtualisering ned til den fysiske sikkerheten til anleggene tjenesten opererer i.
- **Automasjon** – bygge inn automasjon i skyarkitekturen for å forbedre evnen til raskere og mer kostnadseffektiv sikker skalering.
- **Skyadministrasjon** – (1) starte med en full oversikt over alle IT-aktivaer; (2) administrere alle disse aktivaen sentralt; og (3) lage varsler om bruk/fakturering/sikkerhet osv. – med muligheter for aktivasporing, lagerstyring, endringsledelse, styring av logg og analyse, samt generell synlighet og skystyring.
- **Kontroll** – få full oversikt over hvordan IT-tjenester forbrukes, og hvor de kan justeres for sikkerhet, pålitelighet, ytelse og kostnader.
- **Reversibilitet** – portabilitetsverktøy og -tjenester som hjelper til med å migrere til og fra CISP-infrastruktur, minimere bindinger til leverandører og respektere etiske retningslinjer i bransjen.
- **Databeskyttelse** – evne til å demonstrere samsvar med EUs personvernforordning (GDPR), gjennom bransjens egne etiske retningslinjer for skyinfrastruktur-tjenester: [CISPEs etiske retningslinjer for databeskyttelse](#).
- **Gjennomsiktighet** – kundene bør ha rett til å vite hvor infrastruktur som brukes til å behandle og lagre dataene deres, befinner seg (byområde).
- **Klimanøytralitet** – kundene bør arbeide med CISP-er som treffer velprøvde, spesifikke tiltak for å oppfylle mål om klimanøytralitet innen 2030, og som har undertegnet Pakten for klimanøytrale datasentre. Dette vil hjelpe kundene å oppfylle sine egne mål om klimanøytralitet.

2.1.2 Tidslinje for respons på RFP

Det er god praksis å gi budgivere en tidslinje for forventet budaktivitet når du oppretter en rammeavtale for skytjenester og tilhørende skybasert RFP. Jo mer engasjement med bransjen desto bedre, siden det vil bidra til at det er en klar forståelse fra alle parter om RFP-kravene, og faktisk hvordan alle leverandørtjenester passer inn i skytjenestemodellen.

Merk at RFP-tidslinjen er underlagt lokale lover og juridiske forpliktelser, og listen nedenfor er ment som en veiledning for beste praksis i motsetning til en liste over aktiviteter og tidsrammer.

Eksempler på RFP-formuleringer: Responstidslinje

Se RFP-tidslinjen for RFP for skytjenester under:

Tidslinje for RFP for skytjenester
• Forespørsel om informasjon (RFI) – utgivelse: • RFI – respons: • Utkast til invitasjon til anbudskonkurranse (RFP) – utgivelse: • Utkast til RFP-respons – frist: • Bransjekonsultasjonsfase: <tidslinjer> • RFP før kvalifisering – utgivelse: • RFP før-kvalifisering – respons: • RFP – utgivelse: • Runde 1 – frist for spørsmål: • Runde 1 – svar: • Runde 2 – frist for spørsmål: • Runde 2 – svar: • RFP – responsfrist: • Anbudsavklaringsperiode: • Forhandlingsperiode: • Planlagt tildeling – dato: • Kontraktstildeling: • Kontraktsvarighet (muligheter for forlengelse):

Merk at RFP-tidslinjen er underlagt lokale lover og juridiske forpliktelser, og listen nedenfor er ment som en veiledning for beste praksis i motsetning til en liste over aktiviteter og tidsrammer.

2.1.3 Definisjoner

En skybasert RFP bør inneholde en detaljert liste over definisjoner. Denne listen inkluderer leverandørroller (f.eks. skytjenesteleverandør, skyforhandler, leverandørpartner), generelle teknologikonsepter (behandling, lagring, IaaS/PaaS, SaaS) og andre viktige deler av avtalen. Følgende er et eksempel på en definisjonsliste:

Eksempel på RFP-formuleringer: Definisjoner

Definisjonene nedenfor er National Institute of Standards and Technology (NIST) sine definisjoner av databehandling i nettskyen.²

- **Infrastructure as a Service (IaaS).** Muligheten som gis til forbrukeren er å skaffe behandling, lagring, nettverk og andre grunnleggende databehandlingsressurser der forbrukeren kan ta i bruk og implementere vilkårlig programvare, som kan omfatte operativsystemer og programmer. Forbrukeren administrerer eller kontrollerer ikke den underliggende skyinfrastrukturen, men har kontroll over operativsystemer, lagring og implementerte programmer – og muligens også begrenset kontroll over enkelte nettverkskomponenter (f.eks. brannmur i vertssystemet).
- **Platform as a Service (PaaS).** Forbrukeren får muligheten til å implementere programmer kunden selv har utviklet eller anskaffet ved hjelp av programmeringsspråk, biblioteker, tjenester og verktøy leverandøren støtter, på skyinfrastrukturen. Forbrukeren verken administrerer eller kontrollerer den underliggende skyinfrastrukturen, deriblant nettverk, servere, operativsystemer og lagring, men kontrollerer de implementerte programmene og muligens også konfigurasjonsinnstillinger for miljøet der programmet kjøres.

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

- **Software as a Service (SaaS).** Forbrukeren får muligheten til å bruke leverandørens programmer som kjører på en skyinfrastruktur. Programmene er tilgjengelige fra forskjellige klientenheter, enten via grensesnittet på en tynn klient, som en nettleser (f.eks. nettbasert e-post) eller via et programgrensesnitt. Forbrukeren verken administrerer eller kontrollerer den underliggende skyinfrastrukturen, inkludert nettverk, servere, operativsystemer, lagring eller til og med individuelle programfunksjoner, med mulig unntak av begrensede brukerspesifikke konfigurasjonsinnstillinger for programmer.
- **Offentlig sky.** Skyinfrastrukturen klargjøres for åpen bruk av allmennheten. Den kan eies, administreres og drives av en organisasjon i næringslivet, academia eller offentlig sektor, eller en kombinasjon av dem. Den finnes i lokalene til skyleverandøren.
- **Lokal sky.** Skyinfrastrukturen klargjøres til å brukes utelukkende av et spesifikt forbrukerfellesskap fra organisasjoner som har felles interesser (f.eks. oppdrag, sikkerhetskrav, retningslinjer og samsvarshensyn). Den kan eies, administreres og drives av en eller flere av organisasjonene i fellesskapet, en tredjepart eller en kombinasjon av disse, og den kan finnes i eller utenfor lokalene.
- **Hybrid sky.** Skyinfrastrukturen er en sammensetning av to eller flere adskilte skyinfrastrukturer (privat, lokal eller offentlig) som forblir unike enheter, men som er bundet sammen av standardisert eller proprietær teknologi som muliggjør data- og programportabilitet (for eksempel økning av skyttelse for lastbalansering mellom skyer).
- **Privat sky.** Skyinfrastrukturen klargjøres til å brukes utelukkende av en enkelt organisasjon som består av flere forbrukere (f.eks. forretningsenheter). Den kan eies, administreres og drives av organisasjonen, en tredjepart eller en kombinasjon av disse, og den kan finnes i eller utenfor lokalene.

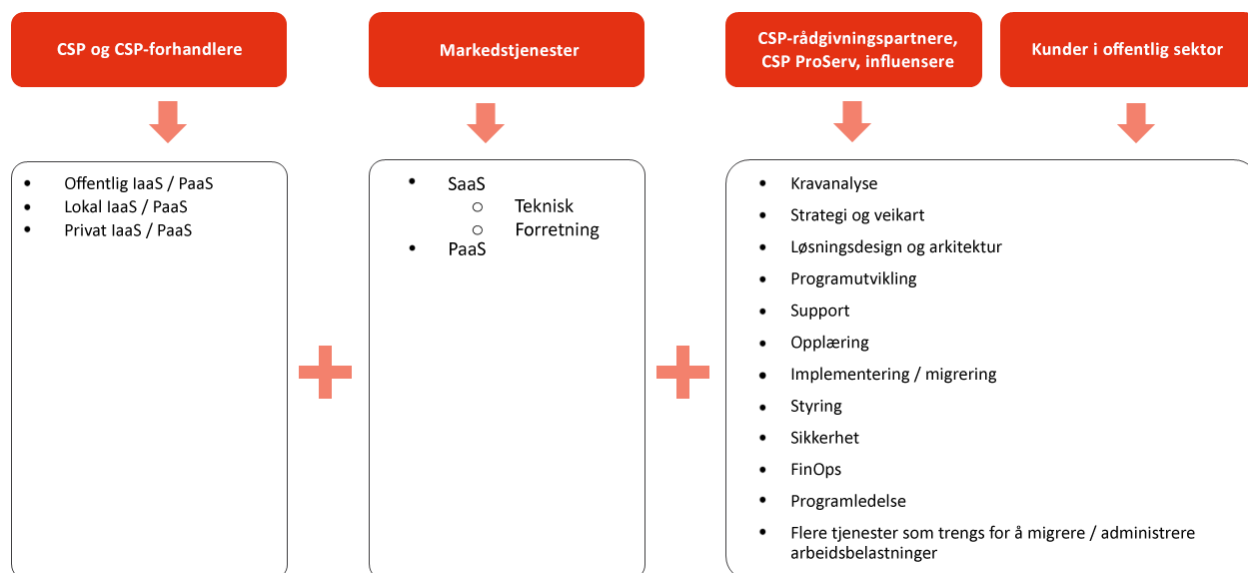
2.1.4 Detaljert beskrivelse av kjøpsmodell og konkurranse innenfor rammeavtalen

Som nevnt ovenfor, bør offentlige organisasjoner identifisere modellen for hvordan en rammeavtale vil fungere som en innkjøpsmekanisme for skyteknologier og relaterte implementerings- og administrasjonstjenester. Dette bør gjøres klart i den skybaserte RFP-en, slik at leverandører av skyteknologi, relaterte konsulentbedrifter, markedsdistributører og innkjøpsenheter forstår sine respektive roller.

Når det gjelder omfanget av rammeavtalen, og etter gjennomføring av løpende ordrer og minikonkurranser, bør organisasjoner vurdere følgende:

- Hvem vil være ansvarlig for integrering og administrerte tjenester som involverer bruk av skyteknologier i kontrakten?
- Er det behov for en CISP-forhandler/-partner som tilbyr andre verdiskapende tilleggstjenester enn å opprettholde et kontraktsforhold med CISP, tilbyr samlefakturerings tjenester og gi retttidig og direkte tilgang til bruks- og faktureringsdata knyttet til bruk av skyleverandørtjenestene?
- Er det behov for en forhandler med fullstendig service, en systemintegrator eller en leverandør av administrerte tjenester, eller noen form for IT-arbeidstjenester?

Det er viktig å merke seg at en CISP ikke er en systemintegrator (SI) eller administrert tjenesteleverandør (MSP). Mange kunder i offentlig sektor vil trenge en CISP til deres IaaS/PaaS, og kontrahere ut rådgivning, planlegging, migrering og administrasjonsarbeid til en SI eller MSP. Avgrensningen av roller og ansvar i en skytjenestemodell er skildret i **Figur 2** nedenfor.



Figur 2: En skybasert RFP bør gi sluttbrukerne en meny med alle skytjenestene de trenger. Kunder i offentlig sektor vil trenge en CISP for skyteknologier og en markeds plass for PaaS- og SaaS-produkter om nødvendig. Deretter kan kunden bestemme hvor stor rolle kunden vil påta seg i å levere skytjenester og hvor mye som skal kontraheres ut til et konsulentfirma/en systemintegrator/en leverandør av administrerte tjenester osv.

Eksempelformuleringen nedenfor er formet av rollene og ansvaret som er vist i figur 2 ovenfor. En skyrammeavtale og tilhørende RFP-er for skytjenester bør sikre at kjøperne sitter igjen med muligheten til å vurdere hver leverandørs tilbud på en tilstrekkelig måte, slik at de kan velge og vrake blant tjenestene som trengs for arbeidsbelastningen/prosjektet. Dette gjøres best ved å dele opp tjenester i partier, som drøftet over, og ved å være tydelig på hvordan løpende ordrer og minikonkurranse gjennomføres under rammeavtalen.

Eksempel på RFP-formuleringer: Innkjøpsmodell

Denne kontrakten skal fungere som et **rammeverk** for innkjøp. Denne rammeavtalen for skytjenester skal omfatte flere **partier med tjenester**, som definert av <ORGANISASJONEN>, for skyteknologier og relaterte markedstjenester/-produkter, konsulenttjenester, profesjonelle tjenester/systemintegrasjon administrerte tjenester/profesjonelle migreringstjenester, opplæring og support som definert av <ORGANISASJONEN>, som brukes av flere kvalifiserte kjøpere tilknyttet <ORGANISASJONEN>. Dette vil forenkle anskaffelsesprosessen og samtidig optimalisere stordriftsfordeler.

Når denne rammeavtalen er etablert, kan en organisasjon kjøpe de spesifikke skyteknologiene og skyrelaterte tjenestene den ønsker, når den trenger dem – i motsetning til å kjøpe gjennom adskilte innkjøp. Denne tilnærmingen reduserer de administrative kravene og gjør innkjøpene mindre komplekse og innkjøpssyklusen kortere.

Rammeavtalen skal vare i maksimalt <X> år inkludert fornyelser. Maksimal lengde på kontrakt for en løpende ordre innen rammeverket er normalt <X> måneder. Dette kan forlenges med <X> måneder og deretter ytterligere <X> måneder, gitt eventuelle interne godkjenninger som trengs for å forlenge kontrakten. Dette vil bli spesifisert i hver spesifikke **løpende ordre**.

RAMMEVERKET er inndelt i **3 (tre) tjenester**.

1. **TJENESTE 1: SKYTEKNOLOGIER** – fullt omfang av skyleverandørteknologier (direkte fra CISP, fra forhandler eller fra forhandler med verdiskapende tjenester/støtte):

- i. **IaaS- og PaaS-tjenester** – en meny med skyteknologier, f.eks. beregning, lagring, nettverk, database, analyse, programtjenester, implementering, administrasjon, utvikler, tingenes internett (IoT), osv. Inkluderer kombinerte skyteknologiløsninger som DR/COOP, arkiv, store datamengder og analyse, DevOps osv.

2. **TJENESTE 2: MARKEDSPASS** – fullt omfang av PaaS- og SaaS-tjenester/produkter som regnskap, CRM, design, HR, GIS og kartlegging, HPC, BI, innholdsadministrasjon, analyse av logg osv.

3. **TJENESTE 3: SKYRÅDGIVNING** – komplett omfang av konsulenttjenester (administrerte tjenester, profesjonelle tjenester, rådgivningstjenester, merverditjenester, FinOps, teknisk støtte) relatert til skyoverføring og bruk. Disse tjenestene kan omfatte planlegging, design, migrering, ledelse, support, kvalitetssikring, sikkerhet, opplæring osv.

Leverandører kan levere sine tilbud til flere tjenester.

Leverandører vil levere sine tilbud og tilhørende priser i sitt valgte format.

KONKURRANSE INNEN RAMMEVERKET OG TILDELENDE KONTRAKTER

LØPENDE ORDRER

Organer i offentlig sektor som er part i rammeavtalen kan bestille eller lage en løpende ordre på tjenestene de trenger, når de trenger dem. En kontrakt med løpende ordrer i rammeavtalen gjør det mulig for kjøpere å forbedre kravene med ytterligere funksjonell spesifisering for en løpende ordre, samtidig som de beholder fordelene som tilbys under rammeavtalen.

Kontrakter tildelt gjennom rammeavtalen vil kunne vise et tydelig revisjonsspor når det gjelder kravene som brukes til å velge leverandør innen hver tjeneste. Sluttkjøpere vil føre oversikt over kommunikasjon med leverandører, inkludert eventuelle tidlige markedsengasjementer, avklaringsspørsmål, e-poster og fysiske samtaler.

1. SKRIVE KRAV TIL LØPENDE ORDRER OG SØKE INTERN GODKJENNING FOR KJØP

Alle sluttkjøpere som er kvalifisert til å bruke rammeavtalen, vil opprette felles team av forretningssluttbukere, innkjøpsspesialister og tekniske eksperter for å utarbeide en liste over behov og ønsker. Disse kravene vil være med på å bestemme hvilket eller hvilke tjenester som er aktuelle, og hvilken leverandør som er best kvalifisert til å oppfylle kravene. Ved utarbeidelse av kravene, vil kjøpere vurdere følgende:

- midler tilgjengelig for å bruke tjenesten
- tekniske krav og anskaffelseskrav til prosjektet
- kriterier som valget skal baseres på

2. SØK ETTER TJENESTER

Kjøpere som dekkes av rammeavtalen vil bruke en nettbasert rammeverkskatalog (en portal der kvalifiserte tildelte under rammeavtalen og deres tjenester blir oppført) for å finne produkter/tjenester som oppfyller deres identifiserte behov. De vil velge de aktuelle tjenestepartiene, og deretter søke etter tjenester.

3. GJENNOMGANG OG EVALUERING AV TJENESTER

Kjøpere under rammeavtalen vil gjennomgå tjenestebeskrivelser for å finne de tjenestene som best oppfyller behovene basert på både krav og budsjett. Hver tjenestebeskrivelse vil inneholde følgende:

- Et dokument med tjenestedefinisjoner eller koblinger til tjenestedefinisjoner
- Et dokument med vilkår og betingelser
- Et prisdokument (koblinger til offentlige priser kan godtas, så lenge en fullstendig prisliste eller et dokument med priser er tilgjengelig på forespørsel)

Prisen skal være prisen på den vanligste konfigurasjonen av tjenesten. Prissettingen er imidlertid normalt volumbasert, slik at kjøperne alltid skal se på leverandørens prisdokument eller offentlige priser samt priskalkulatorverktøy for å regne ut den faktiske prisen på det som blir kjøpt, og den totale verdien som leveres til kjøperen (for eksempel tjenester for optimalisering og medfølgende kostnadsreduksjon).

Kjøpere under rammeavtalen kan kontakte leverandører og be dem om å forklare tjenestebeskrivelsen, vilkårene, prisene og dokumentene med eller modellen for priser eller tjenestedefinisjoner. Eventuelle samtaler med leverandører blir tatt opp.

4. VALG AV TJENESTE OG TILDELING AV KONTRAKT

En leverandør

Hvis bare en leverandør oppfyller kravene, kan kontrakt tildeles denne leverandøren.

Flere leverandører

Hvis det er flere tjenester på en kortliste, velger kjøperen tjenesten med det mest økonomisk fordelaktige anbudet (MEAT, Most Economically Advantageous Tender). Se kriteriene i tabellen nedenfor for MEAT-basert vurdering. Kjøpere kan bestemme hvilke detaljerte egenskaper som skal brukes og hvordan de skal vektas.

Merk at kjøperen kan ha behov for følgende:

- se på kombinasjoner av forskjellige leverandører
- få spesifikk informasjon om volum- eller bedriftsrabatter og kostnadsoptimaliseringstjenester for leverandører

Vurderingen av leverandører skal alltid være rettferdig og gjennomslutlig. Valget skal være basert på beste tilpasning, og leverandører/tjenester skal ikke bli ekskludert uten henvisning til prosjektkravene.

Tabell 2: MEAT-basert vurdering

Tildelingskriterier
Levetidskostnad: kostnadseffektivitet, pris og driftskostnader
Tekniske meritter og funksjonell tilpasning: dekning, nettverkskapasitet og ytelse som spesifisert i relevante tjenestenivåer
Tjenesteadministrasjon etter salg: helpdesk, dokumentasjon, kontoadministrasjonsfunksjon og forsikring om levering av en rekke tjenester
Ikke-funksjonelle egenskaper

MINIKONKURRANSER

Hvis det anses nødvendig, kan det avholdes en minikonkurranse for å identifisere den beste leverandøren for en bestemt arbeidsbelastning eller et bestemt prosjekt. En minikonkurranse er når en kunde øker konkurransen i rammeavtalen, ved å invitere alle leverandører av en tjeneste til å svare på et sett med krav. Kunden vil invitere alle aktuelle leverandører av tjenesten til å gi anbud. Se mer informasjon om sammenligning i avsnittene nedenfor angående det tekniske, sikkerhet og pris/verdi.

KONTRAKT

Kjøperen og leverandøren skal begge signere en kopi av kontrakten før tjenesten kan brukes. Maksimal lengde på en kontrakt innen rammeverket er normalt <x> måneder. Dette kan utvides med <x> måneder og deretter ytterligere <x> måneder, gitt eventuelle interne godkjenninger som trengs for å forlenge kontrakten.

En kopi av kontrakten må signeres av alle interesserte parter (kjøper og leverandør) før tjenesten kan brukes.

2.1.5 Minstekrav til budgivere – administrativt

Ved å angi kvalifikasjonskriterier for rammeavtaler med klart og tydelig språk bidrar man til å unngå anbud fra tradisjonelle datasenter- eller maskinvareleverandører som pakker inn en tradisjonell løsning som en «sky». RFP-deltakere bør vise hvordan de oppfyller de administrative minstekravene til budgivere nedenfor.

Merk at denne artikkelen fokuserer på **TJENESTE 1 – SKYTEKNOLOGI**. Vi har imidlertid lagt til ytterligere informasjon om **TJENESTE 2 – MARKEDSPASS** og **TJENESTE 3 – SKYRÅDGIVNING** når dette bidrar til å gi en generell kontekst om krav og RFP-omfang. For eksempel er det viktig å inkludere minimumskvalifikasjonskriterier for en CISP-forhandler/MSP/Sl/konsulentfirma osv., og det hjelper å sikre at de er (1) direkte tilknyttet CISP som forhandler eller kanalpartner, (2) sertifisert av en CISP for å videreselge direkte tilgang til CISP-tilbud til tredjepartsenheter, og (3) har sertifiseringer fra disse CISP-ene som angir deres evner og ekspertise.

Eksempel på RFP-formuleringer: Minimumskrav for budgiver – administrativt

Denne rammeavtalen vil tildele kontrakter til flere leverandører i følgende kategorier. Leverandøren må være en kommersiell CISP, en tredjepartsforhandler for en CISP, en distributør av markedstjenester og/eller en leverandør av tjenester for bruk av en CISP (f.eks. konsulenttjenester, migreringstjenester, administrerte tjenester, FinOps osv.). Vennligst identifiser rollene du byr på:

TJENESTE 1

- _____ - Direkte leverandør (CISP) av offentlige skytjenester (IaaS OG PaaS)
- _____ - Direkte leverandør (CISP) av lokal skytjeneste (IaaS OG PaaS)
- _____ - Direkte leverandør (CISP) av privat skytjeneste (IaaS OG PaaS)
- _____ - Tredjepartsforhandler for CISP (mulighet til å gi direkte tilgang til de nettbaserte tilbudene til en CISP)

- Identifiser CISP-en som tilbyr deg å videreselge direkte tilgang til tjenesten deres: _____
- Legg frem brev fra CISP-en om at du er en autorisert forhandler av tilbudene deres: _____

TJENESTE 2

- _____ - Direkte leverandør av markedstjenester som kjører på en CISP (PaaS og/eller SaaS)
- _____ - Distributør av markedstjenester som kjører på en CISP (PaaS og/eller SaaS)

TJENESTE 3

- _____ - CISP som tilbyr profesjonelle tjenester
- _____ - Leverandør av teknisk support for CISP
- _____ - CISP-partner som tilbyr tjenester for å bruke eller operere på en CISP
- _____ - Influenser/rådgiver som tilbyr tjenester for bruk eller drift av en CISP

Identifiser tilbudstype:

- Administrerte tjenester for arbeidsbelastninger på en CISP (J/N): _____
 - Identifiser spesialiteter hvis aktuelt: _____
- Profesjonelle tjenester (J/N): _____
- Rådgivning – opplæring (J/N): _____
- Rådgivning – strategi (J/N): _____
- Rådgivning – migrering (J/N): _____
- Rådgivning – skyadministrasjon (J/N): _____
- Rådgivning – FinOps (J/N): _____
- Rådgivning – annet (oppgi hva): _____

Identifiser CISP-en(e) du tilbyr tjenester for: _____

Legg frem brev fra CISP-en som bekrefter at du er utpekt til partner etter CISP-ens modell: _____

TJENESTE 1: ADMINISTRATIVE MINIMUMSKRAV**Skytjenesteleverandører (CISP-er)**

For å kvalifisere som en CISP, må kravene nedenfor oppfylles.

Foreslåtte kvalifikasjonskriterier for CISP	Årsak
Organisatoriske detaljer som f.eks. navn, juridisk struktur, registreringsnummer, mva osv.	
Selskapets størrelse, økonomiske og finansielle forhold. ³	Kunden kan kontrollere at CISP-en vil kunne effektivere kontrakten.
Begrunnelse for ekskludering, f.eks. kriminell eller uredlig virksomhet, osv.	
Casestudier/kundereferanser (spesifiser nummer/type).	Kunden kan måle CISP-opplevelsen for å levere de nødvendige tjenestene.
Bedriftens sosiale ansvar.	Disse bør være offentlig tilgjengelige versjoner som CISP leverer.
Offentlig tilgjengelige bærekraftsforpliktelser og -praksiser.	Kunden kan se at en CISP har forpliktet seg til å drive virksomheten sin på en mest mulig miljøvennlig måte.
CISP-en må bevise erfaring med å innovere og gi ut nye nyttige tjenester og funksjoner de siste fem årene, spesielt innen PaaS, maskinlæring og analyse, store datamengder, administrerte tjenester og optimalisering av skybruk. Offentlig tilgjengelige endringslogger eller oppdateringsfeeder kan brukes som slikt bevis.	Demonstrerer at CISP-en jobber for å få nye produkter raskt i hendene på kundene, og deretter justerer og forbedrer produktene raskt. Dette hjelper kundene med å opprettholde den nyeste IT-infrastrukturen uten å måtte investere i rekapitalisering.

Forhandler- eller partnerforhold med CISP

<ORGANISASJONEN> krever at hovedentreprenøren er direkte tilknyttet CISP som en forhandler eller kanalpartner, sertifisert av en CISP for å videreselge direkte tilgang til CISP-tilbud til tredjepartsenheter, med sertifiseringer fra disse CISP-ene som angir deres evner og ekspertise. Dette eliminerer <ORGANISASJONENS> behov for gjennomgang av vilkårene og tjenestene knyttet til et ekstra lag med underleverandører mellom hovedentreprenøren i rammeavtalen og CISP-en. Dette kravet reduserer også kompleksiteten som flere forhandlerlag genererer når (1) <ORGANISASJONEN> utfører sin selskapsgjennomgang for å sikre klar ansvarsfordeling med hensyn til tjenestene som skal leveres, og (2) <ORGANISASJONEN> utfører daglige aktiviteter som involverer forbruk av skytjenester.

³Merk at en skybasert RFP ser på bedriftsinformasjon på høyt nivå, i motsetning til antall ansatte i selskapet og de interne ansattes teamstruktur. Med skyteknologi er det ingen sammenheng mellom garanti for ytelse av tjenesten og antall ansatte. I stedet fokuserer skybaserte RFP-er på selskapets totale størrelse for å oppfylle kravene (tilstrekkelig skala) og bevist erfaring/ytelse.

2.2 Teknisk

En skybasert RFP bør heve listen for CISP-er ved å kreve at de leverer de standardiserte skyteknologiene som er nødvendige for at en kunde skal kunne bygge sin tilpassede løsning. Som nevnt tidligere er denne forskjellen mellom det som er standardisert og det som er tilpasset veldig viktig når man nærmer seg en skybasert RFP. CISP-er tilbyr standardiserte tjenester til millioner av kunder, så tilpasninger i en skybasert RFP fokuserer på høyere løsninger og resultater, i motsetning til de underliggende metodene, infrastrukturen eller maskinvaren som brukes til å tilby skytjenestene som brukes til å oppnå løsningsresultater.

2.2.1 Minimumskrav

Tradisjonelle IT-anskaffelser er ofte avhengige av forretningskrav utviklet gjennom en serie arbeidsøker som dokumenterer hvordan organisasjonen for tiden driver sin virksomhet. Det å få disse kravene helt riktig er en vanskelig prosess under selv de beste omstendigheter. Hvis det lykkes, dokumenterer disse kravene den historiske forretningsprosessen som i seg selv kan være gammeldags og ineffektiv. Hvis disse kravene blir gjort til en del av RFP som skal replikeres av CISP, kan den eneste løsningen være en skreddersydd løsning. Denne modellen er inkompatibel med skyanskaffelser.

Offentlige organisasjoner bør forstå deres forretningsmål og ytelsesbehov, men RFP bør ikke diktere systemdesign og funksjonalitet. I stedet burde organisasjonen skaffe seg det som passer best til virksomheten. Fremfor å evaluere forslag til hundrevis eller til og med tusenvis av krav som kanskje ikke fører til vellykkede tjenester, bør organisasjoner inkludere evalueringskriterier basert på hvor godt teknologien og tilknyttede tjenester vil oppfylle eller forbedre forretningsmålene, hvorvidt de imøtekommer deres ytelsesbehov og hvilken evne de har til å finjustere forretningsregler gjennom konfigurering.

*Skybaserte RFP-er bør stille de riktige spørsmålene for å oppnå de beste løsningene. Gitt at det ikke kjøpes fysiske aktiva i en skymodell, følger det at mange tradisjonelle innkjøpskrav for datasentre ikke gjelder. **Resirkulering av datasenterspørsmål vil uunngåelig føre til datasentersvar, noe som resulterer i at CISP-er ikke kan by, eller fører til dårlig utformede kontrakter som hindrer offentlige kunder i å hente ut alle muligheter og fordeler med skyen.***

En skybasert RFP fokuserer på de viktigste kravene som stilles til en CISP og skytjenester, og sørger for at leverandører som kvalifiserer for TJENESTE 1 oppfyller strenge krav. Kravene bør også unngå å være for veiledende, for ikke å begrense offentlig sektors tilgang til et bredt spekter av kvalifiserte CISP-er.

Eksempel på RFP-formuleringer: Skyleverandørfunksjoner

Se også de ovennevnte CISP-minimumskravene for TJENESTE 1

Foreslåtte kvalifikasjonskriterier for CISP	Årsak
Infrastruktur	
CISP-infrastrukturen bør tilby minst to grupper av datasentre. Hver gruppe må bestå av minst to datasentre forbundet via en kobling med lav ventetid for å gjøre det mulig med høyt tilgjengelige aktiv-aktiv-implementeringer og implementeringer av scenarioer for nødgjenoppretting og forretningskontinuitet (DR/BC, Disaster Recovery and Business Continuity). Datasentrene som utgjør hver av gruppene, må være fysisk isolerte og feiluvhengige fra hverandre.	CISP må kunne tilby en infrastruktur som er egnet til å bygge svært tilgjengelige programmer der enkeltfeilpunkter kan unngås.

<i>CISP bør by på logisk og geografisk isolerte regioner. Kundedata må ikke replikeres utenfor disse regionene av CISP.</i>	<i>Krav til datalagring krever at kunden har full kontroll over hvor dataene befinner seg.</i>
<i>CISP må ha muligheten til å levere direkte, dedikert og privat tilkobling mellom CISP-datasentrene.</i>	<i>Privat tilkobling er et grunnleggende krav for å kunne bygge en hybrid, sikker infrastruktur.</i>
<i>CISP bør levere tilstrekkelige mekanismer, noe som inkluderer kryptering for data under overføring.</i>	<i>Kunden kan kreve en funksjon for at ingen data skal kunne overføres ukryptert.</i>
Minimale CISP-sertifiseringer	
<i>CISP-en må være sertifisert etter ISO 27001.</i>	<i>Tredjepartsrevisjon, sertifisering og akkreditering sikrer at kunder kan benchmarke tjenester (og spesielt plattformen) for kvalitet, sikkerhet og pålitelighet. Det er viktig at et minimum av sertifiseringer oppfylles.</i>
<i>CISP-en må overholde CISPEs etiske retningslinjer for databeskyttelse for å kunne tilby funksjoner og tjenester som kan brukes i samsvar med GDPR, noe som lar kundene bygge applikasjoner i samsvar med GDPR.</i>	<i>Kunden må kunne bygge eller kjøre applikasjoner i samsvar med GDPR.</i>
<i>CISP-en må gjøre tilgjengelig reviderte tredjepartsrapporter, f.eks. som SOC 1- og 2-rapporter (som dekker lokasjonene og tjenestene som brukes av EC) for å tillate gjennomskiktighet med hensyn til CISP-kontroller og prosedyrer.</i>	<i>CISP må være gjennomskiktig med hensyn til hvordan programmet drives og administreres. SOC-rapporter medvirker til å sikre tillit og åpenhet.</i>
<i>CISP-en må ha sluttet seg til Pakten for klimanøytrale datasentre.</i>	<i>Pakten for klimanøytrale datasentre forplikter CISP-en til å oppnå klimanøytralitet innen 2030, og gjør det derfor mulig for brukeren å støtte sine egne bærekraftsmål. Tredjepartsrevisorer er obligatoriske for leverandører over 250 ansatte (ikke for små og mellomstore bedrifter).</i>
<i>CISP-en må ha sluttet seg til SWIPO sine etiske retningslinjer for IaaS-portabilitet.</i>	<i>SWIPO sine etiske retningslinjer for IaaS-portabilitet sikrer at tjenester oppfyller de mest avanserte kravene. 6 «Dataoverføring» fra EU-forordningen om fri flyt av andre opplysninger enn personopplysninger.</i>
Tjenesteegenskaper	
<i>CISP-infrastrukturen må være tilgjengelig gjennom programmatisk grensesnitt (API-er) og nettbasert administrasjonskonsoll.</i>	<i>Selvbetjeningstilgang og programmatisk grensesnitt er en obligatorisk standard for CISP-leverandører for å fjerne mellomledd mellom brukertilgang og selve leverandøren så langt som mulig.</i>
<i>CISP-en må tilby et grunnleggende sett med tjenester, blant annet objektlagring, administrert relasjonsdatabase, administrert ikke-relasjonsdatabase, administrert belastningsbalansering, overvåking og integrert autoskalering.</i>	<i>Bare et tilbud om virtuelle maskiner er ikke tilstrekkelig for å kvalifisere en leverandør som en skyleverandør. Skyleverandører bør tilby et sett med PaaS- og IaaS-tjenester for å fremskynde og forbedre kundens programmer.</i>
<i>CISP må tillate kunden å fritt endre tjenestebruken og konfigurasjonen, eller flytte data innenfor og utenfor CISP-en (selvbetjeningstilbud).</i>	<i>Selvbetjeningstilgang til tjenester og data er et absolutt krav som gjør at kunden kan være helt uavhengig.</i>
<i>CISP må tillate «betal per bruk»-basert fakturering for tjenestene sine.</i>	<i>Betaling per bruk gjør det mulig for kunden å kostnadsoptimalisere arbeidsbelastningene, minimere risiko og utnytte CISP-en til kortvarige applikasjoner og prøveversjoner.</i>

<i>Data- og systemsikkerhet</i>	
<i>CISP må tillate kunden å beholde full kontroll over dataene sine, gi kunden frihet til å velge hvor data lagres (område), og garantere at ingen kundedata blir flyttet med mindre slik flytting initieres av kunden selv.</i>	<i>Kunden må ha kontroll over hvor data lagres, hvordan man administrerer tilgang til innhold, og brukertilgang til tjenester og ressurser.</i>
<i>CISP-egenskapene må gi kunden full kontroll over sine sikkerhetsretningslinjer, inkludert konfidensialitet, integritet og tilgjengelighet for kundedata og -systemer.</i>	<i>Kunden må kunne definere og implementere sikkerhetsstandardene på tvers av arbeidsbelastninger. Det er ikke nok å stole på at leverandøren «gjør det rette» med kundens data.</i>
<i>Kostnadskontroll</i>	
<i>CISP må ha mekanismer og verktøy som gjør det mulig for kunden å overvåke forbruket over tid. Verktøy må tillate grunnleggende segmentering av kostnader basert på arbeidsbelastning, tjeneste og konto.</i>	
<i>CISP må tilby verktøy for å varsle kunden når en kostnadsgrense overskrides.</i>	
<i>CISP må levere detaljerte fakturaer til kunden. Det må være mulig å strukturere fakturaen for å fordele kostnadene etter arbeidsbelastning, miljø og konto.</i>	

CISP bør også gi svar på spørsmålene om tekniske krav nedenfor.

LØSNINGER

CISP bør demonstrere hvordan den kan tilby forhåndsbygde maler og programvareløsninger som enten har CISP som vert eller integreres med CISP, for følgende løsninger:

- Lagring
- DevOps
- Sikkerhet/samsvar
- Store datamengder/analyse
- Forretningsprogrammer
- Telekommunikasjon og nettverk
- Georomlig
- IoT
- [Annet]

Gi en oversikt over hvordan CISP har blitt brukt til følgende arbeidsbelastninger:

- Nødgjenoppretting
- Utvikling og testing
- Arkivering
- Sikkerhetskopiering og gjenoppretting
- Store datamengder
- Databehandling med høy ytelse (HPC)
- Tingenes internett (IoT)
- Nettsider
- Serverløs databehandling
- DevOps
- Innholdslevering
- [Annet]

2.2.2 Sammenligning mellom leverandører

I tillegg til minimumskravene i en skybasert RFP er det viktig å gi kriterier som CISP-teknologier kan sammenlignes med under en konkurransevaluering.

Skybaserte RFP-er bør be om de skyfunksjonene en organisasjon trenger, med en forståelse av at kunden eier slike funksjoner for å bygge løsningen. Funksjonalitet utover standarden som en CISP kan levere (for eksempel forhåndsbygde løsninger via CISP, eller automatiseringsfunksjoner) kan brukes til en mer meningsfull analyse av «verdiskapende alternativer» eller «best verdi» i en RFP for skytjenester.

Offentlig sektor krever ofte konkurranse mellom budgivere der det brukes evalueringsvilkår som beste verdi, mest økonomisk fordelaktige anbud eller laveste pris. Når offentlige enheter planlegger denne delen av en skybasert RFP, er det viktig å bygge en tilnærming som tar hensyn til de unike egenskapene til skyen. For eksempel å forstå at bare å sammenligne budsjettposter mellom skyleverandørers tilbud (f.eks. beregning eller lagring) ikke er en effektiv måte å sammenligne tilbud på. I stedet anbefaler vi sterkt å fokusere på løsninger på høyere nivå, som de som er oppført ovenfor i avsnitt 2.2.1. Offentlige virksomheter kan deretter se på krav som er spesifikke for skyen, f.eks. de som er oppført i *Tillegg A: tekniske krav for sammenligning mellom budgivere*.

RFP-er bør oppgi de essensielle skyegenskapene som trengs for å bygge skyløsningen. For å gjøre dette, kan offentlige organisasjoner utnytte «National Institute of Standards and Technology (NIST) Essential Cloud Characteristics», i tillegg til å bruke analyserapporter fra tredjeparter for å sikre at CISP har det best egnede «ekte sky»-tilbudet i massiv skala.

Eksempel på RFP-formuleringer: Sammenligning mellom leverandører

*CISP-er skal også gi svar på alle spørsmål om tekniske krav i **Tillegg A**.*

Respondentene må ha følgende attributter og må beskrive hvordan deres tilbud om skytjenester oppfyller de fem essensielle egenskapene til databehandling i nettskyen⁴.

- 1) **Behovsbasert selvbetjening:** Respondenten må tilby muligheten til ensidig å klargjøre databehandlingsmuligheter, for eksempel servertid og nettverkslagring, automatisk etter behov uten å kreve menneskelig interaksjon med hver tjenesteleverandør. Respondenten skal tilby funksjoner for at den bestilte aktiviteten ensidig (dvs. uten leverandørgjennomgang eller -godkjenning) kan levere tjenester. Forklar hvordan dette fungerer i tilbudet deres eller tilbudet dere representerer.
- 2) **Allestedsnærværende nettverkstilgang:** Respondenten må tilby flere nettverkstilkoblingsalternativer, og ett av dem må være internettbasert. Forklar hvordan dette fungerer i tilbudet deres eller tilbudet dere representerer.
- 3) **Ressurssammenslåing:** Respondentens CISP må tilby samlede databehandlingsressurser som betjener flere forbrukere ved hjelp av en flerleiermodell med forskjellige virtuelle ressurser som blir dynamisk tildelt og tildelt på nytt i henhold til forbrukernes etterspørsel. Brukeren er i stand til å spesifisere plassering på et høyere abstraksjonsnivå (f.eks. land, region eller datasenterbeliggenhet). Respondenten skal støtte skalering av disse ressursene innen få minutter eller timer etter en forespørsel om klargjøring. Forklar hvordan dette fungerer i tilbudet deres eller tilbudet dere representerer.

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

4) **Rask elastisitet:** Respondentens CISP skal støtte tjenesteklargjørings- og avbestillingsfunksjoner (skalere opp og ned), og gjøre tjenesten tilgjengelig innen minimumstiden (maksimalt «x» timer) etter forespørsel om klargjøring. Respondenten skal støtte faktureringsjusteringer som følge av disse forespørselene om klargjøring på timebasis eller daglig basis.

5) **Målt service:** Respondenten skal tilby innsyn i tjenestebruken via et elektronisk dashbord eller lignende elektroniske midler.

I tillegg må CISP:

- Være en anerkjent leder innen skytjenester som demonstrert av Gartners magiske kvadrant for IaaS.⁵
- Legge frem rapporter fra anerkjente tredjepartsanalytikere som viser CISP-ens dokumenterte evner og pålitelighet.

Til slutt vil CISP-er bli sammenlignet ved hjelp av scenarioene gitt i Tillegg B.

2.2.2.1 Tjenestenivåavtaler (SLA-er)

CISP-er tilbyr standardiserte kommersielle tjenestenivåavtaler til millioner av kunder og kan derfor ikke tilby tilpassede tjenestenivåavtaler som med lokale datasentermødeller. CISP-kundene (ofte med hjelp fra CISP-partnere) utforme bruken av skytjenester slik at de utnytter en CISP's kommersielle tjenestenivåavtaler til å oppfylle og overgå kundespesifikke krav og unike tjenestenivåavtaler.

Skybaserte RFP-er bør sikre at CISP-er tilbyr funksjonene og veiledningen som trengs for å utnytte tjenestene og de kommersielle tjenestenivåavtalene deres, slik at individuelle sluttbrukere kan oppfylle ytelseskrav og tilgjengelighetskrav.

Eksempel på RFP-formuleringer: Tjenestenivåavtaler

Gi informasjon om og lenker til CISP-enes tilnærming til tjenestenivåavtaler (SLA-er, Service Level Agreements).

<ORGANISASJONEN> vil være oppmerksom på CISP-ens tjenestenivåavtaler og implementere viktige arbeidsbelastninger og programmer på en slik måte at de fortsetter å operere i tilfelle en tjenestenivåavtale ikke blir oppfylt.

<ORGANISASJONEN> vil være ansvarlig for å opprettholde passende tjenestenivåavtaler knyttet til alt utstyr eid av <ORGANISASJONEN> eller opererte tjenester til <ORGANISASJONEN> som brukes med CISP-en.

CISP-en bør gi <ORGANISASJONEN> evne til kontinuerlig synlighet og rapportering av sin operasjonelle SLA-ytelse, og dokumenterte anbefalte fremgangsmåter for å utnytte CISP-infrastruktur til å utforme tjenester med henblikk på ytelse, holdbarhet og pålitelighet.

2.2.3 Kontrahering

CISP-vilkårene er utformet for å gjenspeile hvordan en skytjenestemodell fungerer (det blir ikke kjøpt fysiske aktiva og CISP-er opererer i stor skala og tilbyr standardiserte tjenester). Derfor er det avgjørende at vilkårene og betingelsene til en CISP blir innlemmet og utnyttet i størst mulig grad. Se avsnitt 2.5 nedenfor for mer informasjon om vilkår og kontrahering.

2.2.3.1 Nye tjenester og tjenester i endring

CISP-er leverer ytelse gjennom en tjeneste. I motsetning til tradisjonelle lokale løsninger som krever oppgraderinger og servicevedlikeholds kontrakter som utløper, tilbyr skyleverandører bare standardiserte tjenester. For at skymodellen skal oppnå stordriftsfordeler, blir oppgraderinger og endringer i underliggende infrastruktur rullet ut til alle, ikke til individuelle brukere, og kundene velger deretter tjenestene de bruker. Tjenesten er mer sømløs enn lokale systemer, og skyleverandører legger stadig til nye og forbedrede tjenester som kundene kan bruke som de ønsker.

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

Hvis nye eller forbedrede CISP-tjenester ikke kan legges til etter en frist for innlevering av RFP, begrenser offentlige organisasjoner seg fra å kunne benytte seg av nye tjenester og forbedrede funksjoner til neste iterasjon av en rammeavtale blir utgitt. Vi anbefaler derfor på det sterkeste at tilbudet av tjenestene som er beskrevet i rammeavtalen er bredt, slik at det kan legges til nye CISP-tjenester etter innleveringsfristen. EUs anskaffelseslovgivning kan begrense innføringen av vesentlige nye CISP-tjenester som skal legges til rammeavtalen, men oppdateringer og nye versjoner av tjenester som ikke anses som vesentlige endringer, kan legges uten at anskaffelsen blir bestridt.

Eksempel på RFP-formuleringer: Nye tjenester og tjenester i endring

CISP-en skal levere en kostnadseffektiv løsning som bruker både velprøvde, stabile virtualiseringsteknologier og banebrytende teknologier som kontinuerlig oppdateres. <ORGANISASJONEN> erkjenner og godtar at skyteknologier kan leveres til <ORGANISASJONEN> og andre av CISP-ens klienter som delte tjenester fra en felles kodebase og/eller felles miljø, og CISP-en kan fra tid til annen endre, legge til eller slette funksjoner, egenskaper, ytelse eller andre egenskaper ved skytjenestene. Hvis en slik endring, tillegg eller sletting gjøres, skal spesifikasjonene til skytjenestene endres tilsvarende.

*Omfanget til denne leveringsordren inkluderer alle eksisterende og nye eller forbedrede CISP-tjenester **INNENFOR OMFANGET TIL RAMMEVERKET**. CISP-leverte skytjenester som er tilgjengelige for kommersielle kunder skal gjøres tilgjengelige for <ORGANISASJONEN>.*

2.2.3.2 Leverandørbinding/reversibilitet

Skyteknologi reduserer bindinger til leverandører ettersom det ikke kjøpes fysiske aktiva og kunder kan når som helst flytte dataene fra en skyleverandør til en annen.

En viss grad av leverandørbinding er imidlertid uunngåelig ved kjøp av skytjenester: Ikke alle skyer er like, og derfor kan en CISP tilby tjenester og funksjoner som en annen ganske enkelt ikke kan tilby, noe som reduserer muligheten til å bruke slike tjenester hos en annen leverandør. En forsvarlig tilnærming er å kreve at CISP-er tilbyr de nødvendige funksjonene og tjenestene for å forlate skyen deres, med dokumentasjon på hvordan disse tjenestene fungerer som en rimelig «utgangsstrategi» – gitt at det er umulig for en CISP å kjenne til den unike konfigurasjonen av kundens bruk av deres standardiserte tjenester, og som sådan tilbyr en tilpasset utgangsplan.

Se avsnitt 2.3.1.2 for informasjon om bransjenormer som tar opp «dataoverføring» og «skifte av skyleverandører» for å oppfylle krav i EU-forordningen om fri flyt av andre opplysninger enn personopplysninger artikkel 6.

Eksempel på RFP-formuleringer: Påmønstring og avmønstring

<ORGANISASJONEN> ber om forslag som gir en rimelig utgangsstrategi for å forhindre bindinger. <ORGANISASJONEN> kjøper ikke fysiske aktiva, og CISP-en vil gi muligheten til å bevege seg opp og ned på IT-stakken. CISP-en vil tilby overføringsverktøy og -tjenester for å hjelpe til med å migrere til og fra CISP-plattformen og minimere bindinger. Detaljert dokumentasjon for hvordan du bruker CISP-leverte overføringsverktøy og -tjenester, vil tjene som en rimelig utgangsplan.

*CISP-en bør ikke ha **påkrevde** minimumsforpliktelser eller **påkrevde** langsiktige kontrakter.*

Kunden kan når som helst eksportere data som er lagret hos en tjenesteleverandør. CISP-en skal tillate <ORGANISASJONEN> å flytte data på og av CISP-ens lager etter behov. CISP-en skal også tillate at virtuelle maskinbilder lastes ned og overføres til en ny skyleverandør. <ORGANISASJONEN> kan eksportere maskinbildene og bruke dem lokalt eller hos en annen leverandør (underlagt begrensninger for programvarelisensiering).

2.3 Sikkerhet

Ansvar for sikkerhet og samsvar deles mellom en CISP og skykundene. I denne modellen kontrollerer skykunder hvordan de designer og sikrer sine applikasjoner og data på infrastrukturen, mens CISP-er er ansvarlige for å tilby tjenester på en svært sikker og kontrollert plattform, og for å tilby et bredt utvalg av ekstra sikkerhetsfunksjoner. Nivået på CISP og kundeansvar i denne modellen avhenger av skyimplementeringsmodellen (IaaS/PaaS/SaaS), og kundene bør være tydelige med hensyn til deres ansvar i hver modell.

En forståelse av denne delte ansvarsmodellen er avgjørende for å utvikle en vellykket skybasert RFP. Offentlige organisasjoner bør sikre at de vet hva en CISP er ansvarlig for, hva de selv er ansvarlige for, og hvor rådgivende/ISV-partnere og deres løsninger passer inn for å hjelpe.

2.3.1 Minimumskrav

Stikkordet når det gjelder sikkerhet i skyen er **funksjon**. Offentlige organisasjoner bør kreve at CISP-er gir sikkerhetsmulighetene som er nødvendige for å sikre at kundene kan oppfylle sitt ansvar i modellen for delt ansvar. Som det fremgår av den representative kravlisten nedenfor, blir CISP bedt om å tilby en standardisert evne, slik at kunden kan bruke den til å gjøre det unike skymiljøet sitt sikkert.

- **Tilby funksjoner** for nettverksbrannmurer og nettapplikasjoner for å opprette private nettverk og kontrollere tilgang til forekomster og applikasjoner.
- **Tilby alternativer** for tilkobling som muliggjør private eller dedikerte tilkoblinger fra kontoret eller lokalt miljø.
- **Tilby funksjoner** for å implementere en forsvarlig dybdestrategi og hindre DDoS-angrep.
- **Datakrypteringsfunksjoner** tilgjengelig i lagrings- og databasetjenester.
- **Tilby fleksible alternativer** for nøkkeladministrasjon, slik at du kan velge om CISP-en skal administrere krypteringsnøkklene eller gjøre det mulig for kunden å ha full kontroll over nøkler.
- **Tilby API-er** for kunder til integrering av kryptering og databeskyttelse med alle tjenestene som utvikles eller implementeres i et AWS-miljø.
- **Tilby implementeringsverktøy** for implementering for å administrere oppretting og avvikling av CISP-ressurser i henhold til organisasjonens standarder.
- **Tilby verktøy** for lager- og konfigurasjonsadministrasjon som identifiserer CISP-ressurser og deretter sporer og administrerer endringer i disse ressursene over tid.
- **Tilby verktøy og funksjoner** som gjør det mulig for kundene å se nøyaktig hva som skjer i deres CISP-miljø.
- **Muliggjør dyp synlighet** i API-samtaler – inkludert hvem, hva når og hvor samtaler ble foretatt fra.
- **Tilby alternativer** for aggregering av logg, effektivisering av undersøkelser og rapportering om samsvar.
- **Tilby funksjoner** for å konfigurere varslinger når spesifikke hendelser inntreffer eller terskler overskrides.
- **Tilby funksjoner** for å definere, håndheve og administrere brukertilgangsretningslinjer på tvers av CISP-tjenester.
- **Tilby funksjoner** for å definere individuelle brukerkontoer med tillatelser på tvers av CISP-ressurser.
- **Tilby funksjoner** for integrering og forbindelse med bedriftskataloger for å redusere administrasjonsomkostninger og forbedre sluttbrukeropplevelsen.

Flere slike krav finnes i *Tillegg A: tekniske krav for sammenligning mellom budgivere*.

Funksjonalitet utover minimumsstandarden for sikkerhet kan brukes til en mer meningsfull analyse av «verdiøkende alternativer» eller «best verdi» i en RFP. Og jo mer funksjonalitet som er innebygd eller automatisert når det gjelder sikkerhet, jo bedre. Som nevnt, se *Tillegg A: tekniske krav for sammenligning mellom budgivere* for krav til bruk for sammenligning mellom budgivere.

Offentlige organisasjoner bør se på sertifiseringer og evalueringer av skyakkreditering for å sikre at de nødvendige CISP-sikkerhetskontrollene er på plass. For eksempel: Tenk på en CISP som er validert og sertifisert av en uavhengig revisor for å bekrefte samsvar med ISO 27001-sertifiseringsstandard. ISO 27001 vedlegg A, domene 14 fokuserer på de spesifikke kontrollene som en CISP følger i henhold til ISO-krav rundt systeminnsamling, utvikling og vedlikehold. Det er sannsynlig at disse kontrollene dekker flertallet, om ikke alle, kontrollene rundt systeminnhenting, utvikling og vedlikehold som vanligvis blir bedt om av en organisasjon i en IT-relatert RFP. Derfor er det rimelig at en organisasjon krever at en CISP er ISO 27001-sertifisert, fremfor å duplisere innsats og liste opp kontrollkrav angående systeminnhenting, utvikling og vedlikehold i en skybasert RFP.

Denne tilnærmingen til å utnytte tredjeparts samsvarsrapporter kan brukes på de fleste sikkerhets- og samsvarskontroller, for eksempel: CISPE-retningslinjer for GDPR, ISO, SOC, osv.

Eksempel på RFP-formuleringer: Sikkerhet

CISP-en skal gi <ORGANISASJONEN> innsyn i sine ikke-proprietære sikkerhetsprosesser og tekniske begrensninger, slik at tilstrekkelig beskyttelse og fleksibilitet kan oppnås mellom <ORGANISASJONEN> og tjenesteleverandøren.

CISP-en skal oppgi sine roller og ansvar når det gjelder sikkerhet og samsvar:

- *Beskriv sikkerhetsrelaterte roller og ansvar for CISP-en og <ORGANISASJONEN> i det foreslåtte tilbudet. Vær tydelig med ansvarsavgrensningen, og skisser CISP-tjenester for å hjelpe <ORGANISASJONEN> med å bygge og automatisere sikkerhetsfunksjoner i skymiljøet.*
- *Gi svar på de tekniske spesifikasjonene i TILLEGG A relatert til <ORGANISASJONENS> sikkerhetskrav.*

EIERSKAP OG KONTROLL OVER <ORGANISASJONENS> INNHOLD

Beskriv hvordan CISP-funksjoner kan beskytte personvernet til <ORGANISASJONEN>. Inkluder kontrollene som er på plass for å beskytte innholdet til <ORGANISASJONEN>. CISP-en må gi sterk regional isolasjon, slik at gjenstander som er lagret i en region, aldri forlater regionen med mindre <ORGANISASJONEN> eksplisitt overfører dem til en annen region.

- *<ORGANISASJONEN> skal administrere tilgang til innhold, tjenester og ressurser. CISP-en bør tilby et avansert sett med tilgangs-, krypterings- og loggfunksjoner for å hjelpe <ORGANISASJONEN> med å gjøre dette effektivt. CISP skal ikke gå inn på eller bruke innholdet til <ORGANISASJONEN> til noe annet formål enn det som er lovpålagt og for å opprettholde CISP-tjenestene og levere dem til <ORGANISASJONEN> og sluttbrukerne.*
- *<ORGANISASJONEN> skal velge regionen(e) der innholdet skal lagres. CISP skal ikke flytte eller replikere innholdet til <ORGANISASJONEN> utenfor de(n) valgte regionen(e), bortsett fra det som er lovpålagt og nødvendig for å opprettholde CISP-tjenestene og levere dem til <ORGANISASJONEN> og sluttbrukerne.*
- *<ORGANISASJONEN> skal velge hvordan innholdet er sikret. CISP-en må gi sterk kryptering for innholdet til <ORGANISASJONEN> under overføring eller i ro, og gi <ORGANISASJONEN> muligheten til å administrere sine egne krypteringsnøkler.*
- *CISP-en må ha et sikringsprogram for sikkerhet som bruker globalt anbefalte fremgangsmåter for personvern og databeskyttelse slik at <ORGANISASJONEN> kan opprette, betjene og utnytte CISP-ens sikkerhetskontrollmiljø. Sikkerhetsbeskyttelse og kontrollprosesser må valideres uavhengig av flere uavhengige tredjepartsvurderinger.*

Sertifiseringer og evalueringer av skyakkreditering gir organisasjoner i offentlig sektor forsikring om at CISP-ene har effektive fysiske og logiske sikkerhetskontroller på plass. Når disse akkrediteringene er utnyttet i RFP, effektiviserer det anskaffelsesprosessen og hjelper til med å unngå dupliserende, altfor belastende prosesser eller godkjenningsarbeidsflyter som kanskje ikke er nødvendige for et skymiljø.

Skybaserte RFP-er bør gi CISP-er mulighet til å bevise at de stemmer overens med akkrediteringer og evalueringer av samsvar. Som nevnt ovenfor er det betydelig overlapping i risikoscenarioer og risikostyringspraksis på tvers av disse akkrediteringsordningene. Ettersom kontroller og krav er samlet i slike akkrediteringer, er krav til at CISP-er overholder akkrediteringer en raskere måte å behandle samsvar på i en RFP enn å duplisere innsats for å liste opp slike individuelle kontroller (**hvorav mange kan hentes fra tidligere RFP-er som er direkte på lokale datasentre, og som sådan ikke nødvendigvis gjelder databehandling i nettskyen**).

MERK: Det er også veldig viktig å forstå hvordan rapportene nedenfor er tilgjengelige. For eksempel er SOC 1- og SOC 2-rapporter vanligvis sensitive dokumenter. Forstå avtalene som er nødvendige for å få tilgang til dem (f.eks. fortrolighetsavtale), og ikke bare be om at disse dokumentene blir sendt inn som en del av RFP-responsen (slike dokumenter kan bli offentliggjort gjennom innsynskrav etter offentlighetsloven e.l., noe som ville true skysikkerheten).

Eksempel på RFP-formuleringer: Samsvar

Bruk av anerkjente sikkerhets-, samsvar- og driftsstandarter, avledet av beste praksis i skytjenesteoperasjoner – inkludert datahåndtering, datasikkerhet, konfidensialitet, tilgjengelighet osv. – effektiviserer anskaffelsen av skyteknologi.

<ORGANISASJONEN> skal evaluere unike tilbud mot aksepterte sikkerhets-, samsvars- og driftsstandarter som beskrevet nedenfor og i **Tillegg A**. Ved å stole på leverandørens sertifisering av samsvar med hver standard, kan **<ORGANISASJONEN>** bruke minimumssamsvar med standarden som grunnlag for evaluering av forslaget.

Krav om at CISP-en fortsetter å overholde minimumsstandarden i løpet av kontraktens levetid, har den fordelen tjenestesamsvaret holdes oppdatert.

CISP-en bak anbudet (direkte eller gjennom en forhandler) skal kunne demonstrere sin evne til å oppfylle kravene i følgende uavhengige tredjepartsattester, rapporter og sertifiseringer (merk at hvis noen av disse attestene, rapportene og sertifiseringene er underlagt begrensninger grunnet sikkerhetsspørsmål, skal **<ORGANISASJONEN>** samarbeide med CISP-en for å oppnå tilgangen de blir enige om):

Sertifiseringer og attester	Lover, forskrifter og personvern	Retningslinjer og rammeverk
- ISO 27001 (Tyskland) - ISO 27001 etiske retningslinjer for databeskyttelse (GDPR) - CNDP (Climate Neutral Data Centre Pact) - DIACAP - DoD SRG nivå 2 og 4 - HDS (Frankrike, helsetjenester) - FedRAMP - FIPS 140-2 - ISO 9001	- EU's databeskyttelsesdirektiv - EU-modellklausuler - FERPA - GDPR - GLBA	- GDPA - IS - Criminal Justice Info. Service (CJIS) - CSA - EU-US Privacy Shield - EU Safe Harbor

ISO 27001	HIPAA	FISC
ISO 27017	HITECH	FISMA
ISO 27018	RS 1075	G-Cloud [Storbritannia]
RAP [Australia]	TAR	GxP (FDA CFR 21 del 11)
MTCS Tier 3 [Singapore]	PDPA – 2010 [Malaysia]	CREA
PCI DSS Level 1	PDPA – 2012 [Singapore]	T Grundschutz [Tyskland]
EC Rule 17-a-4(f)	PIPEDA [Canada]	MARS – E
BecNumCloud (Frankrike)		
OC1/ISAE 3402	Privacy Act [Australia]	MITA 3.0
OC2/SOC3	Privacy Act [New Zealand]	MPAA
WIPOs retningslinjer for IaaS		
	Det spanske datatilsynets autorisasjon	NIST
	U.K. DPA – 1988	Uptime Institute Tiers
	VPAT/Section 508	UK Cloud Security Principles

Listen ovenfor er kun gitt for illustrasjonsformål og skal ikke betraktes som noen uttømmende liste over sertifiseringer og standarder som kan gjelde for skytjenester.

2.3.1.1 Databeskyttelse

Et vesentlig hensyn ved bruk av skytjenester er at behandlingen av personopplysninger må utføres i samsvar med den gjeldende EU-lovgivningen om personvern, inkludert Personvernforordningen (GDPR). GDPR er en prinsippbasert forordning og gir derfor ikke sektorspesifikk veiledning for å bidra til å sikre samsvar. GDPR oppfordrer imidlertid til å ta i bruk etiske retningslinjer og lignende samsvarsredskaper for å gi slik veiledning. CISPE har i samarbeid med det franske datatilsynet (CNIL) utviklet etiske retningslinjer for databeskyttelse (CISPE-retningslinjene⁶) som støttes av det europeiske Personvernrådet, med generell anvendelse i Europa. Formålet med retningslinjene er å hjelpe CISP-er til å overholde GDPR og veilede kunder i å vurdere om CISP-er er egnet til den behandlingen av personopplysninger som kunden ønsker utført.

- Retningslinjene fokuserer utelukkende på IaaS-sektoren og tar opp de spesifikke rollene og ansvarene til IaaS-leverandører.
- De bidrar til å gjøre det klarere hva rettfærdig og åpen behandling og egnede sikkerhetstiltak innebærer i sammenheng med skyinfrastruktur tjenester (GDPR artikkel 40 [2]).
- De hjelper kunder å forstå hvordan de kan beholde herredømmet over dataene sine ved å sikre at de forblir innenfor EU.
- De fremmer anbefalte fremgangsmåter for databeskyttelse som støtter EUs GAIA-X-initiativ om utvikling av europeiske skydata tjenester.

Når en CISP følger etiske retningslinjer for databeskyttelse, som CISPE-retningslinjene, gir det trygghet for at personopplysninger behandles i strengt samsvar med GDPR.

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

Eksempel på RFP-formuleringer: Databeskyttelse

CISP-en bak anbudet (direkte eller via forhandler) bør kunne demonstrere sin evne til samsvar med etiske retningslinjer for databeskyttelse, f.eks. CISPEs retningslinjer. Retningslinjene for databeskyttelse må være i tråd med kravene som stilles i GDPR-rammeverket. Retningslinjene bør minst omfatte (1) en klar definisjon av CISP-ens roller og ansvar, (2) krav om at CISP-en ikke skal bruke kundedata til markedsførings- eller reklameformål, og (3) at kundene skal kunne velge CISP-tjenester som kun lar dataene bli behandlet innenfor EØS-området. Samsvar med retningslinjene må verifiseres av eksterne, uavhengige revisorer (overvåkingsorganer) autorisert av EUs datatilsyn.

2.3.1.2 Skifte av skyleverandør og overføring av data

Kundene skal ha frihet til å velge skytjenestene de ønsker å bruke, og ikke bli bundet til en CISP eller PaaS- eller SaaS-leverandør.

CISP-leverte skytjenester er standardiserte og tilbys på «en til mange»-basis, med tjenester som konfigureres, klargjøres og kontrolleres av kunden. En fordel ved databehandling i nettskyen er at kundene fritt kan velge de standardiserte tjenestene de måtte trenge til å utvikle sine unike applikasjoner og løsninger. Denne fordelene omfatter også muligheten til å skifte til nye eller forskjellige tjenester som oppfyller kundens behov til enhver tid.

Akkurat som med databeskyttelse kan etiske retningslinjer bidra til å gi kunder trygghet når det gjelder å gå over til skyen fra lokal infrastruktur, eller når de skifter CISP. Sammen med EuroCIO (den europeiske foreningen for IT-ledere) har CISPE vært med på å lede utviklingen av de etiske retningslinjene for dataoverføring og skifte av skytjenester for IaaS-skytjenester (SWIPO sine retningslinjer for IaaS^{7,8}). Den første versjonen av retningslinjene ble utviklet i henhold til EU-forordningen om fri flyt av opplysninger, overrakt EU-kommisjonen i november 2019 under det finske EU-formannskapet og utgitt av foreningen SWIPO AISBL i mai 2020. I april 2021 erklærte SWIPO AISBL de første tjenestene i samsvar med retningslinjene, og i mai 2021 ble de første tjenestene til CISPE-medlemmer erklært i samsvar.

Eksempel på RFP-formuleringer: Skifte av skyleverandør og overføring av data

CISP-en bak anbudet (direkte eller via forhandler) bør kunne demonstrere sin evne til samsvar med etiske retningslinjer for «leverandørskifte og dataoverføring», f.eks. SWIPO sine etiske retningslinjer for IaaS. Retningslinjene må gjøre detaljert rede for hvordan en CISP byr kundene på sikker overføring av forretningsdata hvis de bestemmer seg for å skifte CISP.

2.3.2 Sammenligning mellom leverandører

Som for de tekniske kriteriene i avsnittene ovenfor: I tillegg til minimumssikkerhetskravene i en skybasert RFP, er det viktig å gi kriterier som CISP-sikkerhetsfunksjoner og -tjenester kan sammenlignes med under en konkurranseevaluering.

Se *Tillegg A: tekniske krav for sammenligning mellom budgivere* for eksempler på sikkerhetskrav til CISP-er. Vi anbefaler på det sterkeste at offentlige enheter som vurderer CISP-er, betrakter funksjonene nedenfor som viktige sikkerhetssyn:

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/>

Eksempel på RFP-språk: Viktige sikkerhetshensyn

- *CISP-ens forståelse av modellen for delt ansvar, og dokumentasjon for å hjelpe kunder med å forstå avgrensningen av sikkerhetsansvar for CISP-funksjoner og -tjenester (for eksempel i sammenheng med GDPR)*
- *Påviselig erfaring med CISP-infrastruktursikkerhet, med offentlig tilgjengelig ikke-proprietær dokumentasjon av CISP-sikkerhetsstilling samt fysiske og logiske kontroller*
- *CISP-støtte spesifikt for skysikkerhet*
- *Tjenester som gjør det mulig for kunder å formalisere kontodesign, automatisere sikkerhetskontroll og skystyringskontroll og effektivisere revisjon*
- *Muligheten til å opprette, klargjøre og administrere en samling av ressurser som en mal (inkludert sikkerhetsmaler av gullstandard utviklet av CISP-en eller en CISP-partner)*
- *Muligheten til å etablere pålitelig og repeterbar drift av kontroller*
- *Funksjoner for kontinuerlig revisjon og sanntidsrevisjon*
- *Muligheten til teknisk skripting av retningslinjer for styring i skyen*
- *Muligheten til å opprette tvangsfunksjoner som ikke kan overstyres av brukere som ikke har tillatelse til å endre disse funksjonene*
- *Muligheten til pålitelig implementering av ting som tidligere var nedskrevet i retningslinjer, standarder og forskrifter, sammen med oppretting av sikkerhet og samsvar som er mulig å håndheve, noe som i sin tur skaper en funksjonell og pålitelig styringsmodell i skyen for IT-miljøer*
- *Tjenester for å beskytte mot vanlige DDoS-angrep (distribuerte tjenestenektangrep) på nettverks- og transportnivå, sammen med muligheten til å skrive tilpassede regler for å avverge avanserte angrep på programnivå*
- *Administrert tjeneste for å oppdage trusler*

2.3.3 Kontrahering

Som notert ovenfor er CISP-vilkårene utformet for å gjenspeile hvordan en skytjenestemodell fungerer (det kjøpes ikke fysiske aktiva, og CISP-er driver i massiv skala og tilbyr standardiserte tjenester). Derfor er det svært viktig at vilkårene til en CISP innlemmes og utnyttes så langt som mulig. Se avsnitt 2.5 nedenfor for mer informasjon om vilkår og kontrahering.

Når det gjelder sikkerhet, vil vi nok en gang på det sterkeste anbefale at det tillates at CISP-er kan oppdatere tilbud kontinuerlig, eller at leverandører kan legge til produkter etter innsendingsfristen, så lenge de overholder de opprinnelige parameterne i RFP-en. Dette gjenspeiler det faktum at sikkerhetsfunksjoner og -tjenester utvikles raskt, og CISP-er lanserer sikkerhetsfokusede tjenester ofte, som i mange tilfeller er gratis. Merk at det er viktig å ha et grunnleggende sikkerhetsnivå (se minimumskravene ovenfor), for å garantere at endringer i sikkerhetstilbud ikke reduserer sikkerheten.

Modellen med delt ansvar står selvsagt i sentrum av sikkerheten i en RFP for skytjenester. Hver part må være tydelig på sikkerhetsansvaret sitt, og CISP-er bør pålegges å dokumentere sikkerhetsansvar for seg selv og kundene for skyteknologi levert av dem, sammen med dokumentasjon for å hjelpe kundene med innbygging og automatisering av gode sikkerhetsrutiner.

En rammeavtale for skyen bør være fleksibel nok til å kunne fjerne en leverandør hvis vedkommende ikke lenger overholder minimumskravene for sikkerhet og samsvar, slik de er fremsatt i RFP-en for skytjenester.

2.4 Priser

Når organisasjoner i offentlig sektor skal inngå en kontrakt for skyteknologi som tar høyde for varierende behov, trenger de en kontrakt der de kan betale for tjenester etter hvert som de forbrukes – med nødvendig styring i skyen og synlighet rundt forbruk og utgifter.

Det som er viktig, er at RFP-er for skytjenester må se på verdi og totale eierkostnader (TCO), i motsetning til bare å sammenligne enhetspriser krone for krone. Den tradisjonelle praksisen med å se på laveste enhetspris fungerer ikke for skymodellen, og pleier derfor ikke å gi det mest økonomisk fordelaktige anbudet eller den laveste prisen generelt.

*For hjelp til evaluering av priser fra CISP-er det nyttig å forhåndskvalifisere eller sile ut CISP-er først, med **minimumskrav relatert til pris**, slik at CISP-er med lignende egenskaper kan kvalifisere seg til rammeavtalen. Evalueringsprosessen for løpende ordrer og minikonkurranser kan deretter se på et utvalg av typiske eksempler på skyarkitektur og **prisscenarioer** som samsvarer med vanlige arbeidsbelastninger i offentlig sektor, og få CISP-er til å oppgi pris på dem. Direkte testdemonstrasjoner anbefales også for sammenligning av ytelse og elastisitet for skyteknologitjenester som tilbys av CISP-er. Se Tillegg B for et eksempel på et testskript for demonstrering av skyteknologi.*

2.4.1 Minimumskrav

Prisdelen i en RFP for skytjenester har fire nøkkelementer:

1. **Bruksbaserte priser:** Skykunder bruker en forbruksbasertmodell, der de ganske enkelt betaler for forbruket ved slutten av hver måned, noe som er optimalt for utnyttelses- og ressursmålinger.
2. **Transparente priser:** Priser fra CISP-er skal være offentlig tilgjengelige og gjennomsiktlige.
3. **Dynamiske priser:** Inkluder fleksibilitet for å tillate at skyprisene varierer etter markedsprisen. Denne fremgangsmåten drar nytte av at priser i skyen er dynamiske og konkurranseutsatte, og den støtter innovasjon og prisreduksjoner.
4. **Kontrollert forbruk:** CISP-er bør tilby verktøy for rapportering, overvåking og prognoser, slik at kundene kan (1) overvåke forbruk og utgifter både på totalt og detaljert nivå, (2) få varsler om når forbruket og utgiftene når egendefinerte grenseverdier, og (3) estimere forbruk og utgifter for å kunne planlegge fremtidige budsjetter for skyen.

Eksempel på RFP-formuleringer: Priser

<ORGANISASJONEN> ber om at CISP-ene som svarer, inkluderer en foreslått metode og prismodell for hver tjeneste som tilbys til slutt kunder som en kommersiell skyfunksjon.

CISP-en må levere:

- Et dokument med tjenestedefinisjoner eller koblinger til tjenestedefinisjoner
- Et dokument med vilkår og betingelser
- Et prisdokument (koblinger til offentlige priser kan godtas, så lenge en fullstendig prisliste eller et dokument med priser er tilgjengelig på forespørsel)

Prisen skal være prisen på den vanligste konfigurasjonen av tjenesten. CISP-er må tilby alternativer for volumbaserte rabatter, en priskalkulator for å regne ut den faktiske prisen på det som kjøpes, og den totale verdien som tilbys til kjøperen (for eksempel tjenester for optimalisering og den resulterende kostnadsreduksjonen).

Kjøpere under rammeavtalen kan kontakte leverandører og be dem om å forklare tjenestebeskrivelsen, vilkårene, prisene og dokumentene med eller modellen for priser eller tjenestedefinisjoner. Eventuelle samtaler med leverandører blir tatt opp.

Flere priskrav

- Tilby skyteknologi med en dynamisk prismodell som gir maksimal fleksibilitet, og som støtter skalerbarhet og gir mulighet til vekst.
- Prisattributtene må inkludere følgende:
 - Er prisen oppgitt som behovsbasert, forbruksbasert? Forklar prismodellen deres.
 - Kan kunden få ytterligere rabatt ved å forplikte seg til bruk og/eller kjøpe store kvanta? Forklar nærmere hvordan.
 - Er prisene offentlig tilgjengelige og gjennomsiktede? Inkluder koblinger til offentlig tilgjengelige priser.
 - Er prisene dynamiske, og reagerer de raskt og effektivt på markeds konkurranse?
 - Tilbyr dere gode fremgangsmåter og ressurser for å spore utgifter?
 - Tilbyr dere anbefalte fremgangsmåter og ressurser for kostnadsoptimalisering?

Åpenhet om priser

På grunn av trenden med konstant lavere priser for kommersiell skyteknologi, som et resultat av innovasjon og konkurranse, skal den målte enhetskostnaden for CISP-tjenesten som <ORGANISASJONEN> betaler under rammeavtalen, aldri overskride enhetsprisen fra skyleverandøren som ble publisert på skyleverandørens nettsted og var gjeldende da tjenesten ble forbrukt av kunden.

Budsjettering og faktureringsvarsler/-rapporter

For å demonstrere levering og bruk av skyteknologi skal CISP-er levere verktøy til <ORGANISASJONEN> for å generere detaljerte faktureringsrapporter som viser kostnad fordelt per time, dag eller måned, for hver konto i en organisasjon, etter produkt eller produktressurs eller etter tagger definert av kunden. <ORGANISASJONEN> godtar at <ORGANISASJONEN>, som en del av modellen for delt ansvar i skyen, skal være ansvarlig for bruk av funksjoner og verktøy for budsjettering og fakturering levert av CISP-en for å overholde unike krav til prognoser og rapportering.

- Oppgi informasjon om hvordan <ORGANISASJONEN> kan vise faktureringsinformasjon både på detaljert og oppsummert nivå, visualisere mønstre i forbruk av CISP-ressurser over tid og estimere fremtidig forbruk.
- Oppgi hvordan <ORGANISASJONEN> kan filtrere visning av forbruk/fakturering etter tjeneste, etter koblet konto eller etter egendefinerte tagger brukt på ressurser, og opprette faktureringsalarmer som sender varslinger når bruken av tjenester nærmer seg eller overskrider grenseverdier/budsjetter definert av <ORGANISASJONEN>.
- Oppgi hvordan <ORGANISASJONEN> kan beregne hvor mye den bruker av skytjenester i løpet av en definert tidsperiode, basert på tidligere bruk. CISP-en må tilby et **estimat** over hva <ORGANISASJONENS> CISP-faktura vil lyde på, og <ORGANISASJONEN> må kunne bruke alarmer og budsjetter for forventede beløp, for å oppnå bedre styring over kostnader og forbruk.

2.4.2 Sammenligning mellom leverandører

Organisasjoner i offentlig sektor krever ofte konkurranse mellom budgivere der de bruker evalueringsvilkår som beste verdi, mest økonomisk fordelaktige anbud eller laveste pris. Under planlegging av priser for løpende ordrer og minikonkurranser i rammeavtalen er det viktig å utvikle en tilnærming som tar hensyn til skyens unike egenskaper. Forstå for eksempel at det å sammenligne poster mellom skyleverandørers tilbud (f.eks. databehandling eller lagring) ikke er en effektiv måte å sammenligne på, siden det ikke tar hensyn til funksjoner som ytelse, kostnadsoptimalisering ved hjelp av tjenester utviklet for nettsky og CISP-overvåkingsverktøy eller differensieringstjenester som CISP kan tilby gratis. Katalogprisen til en CISP kan i tillegg bestå av tusenvis av elementer, og prismodellene kan variere fra tjeneste til tjeneste og fra leverandør til leverandør.

Analyse av totale eierkostnader

Vi anbefaler å fokusere på totale eierkostnader (TCO) for definerte brukstilfeller, som tar hensyn til alle aspekter ved en skyløsning (inkludert partnertjenester, standardiserte CISP-rabatter, tekniske funksjoner som kan øke ytelse og redusere/optimalisere kostnader osv.).

Sammenligning av scenarioer

Evalueringsprosessen kan også vurdere de vanlige scenarioene som tilsvarer vanlige systemer eller programmer. Slike scenarioer (for eksempel vertstjenester på nettet eller implementering av et personalsystem med x antall brukere osv.) kan inkludere variabler som hastighet til og omfang av ressurser, ytelsen til programmet eller løsningen, minnetilgangstider, komplekse data med lavt volum sammenlignet med enkle databehandlingsoppgaver med høyt volum osv. Programmene eller systemene kan også ha typiske scenarioer, for eksempel behandling av mange avgiftsrapporter og katastrofevarsler, for eksempel flomvarsler. Scenarioene må være omfattende nok til å inkludere omfanget av teknologi og tjenester som kundene kan bruke under prosjektet. På denne måten kan kunden sammenligne den estimerte totale kostnaden for prosjektet.

Økonomisk og teknisk sammenligning av scenarioer

Det er også viktig å ta hensyn til tekniske fordeler ved sammenligning av priser mellom CISP-tilbud. En CISP kan for eksempel tillate at kundene bygger en aktiv topologi for nødgjenoppretting, takket være modellen der datasentre er plassert i grupper innen en geografisk region. En CISP som ikke har denne typen konfigurasjon av redundans og datasenter, kan være x % dyrere gitt kostnaden ved å regne inn behov for nødgjenoppretting. Som et eksempel på hvorfor en helhetlig tilnærming til priser som inkluderer ekstra tekniske funksjoner, er viktig under evaluering av CISP-er, kan du se på alternativet nedenfor som en enkel sammenligning av to likeverdige alternativer.

Eksempel: En kunde ønsker å sammenligne prisen på objektlagring som tilbys av kvalifiserte CISP-er i en rammeavtale. Prisen på elementet «lagringsenhet» fra CISP 1 er € 0,023/GB. Prisen på samme «enhet» fra CISP 2 er € 0,01/GB. I en enkel sammenligning mellom enheter stiller ikke kunden kritiske spørsmål som følgende:

1. Hvor mange redundante eksemplarer av objektet er tilgjengelig hvis det oppstår en feil? I eksemplet ovenfor kan CISP 1 opprettholde driften ved samtidig tap av data på to ulike anlegg, og de beholder flere kopier av dataene. For CISP 2 blir ikke redundante kopier opprettholdt.
2. I hvilken grad beholdes lagrede objekter? For CISP 1 er det 99,999999999 %, for CISP 2 er det 99 %.
3. Ta hensyn til kostnaden gjennom hele eierskapet av prosjektet eller arbeidsbelastningen totalt sett og hvordan funksjoner for kostnadsoptimalisering kan redusere kostnader når det gjelder hvordan data lagres og brukes (for eksempel kan mer bruk av de serverløse funksjonene til en CISP redusere kostnadene med x %).

Dette er bare noen av de mange tekniske hensynene som spiller inn i prissettingen, spesielt relatert til sikkerhet og samsvar.

Hensyn ved prising av scenarioer omfatter:

Basissatser – dette er i hovedsak de offentlige prisene fra CISP-er. CISP-er må tilby disse prisene offentlig. Som nevnt ovenfor kan imidlertid kunder, for å sammenligne CISP-er effektivt, be om at alle leverandørene oppgir pris på kanskje 3–5 spesifikke scenarioer (alt etter hva kunden foretrekker). Scenarioene må være omfattende nok til å inkludere hele utvalget av tjenester og teknologi som kunden sannsynligvis kommer

til å bruke så lenge prosjektet varer. På denne måten kan kunden sammenligne den estimerte totale kostnaden for prosjektet. Sammenligninger foretatt på budsjettpost/SKU-nivå er ofte mer problematiske enn nyttige for kunder og leverandører (kunder må sammenligne titusenvise av budsjettposter for alle CISP-er, og leverandører må oppgi alle disse detaljene og administrere dem, selv om den faktiske prisen bare fastsettes basert på forbruk av tjenesten).

Evaluering av en CISP-ers overordnede funksjoner er et must for skykunder som ønsker å få best mulig valuta for pengene. CISP-er kan for eksempel ha tjenester som enten er gratis eller bortimot gratis, og en evaluering av priser må ta hensyn til slike tjenester og at andre CISP-er kanskje tar betalt for lignende funksjonalitet.

Evalueringskriterier kan skrives på en slik måte at CISP-er kan fremvise tjenester som er inkludert som standard, og hvordan slike tjenester virker inn på de totale kostnadene. Evalueringskriterier kan også se til CISP-enes volumbaserte/lagdelte priser og kommersielt tilgjengelige rabatter, for eksempel reservert forekomst/spot-forekomst. For eksempel:

- x % besparelse hvis kundene kjøper reservert databehandlingskapasitet (1 år, 3 år osv.)
- x % rabatt på lagdelte eller volumbaserte priser
- x % besparelse basert på gjennomgang av arkitektur og optimalisering av infrastruktur, for eksempel at man skifter til databehandlingsalternativet som passer best
- Som nevnt ovenfor må du ta hensyn til hele levetidskostnaden og hvordan funksjoner for kostnadsoptimalisering kan redusere kostnader

PRISSCENARIOET

Budgivere må oppgi priser for scenarioet nedenfor til evalueringsformål. Den faktiske prisen vil være basert på forbruket av tjenester og en behovsbasert modell der det betales per bruk.

Nedenfor vises representative krav for registrering av pris, med eksplisitt forståelse av at disse nominelle kravene kan endres så lenge kontrakten varer. Oppgi priser både for 12 og 36 måneder behovsbasert og 12 og 36 måneder med reservert kapasitet.

Oppgi:

- Navn på foreslått(e) løsning(er):
- Budgiverens beste priser:
- Tjenestetid: 24 x 7 x 365
- Tjenestetilgjengelighet: 99,95 %

Prisscenarioer kan også inkludere eksempler fra eksisterende kunder med lignende arbeidsbelastning som har optimalisert forbruket over 1/2/3 år – via bruk av CISP-verktøy for overvåking og optimalisering, innføring av optimaliserte løsninger utviklet for nettsky og via prisreduksjoner fra CISP-er.

2.5 Oppsett og vilkår og betingelser for kontraktutførelse

Skyteknologi og drift som leveres av en CISP, er standardisert med hensikt, og derfor er også vilkårene i kontraktene standardisert. Det er imidlertid mulig å justere disse kontraktene marginalt for å tilpasse dem etter lokale lover og forskrifter.

Tradisjonelle IT-innkjøpsmetoder omfatter ofte strenge regler som krever at søkerne overholder mange eller alle kravene til innkjøpet, eller det avvises. Det kan også være snakk om et strengt undersett med obligatoriske krav. Når denne typen utsilingsmetode brukes sammen med skyteknologi, som egentlig er et sett med standardiserte komponenter og verktøy som hjelper deg med å skissere en egendefinert løsning, pleier innkjøp å mislykkes.

2.5.1 Vilkår og betingelser

Det første trinnet når det gjelder å inngå kontrakt i en RFP for skytjenester er å gå gjennom og forstå eksisterende kommersielle vilkår fra CISP-en, som i mange tilfeller er offentlig tilgjengelig på CISP-nettsteder. Enheter i offentlig sektor godtar stadig oftere de kommersielle vilkårene fra CISP-er. En del av innsatsen for å forstå vilkårene handler om å møte CISP-ene og deres partnere for å se på tilnærmingene mer detaljert. Det viktigste spørsmålet å stille er «hvorfor» CISP-er opererer med spesifikke vilkår. Noen av disse vilkårene kan virke annerledes enn tradisjonelle IT-vilkår, men det er svært bestemte grunner til at de er en del av en skykontrakt. Hvis de offentlig tilgjengelige vilkårene ikke kan godtas, har CISP-er ofte avtaler som kan modereres litt for virksomhetskunder, og det kan være verdt å se nærmere på disse.

I tillegg til å gjennomgå CISP-ers vilkår og betingelser, er det viktig å forstå eksisterende retningslinjer, forskrifter og/eller lover (f.eks. de som involverer teknologi, dataklassifisering, personvern, personell, etc.). Ofte finnes det eksisterende retningslinjer, forskrifter eller lover som er utviklet for kjøp og bruk av tradisjonelle IT-tilbud, og de kan være på kant med en CISP-ers modell. Dette kan for eksempel være å kun tillate bruk av skyteknologi som var inkludert i det opprinnelige rammeavtalebudet via RFP-en for skytjenester. CISP-er legger stadig vekk til nye tjenester og nye funksjoner. Begrensning av tilgang til disse nye tjenestene bare fordi du følger en tradisjonell tilnærming til oppdatering av IT-produkter gir ingen mening for sluttkunden. Hvis dette er tilfelle, er det viktig å ha grundige diskusjoner med CISP-er der man ser nærmere på disse retningslinjene, forskriftene og/eller lovene.

Dra fordel av diskusjoner i forkant av RFP

Som nevnt ovenfor, før man utarbeider en RFP bør man ta seg tid til å møte CISP-er og relaterte leverandører for å forstå deres vilkår og betingelser og for å opplyse dem om enhetens tilnærming, retningslinjer, forskrifter og lover. Den viktigste delen av disse diskusjonene er at begge sider lærer «hvorfor» de relevante vilkårene fungerer slik de gjør. Vilkår og betingelser i nettskyen er for eksempel forskjellige fra vilkårene for et tradisjonelt datasenter, administrerte tjenester, maskinvare, krympepakket programvare og systemintegrering. Siden dette er enkeltstående modeller og involverer konstant innovasjon, krever forretningsmodellene at RFP-prosessen er så fleksibel at det er mulig med forhandlinger eller diskusjoner for tydeliggjøring.

Ved å inkludere muligheten til å klargjøre vilkår og betingelser gjennom diskusjoner eller forhandlinger, får organisasjoner i offentlig sektor større forståelse av skymodeller og unngå problemet med å avvise leverandører som faktisk kan oppfylle organisasjonens behov. En typisk prosess er at organisasjonen identifiserer enkelte vilkår på forhånd som de ønsker å diskutere og forhandle om, før de inngår en avtale. Ved å forhandle om akseptable vilkår med budgiverne på forhånd kan organisasjonen sørge for at de inngår en avtale med budgiveren som passer best, og at de håndterer uoverensstemmelser som ellers kunne ført til avvisning av et gyldig forslag. Enheter i offentlig sektor kan også se gjennom sine retningslinjer, forskrifter og lover, og begge sider kan få en forståelse av hvordan bruk av skyen passer inn i disse modellene. Som regel finnes det metoder for å arbeide med de eksisterende klausulene. Hvis det er et område som er problematisk, kan imidlertid begge teamene samarbeide for å finne en løsning (det er best å ha disse diskusjonene i god tid før en RFP og påfølgende kontraktsforhandlinger).

Fleksibilitet ved forhandlinger

For å kunne signere kontrakter i overensstemmelse med det lokale lovverket og samtidig basere seg på standardiserte kontraktmessige vilkår fra CISP-en, anbefales følgende: (1) be om en standardkontrakt fra søkerne, (2) ikke vedta upassende kontraktsbetingelser når rammeavtalen for RFP-en for skytjenester settes opp, og (3) gi mulighet til forhandlinger om alle bestemmelsene i rådslagningen og forslagene som leder frem mot rammeavtalen (selvsagt bortsett fra obligatoriske klausuler som ligger fast i lovverket).

Obs! Graden av delt ansvar ligger innebygd i skymodellen og må gjenspeiles i vilkårene i kontrakten (CISP-en bekrefter for eksempel at kundene eier sine egne data der de befinner seg, og tilbyr verktøy for å sørge for at valget av dataplasseringer er begrenset, **MEN** det er kundens eller partnerens ansvar å bruke disse verktøyene).

*Merk at det er viktig at det finnes **separate sett med vilkår og betingelser** for kontrakter for hvert parti med tjenester i en rammeavtale for skyen. En ensartet tilnærming til kontrahering for alle tjenester medfører problemer med teknisk gjennomførbarehet og kompatibilitet.*

Som allerede nevnt utgjør RFP-er som inkluderer obligatoriske vilkår som det ikke kan forhandles om, strengt tatt et forslag som tilbydere må godta som det er, og dette kan gjøre at et ellers akseptabelt forslag blir avvist. Organisasjoner i offentlig sektor bør nøye vurdere konsekvensene av å bruke obligatoriske vilkår, **med mindre loven krever det**. Organisasjoner må være sikre på behovet for et obligatorisk krav eller vilkår fordi utfallet av fremtidige forhandlinger allerede kan være gitt på grunn av klassifiseringen som obligatorisk. Bruken av obligatoriske krav eller vilkår må holdes på et absolutt minimum, slik at organisasjonen er fleksibel nok til å skaffe seg den beste teknologien og løsningen.

Merk at skyteknologi fra CISP-er er fullstendig standardisert, og den leveres på en helautomatisk måte. En CISP kan derfor ikke endre vilkår og betingelser som ville krevd underliggende tilpasning av tjenestene. Videre er prisene på tjenestene som regel offentlige og standardiserte for alle brukere, noe som betyr at en CISP ikke kan justere priser for å kalkulere for mer risiko på vegne av en bestemt kunde.

Indirekte kjøp

Et alternativ til å kjøpe skyteknologi direkte fra en CISP, er å kjøpe fra en CISP-forhandler i stedet. Du finner mer informasjon om CISP-forhandlere i avsnitt 2.1.3 ovenfor.

Eksempel på RFP-formuleringer: Vilkår og betingelser

CISP-er eller representative leverandører må oppgi sine offentlig tilgjengelige vilkår og betingelser og gi tilbakemelding på viktige vilkår og betingelser oppgitt av <ORGANISASJONEN>.

<ORGANISASJONEN> har til hensikt å inngå en skriftlig kontrakt med budgiveren som vinner anbudet, basert på budgiverens kontraktsvilkår. Budgiveren må oppgi et sett med foreslåtte kontraktsvilkår som <ORGANISASJONEN> kan gå gjennom, og som representerer det beste kommersielle og juridiske tilbudet den har å gi. Tilbyderne og <ORGANISASJONEN> kan diskutere begge settene med vilkår og betingelser under <DISKUSJONS/FORHANDLINGS>-fasen.

- *Hovedvilkårene på høyt nivå i rammeverket består som regel av følgende komponenter:*
 - *Varigheten til rammeverket*
 - *Styringen av rammeverket*
 - *Ytelse i rammeverket*
 - *Opphør av rammeverket*

- Omfanget til rammeverket
- Bestillingsprosessen
- Konfidensialitetsforskrifter
- Kategorispesifikk IP og informasjon
- Minimale tekniske krav som må oppfylles av CISP-er – f.eks. kvalitetsstandarder, akkreditering, sikkerhet og databeskyttelse

- **Det vil være ulike vilkår for hver av tjenestene i rammeavtalen**
- Spesifikk informasjon fra CISP-er om tjenestene kan vurderes og håndteres under den løpende ordren.
- Tillat kontraktsendringer – vilkårene bør ikke begrense kunder og leverandører fra å bli enige om kontraktsendringer for å skru på nye tjenester eller forbedringer. Skytjenester er i stadig utvikling, så forbedringer av tjenestene vil bli løpende tilgjengelig. Alt dette kan bidra til å levere effektivitet til kundene.
- Tjenestenivåavtaler (SLA-er) bør ikke være spesifisert av kunden. Kundeavtaler bør ikke definere bestillingsspesifikke, skreddersydde tjenestenivåavtaler som er forskjellige fra CISP-enes standardmodeller for levering av tjenester. Ved å gå med på CISP-enes standard tjenestenivåavtaler, kan CISP-ene holde kostnadene nede og la kundene nyte godt av dette, samtidig som kundene kan føle seg trygge på at CISP-en oppfyller avtalen.
- Ansvarsbegrensningene bør være forholdsmessige. Erstatningsansvaret bør stå i forhold til tjenestene som kjøpes, og det bør ikke settes uforholdsmessig høye tak på ansvar. Hvis takene er uforholdsmessig høye, kan det avskrekke CISP-er fra å godta prosjekter med lav verdi. Disse prosjektene fungerer ofte som en nyttig introduksjon og «testsak» kundene kan bruke til å avgjøre om bestemte skyløsninger er effektive for organisasjonen.
- Kundene bør eie sine egne data. Kundene bør styre og eie sine egne data og kunne bestemme hvor de skal oppbevares geografisk. Dermed unngår kundene binding til leverandøren, og de kan fritt flytte data til nye leverandører.

2.5.2 Vilkår og betingelser for programvare

Selv om denne håndboken fokuserer på innkjøp av IaaS- og PaaS-skyteknologier som leveres av en CISP, er det viktig å fremheve villkår og betingelser for programvare som organisasjoner i offentlig sektor kan vurdere når de kjøper programvare fra leverandørene. Se Figur 1 (side 5) for å repetere hvordan programvare kjøpes som del av en velstrukturert RFP for skytjenester.

Programvare spiller en kritisk viktig rolle i nesten alle virksomheter, også i offentlig sektor. Når forpliktelser som f.eks. vilkår og betingelser for programvarelisensiering tas med i en RFP for skytjenester, bidrar det til å sikre at enheter i offentlig sektor får best verdi og har frihet til å velge leverandører når de kjøper programvare.

Se de ti prinsippene for rettferdige programvarelisenser for skykunder⁹ for mer informasjon. Prinsippene er utviklet av Cigref¹⁰, en forening for store franske selskaper og offentlige myndigheter som representerer brukerne av digital teknologi, i samarbeid med CISPE og med støtte fra andre europeiske bransjeforeninger for IT-ledere og leverandører, for å hankses med metoder som begge foreningene betrakter som skadelige for den digitale fornyelse i organisasjoner av alle størrelser som flytter til skyen.

Eksempel på RFP-formuleringer: Programvare

<ORGANISASJONEN> har til hensikt å inngå en skriftlig kontrakt med budgiveren som vinner anbudet, basert på budgiverens kontraktsvilkår. Budgiveren må oppgi et sett med foreslåtte kontraktsvilkår som <ORGANISASJONEN> kan gå gjennom, og som representerer det beste kommersielle og juridiske tilbudet den har å gi. Tilbyderne og <ORGANISASJONEN> kan diskutere begge settene med vilkår og betingelser under <DISKUSJONS/FORHANDLINGS>-fasen.

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

¹⁰ <https://www.cigref.fr/>

Krav 1.0. Programvareleverandører <u>må</u> by på klare lisensvilkår, herunder en kostnadsanalyse i sammendrag og på detaljnivå. Krav 1.1. Alle gebyrer for eventuelle brudd på lisensvilkårene <u>må</u> oppgis i sammendrag og på detaljnivå.
Krav 2.0. Programvarelisenser <u>må</u> gi <organisasjonen> muligheten til å migrere den lisensierte programvaren fra lokal bruk til selvvalgt sky, uten krav om kjøp av separate, dupliserte lisenser for samme programvare. Krav 2.1. Programvarelisenser <u>må</u> være frie for lisensrestriksjoner og økte kostnader som innskrenker <organisasjonens> evne til å kjøre den lisensierte programvaren i den selvvalgte skyen.
Krav 3.0. Programvarelisenser <u>må</u> tillate <organisasjonen> å kjøre den lisensierte programvaren både på sin egen maskinvare (typisk kalt «lokal» programvare) og i selvvalgt sky.
Krav 4.0. Programvarelisenser <u>må ikke</u> kreve at den lisensierte programvaren kun skal kjøre på maskinvare dedikert kun til <organisasjonen>.
Krav 5.0. Programvareleverandører <u>må ikke</u> straffe <organisasjonen> hvis leverandørens lisensierte programvare brukes på skytilbudet til en annen leverandør, for eksempel ved å legge inn rettigheter til å foreta økte eller påtrengende programvarerevisjoner eller illegge høyere lisensgebyrer.
Krav 6.0. Katalogprogramvare <u>må</u> støtte åpne standarder for synkronisering og autentisering av brukeridentiteter på en ikke-diskriminerende måte med andre identitetstjenester.
Krav 7.0. Programvareleverandører <u>må ikke</u> ta forskjellig pris for den samme programvaren kun basert på hvem som eier maskinvaren den er installert på. Krav 7.1. Priser på programvare <u>må ikke</u> diskriminere mellom programvare som er installert i <organisasjonens> eget datasenter, i et datasenter som administreres av en tredjepart, på datamaskiner som leases av en tredjepart eller hos skyleverandøren <organisasjonen> velger.
Krav 8.0. Under kontraktperioden <u>må ikke</u> programvareleverandører gjøre vesentlige endringer i lisensvilkår som forhindrer <organisasjonen> fra bruk som har vært tillatt tidligere, med mindre loven eller sikkerhetshensyn krever det.
Krav 9.0. Programvareleverandører <u>må ikke</u> villedende <organisasjonen> ved å fremstille det som om programvarelisensene vil dekke <organisasjonens> tiltenkte bruk av programvaren som skissert i <organisasjonens krav>, selv om det kan bli nødvendig å kjøpe ytterligere lisenser for å dekke slik bruk.
Krav 10.0. Hvis <organisasjonen> har rett til å videreselge og overføre programvarelisenser, <u>må</u> programvareleverandørene fortsette å tilby support og oppdateringer på rettferdige vilkår til <organisasjonen> som har kjøpt en videresolgt lisens lovlig.

2.5.3 Hvordan velge mellom tildelte per prosjekt

Enheter i offentlig sektor som er en part i rammeverket, kan bestille eller lage en løpende ordre på tjenestene de trenger, når de trenger dem. En kontrakt med løpende ordrer i rammeavtalen gjør det mulig for kjøpere å forbedre kravene med ytterligere funksjonell spesifisering for en løpende ordre, samtidig som de beholder fordelene som tilbys under rammeavtalen.

Hvis det anses nødvendig, kan det avholdes en minikonkurranse for å identifisere den beste leverandøren for en bestemt arbeidsbelastning eller et bestemt prosjekt. En minikonkurranse er når en kunde øker konkurransen i rammeverket ved å invitere alle leverandører av en tjeneste til å svare på et sett med krav. Kunden vil invitere alle aktuelle leverandører av tjenesten til å gi anbud, derav viktigheten av minimumskrav for tildelte på en skybasert RFP. Dermed sikres det høy standard på alternativene innen hver tjeneste.

Legg nok en gang merke til at det er viktig at det finnes særskilte sett med vilkår og betingelser i kontrakten for hver av tjenestekategoriene som inngår i tilbudstypen (f.eks. offentlig IaaS/PaaS, lokal IaaS/PaaS, privat IaaS/PaaS), siden en ensartet tilnærming til kontrahering for alle tjenester medfører problemer med teknisk gjennomførbarhet og kompatibilitet.

Se avsnitt 2.1.4 for eksempel på RFP-formuleringer når det gjelder valg mellom de tildelte.

2.5.4 Påmønstring og avmønstring

En vurdering å ta hensyn til når du skal sette opp en rammeavtale for skyen, er muligheten til å inkludere et dynamisk innkjøpssystem (DPS, Dynamic Purchasing System). Med en DPS-modell får alle leverandører som oppfyller minimumskravene i rammeavtalen, tilgang til rammeverket. Det er ingen hard grense for antall leverandører som kan bli med i rammeverket, og i motsetning til den tradisjonelle rammemodellen kan leverandører også søke om å bli med i «DPS-rammeverket» når som helst i løpet av levetiden.

Vi anbefaler på det sterkeste at enheter innen offentlig sektor setter høye standarder for å sørge for kvalitet og sikker levering av tjenesten fra kvalifiserte leverandører, men uten å være for spesifikke og diskvalifisere CISP-er på en måte som ikke gir rettferdig konkurranse. Målet er til syvende og sist å unngå at sluttbrukeren blir overveldet av for mange alternativer, men at den tilgjengelige skyteknologien skal holde høy standard.

3.0 anbefalte fremgangsmåter og nyttig lærdom

Nedenfor fremhever vi litt nyttig lærdom om hvordan en vellykket rammeavtale kan inngås med en velskrevet RFP for skytjenester.

3.1 Skyadministrasjon

Administrasjon i skyen er et delt ansvarsområde. CISP-er tilbyr funksjoner og tjenester for å bygge inn skyadministrasjon i alle aspekter i et skymiljø, mens kundene tar med seg sine egne standarder for skyadministrasjon og finner ut hvordan selve skyen muliggjør skyadministrasjon.

I skyen kan kundene bygge IT-miljøet de ønsker, fremfor bare å administrere det de har. Med skyen kan kundene gjøre følgende: (1) starte med en full beholdning av alle IT-ressurser, (2) administrere alle disse ressursene sentralt og (3) opprette varsler for forbruk/fakturering/sikkerhet osv. Alle disse vitale fordelene i skyen bidrar til at kundene kan ha en optimalisert, og så langt det er mulig, automatisert arkitektur, uten behov for stadig vekk å kjøpe og installere ny maskinvare. Dette tar CISP-en seg av, slik at kundene kan bytte fokus fra administrasjon av infrastruktur til det bedriftskritiske driftsnivået.

Det er nyttig å se på en CISP-sky essensielt som en svært stor API. Enten du lanserer en ny server eller endrer en sikkerhetsinnstilling, foretar du bare API-kall. Enhver endring i miljøet loggføres og registreres (hvem, hva, hvor og når for hver endring lagres). Dette gir et nivå av administrasjon, kontroll og synlighet som bare er mulig i et skymiljø. Det gjør at kundene kan tenke nytt om sine eksisterende IT-styringsmodeller og finne ut hvordan dette kan strømlinjeformes og forbedres, gitt fordelene som skyen medfører.

Skyadministrasjon kan også bety kommunikasjon og innlemming av de positive prosessendringene og nye kompetansesettene som skyen medfører. Eksempel: Prosjektledere er vant til å vente i månedsvis på at et IT-miljø blir utbygd, og de kan derfor overestimere planer for å opprette et utviklings- eller testmiljø i skyen betydelig (med skyen kan dette ta bare noen få minutter). Tilpassing til denne nye smidigheten vil være en utviklingsprosess som skjer fra program til program. Slik nyttig lærdom bør deles, slik at en rammeavtale for skyen kan fortsette med å utvikle seg slik at kravene passer perfekt til nye prosesser og ny smidighet.

3.2 Budsjetter for skyen

Når det gjelder hvordan forbruksbaserte skypriser passer med krav til innkjøp og budsjettering i offentlig sektor, har vi oppdaget at det hjelper å knytte sammen CISP-tjenester til en enkelt budsjettpost (databehandling, lagring, nettverk, database, IoT osv.), under budsjettposten **skyteknologi**. Denne tilnærmingen gir nok fleksibilitet til å kunne tilby all nåværende og nye CISP-teknologi til brukere i sanntid, og brukerne får rask tilgang til ressursene de trenger, når de trenger dem. En slik tilnærming tar også høyde for varierende behov, noe som i sin tur bidrar til optimalisert utnyttelse og lave kostnader.

Organisasjoner i offentlig sektor kan legge til flere poster for bestillinger fra andre partier i et skyrammeverk, hvis de trenger rådgivende, profesjonelle eller administrerte tjenester, programvare fra en markeds plass, skysupporttjenester og opplæring i CISP-ens tilbud.

Ekstra kontraktfleksibilitet kan tilbys ved å legge inn valgfrie kontraktposter i aktuelle ressurskategorier for å legge til rette for fremtidig vekst. Alternativt, hvis en organisasjon ønsker å knytte skyteknologier sammen med rådgivende, profesjonelle og administrerte tjenester til én budsjettpost, kan det gjøres f.eks. med posten «skyteknologier og hjelpearbeid».

Nedenfor vises et eksempel på denne tilnærmingen. I eksemplet nedenfor tilsvarer hver enhet i posten «#1001 – Skyteknologi» € 1,00 i forbruk av «skyteknologi». Hver måned kan tillegg til bestillingen finansieres basert på nåværende og estimerte forbruksprognoser.

Tabell 3: Eksempel på prisstruktur med én post.

POST NR.	PRODUKTER/TJENESTER	ANTALL	ENHET	ENHETSPRIS	BELØP
1001	Skyteknologi	1000	Per stykk	€ 1	€ 1000
1002	Konsulenttjenester	1	Per uke	€ 3000	€ 3000
1003	Støtte for skytjenester	1	Per måned	€ 1000	€ 1000
1004	Opplæring knyttet til skytjenester	1	Per dag	€ 3,00	€ 3000
1005	Markeds plass for skytjenester	10	Per stykk	€ 10	€ 100

Her er et eksempel på hvordan denne strukturen kan fungere: En organisasjon innen offentlig sektor engasjerer seg med en CISP for å estimere mengden skyteknologitjenester organisasjonen kommer til å bruke. Organisasjonen godtar vilkårene fra leverandøren, for eksempel € 10 millioner over 5 år, som utgjør € 2 millioner per år. Organisasjonen avsetter det første årlige beløpet på € 2 millioner. Hver måned får de en faktura, og pengene trekkes fra midlene for å betale den. Kontoen blir trukket for beløpet. De resterende midlene overvåkes for forbruksfrekvens ved hjelp av CISP-verktøy for overvåking og prognoser. Hvis det er lite midler igjen, ber organisasjonen om flere midler fra økonomisk ledelse, som kan avsettes for å opprettholde tjenestene.

Eksempel på RFP-formuleringer: Priser – kontrahering

BETALINGSVILKÅR

Betalingsvilkårene må struktureres tilsvarende for å betale kun for ressursene som brukes av <ORGANISASJONEN>, som angitt nedenfor:

1. Månedlig betaling skal være basert på faktisk forbruk av tjenestene og i henhold til CISP-ens offentlig tilgjengelige priser.

MINIMUMSGARANTI OG MAKSIMALT FORBRUK

Siden det er umulig for <ORGANISASJONEN> å fastslå nøyaktig hvor mye av ressursene til en skytjenesteleverandør de vil bruke i løpet av en gitt tidsperiode, blir ordrene spesifisert som antall enheter til fast pris for en enkelt bestillingspost for «skyteknologi».

Hver enhet av den bestilte posten utgjør en verdi på <€ 1,00> av den bestilte skyteknologien. Trinnvise bestillinger legges inn regelmessig via endring av diverse størrelser i denne bestillingen, slik at <ORGANISASJONEN> får fleksibilitet til å forhåndsbestille diverse mengder av CISP-ens skyteknologi målt i euro, basert på estimert forbruk for behov av ulik varighet. Mengdene forhåndsbestilles regelmessig av <ORGANISASJONEN> med beløp som er store nok til å dekke den estimerte kostnaden for skyteknologi som brukes til å oppfylle varierte behov.

Post nr.	Beskrivelse	Ant.	Enhet	Pris
01	CISP-skyteknologi	1000	Per stykk	€ 1000,00

MINIMUMSBESTILLING OG TRINNVIS BESTILLING

Det legges regelmessig inn bestillinger på diverse mengder av <10 000> budsjettpostenheter basert på <ORGANISASJONENS> estimerte bruk av skyteknologi. Denne ordningen gir <ORGANISASJONEN> fleksibilitet til å forhåndsbestille <10 000> enheter skyteknologi etter behov for å støtte virksomheten og følge forretningspraksisen for databehandling i nettskyen med forbruksbasert betaling.

Et første tillegg på <100 000> enheter til en pris av <€ 100 000> bestilles når den løpende ordren legges inn. Minimum totalt antall postenheter som kan legges inn i én trinnvis ordre, ved bruk av én eller flere poster, er <x>. Det maksimale antallet enheter som kan bestilles under leveringsordren, kan ikke overskride <x>, men dette er under forutsetning av at verdien i den løpende ordren aldri overskrides når den kombineres med alle tidligere bestilte enheter. <ORGANISASJONEN> har ansvar for å sørge for at alle bestillinger er innenfor grensene som er spesifisert i dette avsnittet.

MAKSIMAL BESTILLINGSVERDI

Den maksimale bestillingsverdien er <x> og består av opptil <x> enheter under én post til en pris av <x> per enhet. Verdien er basert på et estimat over <ORGANISASJONENS> behov i ytelsesperioden, men er ikke garantert.

3.3 Forstå partnerens forretningsmodell

Enheter i offentlig sektor bør gå inn for å forstå modellene som CISP-er bruker til tilbudene sine, og erkjenne at partnere som tilbyr konsulenttjenester, administrerte tjenester, videresalg og mye mer, er kritisk viktige for prosessen. Mange kunder krever en skyleverandør for infrastrukturen, og kontraherer ut «hands on keyboard»-planlegging, -migrering og -administrasjonsarbeid til en systemintegrator (SI) eller leverandør av administrerte tjenester. Gitt denne blandingen av «tjenester», kan det foreligge krav som ikke angår skyleverandørene, for eksempel nedstrømsklausuler for underleverandører.

Vi kan se på slike nedstrømsklausuler for å illustrere hvorfor det er viktig å forstå hvordan partnere og forhandlere opererer overfor CISP-er. For enkelte typer innkjøp gjelder klausuler som krever at hovedleverandøren viderefører enkelte obligatoriske klausuler til alle sine partnere/underleverandører. Vanligvis vil ikke CISP-er levere eller gi bud som formelle underleverandørpartnere, siden de tilbyr en standardisert tjeneste i massiv skala som ikke er skreddersydd til de unike behovene til en bestemt sluttkunde (inkludert behovene til en kunde i offentlig sektor etter en kontrakt for offentlig sektor). I en indirekte innkjøpsmodell (anskaffelse av skytjenester gjennom en CISP-forhandler) kan en CISP avvise disse klausulene fra sin forhandler med at de ikke gjelder for et «lag 2»-leverandør av kommersielle tjenester. I slike tilfeller er det ikke selve CISP-en som utfører arbeidet kontrakten gjelder. I stedet er det en CISP-partner som bruker CISP-infrastrukturen til å utføre det. CISP er derfor en kommersiell leverandør (ikke en underleverandør) til en partners virksomhet. I en direkte innkjøpsmodell (innkjøp av skytjenester direkte fra en CISP) vil en CISP vanligvis avvise disse obligatoriske klausulene som er aktuelle for en vanlig underleverandør, fordi de kontraherte tjenestene er av kommersiell art og fordi de fleste CISP-er ikke trenger underleverandører til å tilby sine kommersielle tjenester.

3.4 Skymeglere

Konseptet med en skymegler som en metode for å redusere muligheten for sperring fra leverandøren kan være problematisk. Selv om en skymegler kan virke som en fornuftig idé i teorien, kan dette i praksis gjøre ting mer komplekse og forvirrende enn det er verdt i praksis.

Forsøk på å opprette programmer som fungerer i flere skymiljøer samtidig, eller som kan skiftes ut med hverandre, går uansett på bekostning av funksjonalitet (**det finnes ingen Rosetta-stein for skyen**). Denne tilnærmingen kan til syvende og sist medføre unødvendig ekstra kompleksitet mellom kunder i offentlig sektor og skytjenestene deres, noe som kan gå på bekostning av effektiviteten og den forbedrede sikkerheten man ville oppnå – noe som kan føre til redusert skalerbarhet og smidighet, økte kostnader og tregere innovasjon.

3.5 Markedsundersøkelser før RFP

Når en enhet innen offentlig sektor planlegger en RFP for skytjenester, må man inkludere interessenter fra alle aspekter av organisasjonen – toppledelsen, forretningsinteressentene, teknologi, økonomi, innkjøp, juridisk og kontrakter – helt fra starten av prosessen. Denne tilnærmingen sørger for at alle interessenter har en forståelse av skomodellen og følgelig en velinformert tilnærming til revurdering av tradisjonelle metoder for IT-innkjøp.

Når det gjelder dialog med bransjen, anbefaler vi på det sterkeste at offentlige enheter tar seg tid til inngående samtaler for å innhente tilbakemeldinger fra bransjen – CISP-er, CISP-partnere, leverandører i PaaS- og SaaS-markedet og bransjeeksperter. En slik dialog kan for eksempel ta form av bransjedager eller seminarer om sikkerhet og innkjøp. En annen effektiv måte for å få forståelse for anskaffelse av skytjenester er å utgi en RFI, eller ideelt sett et RFP-dokumentutkast. Disse inkluderer ofte potensielle problemer som kan identifiseres, diskuteres og justeres før den endelige RFP-en for skytjenester utgis.

3.6 Bærekraft

Bærekraft er en iboende del av databehandling i nettskyen. Å flytte til skyen gir en gevinst i energieffektivitet sammenlignet med lokale servere eller bedriftsdatasentre. Ved å finne en CISP som prioriterer bærekraft og har forpliktet seg offentlig til å oppnå bærekraftsmål kan man ytterligere forsikre seg om at skyen er bærekraftig. Europeiske CISP-er og datasenteroperatører (med støtte fra EU-kommisjonen) har opprettet Pakten for klimanøytrale datasentre¹¹, et selvreguleringsinitiativ som skal slå fast klare, enkle og vidtrekkende kriterier på bærekraft for datasenterindustrien og sikre at datasenteroperatører og skytjenesteleverandører blir klimanøytrale innen 2030. Selvreguleringsinitiativet omfatter klare mål for datasentrene når det gjelder energieffektivitet, sparing på vann, gjenbruk og reparasjon av servere samt bruk av karbonfri energi til å drive datasentrene. CISP-er som melder seg på selvreguleringsinitiativet, påtar seg å oppnå disse målene og sertifisere seg etter kriteriene for å bli regnet som klimanøytrale operatører.

En RFP for skytjenester bør spørre CISP-er om de har forpliktet seg på slike kriterier, og bør spesifikt spørre om de har meldt seg på selvregulering og når de påtok seg denne forpliktelsen.

Eksempel på RFP-formuleringer: Bærekraft

Har dere forpliktet dere til å drive klimanøytrale datasentre ved å melde dere på selvreguleringsinitiativet for klimanøytrale datasentre? Hvis ja, når undertegnet dere?

Kan dere bevisse at dere er tildelt retten til å bruke seglet til Pakten for klimanøytrale datasentre?

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

Tillegg A: tekniske krav for sammenligning mellom budgivere

Nedenfor er det ført opp noen generelle krav til skyteknologi som kan brukes til å sammenligne CISP-er under løpende ordrer og minikonkurranser i en rammeavtale for skyen.

1. Skyleverandørprofil

	Krav
1.	ERFARING PÅ MARKEDET: Hvor mange år har skyleverandøren drevet på skymarkedet?
2.	ÅPENHET OG DATABESKYTTELSE: Overholder skyleverandøren bransjens etiske retningslinjer for databeskyttelse eller reverserbarhet? Overholder skyleverandøren prinsippene for utvikling av åpen kildekode og åpen API?

2. Global infrastruktur

	Krav
1.	GLOBAL REKKEVIDDE: Tilbyr skyleverandøren en global infrastruktur som hjelper brukerne med å oppnå lav ventetid og høy gjennomstrømming?
2.	REGIONER: Har skyleverandøren en regional tilstedeværelse i de aktuelle geografiske områdene?
3.	DOMENER/SONER: Støtter skyleverandøren konseptet med domener eller soner, der flere datasentre grupperes på et nettverk med lav ventetid, for å oppnå enda høyere tilgjengelighet og bedre feiltoleranse? Hvis ja, før opp antall domener eller soner og antall datasentre i det aktuelle geografiske området.
4.	AVSTANDER INNEN DOMENER/SONER: Har skyleverandøren bygd opp domenene eller sonene med datasentre som er plassert i fysisk avstand fra hverandre, for å understøtte redundans, høy tilgjengelighet og lav ventetid?
5.	DATASENTER SOM ER BYGD: Tilbyr skyleverandøren datasentre som er utviklet for å være isolert fra feil i andre datasentre, med redundant strøm, avkjøling og nettverk?
6.	DATASENTER-REPLIKERING: Tilbyr skyleverandøren datareplikering på tvers av datasenter i et domene eller en sone med automatisk failover?
7.	DOMENE- OG SONEREPLIKERING: Tilbyr skyleverandøren datareplikering på tvers av domener eller soner innen en region?

3. Infrastruktur

3.1 Databehandling

	Krav
1.	DATABEHANDLING – VANLIG FOREKOMST – GENERELT FORMÅL: Tilbyr skyleverandøren følgende forekomsttyper? • Til generell bruk – optimalisert for generiske programmer og med balanse mellom databehandling, minne og nettverksressurser ○ Hvis ja, hva er den største forekomsten?
2.	DATABEHANDLING – VANLIG FOREKOMST – MINNEOPTIMALISERT: Tilbyr skyleverandøren følgende forekomsttyper? • Minneoptimalisert – optimalisert for minneintensive programmer ○ Hvis ja, hva er den største forekomsten?
3.	DATABEHANDLING – VANLIG FOREKOMST – OPTIMALISERT FOR DATABEHANDLING: Tilbyr skyleverandøren følgende forekomsttyper? • Optimalisert for databehandling – optimalisert for beregningsintensive ○ Hvis ja, hva er den største forekomsten?
4.	DATABEHANDLING – VANLIG FOREKOMST – OPTIMALISERT FOR LAGRING: Tilbyr skyleverandøren følgende forekomsttyper? • Lagringsoptimalisert – gir stor lokal lagringskapasitet ○ Hvis ja, hva er den maksimale lagringskapasiteten (5, 10, 20, 50 TB) og det maksimale antallet disker (HDD/SSD) som kan klargjøres og knyttes til en forekomst?
5.	DATABEHANDLING – VANLIG FOREKOMST – OPTIMALISERT FOR GRAFIKK: Tilbyr skyleverandøren følgende forekomsttyper? • Rimelig grafikk – gir beregningsforekomster grafikkakselerasjon for å beregne forekomster ○ Hvis ja, hva er den største forekomsten?
6.	DATABEHANDLING – VANLIG FOREKOMST – GPU-OPTIMALISERT: Tilbyr skyleverandøren følgende forekomsttyper? • GPU – tilbyr grafikkprosessorer (GPU-er) for grafikkintensive programmer ○ Hvis ja, hvor mange GPU-er og hvilke GPU-modeller kan skyleverandøren tilby per forekomst?
7.	DATABEHANDLING – VANLIG FOREKOMST – FPGA-OPTIMALISERT: Tilbyr skyleverandøren følgende forekomsttyper? • FPGA – tilbyr programmerbare portmatriser (FPGA-er) for utvikling og implementering av tilpasset maskinvareakselerasjon for programmer ○ Hvis ja, hvor mange FPGA-er kan skyleverandøren tilby per forekomst?
8.	DATABEHANDLING – OVERSKRIDBAR FOREKOMST: Tilbyr skyleverandøren overskridbare forekomster som tilbyr prosessorytelse på et grunnleggende nivå med mulighet til å overskride det? • Hvis ja, hva er den største overskridbare forekomsten?

9.	DATABEHANDLING – I/U-INTENSIV FOREKOMST: Tilbyr skyleverandøren forekomster som bruker NVMe (non-volatile memory express) SSD-er (solid state drives) som er optimalisert for lav ventetid, svært høy tilfeldig I/U-ytelse og høy sekvensiell lesegjennomstrømming? Hvis ja, hva er maksimal kapasitet for operasjoner med inndata/utdata per sekund (IOPS) i den største forekomsten?
10.	DATABEHANDLING – MIDLERTIDIG LOKAL LAGRING: Tilbyr skyleverandøren lokal lagring for databehandlingsforekomster til bruk for midlertidig lagring av informasjon som endres ofte?
11.	DATABEHANDLING – STØTTE FOR FLERE NETTVERKSKORT (NIC): Støtter skyleverandøren at flere nettverkskort (primære kort og tilleggskort) kan tildeles for en gitt forekomst? Hvis ja, hva er det maksimale antallet nettverkskort per forekomst?
12.	DATABEHANDLING – FOREKOMSTAFFINITET: Tilbyr skyleverandøren muligheten til å gruppere forekomster sammen på en logisk måte innen ett datasenter?
13.	DATABEHANDLING – ANTI-AFFINITET FOR FOREKOMSTER: Tilbyr skyleverandøren muligheten til å gruppere forekomster sammen på en logisk måte og plassere dem i ulike datasentre innen en region?
14.	DATABEHANDLING – SELVBETJENT KLARGJØRING: Tilbyr skyleverandøren selvbetjent klargjøring av flere forekomster, enten via et programmatisk grensesnitt, en administrasjonskonsoll eller en nettportal?
15.	DATABEHANDLING – TILPASNING: Tilbyr skyleverandøren tilpassbare forekomster, dvs. muligheten til å endre konfigurasjonsinnstillinger, for eksempel virtuelle prosessorer (vCPU-er) og RAM?
16.	DATABEHANDLING – LEIEFORHOLD: Tilbyr skyleverandøren enkeltleieforekomster som kjører på maskinvare som er dedikert til én enkelt bruker? Hvis ja, hva er den største tilgjengelige enkeltleieforekomsten?
17.	DATABEHANDLING – VERTSAFFINITET: Tilbyr skyleverandøren muligheten til å starte en forekomst og angi at denne forekomsten alltid skal startes på nytt på den samme fysiske verten?
18.	DATABEHANDLING – ANTI-AFFINITET FOR VERT: Tilbyr skyleverandøren muligheten til å dele opp og drifte spesifikke forekomster på tvers av ulike fysiske verter?
19.	DATABEHANDLING – AUTOMATISK SKALERING: Tilbyr skyleverandøren muligheten til å øke antall forekomster automatisk under behovstopper for å opprettholde ytelsen (dvs. utskalering)?
20.	DATABEHANDLING – MEKANISME FOR BILDEIMPORT: Tilbyr skyleverandøren brukerne muligheten til å importere sine eksisterende maskinbilder og lagre dem som nye, privat tilgjengelige bilder som deretter kan brukes til å klargjøre forekomster i fremtiden? Hvis ja, hvilke formater støttes?
21.	DATABEHANDLING – MEKANISME FOR BILDEEKSPORT: Støtter skyleverandøren muligheten til å ta en eksisterende, kjørende forekomst eller en kopi av en forekomst og eksportere forekomsten til et virtuelt maskinformat? Hvis ja, hvilke formater støttes?
22.	DATABEHANDLING – TJENESTEAVBRUDD: Tilbyr skyleverandøren mekanismer for å unngå forekomster med avbrudd eller nedetid når leverandøren utfører en eller annen form for maskinvare- eller tjenestevedlikehold på vertsnivå?

23.	DATABEHANDLING – OMSTART AV FOREKOMST: <i>Tilbyr skyleverandøren mekanismer for å starte forekomster på en fungerende vert på nytt automatisk hvis det oppstår en feil på den opprinnelige fysiske verten?</i>
24.	DATABEHANDLING – VARSLINGER: <i>Når det gjelder en elastisk hendelse innen databehandling, har skyleverandøren mulighet til å varsle brukeren om at en slik hendelse er inntruffet, og kan brukeren velge å motta disse beskjedene eller ikke på en selvbetjent måte?</i>
25.	DATABEHANDLING – HENDESEPLANLEGGING: <i>Tilbyr skyleverandøren muligheten til å planlegge hendelser for brukernes forekomster, for eksempel omstart, stopping, starting eller avvikling av forekomsten?</i>
26.	DATABEHANDLING – MEKANISME FOR SIKKERHETSKOPIERING OG GJENOPPRETTING: <i>Tilbyr skyleverandøren en integrert mekanisme for sikkerhetskopiering og gjenoppretting?</i>
27.	DATABEHANDLING – MEKANISME FOR ØYEBLIKKBILDER: <i>Tilbyr skyleverandøren en manuell, behovsbasert mekanisme for øyeblikksbilder?</i>
28.	DATABEHANDLING – METADATA: <i>Tilbyr skyleverandøren en metadatatjeneste for forekomsten som lar brukerne angi tilfeldige par av nøkler/verdier for forekomsten?</i>
29.	DATABEHANDLING – METADATAKALL: <i>Tilbyr skyleverandøren en metadatatjeneste for forekomsten som tilbyr en API som forekomsten kan kalle for å finne informasjon om seg selv?</i>
30.	DATABEHANDLING – MEKANISME FOR BUDGIVNING: <i>Tilbyr skyleverandøren en mekanisme for budgivning på rimelige forekomster som kan startes umiddelbart for å være vert for ikke-bedriftskritiske arbeidsbelastninger?</i>
31.	DATABEHANDLING – MEKANISME FOR PLANLEGGING: <i>Tilbyr skyleverandøren mulighet for å planlegge og reservere ekstra databehandlingskapasitet på gjentatt basis, f.eks. en daglig, ukentlig eller månedlig tidsplan?</i>
32.	DATABEHANDLING – MEKANISME FOR RESERVERING: <i>Tilbyr skyleverandøren mulighet for å reservere ekstra databehandlingskapasitet for fremtiden (f.eks. 1 år, 2 år, 3 år osv.)?</i>
33.	DATABEHANDLING – OPERATIVSYSTEMET LINUX: <i>Støtter skyleverandøren de to siste versjonene av minst én Linux-distribusjon for bedrift med langsiktig støtte (for eksempel Red Hat, SUSE) og én vanlig gratis Linux-distribusjon (for eksempel Ubuntu, CentOS og Debian)?</i>
34.	DATABEHANDLING – OPERATIVSYSTEMET WINDOWS: <i>Støtter skyleverandøren de siste to hovedversjonene av Windows Server (Windows Server 2017 og Windows Server 2016)?</i>
35.	DATABEHANDLING – LISENSSPORTABILITET: <i>Tilbyr skyleverandøren lisensportabilitet og -støtte?</i> • Hvis ja, oppgi programvareleverandør, programvarenavn, -utgaver og -versjoner.
36.	DATABEHANDLING – TJENESTEBEGRENSNINGER: <i>Har skyleverandøren noen begrensninger (dvs. tjenestebegrensninger) når det gjelder databehandlingsdelen ovenfor?</i> <i>Eksempel:</i> <i>Maksimalt antall forekomster per konto</i> <i>Maksimalt antall dedikerte verter per konto</i> <i>Maksimalt antall reserverte IP-adresser</i>

3.2 Nettverk

	Krav
1.	NETTVERK – VIRTUELLE NETTVERK: Støtter skyleverandøren muligheten til å opprette et logisk, isolert virtuelt nettverk som representerer en bedrifts eget nettverk i skyen?
2.	NETTVERK – TILKOBLING INNEN SAMME REGION: Støtter skyleverandøren tilkobling av to virtuelle nettverk innen samme region for å rute trafikk mellom dem ved å bruke private IP-adresser?
3.	NETTVERK – TILKOBLING MELLOM ULIKE REGIONER: Støtter skyleverandøren tilkobling av to virtuelle nettverk på tvers av flere regioner for å rute trafikk mellom dem ved å bruke private IP-adresser?
4.	NETTVERK – PRIVAT DELNETT: Tilbyr skyleverandøren muligheten til å opprette fullstendig isolerte (private) virtuelle nettverk og delnett der forekomster kan klargjøres uten en offentlig IP-adresse eller Internett-ruting?
5.	NETTVERK – ADRESSEOMRÅDE PÅ VIRTUELT NETTVERK: Støtter skyleverandøren IP-adresseområder som er spesifisert i forespørselen om kommentarer (RFC) 1918, og offentlige rutbare Classless Inter-Domain Routing (CIDR)?
6.	NETTVERK – FLERE PROTOKOLLER: Støtter skyleverandøren flere protokoller, inkludert TCP (Transmission Control Protocol), UDP (User Datagram Protocol) og ICMP (Internet Control Message Protocol)?
7.	NETTVERK – AUTOMATISK TILORDNING FOR IP-ADRESSER: Støtter skyleverandøren automatisk tilordning av offentlige IP-adresser (Internett-protokoll) til forekomster?
8.	NETTVERK – RESERVERTE STATISKE IP-ADRESSER: Støtter skyleverandøren IP-adresser (Internett-protokoll) som er knyttet til en brukerkonto, ikke en bestemt forekomst? IP-adressen må forbli knyttet til kontoen til den frigis eksplisitt.
9.	NETTVERK – IPV6-STØTTE: Støtter skyleverandøren IPv6 (Internett-protokoll, versjon 6) på gateway- eller forekomstnivå, og er denne funksjonaliteten tilgjengelig for brukerne?
10.	NETTVERK – FLERE IP-ADRESSER PER NETTVERKSKORT: Støtter skyleverandøren tilordning av en primær og en sekundær IP-adresse til et nettverkskort som er knyttet til en gitt forekomst?
11.	NETTVERK – FLERE NETTVERKSKORT: Støtter skyleverandøren tilordning av flere nettverkskort (NIC-er) til en gitt forekomst?
12.	NETTVERK – MOBILITET FOR NETTVERKSKORT OG IP: Støtter skyleverandøren flytting både av nettverkskort og IP-adresser mellom forekomster?
13.	NETTVERK – STØTTE FOR SR-IOV: Støtter skyleverandøren funksjoner som virtualisering av inndata/utdata med én rot (SR-IOV) for høyere ytelse (f.eks. pakker per sekund), lavere ventetid og lavere jitter?
14.	NETTVERK – INNGÅENDE FILTRERING: Støtter skyleverandøren tilføyning eller fjerning av regler som gjelder inngående trafikk til forekomster?
15.	NETTVERK – UTGÅENDE FILTRERING: Støtter skyleverandøren tilføyning eller fjerning av regler som gjelder utgående trafikk som kommer fra forekomster?

16.	NETTVERK – TILGANGSKONTROLLISTER: <i>Tilbyr skyleverandøren tilgangskontrolliste (ACL) for å kontrollere inngående og utgående trafikk til og fra delnett?</i>
17.	NETTVERK – STØTTE FOR FLYTLOGG: <i>Tilbyr skyleverandøren muligheten til å registrere flytlogger for nettverkstrafikken?</i>
18.	NETTVERK – NAT: <i>Tilbyr skyleverandøren en NAT-gateway (oversettelse av nettverksadresser) som administrert tjeneste, slik at forekomster på et privat nettverk kan kobles til Internett eller andre skytjenester, men som forhindrer selve Internett fra å starte en tilkobling til disse forekomstene?</i>
19.	NETTVERK – KONTROLL AV KILDE/MÅL: <i>Kan skyleverandøren aktivere kontroll av kilde/mål på nettverkskort?</i>
20.	NETTVERK – VPN-STØTTE: <i>Støtter skyleverandøren VPN-tilkobling (virtuelt privat nettverk) mellom skyleverandøren og brukerens datasenter?</i>
21.	NETTVERK – VPN-TUNNELER: <i>Støtter skyleverandøren flere VPN-tilkoblinger per virtuelle nettverk?</i>
22.	NETTVERK – IPSEC VPN-STØTTE: <i>Gir skyleverandøren brukere tilgang til skytjenester enten via IPsec (Internet Protocol security) virtuelt privat nettverk (VPN)-tunnell eller SSL (Secure Sockets Layer) virtuelt privat nettverk (VPN)-tunnel over offentlig Internett?</i>
23.	NETTVERK – BGP-STØTTE: <i>Bruker skyleverandøren Border Gateway Protocol (BGP) til å forbedre failover i (IPsec) virtuelt privat nettverk (VPN)-tunneler?</i>
24.	NETTVERK – PRIVAT DEDIKERT TILKOBLING: <i>Tilbyr skyleverandøren en direkte, privat tilkoblingstjeneste mellom plasseringene til skyleverandøren og en brukers datasenter, kontor eller samlokaliseringsmiljø som tillater store og raske dataoverføringer?</i>
25.	NETTVERK – BELASTNINGSBALANSERING I FRONT: <i>Tilbyr skyleverandøren belastningsbalansering i front (vendt mot Internett) som tar forespørsler fra klienter over Internett og fordeler disse forespørslene på forekomster som er registrert i belastningsbalanseringen?</i>
26.	NETTVERK – BELASTNINGSBALANSERING I BAKGRUNNEN: <i>Tilbyr skyleverandøren belastningsbalansering i bakgrunnen (privat) som ruter trafikk til forekomster som driftes på private delnett?</i>
27.	NETTVERK – BELASTNINGSBALANSERING PÅ LAG 7: <i>Tilbyr skyleverandøren belastningsbalansering på lag 7 (HTTP) som støtter belastningsbalansering av nettverkstrafikk på tvers av flere forekomster?</i>
28.	NETTVERK – BELASTNINGSBALANSERING PÅ LAG 4: <i>Tilbyr skyleverandøren belastningsbalansering på lag 4 (TCP) som støtter belastningsbalansering av nettverkstrafikk på tvers av flere forekomster?</i>
29.	NETTVERK – ØKTAFFINITET FOR BELASTNINGSBALANSERING: <i>Tilbyr skyleverandøren belastningsbalansering som støtter øktaffinitet?</i>
30.	NETTVERK – DNS-BASERT BELASTNINGSBALANSERING: <i>Tilbyr skyleverandøren belastningsbalansering som kan balansere trafikk til forekomster som driftes på flere verter som tilhører ett domene?</i>
31.	NETTVERK – LOGGER FOR BELASTNINGSBALANSERING: <i>Tilbyr skyleverandøren logger som registrerer detaljert informasjon om alle forespørsler som er sendt angående belastningsbalansering?</i>

32.	NETTVERK – DNS: <i>Tilbyr skyleverandøren en skalerbar domenenavnsystem (DNS)-tjeneste med høy tilgjengelighet?</i>
33.	NETTVERK – VENTETIDSBASERT DNS-RUTING: <i>Tilbyr skyleverandøren en domenenavnsystem (DNS)-tjeneste som støtter ventetidsbasert ruting (dvs. at DNS-tjenesten svarer på DNS-forespørsler med ressursene som gir lavest ventetid)?</i>
34.	NETTVERK – GEOGRAFISK BASERT DNS-RUTING: <i>Tilbyr skyleverandøren en domenenavnsystem (DNS)-tjeneste som støtter geografisk basert ruting (dvs. at DNS-tjenesten svarer på DNS-forespørsler basert på den geografiske posisjonen til brukerne)?</i>
35.	NETTVERK – FAILOVER-BASERT DNS-RUTING: <i>Tilbyr skyleverandøren en domenenavnsystem (DNS)-tjeneste som støtter failover-basert ruting (dvs. at DNS-tjenesten ruter DNS-spørringer til ressursen som er aktiv for øyeblikket, mens en sekundær ressurs venter og bare blir aktiv hvis det oppstår en feil i den primære resursen)?</i>
36.	NETTVERK – DOMENEREGISTRERINGSTJENESTE: <i>Tilbyr skyleverandøren domenerregistreringstjenester (dvs. at brukerne kan søke etter og registrere tilgjengelige domenenavn)?</i>
37.	NETTVERK – DNS-TILSTANDSSJEKK: <i>Tilbyr skyleverandøren en domenenavnsystem (DNS)-tjeneste som bruker tilstandssjekk til å overvåke tilstanden og ytelsen til ressurser?</i>
38.	NETTVERK – INTEGRERING AV DNS OG BELASTNINGSBALANSERING: <i>Tilbyr skyleverandøren en domenenavnsystem (DNS)-tjeneste som integreres med skyleverandørens belastningsbalansering?</i>
39.	NETTVERK – VISUELL REDIGERING: <i>Tilbyr skyleverandøren et verktøy som brukerne kan bruke til å utvikle retningslinjer for trafikkstyring?</i>
40.	NETTVERK FOR INNHOLDSLEVERING (CDN): <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) for å distribuere innhold med lav ventetid og rask dataoverføring?</i>
41.	NETTVERK – UTLØP AV CDN-BUFFER: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som tillater fjerning av et objekt fra kantbuffer før det utløper, inkludert funksjoner som ugyldiggjøring av objekter og versjonskontroll for objekter?</i>
42.	NETTVERK – EKSTERN CDN-OPPRINNELSE: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som støtter en egendefinert opprinnelse, f.eks. en HTTP-server?</i>
43.	NETTVERK – CDN-OPTIMALISERING: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) med detaljert kontroll for konfigurasjon av flere opprinnelseserver og bufringsegenskaper for ulike URL-adresser?</i>
44.	NETTVERK – GEOGRAFISK BEGRENSET CDN: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som støtter geografisk begrensning, dvs. forhindrer brukere i spesifikke geografiske områder fra å få tilgang til innhold?</i>
45.	NETTVERK – CDN-TOKENER: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som støtter signerte URL-adresser som vanligvis inkluderer tilleggsinformasjon, for eksempel utløpsdato/-tidspunkt, for å gi brukerne mer kontroll over tilgangen til innholdet?</i>
46.	NETTVERK – CDN-SERTIFIKATER: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som støtter egendefinerte SSL-sertifikater (Secure Sockets Layer), for å levere innhold sikkert over HTTPS fra kantplasseringer?</i>

47.	NETTVERK – CDN-BUFFER MED FLERE LAG: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som bruker en tilnærming med buffere med flere lag når regionale kantbuffere brukes, for å redusere ventetid?</i>
48.	NETTVERK – CDN-KOMPRIMERING: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som støtter filkomprimering?</i>
49.	NETTVERK – CDN-KRYPTERTE OPPLASTINGER: <i>Tilbyr skyleverandøren et nettverk for innholdslevering (CDN) som gjør at brukerne kan laste opp sensitive data slik at denne informasjonen bare kan vises av enkelte komponenter og tjenester i brukerens opprinnelige infrastruktur?</i>
50.	NETTVERK – SLUTTPUNKTER: <i>Tilbyr skyleverandørens nettverkstjeneste brukerne slutt punkter som kan rute trafikk gjennom leverandørens interne nettverkstilkobling (dvs. privat tilkobling), for å redusere kommunikasjonskostnader og forbedre trafikk sikkerheten?</i>
51.	NETTVERK – TJENESTEBEGRENSNINGER: <i>Har skyleverandøren tjenestebegrensninger med hensyn til avsnittet om nettverk ovenfor?</i> <i>Eksempel:</i> <i>Maksimalt antall virtuelle nettverk per konto</i> <i>Maksimal størrelse på et virtuelt nettverk</i> <i>Maksimalt antall delnett per konto</i> <i>Maksimalt antall belastningsbalanseringer per konto</i> <i>Maksimalt antall ACL-oppføringer (tilgangskontrolliste)</i> <i>Maksimalt antall virtuelt privat nettverk (VPN)-tunneler</i> <i>Maksimalt antall opprinnelser per distribusjon</i> <i>Maksimalt antall sertifikater per belastningsbalansering</i>

3.3 Lagring

	Krav
1.	BLOKKLAGRINGSTJENESTE: <i>Tilbyr skyleverandøren volumer for lagring på blokknivå som kan brukes med databehandlingsforekomster?</i>
2.	BLOKKLAGRING – IOPS: <i>Tilbyr skyleverandøren muligheten til å kjøpe et eksplisitt ytelsesmål eller et ytelsesnivå i blokklagringsvolumer, for eksempel et visst antall inndata-/utdataoperasjoner per sekund (IOPS) eller megabyte per sekund (MB/s) med gjennomstrømming?</i>
3.	BLOKKLAGRING – HALVLEDERSTASJONER: <i>Tilbyr skyleverandøren SSD-lagringsmedier (halvlederstasjoner) som tilbyr ventetider under ti millisekunder?</i> Hvis ja, hva er det maksimale antallet SSD-er som kan kobles til per forekomst?
4.	BLOKKLAGRING – SKALERING: <i>Tilbyr skyleverandøren brukerne muligheten til å øke størrelsen på et eksisterende blokklagringsvolum uten at de må klargjøre et nytt volum og kopiere/flytte dataene?</i>
5.	BLOKKLAGRING – ØYEBLIKKSBLIDER: <i>Støtter skyleverandøren øyeblikksbilder for blokklagringstjenesten?</i>

6.	BLOKKLAGRING – FJERNING AV DATA: <i>Støtter skyleverandøren fullstendig fjerning av data, slik at dataene ikke lenger kan leses eller er tilgjengelige for uautoriserte brukere og/eller tredjeparter?</i>
7.	BLOKKLAGRING – KRYPTERING I RO: <i>Tilbyr skyleverandøren kryptering av data som er lagret på volumer og øyeblikksbilder på serversiden?</i> • Hvis ja, hvilken krypteringsalgoritme brukes?
8.	OBJEKTLAGRINGSTJENESTE: <i>Tilbyr skyleverandøren sikker, robust og svært skalerbar objektlagring for lagring og henting av en hvilken som helst datamengde fra nettet?</i>
9.	OBJEKTLAGRING – SJELDEN BRUK: <i>Tilbyr skyleverandøren et lagringsnivå til rimelig pris som er ment for lagring av objekter og filer som ikke brukes så ofte?</i>
10.	OBJEKTLAGRING – REDUSERT HOLDBARHET: <i>Tilbyr skyleverandøren et lag med redusert redundans der en bruker kan lagre ikke-kritiske objekter som enkelt kan reproduseres, til en lavere pris?</i>
11.	OBJEKTLAGRING – MINDRE HYPPIG BRUK: <i>Tilbyr skyleverandøren et nivå for data som ikke brukes så mye, men som likevel krever hurtig tilgang?</i>
12.	OBJEKTLAGRING – LAGRINGSNIVÅER FOR OBJEKTER: <i>Tilbyr skyleverandøren lagringsnivåer for objekter, dvs. muligheten til å anbefale at et objekt kan bytte lagringsklasse eller -nivå basert på hvor ofte det brukes?</i>
13.	OBJEKTLAGRING – ADMINISTRASJON AV LIVSSYKLUS: <i>Støtter skyleverandøren administrasjon av livssyklusen til et objekt gjennom en konfigurasjon som definerer hvordan objekter administreres gjennom hele levetiden, fra opprettelse til sletting?</i>
14.	OBJEKTLAGRING – ADMINISTRASJON DREVET AV RETNINGSLINJER: <i>Tilbyr skyleverandøren muligheten til å opprette og bruke retningslinjer for administrasjon av lagrede data, dataenes livssyklus og innstillinger for lagringsnivåer?</i>
15.	OBJEKTLAGRING – RETNINGSLINJER BASERT PÅ STED OG TID: <i>Tilbyr skyleverandøren muligheten til å opprette retningslinjer som kan begrense tilgangen til dataene, basert på hvor brukeren befinner seg og tidspunktet for forespørselen?</i>
16.	OBJEKTLAGRING – DRIFTING AV NETTSTED: <i>Tilbyr skyleverandøren drifting av statiske nettstedet som ikke er en del av objektlagringstjenesten?</i>
17.	OBJEKTLAGRING – KRYPTERING I RO: <i>Støtter skyleverandøren kryptering på serverside (SSE) av inaktive data, der skyleverandøren administrerer krypteringsnøklerne?</i> • Hvis ja, hvilken krypteringsalgoritme brukes?
18.	OBJEKTLAGRING – KRYPTERING MED BRUKERNØKLER: <i>Tilbyr skyleverandøren kryptering på serverside (SSE) ved å bruke kryptografiske nøkler oppgitt av kunden?</i>
19.	OBJEKTLAGRING – TJENESTE FOR NØKKELADMINISTRASJON: <i>Støtter skyleverandøren kryptering på serversiden ved å bruke en tjeneste for nøkkeladministrasjon som oppretter krypteringsnøkler, definerer retningslinjene som styrer hvordan nøklene kan brukes, og overvåker bruken av nøklene for å bevise at de brukes på riktig måte?</i>
20.	OBJEKTLAGRING – HOVEDNØKKELE PÅ KLIENTSIDEN: <i>Tilbyr skyleverandøren brukerne et alternativ for å beholde kontroll over krypteringsnøklerne og utføre kryptering/dekryptering av objekter på klientsiden?</i>

21.	OBJEKTLAGRING – STERK KONSISTENS: <i>Støtter skyleverandøren lese-etter-skrive-konsistens for PUT-operasjoner for nye objekter?</i>
22.	OBJEKTLAGRING – DATALOKALITET: <i>Tilbyr skyleverandøren sterk regional isolering, slik at objekter som er lagret i en region, aldri forlater regionen med mindre brukeren eksplisitt overfører dem til en annen region?</i>
23.	OBJEKTLAGRING – REPLIKERING: <i>Tilbyr skyleverandøren en replikeringsfunksjon på tvers av regioner som automatisk replikerer objekter på tvers av regioner som brukeren velger?</i>
24.	OBJEKTLAGRING – VERSJONSKONTROLL: <i>Støtter skyleverandøren versjonskontroll, dvs. muligheten til å lagre og opprettholde flere versjoner av et objekt?</i>
25.	OBJEKTLAGRING – «IKKE SLETT»-MERKING: <i>Tillater skyleverandøren at en bruker markerer at et element ikke kan slettes?</i>
26.	OBJEKTLAGRING – SLETTING MED MFA: <i>Støtter skyleverandøren bruk av flertrinnsbekreftelse (MFA) for sletteoperasjoner som et ekstra sikkerhetsalternativ?</i>
27.	OBJEKTLAGRING – OPPLASTING I FLERE DELER: <i>Tillater skyleverandøren opplasting av et objekt som et sett med deler, der hver del er en sammenhengende andel av objektets data, og der disse objektene kan lastes opp uavhengig av hverandre og i enhver rekkefølge?</i>
28.	OBJEKTLAGRING – TAGGER: <i>Tilbyr skyleverandøren muligheten til å opprette og tilknytte dynamiske tagger som kan deaktiveres, på objektnivå?</i>
29.	OBJEKTLAGRING – VARSLINGER: <i>Tilby skyleverandøren muligheten til å sende varslinger når bestemte hendelser inntreffer på objektnivå (f.eks. når noe legges til eller slettes)?</i>
30.	OBJEKTLAGRING – LOGGER: <i>Tilbyr skyleverandøren generering av revisjonslogger som inkluderer informasjon om én enkelt tilgangsforespørsel, for eksempel bestilleren, forespørselstidspunktet, forespørselshandlingen, forespørselsstatusen og feilkoden?</i>
31.	OBJEKTLAGRING – LAGERBEHOLDNING FOR OBJEKTER: <i>Tilbyr skyleverandøren lagerbeholdning for objekter som gir brukerne muligheten til raskt å visualisere objekter og deres status, slik at brukerne raskt kan oppdage objekter med offentlig tilgang?</i>
32.	OBJEKTLAGRING – LAGERBEHOLDNING FOR METADATA: <i>Tilbyr skyleverandøren lagerbeholdning for objekter, slik at brukerne raskt kan visualisere metadata for objektene?</i>
33.	OBJEKTLAGRING – OPTIMALISERING AV OPPLASTINGER: <i>Har skyleverandøren mulighet til å rute data fra kantplasseringer til lagringstjenesten ved å bruke en optimalisert nettverksbane?</i>
34.	OBJEKTLAGRING – MULIGHET FOR SPØRRINGER: <i>Tilbyr skyleverandøren brukerne mulighet til å spørre objektlagringstjenesten ved hjelp av SQL-setninger (strukturert spørringsspråk)?</i>
35.	OBJEKTLAGRING – HENTING AV DELSETT: <i>Tilbyr skyleverandøren brukerne muligheten til å hente bare en delmengde av dataene fra et objekt, ved å bruke enkle SQL-uttrykk (strukturert spørringsspråk)?</i>
36.	FILLAGRINGSTJENESTE: <i>Tilbyr skyleverandøren en enkel og skalerbar fillagringstjeneste som kan brukes sammen med databehandlingsforekomster i skyen?</i>

37.	FILLAGRING – REDUNDANS: <i>Lagrer skyleverandøren filsystemobjektene med redundans (dvs. kataloger, filer og koblinger) på tvers av flere datasentre eller anlegg, for å oppnå økt tilgjengelighet og robusthet?</i>
38.	FILLAGRING – FJERNING AV DATA: <i>Støtter skyleverandøren fullstendig fjerning av fillagringsdata, slik at dataene ikke lenger kan leses eller er tilgjengelige for uautoriserte brukere eller tredjeparter?</i>
39.	FILLAGRING – HØY TILGJENGELIGHET: <i>Har det administrerte filsystemet til skyleverandøren høy tilgjengelighet?</i>
40.	FILLAGRING – NFS: <i>Støtter skyleverandøren NFS-protokollen (Network File System)?</i>
41.	FILLAGRING – SMB: <i>Støtter skyleverandøren SMB-protokollen (Server Message Block)?</i>
42.	FILLAGRING – KRYPTERING I RO: <i>Støtter fillagringstjenesten til skyleverandøren kryptering i ro?</i>
43.	FILLAGRING – KRYPTERING UNDER OVERFØRING: <i>Støtter fillagringstjenesten til skyleverandøren kryptering av data under overføring?</i>
44.	FILLAGRING – DATAOVERFØRINGSVERKTØY: <i>Tilbyr skyleverandøren et dataoverføringsverktøy for å flytte data fra lokale systemer til det skybaserte filsystemet?</i>
45.	ARKIVLAGRINGSTJENESTE: <i>Tilbyr skyleverandøren en lagringstjeneste til svært rimelig pris som er ment for arkivering av objekter og filer som ikke brukes så ofte, og som nærmest er uforanderlige?</i>
46.	ARKIVLAGRING – FEILTOLERANSE: <i>Tilbyr skyleverandøren feiltoleranse for arkivlagringstjenesten?</i>
47.	ARKIVLAGRING – UFORANDERLIGHET: <i>Tilbyr skyleverandøren uforanderlighet for arkiverte objekter og filer?</i>
48.	ARKIVLAGRING – WORM: <i>Tilbyr skyleverandøren WORM-funksjonalitet (skriv én gang, les mange)?</i>
49.	ARKIVLAGRING – HENTING AV DELMENGDE: <i>Tilbyr skyleverandøren brukerne muligheten til å hente bare en delmengde av dataene fra et arkivert objekt, ved å bruke enkle SQL-uttrykk (strukturet spørringsspråk)?</i>
50.	ARKIVLAGRING – HURTIGHENTING: <i>Tilbyr skyleverandøren brukerne flere alternativer for datahenting, med ulike kostnader og hentetider?</i>
51.	ARKIVLAGRING – KRYPTERING I RO: <i>Støtter arkivlagringstjenesten til skyleverandøren kryptering i ro?</i>

52.	LAGRING – TJENESTEBEGRENSNINGER: Har skyleverandøren tjenestebegrensninger med hensyn til avsnittet om lagring ovenfor? Eksempel: Maksimal volumstørrelse Maksimalt antall stasjoner koblet til en forekomst Maksimalt antall operasjoner med inndata/utdata per sekund (IOPS) Maksimal objektstørrelse Maksimalt antall objekter per lagringskonto Maksimalt antall øyeblikksbilder
-----	---

4. Administrasjon

	Krav
1.	ADMINISTRASJON – BRUKERE OG GRUPPER: Tilbyr skyleverandøren en tjeneste for å opprette og administrere brukere og grupper av brukere som bruker leverandørens infrastruktur og ressursene i denne?
2.	ADMINISTRASJON – TILBAKESTILLING AV PASSORD: Tillater skyleverandøren at brukerne selv tilbakestiller egne passord?
3.	ADMINISTRASJON – TILLATELSER: Tilbyr skyleverandøren muligheten til å legge til tillatelser for brukere og grupper på ressursnivå?
4.	ADMINISTRASJON – MIDLERTIDIGE TILLATELSER: Tilbyr skyleverandøren muligheten til å opprette tillatelser som er gyldige i et spesifikt tidsrom?
5.	ADMINISTRASJON – MIDLERTIDIG LEGITIMASJON: Tilbyr skyleverandøren brukerne muligheten til å opprette og tilby midlertidig sikkerhetslegitimasjon til klarerte brukere, som er konfigurert til å vare i alt fra noen minutter til flere timer?
6.	ADMINISTRASJON – TILGANGSKONTROLL: Tilbyr skyleverandøren findetaljerte tilgangskontroller til infrastrukturressursene? Hvis ja, hvilke betingelser kan brukes av disse kontrollene (f.eks. tidspunkt på dagen, opprinnelig IP-adresse osv.)?
7.	ADMINISTRASJON – INNEBYGDE RETNINGSLINJER: Har infrastrukturen til skyleverandøren innebygde retningslinjer for tilgangskontroll som kan knyttes til brukere og grupper?
8.	ADMINISTRASJON – EGENDEFINERTE RETNINGSLINJER: Tillater infrastrukturen til skyleverandøren oppretting og tilpassing av retningslinjer for tilgangskontroll som kan knyttes til brukere og grupper?
9.	ADMINISTRASJON – SIMULATOR FOR RETNINGSLINJER: Tilbyr skyleverandøren en mekanisme for å teste effektene av retningslinjer for tilgangskontroll, før slike retningslinjer settes i produksjon?
10.	ADMINISTRASJON – MFA I SKYEN: Støtter skyleverandøren bruk av flertrinnsbekreftelse (MFA) som et ekstra lag med tilgangskontroll og godkjenning for infrastrukturen?

11.	ADMINISTRASJON – TJENESTEBEGRENSNINGER: Har skyleverandøren tjenestebegrensninger med hensyn til avsnittet om administrasjon ovenfor? Eksempel: Maksimalt antall brukere Maksimalt antall grupper Maksimalt antall administrerte retningslinjer
-----	---

5. Sikkerhet

	Krav
1.	SIKKERHET – BAKGRUNNSKONTROLLER: Er alt personale hos skyleverandøren som har tilgang til tjenesteinfrastrukturen (både fysisk og ikke-fysisk), underlagt bakgrunnskontroller?
2.	SIKKERHET – FYSISK TILGANG: Begrenser skyleverandøren personalet fra å få tilgang til tjenesteinfrastrukturen, med mindre det foreligger et spesifikt problem, en endringsforespørsel eller en lignende formell autorisasjon?
3.	SIKKERHET – TILGANGSLOGGER: Loggfører skyleverandøren personaltilgangen over infrastrukturen på en slik måte at slik tilgang alltid loggføres, og at loggene beholdes i minimum 90 dager?
4.	SIKKERHET – VERTSPÅLOGGING: Begrenser skyleverandøren personalet fra å logge seg på databehandlingsverter, og automatiserer i stedet alle oppgaver som utføres på databehandlingsverter, der innholdet i disse automatiserte jobbene loggføres, og der loggene beholdes i minimum 90 dager?
5.	SIKKERHET – KRYPTOGRAFISKE NØKLER: Tilbyr skyleverandøren en tjeneste for å opprette og kontrollere de kryptografiske nøklene som brukes til å kryptere brukerdata?
6.	SIKKERHET – ADMINISTRASJON AV TILGANGSNØKKELE: Tilbyr skyleverandøren muligheten til å identifisere når en tilgangsnøkkel sist ble brukt, rotere gamle nøkler og fjerne inaktive brukere?
7.	SIKKERHET – NØKLER OPPGITT AV KUNDEN: Tillater skyleverandøren brukere å importere nøkler fra sin egen infrastruktur for nøkkeladministrasjon til skyleverandørens tjeneste for nøkkeladministrasjon?
8.	SIKKERHET – INTEGRERING AV TJENESTE FOR KRYPTOGRAFISKE NØKLER: Kan skyleverandørens tjeneste for nøkkeladministrasjon integreres med andre skytjenester for mulighet til å kryptere data i ro?
9.	SIKKERHET – HSM: Tilbyr skyleverandøren dedikerte moduler for maskinwaresikkerhet (HSM), dvs. maskinvare som sørger for sikker lagring av nøkler og kryptografiske operasjoner i en tuklingssikker maskinvaremodul?
10.	SIKKERHET – VARIGHET FOR KRYPTOGRAFISKE NØKLER: Støtter skyleverandøren varighet for nøkler, inkludert lagring av flere kopier, slik at nøklene er tilgjengelige når det er behov for dem?
11.	SIKKERHET – SSO: Tilbyr skyleverandøren en administrert SSO-tjeneste (Single Sign-On), der brukerne kan administrere tilgang sentralt til flere kontoer og forretningsprogrammer?

12.	SIKKERHET – SERTIFIKATER: Tilbyr skyleverandøren en administrert tjeneste for å klargjøre, administrere og implementere SSL-sertifikater (Secure Sockets Layer)/Transport Layer Security (TLS)-sertifikater?
13.	SIKKERHET – FORNYELSE AV SERTIFIKATER: Er det mulig å fornye sertifikater via skyleverandørens administrasjonstjeneste for sertifikater?
14.	SIKKERHET – UNIVERSELLE SERTIFIKATER: Støtter skyleverandørens administrasjonstjeneste for sertifikater bruk av universelle sertifikater (wildcard certificates)?
15.	SIKKERHET – SERTIFISERINGSINSTANS: Fungerer skyleverandørens administrasjonstjeneste for sertifikater også som en sertifiseringsinstans?
16.	SIKKERHET – ACTIVE DIRECTORY: Tilbyr skyleverandøren en administrert Microsoft AD-tjeneste (Active Directory) i skyen?
17.	SIKKERHET – ACTIVE DIRECTORY LOKALT: Støtter skyleverandørens administrerte Microsoft AD-tjeneste integrering med Microsoft AD lokalt?
18.	SIKKERHET – LDAP: Støtter skyleverandørens administrerte Microsoft AD-tjeneste LDAP (Lightweight Directory Access Protocol)?
19.	SIKKERHET – ACTIVE DIRECTORY: Støtter skyleverandørens administrerte Microsoft AD-tjeneste SAML (Security Assertion Markup Language)?
20.	SIKKERHET – ADMINISTRASJON AV LEGITIMASJON: Tilbyr skyleverandøren en administrert tjeneste som gjør at brukerne enkelt kan rotere, administrere og hente legitimasjon, for eksempel API-nøkler, databaselegitimasjon og andre hemmeligheter?
21.	SIKKERHET – WAF: Tilbyr skyleverandøren en brannmur for nettbaserte apper (WAF, Web Application Firewall) som bidrar til å beskytte nettbaserte programmer mot vanlige nettbaserte angrep som kan påvirke tilgjengeligheten av apper, kompromittere sikkerheten eller forbruke store ressurser?
22.	SIKKERHET – DDOS: Tilbyr skyleverandøren en tjeneste for å beskytte mot de vanligste og hyppigst forekommende distribuerte tjenestenektangrepene (DDoS-angrep) via nettverket og transportlaget, sammen med muligheten til å skrive tilpassede regler for å avverge avanserte angrep på programnivå?
23.	SIKKERHET – SIKKERHETSANBEFALINGER: Tilbyr skyleverandøren en tjeneste for automatisk vurdering av potensielle sårbarheter i programmer og ressurser?
24.	SIKKERHET – TRUSSELOPPDAGELSE Tilbyr skyleverandøren en administrert tjeneste for trusseloppdagelse?
25.	SIKKERHET – TJENESTEBEGRENSNINGER: Har skyleverandøren noen begrensninger (dvs. tjenestebegrensninger) når det gjelder avsnittet om sikkerhet ovenfor? Eksempel: Maksimalt antall hovednøkler til kundene Maksimalt antall maskinvaresikkerhetsmoduler (HSM-er)

6. Samsvar

Listen nedenfor over sertifiseringer og standarder som kan gjelde for skytjenester, er kun til illustrasjonsformål og skal ikke anses som uttømmende.

Oppgi hvilke internasjonale og bransjespesifikke samsvarsstandarder skytjenesteleverandøren har oppfylt:

Sertifiseringer og attester	Lover, forskrifter og personvern	Retningslinjer og rammeverk
☐ C5 [Tyskland]	☐ EU's databeskyttelsesdirektiv	☐ CDSA
☐ CISPEs etiske retningslinjer for databeskyttelse	☐ EU-modellklausuler	
☐ CNDP (Climate Neutral Data Centre Pact)		
☐ DIACAP	☐ FERPA	☐ CIS
☐ DoD SRG nivå 2 og 4	☐ GDPR	☐ Criminal Justice Info. Service (CJIS)
☐ FedRAMP	☐ GLBA	☐ CSA
☐ FIPS 140-2	☐ HIPAA	☐ EU-US Privacy Shield
☐ HDS (Frankrike, helsetjenester)	☐ HITECH	☐ EU Safe Harbor
☐ ISO 9001	☐ IRS 1075	☐ FISC
☐ ISO 27001	☐ TAR	☐ FISMA
☐ ISO 27017	☐ PDPA – 2010 [Malaysia]	☐ G-Cloud [Storbritannia]
☐ ISO 27018	☐ PDPA – 2012 [Singapore]	☐ GxP (FDA CFR 21 del 11)
☐ RAP [Australia]	☐ PIPEDA [Canada]	☐ CREA
☐ MTCS Tier 3 [Singapore]	☐ Privacy Act [Australia]	☐ T Grundschutz [Tyskland]
☐ PCI DSS Level 1	☐ Privacy Act [New Zealand]	☐ MARS – E
☐ EC Rule 17-a-4(f)	☐ Det spanske datatilsynets autorisasjon	☐ MITA 3.0
☐ SOC1/ISAE 3402	☐ U.K. DPA – 1988	☐ MPAA
☐ SOC2/SOC3	☐ VPAT/Section 508	☐ NIST
☐ WIPOs retningslinjer for IaaS		☐ Uptime Institute Tiers
		☐ UK Cloud Security Principles

Offentlige organisasjoner kan benytte samsvarsrapportene ovenfor til å evaluere hvert enkelt tilbud opp mot akseptert sikkerhet, samsvar og operative standarder. Slike rapporter kan vise at en CISP-leverandør som er i samsvar med dem, oppfyller kontrollpunktene nedenfor til drift av datasentre som kreves av leverandører av skytjenester til det offentlige. Å kreve samsvar med slike rapporter hjelper offentlig sektor å sikre at kontrollene nedenfor er på plass.

- **Kontrollert tilgang:** CISP-leverandøren må begrense den fysiske tilgangen til lokaler til kun å omfatte personer som har en berettiget forretningsmessig grunn til å være der. Hvis det gis tilgang, skal den oppheves så snart det nødvendige arbeidet er fullført.
- **Adgangskontroll og overvåking:** Adgang innenfor datasenterets sikkerhetsperimeter skal være en kontrollert prosess. CISP-leverandøren må bemanne inngangspartier med sikkerhetsmedarbeidere og spesialister som overvåker ansatte og besøkende via sikkerhetskameraer. Når godkjente personer er på et senter, må de tildeles et kort som krever flerfaktoraутentisering og som begrenser tilgangen til å gjelde forhåndsgodkjente områder.
- **CISP-datasentermedarbeidere:** CISP-ansatte som rutinemessig trenger tilgang til et datasenter, må tillates adgang til relevante områder av senteret basert på jobbfunksjon, og tilgangen må regelmessig vurderes. Lister over personalet må gjennomgås rutinemessig av en områdetilgangsleder for å sikre at autorisasjonen til hver enkelt ansatt fortsatt er nødvendig. Hvis ansatte ikke har løpende oppgaver som krever tilgang til et datasenter, må de pålegges å følge den samme prosessen som besøkende.
- **Overvåking for å hindre uautorisert tilgang:** CISP-leverandøren må overvåke datasenterets område kontinuerlig for å hindre uautorisert den, ved hjelp av videoovervåking, inntrengingsdeteksjon og systemer for overvåking av tilgangsslogger. Inngangspartier må sikres med mekanismer som utløser alarmer hvis en dør blir tvunget opp eller holdes åpen.
- **CISP-sikkerhetssentrene overvåking av den globale sikkerheten:** CISP-sikkerhetssentrene (Security Operations Centres) må finnes over hele verden og ha ansvar for å overvåke, styre og gjennomføre sikkerhetsprogrammer for CISP-datasentrene. De må overvåke fysisk tilgangsadministrasjon og innbruddsdeteksjonsrespons samtidig som de gir global støtte døgnet rundt til sikkerhetsteamene i datasentrene på stedet. De må tilby kontinuerlige overvåkingsaktiviteter, for eksempel sporing av tilgangsaktiviteter og tilbakekalling av tilgangstillatelser, og være tilgjengelig for å svare på og analysere potensielle sikkerhetshendelser.
- **Gjennomgang av tilgang lag for lag:** Tilgang til infrastrukturet bør begrenses basert på forretningsbehov. Når man implementerer en gjennomgang av tilgang lag for lag, gis det ikke rett til å gå inn i hvert lag som standard. Tilgangen til ethvert bestemt lag skal bare gis hvis det er et spesifikt behov for å få tilgang til det spesifikke laget.
- **Vedlikehold av utstyr er en del av den ordinære driften:** CISP-teamene må kjøre diagnostikk på maskiner, nettverk og reserveutstyr for å sikre at dette er i orden til enhver tid, og klar for en nødsituasjon. Rutinemessig vedlikeholdskontroll av datasenterutstyr og -verktøy må være en del av den ordinære driften av CISP-datasenteret.
- **Sikkerhetsklart reserveutstyr:** Vann, strøm, telekommunikasjon og Internett-tilkobling skal utformes med redundans, slik at CISP-en kan opprettholde kontinuerlig drift i nødstilfeller. Strømforsyningssystemene må være utformet slik at de er fullstendig redundante. Ved strømbrytning må ikke-avbrytbare strømforsyningsenheter kunne kobles til for visse funksjoner, mens generatorer gir reservestrøm til hele anlegget. Personer og systemer må overvåke og kontrollere temperaturen og fuktigheten for å forhindre overoppheting, noe som ytterligere reduserer mulige tjenesteavbrudd.
- **Teknologi og folk arbeider sammen for ekstra sikkerhet:** Det bør være obligatoriske prosedyrer for å få tillatelse til å gå inn i datalaget. Dette inkluderer at autoriserte personer gjennomgår og godkjenner tilgangssøknader fra andre personer. Samtidig må detekteringssystemer for trusler og elektronisk inntrenging overvåke og automatisk utløse alarmer om identifiserte trusler og mistenkelig aktivitet. Hvis for eksempel en dør holdes åpen eller tvinges opp, må det utløses en alarm. CISP-leverandøren må implementere sikkerhetskameraer og beholde opptak i samsvar med juridiske krav og samsvarskrav.
- **Forhindre fysisk og teknologisk inntrenging:** Tilgangspunkter til serverrom skal forsterkes med elektronisk kontrollutstyr som krever flerfaktoraутorisasjon. CISP-leverandøren må også være forberedt på å forhindre teknologisk inntrenging. CISP-servere må kunne advare ansatte om ethvert forsøk på å fjerne data. Hvis det skulle oppstå brudd, skal serveren deaktiveres automatisk.
- **Servere og medier får omhyggelig oppmerksomhet:** Medielagringsenheter som brukes til å lagre kundedata, bør klassifiseres av CISP-en som kritisk viktige og behandles tilsvarende, som enheter med stor innvirkning, gjennom hele livssyklusen. CISP-leverandøren må ha strenge standarder for hvordan enhetene skal installeres, vedlikeholdes og til slutt destrueres når de ikke lenger er nyttige. Når en lagringsenhet har nådd slutten av levetiden, tar CISP-leverandøren mediene ut av drift ved hjelp av teknikker som er beskrevet i NIST 800-88. Medier som lagrede kundedata ikke har blitt fjernet fra, overvåkes av CISP-leverandøren frem til de har blitt satt ut av drift på en sikker måte.

- **Tredjepartsrevisorer verifiserer CISP-prosedyrer og -systemer:** CISP-leverandøren må revideres av eksterne revisorer som inspisierer datasentrene og utfører dypdykk for å bekrefte at CISP-leverandøren følger etablerte regler som trengs for å oppnå sikkerhetssertifiseringer. Avhengig av samsvarsprogrammet og kravene til dette, kan eksterne revisorer intervjuer CISP-ansatte om hvordan disse håndterer og avhender media. Revisorer kan også gå gjennom sikkerhetskameraopptak og observere inngangspartier og korridorer i datasentrene. De kan undersøke utstyr, f.eks. CISP-leverandørens elektroniske tilgangskontrollenheter og sikkerhetskameraer.
- **Forberedt på det uventede:** CISP-leverandøren må proaktivt gjøre forberedelser til potensielle miljøtrusler, som naturkatastrofer og brann. Installering av automatiske sensorer og responsivt utstyr er to måter CISP-leverandøren sikrer datasentrene på. Vanndetekterende enheter må være installert for å varsle ansatte om problemer samtidig som automatiske pumper settes i drift for å fjerne væske og forhindre skade. Tilsvarende skal automatisk brann-deteksjons- og slukkeutstyr redusere risiko og varsle CISP-ansatte og brannvesenet om problemer.
- **Høy tilgjengelighet gjennom flere tilgjengelighetssoner:** CISP-leverandøren må tilby flere tilgjengelighetssoner for større feiltoleranse. Hver tilgjengelighetssone skal bestå av ett eller flere datasentre, være fysisk atskilt fra hverandre og ha redundant strømforsyning og nettverksforbindelse. Tilgjengelighetssoner er forbundet med hverandre med raskt, privat fiberoptisk nettverk, slik at du enkelt kan strukturere applikasjoner med automatisk failover mellom tilgjengelighetssoner uten avbrudd.
- **Simulering av forstyrrelser og målinger av respons:** CISP-leverandøren må ha en plan for virksomhetskontinuitet som en driftsprosessveiledning som beskriver hvordan forstyrrelser på grunn av naturkatastrofer kan unngås og reduseres – med detaljert beskrivelse av tiltak som skal gjennomføres før, under og etter en hendelse. For å redusere virkningen av og være forberedt på det uventede, må CISP-leverandøren regelmessig teste planen for virksomhetskontinuitet med øvelser som simulerer forskjellige scenarioer. CISP-leverandøren må kunne dokumentere ytelsesnivået til medarbeiderne og prosessene sine, og deretter redegjøre for erfaringer og eventuelle korrigerende tiltak som kan være nødvendige for å forbedre responsgraden. CISP-ansatte må være opplærte og klare til å reagere på forstyrrelser, gjennom en metodisk gjenopprettingsprosess for å minimere ytterligere nedetid på grunn av feil.
- **Bidra til å oppfylle effektivitetsmål:** I tillegg til å ta opp miljørisikoer, bør CISP også inkludere bærekraftighetshensyn i datasenterdesign. CISP-leverandøren bør gi informasjon om i hvilken grad de bruker fornybar energi i datasentrene sine, og hvordan dette kan redusere kundenes karbonutslipp sammenlignet med å ha egne datasentre.
- **Valg av plassering:** Før en plassering velges, må CISP-leverandøren utføre innledende miljømessige og geografiske vurderinger. Datasenterplasseringer må velges etter nøye vurderinger for å redusere miljørisikoer som for eksempel flom, ekstremvær og seismisk aktivitet. CISP-tilgjengelighetssoner bør bygges slik at de er uavhengige og fysisk adskilt fra hverandre.
- **Redundans:** Datasentre bør utformes for å forutse og tolerere feil samtidig som servicenivåene opprettholdes. I tilfelle feil, skal automatiserte prosesser flytte trafikken fra det berørte området. Kjerneprogrammer må implementeres etter N+1-standard, slik at det i tilfelle datasenterfeil er tilstrekkelig kapasitet til at trafikk kan lastbalanseres til de øvrige plasseringene.
- **Tilgjengelighet:** CISP burde identifisert kritiske systemkomponenter som kreves for å opprettholde systemets tilgjengelighet og gjenopprette tjenesten ved strømbrytning. Kritiske systemkomponenter må sikkerhetskopieres på tvers av flere, isolerte plasseringer. Hver plassering eller tilgjengelighetssone må være konstruert for å kunne operere uavhengig og med høy pålitelighet. Tilgjengelighetssoner må være sammenkoblet for å gjøre det mulig med automatisk failover av programmer mellom tilgjengelighetssoner, uten avbrudd. Svært elastiske systemer, og dermed tjenestetilgjengelighet, bør være en funksjon av systemdesignet. Datasenterdesign med tilgjengelighetssoner og replikering av data gjør det mulig for CISP-kunder å oppnå ekstremt korte gjenopprettingstider og gjenopprettingsmål, samt de høyeste nivåene av tjenestetilgjengelighet.
- **Kapasitetsplanlegging:** CISP-leverandøren må kontinuerlig overvåke tjenestebruken for å implementere infrastruktur for å støtte tilgjengelighetsforpliktelser og -krav. CISP-leverandøren må opprettholde en kapasitetsplanleggingsmodell som vurderer CISP-infrastrukturbruk og -krav minst en gang i måneden. Denne modellen skal støtte planlegging av fremtidige krav og inkludere hensyn som informasjonsbehandling, telekommunikasjon og lagring av revisjonslogger.

FORRETNINGSKONTINUITET og NØDGJENOPPRETTING

- **Forretningskontinuitetsplan:** CISP-forretningskontinuitetsplanen skal skissere tiltak for å unngå og redusere miljøforstyrrelser. Den må inneholde operasjonelle detaljer om trinn som skal gjennomføres før, under og etter en hendelse. Forretningskontinuitetsplanen må støttes av testing som inkluderer simuleringer av forskjellige scenarioer. Under og etter testing må CISP-leverandøren dokumentere ytelsen til menneskene og databehandlingen, korrigerende handlinger og læringspunkter med tanke på kontinuerlig forbedring.
- **Pandemirespons:** CISP-leverandøren må inkludere retningslinjer og prosedyrer for pandemirespons i planleggingen av nødgjenoppretting for å forberede seg på å reagere raskt på trusler fra utbrudd av infeksjonssykdommer. Skadeavgrensingsstrategien må inkludere alternative bemanningsmodeller for å overføre kritiske prosesser til ressurser utenfor regionen samt aktivisering av en krisestyringsplan for å støtte kritisk forretningsdrift. Pandemiplaner må referere til internasjonale helseorganisasjoner og forskrifter, inkludert kontaktpunkter for internasjonale byråer.

OVERVÅKING og LOGGING

- **Gjennomgang av tilgangen til datasenteret:** Tilgangen til datasentrene skal gjennomgås regelmessig. Når det registreres i CISP-leverandørens HR-system at en ansatt slutter, må vedkommendes tilgang tilbakekalles automatisk. Når en ansatts eller entreprenørens tilgang utløper i henhold til den godkjente varigheten av godkjenningen, skal hans eller hennes tilgang tilbakekalles, selv om han eller hun fortsatt er ansatt i CISP.
- **Tilgangslogger for datasentre:** Fysisk tilgang til CISP-datasentre skal logges og overvåkes, og loggene skal beholdes. CISP-leverandøren skal sammenstille informasjon hentet fra logiske og fysiske overvåkingssystemer for å forbedre sikkerheten etter behov.
- **Overvåking av tilgang til datasentre:** CISP-leverandøren skal overvåke datasentrene ved hjelp av globale sikkerhetssentre (Security Operations Centres), som er ansvarlig for overvåking, styring og gjennomføring av sikkerhetsprogrammer. De må kunne tilby global, døgntilgjengelig support ved å administrere og overvåke tilgangen til datasentrene og sørge for at lokale team og andre supportteam kan svare på sikkerhetshendelser, ved å styre, gi råd, analysere og respondere.

OVERVÅKING og DETEKSJON

- **CCTV:** Fysiske tilgangspunkter til serverrom skal registreres av CCTV (Closed Circuit Television Camera)-kameraer. Opptakene skal beholdes i henhold til lovmessige krav og samsvarskrav.
- **Datasenterets innganger:** Den fysiske tilgangen må kontrolleres ved å bygge inngangspunkter med profesjonelt sikkerhetspersonell som bruker overvåking, deteksjonssystemer og andre elektroniske midler. Autorisert personell skal bruke mekanismer med flerfaktorausikling for å få tilgang til datasentre. Innganger til serverrom skal sikres med enheter som utløser alarmer for å starte en hendelsesrespons hvis døren tvinges opp eller holdes åpen.
- **Inntrengingsdeteksjon:** Elektroniske anlegg for deteksjon av innbrudd bør installeres i datalaget for å overvåke, oppdage og automatisk varsle rett personell om sikkerhetshendelser. Inngangs- og utgangspunkter til serverrom skal sikres med enheter som krever at hver enkelt person flerfaktorausikles før vedkommende slippes ut eller inn. Disse enhetene skal utløse alarm hvis døren tvinges opp uten godkjenning eller holdes åpen. Døralarmer bør også konfigureres til å oppdage forekomster der en enkeltperson går ut eller går inn i et datalag uten flerfaktorausikling. Alarmer bør umiddelbart sendes til CISP-leverandørens døgntilgjengelige sikkerhetssenter for øyeblikkelig logging, analyse og respons.

ADMINISTRASJON AV ENHETER

- **Administrasjon av aktiva:** CISP-aktiva skal forvaltes sentralt gjennom et lagerstyringssystem som lagrer og sporer eiere, plasseringer, statuser og vedlikeholdsstatuser samt har beskrivende informasjon for CISP-eide aktiva. Etter anskaffelse skal aktiva skannes og spores, og aktiva som er til vedlikehold skal kontrolleres og overvåkes for eierskap, status og resultat.
- **Destruksjon av medier:** Medielagringenheter som brukes til å lagre kundedata, må klassifiseres av CISP-leverandøren som kritiske og behandles tilsvarende, dvs. som enheter med høy grad av innvirkning, gjennom hele livssyklusen. CISP-leverandøren må ha strenge standarder for hvordan enhetene skal installeres, vedlikeholdes og til slutt destrueres når de ikke lenger er nyttige. Når en lagringssenheter har nådd slutten av levetiden, tar CISP mediene ut av drift ved hjelp av teknikker som er beskrevet i NIST 800-88. Medier som lagrede kundedata ikke har blitt fjernet fra, skal kontrolleres av CISP-leverandøren frem til de har blitt satt ut av drift på en sikker måte.

DRIFTSSTØTTESYSTEMER

- **Strøm:** CISP-datasentrenes strømforsyningssystemer må være utformet for å være fullstendig redundante og vedlikeholdbare uten at de påvirker driften, 24 timer i døgnet. CISP skal sikre at datasentrene er utstyrt med reservestrømforsyning for å sikre at strøm er tilgjengelig for å opprettholde driften i tilfelle elektrisk svikt, for kritiske og viktige belastninger i anlegget.
- **Klima og temperatur:** CISP-datasentre må bruke mekanismer for å kontrollere klimaet og opprettholde en passende driftstemperatur for servere og annen maskinvare for å forhindre overoppheting og redusere muligheten for tjenesteavbrudd. Personell og systemer må overvåke og kontrollere at temperaturer og fuktighet holdes på korrekte nivåer.

- **Branneteksjon og -slukking:** CISP-datasentre skal være utstyrt med automatisk branneteksjons- og slukkeutstyr. Branneteksjonssystemene må bruke røykvarslere i områder for nettverk, mekanikk og infrastruktur. Disse områdene skal også beskyttes av brannslukkingssystemer.
- **Lekkasjedeteksjon:** For å oppdage vannlekkasjer, må CISP-leverandøren utstyre datasentrene med funksjonalitet for å oppdage tilstedeværelsen av vann. Hvis det oppdages vann, skal det finnes mekanismer for å fjerne vannet for å forhindre ytterligere vannskader.

INFRASTRUKTURVEDLIKEHOLD

- **Utstysvedlikehold:** CISP-leverandøren skal overvåke og utføre forebyggende vedlikehold av elektrisk og mekanisk utstyr for å opprettholde kontinuerlige drift av systemer i CISP-datasentrene. Prosedyrer for vedlikehold av utstyr skal utføres av kvalifiserte personer og gjennomføres i henhold til dokumenterte vedlikeholdsplaner.
- **Miljøledelse:** CISP-leverandøren skal overvåke elektriske og mekaniske systemer og utstyr for å muliggjøre umiddelbar identifisering av problemer. Dette utføres ved å benytte verktøy for kontinuerlig revisjon samt informasjon fra CISP-leverandørens systemer for overvåking av bygninger og strømforsyning. Forebyggende vedlikehold utføres for å sikre at utstyret til enhver tid er operasjonelt.

STYRING og RISIKO

- **Løpende risikostyring av datasentre:** CISP-sikkerhetssenteret må utføre regelmessige trussel- og sårbarhetsgjennomganger av datasentrene. Løpende vurdering og reduksjon av sårbarheter utføres gjennom risikovurderingsaktiviteter i datasenteret. Denne vurderingen skal utføres i tillegg til risikovurderingsprosessen på foretaksnivå som brukes til å identifisere og håndtere risikoer som presenteres for virksomheten som helhet. Denne prosessen må også ta regionale regulatoriske og miljømessige risikoer i betraktning.
- **Sikkerhetsattestasjon fra tredjeparter:** Tredjepartstesting av CISP-datasentre, som dokumentert i tredjepartsrapporter, sikrer at CISP på riktig måte har implementert sikkerhetstiltak tilpasset etablerte regler som er nødvendige for å oppnå sikkerhetssertifiseringer. Avhengig av samsvarsprogrammet og kravene til det, kan eksterne revisorer utføre testing av mediehandtering, gjennomgå opptak av sikkerhetskameraer, observere innganger og ganger i datasentre, teste elektroniske tilgangskontrollenheter og undersøke datasenterutstyr.

7. Migreringer

	Krav
1.	MIGRERINGSTJENESTER: Hvor mange forskjellige datamigreringstjenester tilbyr skyleverandøren?
2.	MIGRERINGER – SENTRALISERT OVERVÅKING: Tilbyr skyleverandøren organisasjoner en sentralisert tjeneste (f.eks. en hovedvisning), der de kan spore og overvåke statusen til server- og programmmigreringer?
3.	MIGRERINGER – KONTROLLPANEL: Har skyleverandørens migreringsverktøy et kontrollpanel som raskt visualiserer migreringsstatus, relaterte beregninger og migreringshistorikk?
4.	MIGRERINGER – SKYLEVERANDØRVERKTØY: Tilbyr skyleverandørens migreringsverktøy integrasjon med andre migreringsverktøy fra skyleverandøren som kan utføre server- og programmmigreringer?
5.	MIGRERINGER – TREDJEPARTSVERKTØY: Tillater skyleverandørens overføringsverktøy å innlemme overføringsverktøy fra tredjeparter? • Hvis ja, hvilke migreringsverktøy fra tredjeparter er det som støttes?
6.	MIGRERINGER – MIGRERINGER I FLERE REGIONER: Tilbyr skyleverandørens migreringsverktøy sporings- og overvåkingmuligheter for server- og programmmigreringer som skjer i forskjellige regioner?

7.	MIGRERINGER – SERVERMIGRERING: Tilbyr skyleverandørens overføringsverktøy en måte å overføre lokale virtualiserte servere til skyen på? Hvis ja, hvilke virtualiserte miljøer støttes for øyeblikket?
8.	MIGRERINGER – OPPDAGELSE AV SERVERE: Kan skyleverandørens migreringsverktøy automatisk oppdage lokale virtuelle servere som skal overføres til skyen?
9.	MIGRERINGER – YTELSESDATA FOR SERVERE: Har skyleverandørens migreringsverktøy mulighet til å samle og vise server- og/eller virtuell maskinytelse som CPU- og RAM-utnyttelse?
10.	MIGRERINGER – DATABASE: Har skyleverandørens migreringsverktøy muligheten til å lagre alle innsamlede data i en sentralisert database? Hvis ja, har organisasjoner muligheten til å eksportere disse dataene? Til hvilke formater?
11.	MIGRERINGER – KRYPTERING AV INAKTIVE DATA: Krypterer skyleverandøren all informasjon som er samlet inn og lagret i søkdatabasen?
12.	MIGRERINGER – TRINNVIS SERVERREPLIKERING: Tilbyr skyleverandørens migreringsverktøy automatisert, direkte inkrementell serverreplikering under migrering av servere eller virtuelle maskiner for å sikre at alle endringer som er gjort på serveren eller den virtuelle maskinen, blir inkludert i den endelig overførte avbildingen? Hvis ja, hvor lenge kan denne tjenesten kjøre?
13.	MIGRERINGER – VMWARE: Støtter skyleverandørens migreringsverktøy VMWare-overføringer av virtuelle maskiner fra lokale maskiner til skyen?
14.	MIGRERINGER – HYPER-V: Støtter skyleverandørens migreringsverktøy overføringer av virtuelle Hyper-V-maskiner fra lokale maskiner til skyen?
15.	MIGRERINGER – PROGRAMOPPDAGELSE: Kan skyleverandørens migreringsverktøy oppdage og gruppere programmer før de blir migrert?
16.	MIGRERINGER – AVHENGIGHETSKARTLEGGING: Kan skyleverandørens migreringsverktøy oppdage avhengigheter mellom servere og programmer før de blir migrert?
17.	MIGRERINGER – DATABASEMIGRERING: Kan skyleverandørens migreringsverktøy migrere lokale databaser til skyen?
18.	MIGRERINGER – DATABASEMIGRERING, NEDETID: Kan skyleverandørens migreringsverktøy utføre databasemigreringer til skyen med minimum nedetid, dvs. At kildedatabasen forblir fullt operativ under migreringsprosessen?
19.	MIGRERINGER – KILDEDATABASES: Støtter skyleverandørens migreringsverktøy migrering av forskjellige databasekilder som Oracle, SQL Server, etc...? Hvis ja, oppgi alle støttede kildedatabaser som kan overføres til skyen.
20.	MIGRERINGER – HETEROGENE MIGRERINGER: Har skyleverandørens migreringsverktøy muligheten til å utføre heterogene databasemigreringer, dvs. fra én kildedatabase til en annen måldatabase som Oracle til SQL Server? Hvis ja, oppgi alle mulige heterogene kombinasjoner av databasemigreringer.
21.	MIGRERINGER – DATAMIGRERING I PETABYTESKALA: Tilbyr skyleverandøren en datatransportløsning i petabyteskala som bruker sikre apparater til å overføre store mengder data inn og ut av skyen?

22.	MIGRERINGER – DATAMIGRERING I EXABYTESKALA: Tilbyr skyleverandøren en datatransportløsning i exabyteskala for å flytte ekstremt store datamengder til skyen?
23.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT: Tilbyr skyleverandøren en tjeneste for sømløst å integrere en kundes datasenter med skylagringstjenester, slik at man kan overføre og lagre data til skyleverandørens lagringstjeneste?
24.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT – OBJEKTLAGRING: Tilbyr skyleverandørens tjeneste for sikkerhetskopiering integrasjon med leverandørens skytjeneste for objektlagring?
25.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT – FILTILGANG: Tillater skyleverandørens tjeneste for sikkerhetskopiering brukere å lagre og hente objekter ved hjelp av fil-protokoller, f.eks. NFS-protokollen?
26.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT – BLOKKTILGANG: Tillater skyleverandørens tjeneste for sikkerhetskopiering brukere å lagre og hente objekter ved hjelp av blokkprotokoller, f.eks. iSCSI-protokollen (Internet small computer systems interface)?
27.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT – BÅNDTILGANG: Tillater skyleverandørens tjeneste for sikkerhetskopiering brukere å sikkerhetskopiere dataene via et virtuelt båndbibliotek og lagre disse båndsikkerhetskopiene i skyen til leverandøren?
28.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT – KRYPTERING: Tilbyr skyleverandørens tjeneste for sikkerhetskopiering kryptering av data i ro og under overføring?
29.	MIGRERINGER – SIKKERHETSKOPIERING FOR BEDRIFT – INTEGRERING AV TREDJEPARTS PROGRAMVARE: Kan skyleverandørens tjeneste for sikkerhetskopiering omtegnes med vanlig tredjeparts programvare for sikkerhetskopiering?
30.	MIGRERINGER – TJENESTEBEGRENSNINGER: Har skyleverandøren noen begrensninger (f. eks. tjenestebegrensninger) når det gjelder avsnittet om migrering ovenfor? Eksempel: Maksimalt antall samtidige migreringer av virtuelle maskiner Maksimalt antall datatransportløsninger

8. Fakturering

	Krav
1.	FAKTURERING – SPORING OG RAPPORTERING Tilbyr skyleverandøren en sporings- og rapporteringstjeneste for fakturering for å hjelpe brukere med å administrere og overvåke bruken av skytilbudet?
2.	FAKTURERING – ALARMER OG VARSLINGER: Tilbyr skyleverandøren brukere en mekanisme for å sette opp alarmer med varsler for å varsle brukere når kostnadene deres har passert en bestemt terskel?
3.	FAKTURERING – KOSTNADSADMINISTRERING Tilbyr skyleverandøren en mekanisme for å bygge og vise grafikk som oppsummerer kostnader og utgifter?
4.	FAKTURERING – BUDSJETTER: Tilbyr skyleverandøren en mekanisme for å vise og administrere budsjetter og prognoseestimerte kostnader?

5.	FAKTURERING – KONSOLIDERT OVERSIKT: Tilbyr skyleverandøren en mekanisme for å konsolidere fakturering fra flere kontoer under en enkelt, primær betalingskonto?
6.	FAKTURERING – TJENESTEBEGRENSNINGER: Har skyleverandøren noen begrensninger (f. eks. tjenestebegrensninger) når det gjelder avsnittet om fakturering ovenfor? Eksempel: Maksimalt antall kontoer som kan grupperes sammen Maksimalt antall alarmer som kan opprettes Maksimalt antall budsjetter som kan administreres

9. Administrasjon

	Krav
1.	ADMINISTRASJON – OVERVÅKINGSTJENESTE: Tilbyr skyleverandøren en overvåkingstjeneste for å administrere skyressurser og programmer som samler inn, overvåker og rapporter ved hjelp av forhåndsdefinerte målinger?
2.	ADMINISTRASJON – ALARMER: Tillater skyleverandørens overvåkingstjeneste brukere å sette opp alarmer?
3.	ADMINISTRASJON – EGENDEFINERTE BEREGNINGER: Tillater skyleverandørens overvåkingstjeneste brukere å opprette og overvåke egendefinerte målinger?
4.	ADMINISTRASJON – OVERVÅKINGSTETTHET: Tilbyr skyleverandørens overvåkingstjeneste forskjellige tetthetsnivåer for overvåking, ned til 1-minuttnivået?
5.	ADMINISTRASJON – API-SPORINGSTJENESTER: Tilbyr skyleverandøren en tjeneste som logger, overvåker og lagrer aktivitet mot skyressurser både på konsollen og på API-nivå for bedre synlighet? Hvis ja, hvilke tjenester fra skyleverandørens er det som integreres med denne sporingstjenesten?
6.	ADMINISTRASJON – VARSLING: Aktiverer skyleverandøren muligheten til å sende ut varsler basert på API-aktivitetsnivåer?
7.	ADMINISTRASJON – KOMPRIMERING: Tilbyr skyleverandøren en mekanisme for å komprimere logger som genereres av API-sporingssystemet for å hjelpe brukerne med å redusere lagringskostnadene knyttet til denne tjenesten?
8.	ADMINISTRASJON – REGIONSAGGREGERING: Tilbyr skyleverandøren muligheten til å registrere API-aktivitet i alle regioner og levere denne informasjonen på en samlet måte for enkel bruk?
9.	ADMINISTRASJON – RESSURSLAGER: Tilbyr skyleverandøren en tjeneste for å vurdere, revidere og evaluere konfigurasjonene av ressurser som implementeres av en bruker?
10.	ADMINISTRASJON – KONFIGURERINGSENDRINGER: Registrerer skyleverandøren automatisk endringer av ressurskonfigurasjoner når det skjer?
11.	ADMINISTRASJON – KONFIGURERINGS Historikk: Tilbyr skyleverandøren muligheten til å undersøke ressurskonfigurasjonen på et hvilket som helst tidligere tidspunkt?

12.	ADMINISTRASJON – KONFIGURERINGSREGLER: Tilbyr skyleverandøren retningslinjer og anbefalinger for klargjøring, konfigurering og kontinuerlig overvåking av samsvar?
13.	ADMINISTRASJON – RESSURSMALER: Tilbyr skyleverandøren brukerne muligheten til å opprette, klargjøre og administrere en samling ressurser på en mallignende måte?
14.	ADMINISTRASJON – RESSURSMALREPLIKERING: Tilbyr skyleverandøren muligheten til raskt å replikere disse ressursmalene på tvers av forskjellige regioner, til bruk i situasjoner med nødoppretting?
15.	ADMINISTRASJON – MALDESIGNER: Tilbyr skyleverandøren et brukervennlig grafisk verktøy med dra-og-slipp-funksjonalitet som forenkler prosessen med å lage slike ressursmaler?
16.	ADMINISTRASJON – TJENESTEKATALOG: Tilbyr skyleverandøren en tjeneste for å opprette og administrere en katalog med tjenester, dvs. servere, virtuelle maskiner, programvare, databaser osv.?
17.	ADMINISTRASJON – KONSOLLTILGANG: Tilbyr skyleverandøren et nettbasert brukergrensesnitt for å lette administrasjon og overvåking av skytjenestene?
18.	ADMINISTRASJON – CLI-TILGANG: Tilbyr skyleverandøren et samlet verktøy for å administrere og konfigurere flere skytjenester fra kommandolinjegrensesnittet (CLI), og er det tillatt å automatisere administrasjonsoppgaver ved bruk av skript?
19.	ADMINISTRASJON – MOBILTILGANG: Tilbyr skyleverandøren en smarttelefonapp som lar brukerne koble seg til skytjenesten og administrere ressursene sine? • Hvis ja, er denne appen tilgjengelig for både iOS og Android?
20.	ADMINISTRASJON – ANBEFALTE FREMGANGSMÅTER: Har skyleverandøren en tjeneste som hjelper brukere å sammenligne skybruken med beste praksis?
21.	ADMINISTRASJON – TJENESTEBEGRENSNINGER: Har skyleverandøren noen begrensninger (f. eks. tjenestebegrensninger) når det gjelder avsnittet om administrasjon ovenfor? Eksempel: Maksimalt antall konfigurasjonsregler per konto Maksimalt antall alarmer som kan opprettes Maksimalt antall logger som kan lagres

10. Support

	Krav
1.	SUPPORT – SERVICE: Tilbyr skyleverandøren support når som helst, 24 timer i døgnet, 7 dager i uken og 365 dager i året via telefon, chat og e-post?
2.	SUPPORT – SUPPORTNIVÅER: Tilbyr skyleverandøren forskjellige supportnivåer?

3.	SUPPORT – NIVÅALLOKERING: <i>Tillater skyleverandøren brukere å selv tildele ressursene/tjenestene som forbrukes, til forskjellige supportnivåer basert på detaljert klassifisering, og ikke ved å tvinge brukerne til å ha separate skykontoer for å oppnå og motta forskjellige nivåer av support?</i>
4.	SUPPORT – FORUMER: <i>Tilbyr skyleverandøren offentlige supportforumer hvor kunder kan diskutere saker?</i>
5.	SUPPORT – OVERSIKT OVER TJENESTENS TILSTAND: <i>Tilbyr skyleverandøren en oversikt over tjenestens tilstands som viser oppdatert informasjon om tilgjengeligheten til tjenesten i flere regioner?</i>
6.	SUPPORT – TILPASSBAR OVERSIKT: <i>Tilbyr skyleverandøren et instrumentbord som viser en tilpassbar oversikt over ytelsen og tilgjengeligheten til tjenestene som ligger til grunn for brukerens spesifikke ressurser?</i>
7.	SUPPORT – HISTORIKK OVER TJENESTENS TILSTAND: <i>Tilbyr skyleverandøren 365-dagers historikk over tjenestens tilstand?</i>
8.	SUPPORT – SKYRÅDGIVER: <i>Tilbyr skyleverandøren en tjeneste som fungerer som ekspert på tilpasset sky og hjelper til med å sammenligne ressursbruken med anbefalte fremgangsmåter?</i>
9.	SUPPORT – LEDER FOR TEKNISK KORT: <i>Tilbyr skyleverandøren en leder for teknisk kort (TAM) som byr på teknisk ekspertise for hele spekteret av skytjenester?</i>
10.	SUPPORT – TREDJEPARTS PROGRAMSUPPORT: <i>Tilbyr skyleverandøren støtte for vanlige operativsystemer og vanlige komponenter i programstakken?</i>
11.	SUPPORT – OFFENTLIG API: <i>Tilbyr skyleverandøren et offentlig API som programmatisk samhandler med supportsaker for å opprette, redigere og lukke slike saker?</i>
12.	SUPPORT – TJENESTEDOKUMENTASJON: <i>Tilbyr skyleverandøren offentlig synlig teknisk dokumentasjon av god kvalitet for alle tjenestene sine, inkludert, men ikke begrenset til, brukerveiledninger, opplæringsprogrammer, svar på vanlige spørsmål og utgivelsesmerknader?</i>
13.	SUPPORT – CLI-DOKUMENTASJON: <i>Tilbyr skyleverandøren enkelt tilgjengelig teknisk dokumentasjon av god kvalitet for kommandolinjegrensesnittet (CLI)?</i>
14.	SUPPORT – REFERANSEARKITEKTURER: <i>Tilbyr skyleverandøren en gratis, nettbasert samling av referansearkitekturdokumenter for å hjelpe kundene å bygge spesifikke løsninger som kombinerer mange av skyleverandørens skytjenester?</i>
15.	SUPPORT – REFERANSE-IMPLEMENTERING: <i>Tilbyr skyleverandøren en gratis, nettbasert samling av dokumenter som inneholder detaljerte, testede og validerte trinnvise prosedyrer, inkludert anbefalte fremgangsmåter, for å implementere vanlige løsninger (dvs. DevOps, store datamengder, datalager, Microsoft-arbeidsbelastninger, SAP-arbeidsbelastninger osv.) i skytilbudene?</i>

Tillegg B: direkte teknisk evaluering

Ved valg av CISP er det viktig å vurdere skyplattformfunksjonene «direkte» ved bruk av CISP-ens offentlig tilgjengelige tjenester og infrastruktur. Vi anbefaler minst 1 hel dag til teknisk evaluering per CISP på kortlisten. Under evalueringen kan du 1) gjennomføre en evaluering i dybden for å vurdere om de demonstrerte funksjonene stemmer med RFP-kravene dine og CISP-ens skriftlige svar, 2) gi ekspertene dine en plattform til å granske CISP-en for å sikre at den passer til og er på linje med de spesifikke tekniske og organisatoriske behovene dine, og 3) få tillit til CISP-ens tjenester og evne til skalering, sikker drift, robust drift og fortsatt innovasjon for å oppfylle fremtidige behov.

Når CISP-er svarer på kravene i en RFP for skytjenester, oppgir de kanskje samsvar basert på en høynivåtolkning av kravene som ikke tar hensyn til hele konteksten til organisasjonens driftsmiljø/programbehov. Vi anbefaler å bemanne et panel for direkte teknisk evaluering med ledende fagfolk innen teknikk, drift, sikkerhet og programmer. De som evaluerer, bør utfordre CISP-en under hele evalueringen, og som anbefalt fremgangsmåte bør de gi poeng til CISP-er uavhengig av hverandre og bedømme scenarioer på en gitt skala, f.eks. 0–4 (0 = uakseptabelt, 1 = på kanten, 2 = akseptabelt, 3 = bra, 4 = fremragende). Etterpå kan poengsummene for demonstrasjonene slås sammen, så den gjennomsnittlige poengsummen for hvert evalueringsscenario inngår i den samlede CISP-evalueringen. Scenarioer med høyt standardavvik bør drøftes av evalueringsteamet i fellesskap før ferdigstilling. Ved sammenslåing kan scenariene vektas etter hvor kritisk viktige de er.

Når det gjelder omfanget på demonstrasjonen, anbefaler vi å se helhetlig på CISP-ens plattform og deretter gå i dybden og evaluere spesifikke arbeidsbelastninger som kjører på plattformen. En eksempelvis skisse av evaluering av plattform og arbeidsbelastning er gitt nedenfor. Organisasjoner kan bygge videre på dette grunnlaget eller tilpasse det for å sikre at de valgte CISP-ene oppfyller de spesifikke funksjonelle og ikke-funksjonelle kravene. Som anbefalt fremgangsmåte kan leverandører som får forelagt listen med scenarioer og krav, få foreslå en dagsorden for direkteevalueringen som maksimerer dekningen og inkluderer 20 % tid til spørsmål og svar.

Plattformevaluering: Mange CISP-er bruker uttrykket «velstrukturert» (Well Architected) om en tilnærming til skyen som gir optimal verdi og minimerer risiko. Velstrukturerte scenarioer i en direkte teknisk demonstrasjon kan omfatte:

1. **Sikkerhet:** identitet, sentralisert styring, automatisk trusselgjenkjenning, databeskyttelse, beredskap
2. **Effektiv ytelse:** riktig skalering, skalerbarhet/elasticitet, serverløst
3. **Pålitelighet:** høy tilgjengelighet (robust ved svikt), reduisering av endringsrisiko, nødgenoppretting, sikkerhetskopiering
4. **Kostnadsstyring:** økonomistyring, kommersiell optimalisering, budsjetter og kostnadsallokering
5. **Fremragende drift:** automasjon, overvåking, support, administrasjon og funksjoner som trengs for å migrere til og operere i skyen

Evaluering av arbeidsbelastninger: Et sett med vanlige programtyper som kan demonstreres, omfatter:

- **Nettapplikasjon:** offentlig drifting av et dynamisk nettsted, inkludert database og statisk objektlagring i bakgrunnen
- **Dataanalyse:** en datasjøhus eller sjøhus-arkitektur som gjør det mulig å slå sammen data fra forskjellige dataleverandører og å håndtere høyt volum (i TB/PB med data), høy variasjon (strukturert, ustrukturert, forskjellige formater osv.) og høy hastighet (i generering av data, endring og spørringsmønstre)
- **Plattform for datavitenskap:** en plattform som muliggjør utvikling, implementering og bruk av AI/ML-baserte funksjoner i hele organisasjonen
- **IoT-applikasjon:** en IoT-plattform/-funksjon som omfatter skyen, nettverksfunksjonen og enhetene

For hver representative arbeidsbelastning som er viktig for organisasjonen din, kan du definere scenarioene CISP-en skal demonstrere. Scenarioene bør demonstrere overordnede funksjoner som muliggjør implementering av arbeidsbelastningen på en velstrukturert måte. De følgende sidene har eksempler på direkte tekniske evalueringskriterier for 1) CISP-ens plattform og 2) et eksempel på en arbeidsbelastning med nettapplikasjon.

Plattform – eksempel på direkte teknisk evaluering

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Sec.1	Identitetsfederering	4	Demonstrer evnen til forbunds-dannelse fra et eksisterende identitetslager til skytjenesten.	• Støtte for standardprotokoller, f.eks. SAML. • Støtte for SCIM-basert identitetsreplikering. • Evnen til å definere forskjellige tilgangsnivåer i bedriftens identitetslager og få dem anvendt hos skyleverandøren. • Evnen til å begrense spesifikke team/enkelt personer kun til bestemte kontoer/prosjekter/arbeidsbelastninger. • Evnen til å støtte attributtbasert tilgangskontroll (ABAC, Attribute-Based Access Control) og bruke attributtene i skyleverandørens system for Identity and Access Management (IAM) til å kontrollere tilgangen til skyressurser.
Plat.Sec.2	Sentral styring	4	Demonstrer evnen til å trekke opp retningslinjer og krav sentralt, på organisatorisk nivå (globale retningslinjer) såvel som på forretningsenhets- og prosjektnivå.	• Retningslinjene bør omfatte aktivering/deaktivering av tjenester og bruk av geografiske restriksjoner (regionsbegrensning). • Retningslinjene bør også hindre brukerne, administratorer inkludert, i å deaktivere eventuelle revisjons-/styringskontroller.
Plat.Sec.3	Begrensning av brukertillatelser	3	Demonstrer de automatiske anbefalingene for innstramming av brukertillatelser.	• Mulighet for å sammenligne gjeldende tillatelser med påkrevde tillatelser. • Automatisk generering av retningslinjer som fremmer færrest rettigheter.
Plat.Sec.4	Revisjonslogging	4	Demonstrer revisjonslogging av skyaktivitet, både for tillatte og forbudte handlinger.	• Sentraliserte logger for hele organisasjonen. • Konto-/prosjektspesifikke logger til støtte for sporing og ansvarlighet på lavt nivå. • Verktøy for spørringer mot logger. • Verktøy som gjør det mulig å utløse handlinger basert på spesifikke hendelser/loggoppføringer. • Funksjon for å vise supportaktiviteten til leverandøren. • Funksjon for å hindre selv administratorer i å slette logger.
Plat.Sec.5	Nettverksisolering	4	Demonstrer og før om mulig bevis for isolering av forskjellige leietakere i skyen. Demonstrer konfigureringen av isolerte delnett (uten tilkobling), private (uten internett) og offentlige (med internettilgang).	• Adskillelse av leietakere, også på VPN og tverrkoblingstjenester. • Mulighet for å kontrollere trafikkflyten fra utenfor skyinfrastrukturen (lokalt), innenfor den og til internett. • Hvordan adskillelsen gjelder ved bruk av delte tjenester som beholdervert eller funksjon som tjeneste.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Sec.6	Datakryptering i ro	4	Demonstrer evnen til å kryptere data i ro, inkludert mulighetene for BYOK og kryptering på klientsiden.	• Evnen til å kreve kryptering av sensitive data. • Evnen til å bruke enten leverandøradministrerte nøkler eller kundeadministrerte nøkler. • Samsvar med FIPS 140-2. • Evnen til å varsle og loggføre manglende samsvar med krypteringskrav. • Virkning på tilleggs kostnader. • Virkning på ytelse. • Støtte for kvantesikre algoritmer og nøkkelstørrelser.
Plat.Sec.7	Kryptering under overføring	4	Demonstrer evnen til å kryptere data under overføring.	• Kryptering som standard for tjeneste-API-er. • Evnen til å muliggjøre kryptering under overføring (TLS) på belastningsbalansering og administrerte API-er. • Støtte for gjensidig autentisering (klient og server).
Plat.Sec.8	Nøkkeladministrasjon	4	Demonstrer evnen deres til nøkkeladministrasjon. Inkluder hele nøkkelen livssyklus. Inkluder integrering med andre Cloud-tjenester.	• Loggføring av oppretting, bruk, rotering og destruksjon av nøkler.
Plat.Sec.9	Konfigurasjonsadministrasjon	3	Demonstrer evnen deres til å administrere konfigurasjon av skyplattformen.	• Hold databasen for konfigurasjonsadministrasjon (CMDB) pålitelig. • Kontroller samsvar. • Utløs handlinger basert på manglende samsvar automatisk. • Evnen til å evaluere konfigurasjonsendringer opp mot anbefalt fremgangsmåte eller egendefinerte regler.
Plat.Sec.10	Nettverkssikkerhet	3	Demonstrer kapasiteten for brannmur for nettapplikasjoner og brannmur, herunder integrering med tredjeparts regelsett/brannmurer og vern mot volumetriske angrep.	• WAF-evner (brannmur for nettapplikasjoner): skalerbarhet. • Støtte for såvel private som offentlige nettverk. • Evnen til å abonnere på feeder for regelsett fra bransje/leverandør. • Utløs automatisk handlinger innenfor infrastrukturen basert på hendelser fra brannmuren for nettapplikasjoner. • Brannmur-evner: skalerbarhet. • Vertsbaserte og nettverksbaserte brannmurer. • Evnen til å referere til logiske grupper eller objekter i tillegg til evnen til å spesifisere CIDR IP-blokker. • Antall regler som støttes for hvert nivå/hver komponent. • Evnen til å støtte en modell for distribuert drift (nettverksteam + utviklerteam) med konfigurering av retningslinjer og nettverk.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Sec.11	Nettverkstilkobling	3	Demonstrer evnen til å koble til lokale nettverk såvel som sluttpunkter/klienter for private nettverk innenfor skyen.	• Privat tilkobling (høy båndbredde > 10 GB/s). • Evnen til å kontrollere retningslinjer for ruting og brannmur i hele organisasjonen. • VPN-tilkobling (nettsted-til-nettsted og klientbasert). • Støtte for IPv6.
Plat.Sec.12	Forekomstadministrasjon	3	Demonstrer evnen til å administrere forekomster.	• Evnen til å overvåke og administrere oppdateringsstatus for en stor mengde forekomster. • Støtte for administrering av oppdateringer for operativsystemene Linux og Windows. • Evnen til å utføre kommandoer i en hel flåte med servere uten behov for SSH. • Evnen til å kontrollere og revidere ekstern tilgang til virtuelle maskiner sentralt. • Evnen til å endre størrelsen på en forekomster, tilknytte ekstra volumer, endre nettverkskonfigurasjonen osv. via konsoll, kommandolinjen (CLI) og API.
Plat.Sec.13	Anvendelse av retningslinjer	3	Demonstrer evnen til å konfigurere tjenester for å forhindre tilgang fra offentlig Internett.	• Evnen til å isolere trafikk til privat nettverk for tjenester som kan inneholde kritisk viktige eller konfidensielle data. • Evnen til å definere retningslinjer som kontrollerer tilgangen til data basert på kildenettverket. • Anvendelse av disse tilgangsrestriksjonene på alle brukerne, også brukere med påloggingslegitimasjon på høyt nivå.
Plat.Sec.14	Sårbarhetsskanning	2	Demonstrer evnen til å skanne etter sårbarheter i maskinbilder (beholder og VM).	• Evnen til å automatisk skanne beholdere i et register. • Evnen til å skanne etter sårbarheter i virtuelle maskiner. • Evnen til å utføre nettverksskanning.
Plat.Sec.15	Nettverksinspeksjon	2	Demonstrer evnen til å fange opp eller speile nettverkstrafikk (NetFlow og hele pakker) innenfra et kundemiljø.	• Evnen til å speile noe av eller all trafikken innenfor skyleverandørens infrastruktur (fra et kunde- og leietakerperspektiv), inkludert oppfangning av hele pakker. • Evnen til å enkelt velge hvilken trafikk du vil fange opp. • Evnen til å skalere til meget høye trafikkvolumer (> 50 GB/s).

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Sec.16	Trusselgjenkjenning	3	Demonstrer plattformens evne til inntrengingsdeteksjon, for eksempel trusler fra nettverk, bruk av påloggingslegitimasjon og analyse av bruksmønstre.	• Evnen til å oppdage suspekt virksomhet, f.eks. «utvinning». • Evnen til å oppdage angrep med «brute force»-autentisering, f.eks. SSH-innlogging. • Evnen til å oppdage lekkasje eller misbruk av påloggingslegitimasjon. • Bruk av ML, analyse av stort antall hendelser og opphenting av prioriterte hendelser. • Innsatsen som kreves for å aktivere eller konfigurere (det enkle er best). • Evnen til å integrere med eksterne tjenester og utløse varslinger. • Evnen til å konfigurere IDS på globalt nivå for alle prosjekter/kontoer.
Plat.Perf.1	Optimalisering av databehandling	2	Demonstrer automatiske anbefalinger for optimalisering av kostnader ved virtuelle maskiner og funksjoner som tjeneste.	• Anbefalinger basert på mønstre i faktisk bruk og arbeidsbelastning. • Anbefalingene omfatter anslåtte besparelser og innsikt i forventet belastningsnivå og tekniske implikasjoner. • Optimalisering bør omfatte både besparelser og «ytelsesrisiko» når virtuelle maskiner f.eks. kan bli for små.
Plat.Perf.2	Miljøoptimalisering	2	Demonstrer automatiske anbefalinger for andre skykomponenter, f.eks. belastningsbalansering, nettverk, databaser, lagring osv.	• Anbefalingene identifiserer besparelser og potensielle ytelsesforbedringer også i andre komponenter enn kjernen i databehandlingen.
Plat.Perf.3	Autoskalering av databehandling	4	Demonstrer de automatiske skaleringsnivåene til en applikasjon som er implementert bak belastningsbalansering i et virtuelt databehandlingsmiljø. Demonstrer de forskjellige tilgjengelige valgmulighetene og tilnærminger samt evnen til å utløse andre (valgfrie) handlinger før og etter skaleringshendelser, f.eks. varsling.	• Forskjellige valgmuligheter for skalering: utløserbaserte, tidsbaserte, manuelle eller mer intelligente tilnærminger som bruker maskinlæring til å forutsi kapasitetsbehov. • Helautomatisk skalering, inkludert registrering med belastningsbalansering og tilstandssjekk. • Evnen til å kjøre et vilkårlig stykke kode ved spesifikke punkter i skaleringslivssyklusen.
Plat.Perf.4	Skalering for lagring på nett	3	Demonstrer evnen til å skalere både kapasitet og gjennom gjennomstrømming for blokklagring uten avbrudd i arbeidsbelastningen.	• Evnen til å overføre blokklagring mellom forskjellige lagringstyper uten å måtte bygge tjenester helt på nytt. • Evnen til å øke størrelsen på volumer som presenteres for virtuelle maskiner.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Perf.5	Autoskalering for administrerte tjenester	3	Demonstrer evnen objektlageret, API-gatewayen, FaaS-plattformen og NoSQL-databasen har til å skalere fra få (titalls) til flere (tusentalls) samtidige brukere.	• Sømløs autoskalering, ideelt uten administratorinngrep. • Konsekvent ytelse under en gradvis oppskalingsperiode som er på linje med skaleringsbehovene ved produksjon. • For noen komponenter, som FaaS, bør man etter behov også se på muligheter for forvarming og administrasjon av grenser for samtidig kjøring.
Plat.Perf.6	Beholder-baserte arbeidsbelastninger	3	Demonstrer evnen til å være vert for beholder-baserte arbeidsbelastninger.	• Valgmuligheter for plattformer for beholdervert. • Integrering med andre IaaS-komponenter, f.eks. belastningsbalansering. • Tilgang på en tjenestemesh-løsning. • Ikke-proprietære alternativer for beholdervert, f.eks. Kubernetes. • Egen støtte for høy tilgjengelighet innen beholderens kontrollplan. • Evnen til å administrere lokale beholder-verter.
Plat.Rel.1	Regional robusthet	4	Demonstrer automatisk failover i en relasjonsdatabase-forekomst innenfor en region ved simulering av en geografisk avgrenset svikt (f.eks. strømbrydd).	• Automatisk failover. • Isolerte feilsoner innen en skyregion. • Klart avgrenset og lett å strukturere for høy tilgjengelighet.
Plat.Rel.2	Automatisk gjenoppretting av forekomst	2	Demonstrer automatisk gjenoppretting av en forekomst eller et sett med forekomster etter en tilstandssjekk som viser feil.	• Konfigurerbare tilstandssjekk • Helautomatisk gjenoppretting og klargjøring av forekomst
Plat.Rel.3	Tilstandskontroll ved belastningsbalansering	3	Demonstrer hvordan belastningsbalanseringen automatisk detekterer svikt på en forekomst og ruter om trafikken til andre, fungerende verter.	• Konfigurerbare tilstandssjekk • Automatisk trafikkruiting til fungerende verter.
Plat.Rel.4	Failover mellom regioner	3	Demonstrer en arkitektur med flere regioner, herunder automatisk flytting av trafikk til en sekundær region.	• Globalt bevisste tilstandssjekk. • Automatiske rutingalternativer: latens, vektet og failover. • Støtte for arbeidsbelastninger med virtuell maskin samt administrerte tjenester, f.eks. tjeneste for objektlager eller NoSQL-database.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Rel.5	Sikkerhetskopiering og gjenoppretting	4	Demonstrer mulighetene for sikkerhetskopiering og gjenoppretting for virtuelle maskiner, databaser og administrerte tjenester.	• Automatiseringsnivået. • Evnen til å gjenopprette til samme skyregion eller til en annen. • Evnen til å kopiere sikkerhetskopier til en annen skyregion.
Plat.Cost.1	Budsjetter	3	Demonstrer evnen til budsjettstyring, inkludert hvordan det kan struktureres i underkontoer og prosjekter.	• Ta i betraktning muligheten for budsjettkontroll og -overvåking på forskjellige nivåer i organisasjonen. • Sjekk fleksibiliteten, for eksempel evnen til å gruppere komponenter (med merking), sette opp budsjetter for spesifikke skytjenester og konfigurere terskler for varsling og overvåking.
Plat.Cost.2	Budsjettallokering	1	Demonstrer klargjøringen av et nytt prosjektmiljø (en ny konto), inkludert prosessen med budsjettallokering for prosjektet. Klargjøringen bør omfatte manuelle godkjenningstrinn for 1) teknisk vurdering og IT, 2) kommersiell vurdering og økonomi.	• Evnen til å klargjøre seg selv gitt de rette godkjenningene. • Automasjon av konfigureringen av riktig innstilling, varslinger eller retningslinjer for budsjett etter hva som passer for organisasjonen.
Plat.Cost.3	Budsjetttrapportering	2	Demonstrer evnen til å rapportere om budsjetter i hele organisasjonen. Rapport for en bestemt avdeling eller for hele organisasjonen («need to know»). Rapporteringen bør omfatte «faktiske» utgiftstall såvel som forventede eller anslåtte.	• Evnen til å gi innsyn i forskjellige nivåer av organisasjonen og skape bevissthet og gjennomsiktighet, men på «need to know»-basis. • Prognoser bør baseres på nåværende og tidligere trender i forbruk og gi tidlig varsel om potensielle budsjettoverskridelser.
Plat.Cost.4	Budsjettkontroller	1	Demonstrer evnen til å utføre handlinger når en budsjetterskel blir nådd. Slike handlinger kan omfatte varslinger, bruk av restriksjoner eller aktive inngrep for å forhindre budsjettoverskridelse.	• Evnen til enkelt å definere handlinger for forskjellige prosjekter. • Muligheten for at handlingene kan variere fra ett prosjekt til et annet, f.eks. med henblikk på implikasjoner for utvikling kontra produksjon. • Evnen til å definere flere handlinger og terskler for samme budsjett eller prosjekt. • Evnen til å lage egendefinerte handlinger i tillegg til standardmulighetene.
Plat.Cost.5	Budsjettperioder	1	Demonstrer evnen til å anvende budsjetter for forskjellige tidsperioder: daglig, månedlig, årlig, osv. For årlige budsjetter: demonstrer evnen til å anvende en variabel fordeling av forventede utgifter over året.	• Evnen til å definere budsjetter for forskjellige tidsperioder. • Evnen til å konfigurere en fordeling av utgifter over året for årlige budsjetter, noe som er særlig viktig for sesongpregede og meget elastiske arbeidsbelastninger, f.eks. skattemelding.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Cost.6	Markedsplass for tredjeparter	3	Demonstrer evnen til å kjøpe og implementere produkter fra tredjepart. Demonstrer hvordan man setter opp budsjett for et sett med tredjepartsprodukter som er tilgjengelige via en markedsplass, samt evnen til å begrense de tilgjengelige produktene.	• Evnen til å sette opp et budsjett for et spesifikt produkt, et globalt budsjett og et budsjett for et sett med produkter eller kontoer. • Evnen til å kun presentere en mindre del av den videre markedsplassen til skybrukere.
Plat.Cost.7	Prismodeller for databehandling	3	Demonstrer de forskjellige pris- og handelsmodellene som kan anvendes på virtuelle maskiner.	• Mulighetene bør omfatte behovsbasert prissetting, uten krav om langsiktig forpliktelse, samt finkornet prissetting (pr. minutt/time). • Valgfrie langsiktige forpliktelser mot rabatt. • Evnen til å kjøpe forekomster der man godtar avbrudd mot rabatt. • Det er viktig at man kan blande disse modellene innenfor samme prosjekt eller kontoer, og at flere kontoer kan dele fordelene.
Plat.Cost.8	Anbefalinger om kommersiell optimalisering	3	Demonstrer evnen til å få anbefalinger om kommersiell optimalisering for å optimalisere utgifter (uten å måtte gjøre tekniske endringer).	• Helhetlige anbefalinger for flere tjenester, for eksempel virtuelle maskiner og administrerte databaser. • Evnen til å enkelt handle ut fra anbefalingene og forstå den forventede besparelsen eller fordelene.
Plat.Cost.9	Dedikerte verter	4	Demonstrer evnen til å klargjøre en dedikert vert for bruk av lokal lisens knyttet til en bestemt vert.	• Lettvint klargjøring. • Evnen til å administrere utnyttningen av verten. • Evnen til å la forskjellige prosjekter eller leietakere dele verten.
Plat.Ops.1	Migrering av virtuelle maskiner	3	Demonstrer import av en virtuell maskin fra lokalt til en skybasert VM-tjeneste.	• Evnen til å importere både Windows og Linux-baserte operativsystemer. • Evnen til å importere flere maskiner samtidig. • Evnen til å opprettholde en replikeringsøkt for å muliggjøre rask «failover» til skyen.
Plat.Ops.2	DevOps og automasjon	4	Demonstrer evnene til DevOps og automasjon, blant annet hvordan miljøer defineres som kode, støtte fra helautomatiserte implementeringer, automatisk testing og tilbakerullinger.	• Evnen til å definere alle systemkomponenter som kode, inkludert nettverk, virtuelle maskiner, lagre og databaser. • Evnen til å opprette en kanal (pipeline). • Evnen til å opprette et kodearkiv. • Evnen til å automatisere bygging. • Evnen til å utføre blå/grønne implementeringer. • Evnen til å opprette flere miljøer og ha flere stadier i implementeringen. • Automatisk tilbakerulling for mislykkede implementeringer.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Plat.Ops.3	Applikasjonsvert	2	Demonstrer vert for en enkel 2-lagsapplikasjon på en lavkode-/plattformtjeneste. Inkluder en relasjonsdatabase og autoskalering for applikasjons- og nettlaget.	• Enkel konfigurering via brukergrensesnittet. • Inkluder tilstandssjekk, skalering og høy tilgjengelighet. Plattformstøtte: Windows og Linux.
Plat.Ops.4	Sikkerhetsintegrering	2	Demonstrer integreringsevnene til plattformen deres i perspektiv av sikkerhetsinformasjon og hendelsesadministrasjon.	• Evnen til lett å integrere og forbruke sikkerhetsrelaterte logger fra skyleverandøren, pluss API-er til integrering.
Plat.Ops.5	ITSM-integrering	3	Demonstrer integreringsevnene til plattformen deres i ITSM-perspektiv (IT Service Management, IT-tjenesteadministrasjon).	• Evnen til å ta opp, overvåke, og oppdatere en supportsak gjennom en API. • Evnen til å klargjøre tjenester eller sett med tjenester som «produkter» gjennom en API.
Plat.Ops.6	Support	4	Demonstrer supporttilbudet deres.	• Forskjellige supportnivåer for forskjellige slags arbeidsbelastninger. • Evnen til også å støtte operativsystemet, databasemotoren osv., ettersom det passer for en gitt tjeneste. • Evnen til å tilby personlig kvalitetsservice («white glove») med navngitte støtteansvarlige til kritisk viktige arbeidsbelastninger. • Evnen til å tilby en strukturert prosess for beredskap og arkitekturgjennomgang. • Innsyn i leverandørens veikart.
Plat.Ops.7	Reviderbarhet	4	Demonstrer verktøysettet dere har til å støtte samsvarsrevisjoner.	• Evnen til å få detaljer fra samsvarsrevisjonen via konsoll. • Evnen til å administrere og automatisere miljørevisjoner.
Plat.Ops.8	VM til beholder	1	Demonstrer konverteringen av en applikasjon på en virtuell maskin til beholder, og hvordan den leveres via skyleverandørens beholderplattform.	• Brukervennlig konvertering. • Tiden konverteringen tar. • Plattformstøtte: .Net og Java.

Arbeidsbelastning: Nettopplikasjon – eksempel på direkte teknisk evaluering

Det følgende avsnittet gir et eksempel på evalueringsskjema for en bestemt nettopplikasjon-arbeidsbelastning. Når man utvikler et evalueringsskjema for en gitt applikasjon, anbefales det sterkt å involvere brukerne, utviklerne og administratorene av applikasjonen, siden de trolig har den beste forståelsen av behovene, de aktuelle utfordringene og begrensningene.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Web.Sec.1	Sikkerhet – applikasjonsbeskyttelse	3	Demonstrer evnen til å blokkere skadelige forsøk på å utnytte applikasjonen via SQL-innsetting, XSS-angrep og andre angrep.	• Evnen til beskyttelse mot vanlige angrep fra starten av, med standardregler og standardfunksjoner. • Evnen til å opprette egendefinerte kontroller, regler og funksjoner.
Web.Sec.2	Sikkerhet – hastighetsbasert beskyttelse	3	Demonstrer evnen deres til å blokkere eller beskytte mot angrep basert på meget hyppige forespørsler eller datamengder rettet mot en applikasjon.	• Evnen til å konfigurere grenser og begrense hyppigheten på forespørsler fra en gitt IP-adresse eller -adresseliste.
Web.Sec.3	Sikkerhet – kildebasert beskyttelse	3	Demonstrer evnen til å begrense tilgang basert på nettverk eller geografisk kilde.	• Evnen til å begrense etter nettverksblokk eller liste over nettverksblokker. • Evnen til å begrense etter opprinnelsesland (uten behov for å administrere IP-lister).
Web.Sec.4	Sikkerhet – nettverkssegmentering	4	Demonstrer evnen til å isolere og beskytte komponenter (webserver, appserver, DB-server) mot spredning gjennom infrastrukturen både fra klient til server («nord-sør») og mellom servere («øst-vest»).	• Evnen til å plassere komponenter i forskjellige delnett og kontrollere trafikkflyten mellom forskjellige delnett. • Evnen til å kontrollere trafikkflyten på nettverksgrensesnittnivå. • Evnen til å referere til logiske grupper såvel som CIDR-blokker.
Web.Sec.5	Sikkerhet – TLS-støtte og sertifikatadministrasjon	4	Demonstrer evnen til å levere et TLS-sikret sluttunkt og automatisk administrere støttekomponentene for å levere det, for eksempel automatisk rotering av sertifikater.	• Støtte for de nyeste TLS-protokollene og evnen til å deaktivere eldre versjoner etter behov. • Enkel generering, administrering og rotering av sertifikater (helst helautomatisk).

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Web.Perf.1	Ytelse – skalerbarhet	4	Demonstrer evnen til å skalere fra 10 til 100 000 samtidige brukere av nettapplikasjonen via dynamisk autoskalering.	• Evnen til å definere både tidsbaserte og utløserbaserte skaleringsregler. • Sømløs skalering for sluttbruker og administrator. Automatisk utskalering når belastningen øker og innskalering når den avtar. • Sikre at det finnes skalerbarhet i alle lag av nettapplikasjonen (belastningsbalansering, weblaget, datalaget osv.). • Tilgang til bufringstjenester i forskjellige lag av applikasjonen der det passer.
Web.Perf.2	Ytelse – global levering	3	Demonstrer evnene deres innen innholdsleveringsnett (CDN, Content Delivery Network), herunder latens fra forskjellige punkter på kloden, blant annet Australia, Asia, Afrika, Midtøsten, Nord-Amerika, Sør-Amerika og Europa.	• Evnen til å opprette og konfigurere CDN via CISP-ens konsoll eller API-er. • Konfigurerbare distribusjonsregler for forskjellige geografier. • Konfigurerbar bufring for forskjellige brukstilfeller og applikasjoner.
Web.Rel.1	Pålitelighet – robusthet i enkeltregion	4	Demonstrer evnen til å tåle en lokalisert hendelse som for eksempel tap av nettverkstilkobling til CISP-ens datasenter.	• Automatisk failover og høy tilgjengelighet innenfor en skyregion (by).
Web.Rel.2	Pålitelighet – flerregional implementering	3	Demonstrer en flerregional implementering av en nettapplikasjon, inkludert en globalt replikert database.	• Evnen til å implementere en flerregional applikasjon programmatisk. • Replikering mellom regionene for datalageret. • Automatisk ruting av brukere til optimal region for dem.
Web.Rel.3	Pålitelighet – flerregional failover	3	Demonstrer automatisk failover for en nettapplikasjon for tilfellet med et tjenesteproblem med regionale virkninger.	• Automatisk failover og høy tilgjengelighet på tvers av flere skyregioner.
Web.Cost.1	Kostnad – synlighet	2	Demonstrer evnen til å spore kostnad per applikasjon.	• Evnen til å se historiske kostnader for en bestemt applikasjon, blant annet når den skalerer opp eller ned.
Web.Cost.2	Kostnader – budsjetter	2	Demonstrer evnen til å sette opp budsjetter og tilknyttede varslinger per applikasjon.	• Budsjetter som konfigureres per applikasjon og evnen til å utløse handlinger eller varsler basert på konfigurerte terskler.

Scenario-ID	Scenarionavn	Viktighet (1 = lav, 4 = kritisk)	Krav til demonstrasjonen	Hensyn ved poenggivning
Web.Ops.1	Ops – tidsluker for vedlikehold	3	Demonstrer evnen til å konfigurere tidsluker for vedlikehold i henhold til forretningsbehov, spesielt der vedlikeholdet kan virke inn på tilgjengeligheten til applikasjoner.	• Konfigurerbare tidsluker for vedlikehold av komponenter som f.eks. en relasjonsdatabase-tjeneste.
Web.Ops.2	Ops – loggføring	3	Demonstrer evnen til å sentralisere loggføring for en applikasjon med flere komponenter, blant annet med logger som varer ved når virtuelle maskiner avsluttes eller svikter.	• Evnen til å konfigurere en sentralisert loggføringstjeneste som kan skaleres etter applikasjonens behov. • Evnen til å definere regler og filtre for å utløse varsler eller handlinger basert på bestemte logghendelser.
Web.Ops.3	Ops – overvåking	3	Demonstrer overvåking av applikasjonen, inkludert ytelse, tilgjengelighet, responstider, antall feil osv., samt funksjonalitet for å utføre handlinger eller utløse varsler basert på terskler for forskjellige mål.	• Tilgang på en samling standardmålinger, f.eks. lesing og skriving til disk, database, nettverk, belastningsbalansering osv. • Evnen til å angi egendefinerte målinger og terskler. • Evnen til å opprette et egendefinert kontrollpanel for gjengi de viktigste målingene, og dele disse kontrollpanelene med relevante brukere.