Sikkerhet og anskaffelse av skytjenester i offentlig sektor

21.4.2026

Norwegian agency for public and financial management

Trusselbilde og fundament

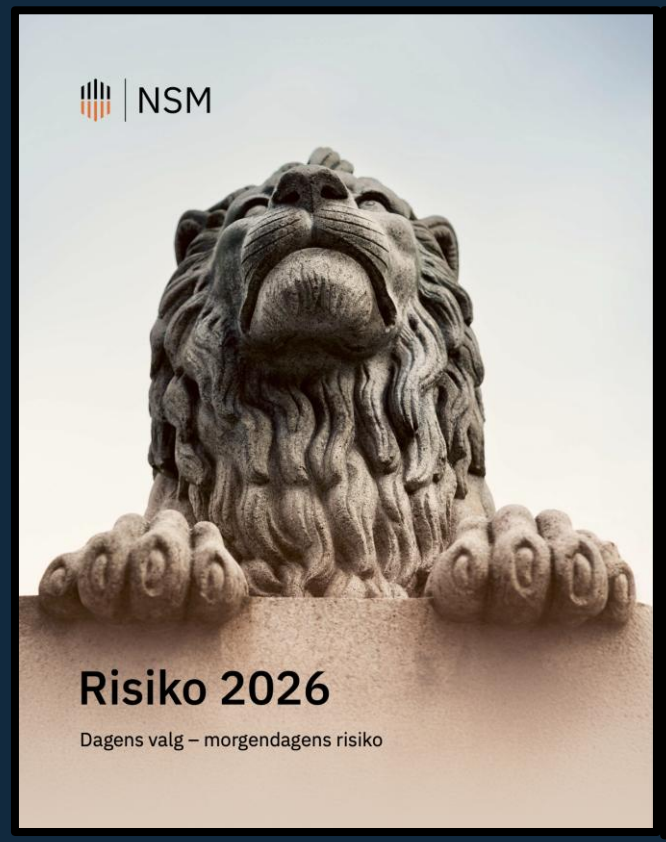
Sverre Stoltz og Ingrid Sørensen

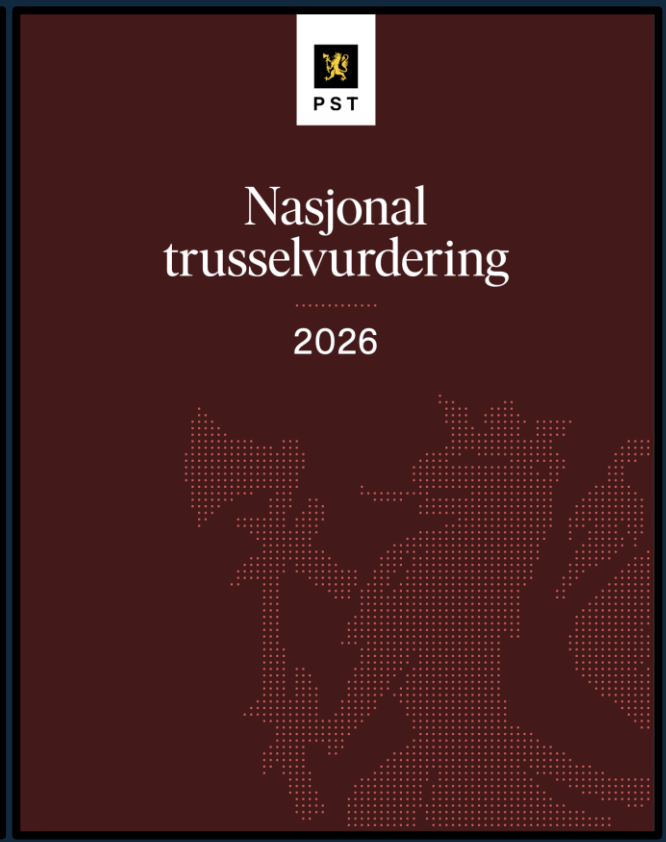
Norwegian agency for public
and financial management

Hva er så spesielt med skytjenester?

Bakgrunn – et stadig mer utfordrende trusselbilde

- Økt digitalisering
- Økt trusselbilde
- Offentlig sektor utsatt





Secure by design & kunstig intelligens

Secure by design

Kunstig intelligens, maskin-læring og automatisering

Diskusjon

Hva betyr "nasjonal kontroll" ved bruk av internasjonale skytjenester?

Klassisk juridiske forhold, spesielle skynære forhold, informasjonssikkerhet, personvern, kommersielle forhold, miljø/sosiale krav, datalagringsgeografi, fiberkabler, strømtilførsel, sikkerhet, programvare, m.m.

Hvordan påvirker tjenesteutsatt drift en anskaffelse?

- Behovsavklaringer
- Funksjonelle og ikke-funksjonelle krav
- Tildelingskriterier
- Kontraktskrav
- Kvalifisering
- Tilbudsbearbeidelse
- Forhandlinger
- Tildeling
- Implementering
- Drift & forvaltning
- Back-up/lokal kopi
- Skifte av leverandør

Anskaffelse

Drift og forvaltning

Hva er skytjenester?

VS

Lokal løsning

Sky

Lokal løsning vs sky

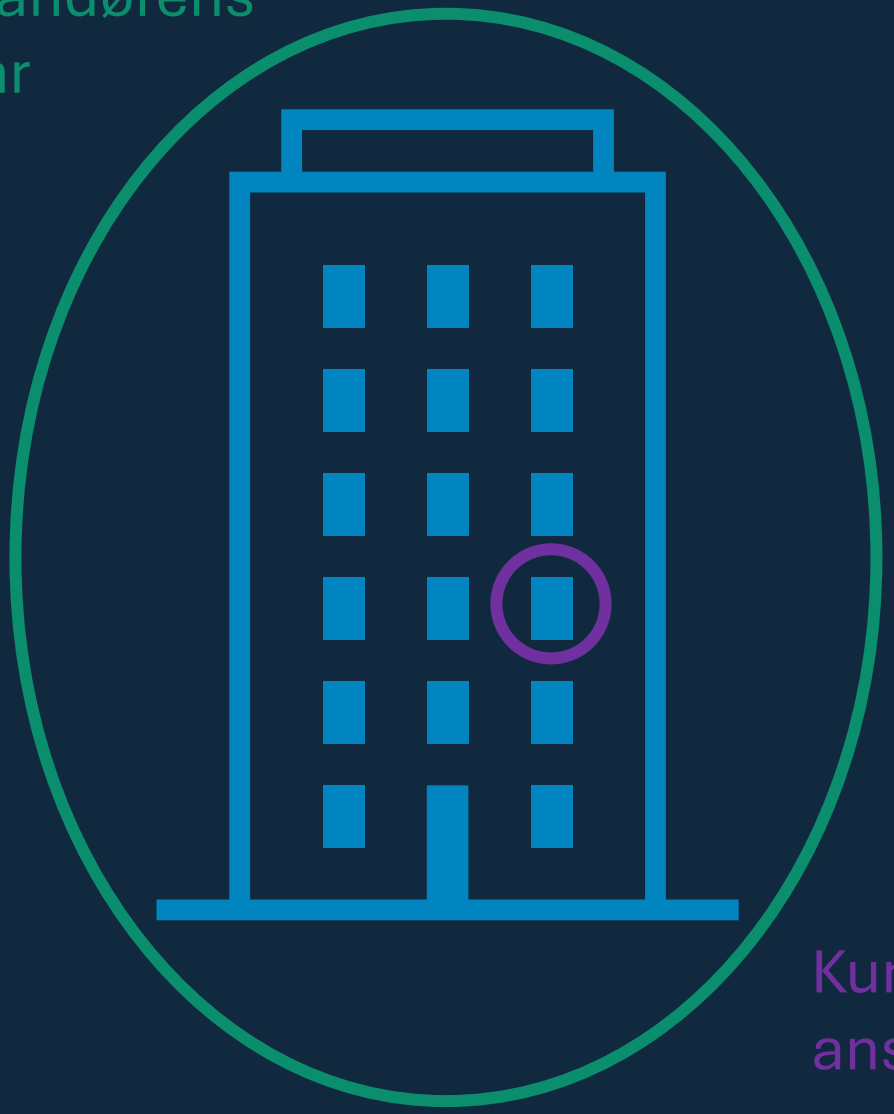
Aspekt	Tradisjonell IT-drift	Skybasert drift
Anskaffelse	Store investeringer i maskinvare og datasenter	Ressurser kjøpes som tjenester
Kostnadsmodell	Kapitalkostnader med flerårige investeringssykluser	Driftskostnader med løpende betaling basert på faktisk bruk
Skalerbarhet	Oppskalering krever nye investeringer og leveringstid	Nærmest ubegrenset skalerbarhet på minutter/timer
Drift og vedlikehold	Alt ansvar ligger hos virksomheten – maskinvare, strøm, kjøling og oppdatering	Leverandøren er ansvarlig for infrastruktur og plattform, virksomheten har ansvar for konfigurasjon og bruk
Fleksibilitet	Fast kapasitet som ikke utnyttes fullt	Dynamisk kapasitet som går opp eller ned basert på behov
Tilgjengelighet	Avhenger av den lokale infrastrukturen, og maskinvare	Global infrastruktur med redundans og høy Service Level Agreement (SLA)
Sikkerhet	Full kontroll – fullt ansvar	Delt ansvar hvor leverandør sikrer infrastrukturen, mens virksomheten sikrer konfigurasjon, egen bruk og data

Skytjenester

- **Definisjoner (NIST):**
  - Leveransemodeller: IaaS, PaaS, SaaS.
  - Tjenestemodeller: Allmenn sky (Public), Privat sky, Hybrid sky.

Skyens delte ansvarsmodell

Leverandørens ansvar



Kundens ansvar

Hovedregel:

Leverandøren er ansvarlig for sikkerheten *av* skyen (infrastruktur, fysisk sikring, nettverk).

Kunden er ansvarlig for sikkerheten *i* skyen (data, brukere, konfigurasjon).

Skyens delte ansvarsmodell

- **Variasjoner etter leveransemodell:**
  - **IaaS (Infrastructure)**
    - Kunden må selv patche OS, konfigurere brannmurer og sikre applikasjoner. Leverandøren sikrer "bærende konstruksjoner" (datasenter/hardware).
  - **PaaS (Platform)**
    - Leverandøren tar over OS og runtime. Kunden fokuserer på applikasjonskoden og dataene.
  - **SaaS (Software)**
    - Leverandøren drifter alt det tekniske. Kundens ansvar koker ned til to kritiske ting: **Data** og **Identitet (tilgangsstyring)**.

DEL 1

Pause

Følg MPS på LinkedIn →

Norwegian agency for public and financial management

Juridisk og sikkerhetsfaglig kjerne

Hanna Hjertås, Sverre Stoltz og Kristina Nikolajeva

Norwegian agency for public
and financial management

Kontrakter – hva er viktig?

SSA-L

Den mest brukte standardavtalen for skyanskaffelser. Hvorfor?

Når SSA-L fungerer godt

- Standardiserte SaaS / ASP-tjenester
- Løpende leveranser over tid
- Direkte kontrakt med skyleverandør

Når SSA-L er mindre egnet

- Store skyplattformer
- Omfattende implementeringer
- Høy grad av tilpasning

VEDLEGG TIL AVTALEN

Alle rubrikkar skal vere kryssa av (ja eller nei)	Ja	Nei
Vedlegg 1: Kunden sin kravspesifikasjon		
Vedlegg 2: Leverandøren si skildring av tenesta		
Vedlegg 3: Plan for etableringsfasen		
Vedlegg 4: Tenestenivå med standardiserte kompensasjonar		
Vedlegg 5: Administrative reglar		
Vedlegg 6: Samla pris og prisreglar		
Vedlegg 7: Endringar i den generelle avtaleteksten		
Vedlegg 8: Endringar av avtalen etter avtaleinngåinga		
Vedlegg 9: Vilkår for Kunden sin tilgang og bruk av tredjepartsleveransar		
Andre vedlegg:		

SSA-L er et godt valg der man kjøper løpende skytjenester med begrenset behov for etablering, og ønsker fleksibilitet, klare ansvarsforhold og mulighet for direkte leveranse fra skyleverandør

Hvordan velge riktig SSA for sky?

Det finnes ikke en riktig SSA for alt – hva passer din skyanskaffelse?

SSA	Når den skal brukes
SSA-L	Standardiserte tjenester – SaaS tjenester.
SSA-Sky	Større skyanskaffelser med betydelig implementering, konfigurering og plattformbruk
SSA-Lille sky	Enklere skykjøp og rene lisenser uten særlig bistand fra leverandøren.

De store skyleverandørenes standardvilkår

Generelle vilkår

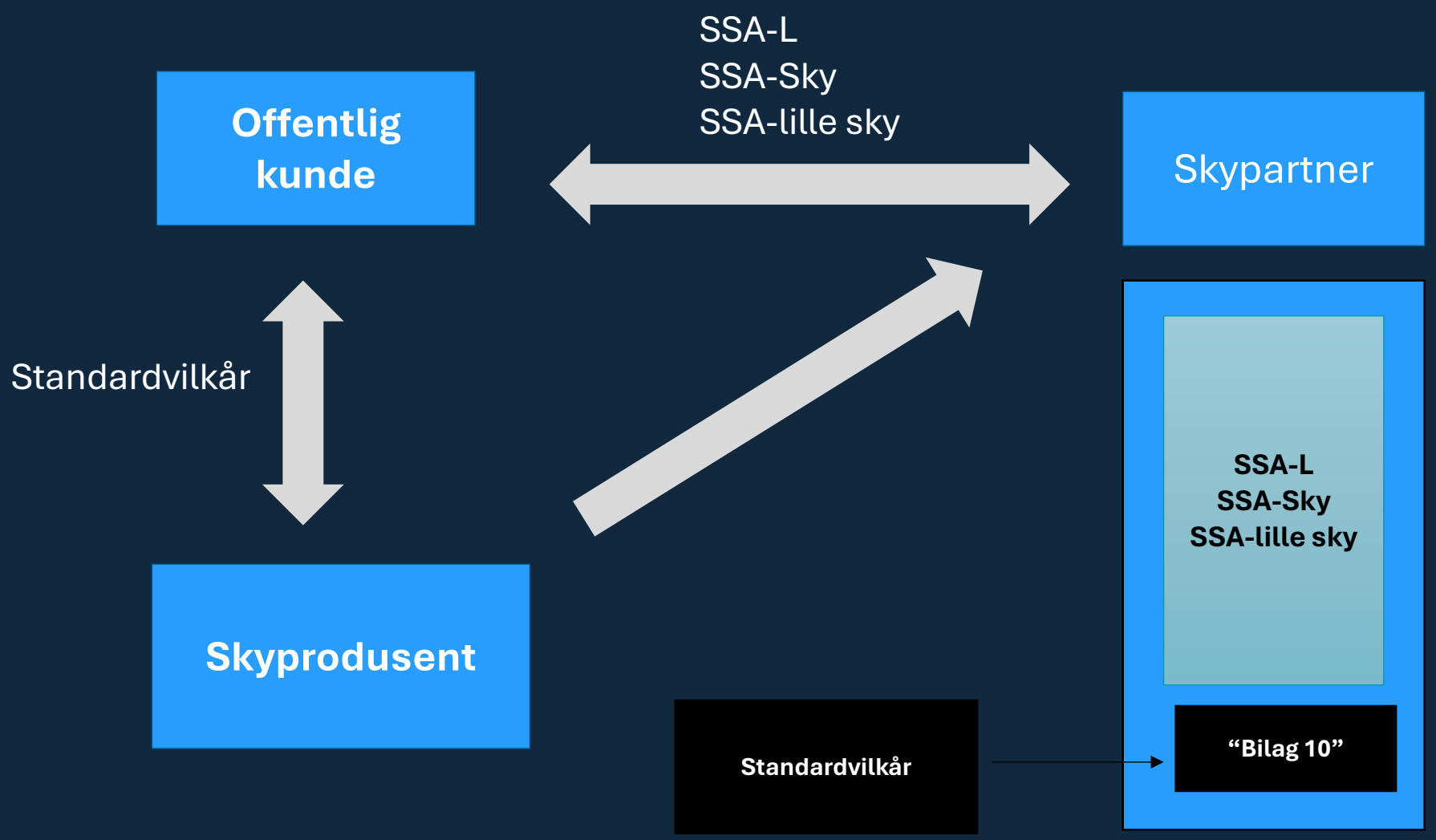
- Generelle kommersielle og juridiske vilkår

Spesielle vilkår

- Mer tjenestespesifikke vilkår
- Informasjonssikkerhet (CRA)
- Personvern

Leverandørens vilkår

De store skyleverandørenes standardvilkår



DBA - Databehandleravtale

Dersom en annen virksomhet behandler personopplysninger på «vegne av dataaansvarlig» skal det inngås en databehandleravtale.

- GDPR artikkel 28

SLA

Service level agreement – det eneste stedet leverandøren tar et ansvar. Og det er ofte ikke stort. En viss påpasselighet må utvises her. Men også for kostnadene.

- 99% = 87,6 timer (eller 3 dager og 16 timer)
- 99,9% = 8 timer og 45 minutter
- 99,999 (five-nines) = 5 minutter og 15 sekunder
- Store kostnadsmessige konsekvenser, balanser behovet for oppetid mot kostnadene

- Tjenestenivået må beskrives presist
- SLAen regulerer ofte i praksis økonomien i tjenesteleveransen
- Brudd på tjenestenivået = repeterende brudd regnes som kontraktsbrudd, eller økt økonomisk ansvar

Hva er planen for å komme ut av leverandørforholdet?

Kontrakter – hva er viktig? (3)

- **Exit-strategi:** Hvordan unngå "vendor lock-in"? Krav til datauttrekk og formater ved avslutning. Teknisk og kommersielt. De vanligste grunnene til at en exit-strategi utløses. Reduser konsentrasjonsrisiko.

Årsaker

- Konkurs
- End of life
- Konkurranse
- Behov
- Eiere

Planer

- Format
- Fra hvor til hvor?
- Linjekapasitet
- Lokal kopi
- Cybersikkerhet/GDPR

Exit-bestemmelser

- Terminering
- Kostnader
- Betalingsforpliktelser
- Assistanse/bistand
- Rådgivning

- Kanskje lurt å ha en to-leverandørstrategi?

Sikkerhet i skyene

Norwegian agency for public and financial management

Regulatoriske krav

- NIS2-direktivet (EU 2022/2555)
- Digitalsikkerhetsloven
- GDPR
- Sikkerhetsloven
- eForvaltningsforskriften § 15

Nasjonale rammeverk for sikkerhetsstyring

- NSM Grunnprinsipper
- Sikkert.no
- DigDir – Internkontroll
- DFØ

Standard, rammeverk og sertifiseringer

- Rammeverk: NIST CSF, NSM
- Standarder: ISO 27001/27002, CSA CCM, C5
- Sertifiseringer: ISO 27001, SOC 2 Type II, CSA STAR

Cloud Reference Architecture

v. 1.2

Norwegian agency for public and financial management

Referansearkitektur v 1.2

CRA v1.2 er forankret og har mapping til NIS2-direktivet [EU, 2022], ISO 27001:2022, ISO 27002:2022, NIST CSF 2.0, NSM Grunnprinsipper 2.1, CSA CCM v4.0, BSI C5:2020 og NIS2 Implementing Regulation.

- Sikkerhet av skyene (leverandør) og Sikkerhet i skyene (kunden)
- Tilpasset norske behov
- Kravbank – Bruk det du trenger

Hva er Cloud Reference Architecture?

Cloud Reference Architecture (CRA) – referansearkitekturen for skytjenester – er et felles krav- og strukturgrunnlag for informasjonssikkerhet og personvern i offentlige skyanskaffelser. CRA er utviklet for å gi virksomheter et praktisk verktøy som kan brukes i hele livsløpet:

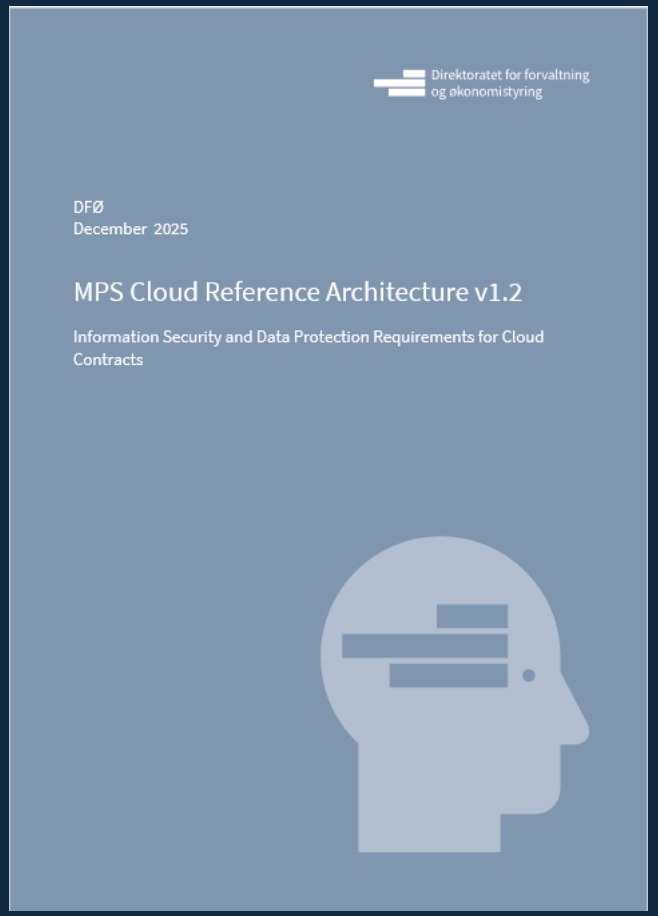
- planlegging og kravstilling
- konkurranse og evaluering
- leverandørdialog og kontraktsoppfølging
- revisjon og kontinuerlig forbedring

CRA bidrar også til å tydeliggjøre skillet mellom:

- **sikkerhet av skyen** (leverandørens ansvar), og
- **sikkerhet i skyen** (kundens bruk og konfigurasjon)

Referansearkitektur – struktur

A-Krav **prinsipielle krav**	**Overordnede krav til kontraktsmessige forhold**
B-Krav **Basiskrav**	**Obligatoriske krav til cybersikkerhet**
C-Krav **Tilleggskrav**	**Leverandørens forslag til cybersikkerhetsarkitektur basert på kundens behov**



#mps

CRA dekker et bredt spekter av krav

	Krav
Identitets- og tilgangsstyring (IAM)	CRA-krav B.IS.24–B.IS.28 dekker tilgangsstyring, rollebasert tilgang (RBAC), minste privilegium, privilegert tilgang, kundeintegrasjon mot IAM og sikker fjernaksess.
Logging og overvåking	CRA B.IS.14, B.IS.33 og B.IS.34 krever tilgang til relevante sikkerhetslogger ved hendelser samt logging av tilgang til kundedata med definerte oppbevaringsperioder [NIST, 2024].
Konfigurasjonsstyring	CRA B.IS.36–B.IS.40 krever sporbar endringsstyring, sikker konfigurasjon, testing og sikker utviklingspraksis: hvem kan endre hva, hvordan endringer godkjennes, og hvordan avdrift fra baseline oppdages.
Kryptering og nøkkelstyring	CRA B.IS.30–B.IS.32 krever beskyttelse av kundedata (både «in transit» og «at rest») samt bruk av moderne kryptografi og dokumentert nøkkelstyring.
Zero Trust-arkitektur	CRA B.IS.24–B.IS.31 og C.1–C.2 understøtter dette prinsippet

Mapping tables

- Mapping – følgende er i tabellene i dag
  - NIST CSF 2.0
  - ISO27001:2022
  - ISO27002:2022
  - NSM Grunnprinsipper 2.1
  - CSA CCSM v 4.0.12
  - BSI C5:2020
  - NIS2 Directive
  - NIS2 Implementing Regulation Annex

Cloud Reference Architecture v1.2

Cloud Reference Architecture er nå oppdatert til v1.2 – nå med tydelig mapping til både NIS2-direktivet og NIS2 implementing regulation.

Markedsplassen for skytjenester (MPS) publiserer nå en oppdatert versjon av **Cloud Reference Architecture (CRA) v1.2** – *referansearkitekturen for skytjenester* – med forbedret sporbarhet mot NIS2. I denne oppdateringen er mappingen strukturert slik at CRA-kravene nå har:

1. egen kolonne for mapping til **NIS2 Directive** (artikler), og
2. **egen** kolonne for mapping til **NIS2 implementing regulation** (Annex-kontroller)

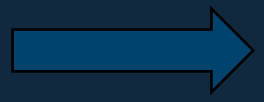
Dette gjør det enklere å skille mellom **"hva som kreves"** (direktivet) og **"hvordan det konkretiseres" (i**mplementing regulation), og gir et mer praktisk grunnlag for anskaffelser, leverandørdialog og oppfølging i drift.

Hvordan støtter CRA NIS2

CRA v1.2 inneholder en detaljert kartlegging av alle krav til NIS2-direktivet [EU, 2022]. Tabellen nedenfor gir en forenklet oversikt over sentrale koblinger:

NIS2-artikkel	CRA-dekning
Art. 20 – Ledelsesansvar	CRA A.1, A.8
Art. 21.2(a) – Risikoanalyse	CRA A.2, B.IS.1-2
Art. 21.2(b) – Hendelseshåndtering	CRA A.6, B.IS.11-16
Art. 21.2(c) – Kontinuitet	CRA B.IS.41-43
Art. 21.2(d) – Forsyningskjede	CRA B.IS.7-8
Art. 21.2(f) – Effektivitetsmåling	CRA A.4, B.IS.4-5
Art. 21.2(g) – Cyberhygiene	CRA B.IS.46, C.11
Art. 21.2(i) – Tilgangskontroll	CRA B.IS.24-34
Art. 23 – Rapportering	CRA A.6, B.IS.12

MPS | CRA | Neste steg



AI Governance Requirements (hvordan kravstille?)

Kahoot!

DEL 2

Pause

Følg MPS på LinkedIn →

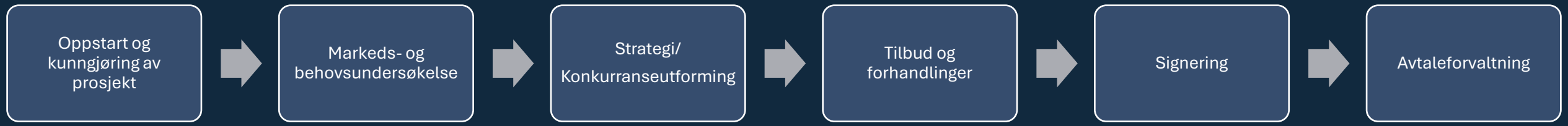
Norwegian agency for public and financial management

Anskaffelsesprosessen

Helene Stunes og Hanna Hjertås

Norwegian agency for public
and financial management

Anskaffelsesprosessen



Anskaffelsesprosedyrer

Ett-trinns prosedyre

Anbudskonkurranse

Tilbudskonkurranse

m.m.

Anskaffelsesloven: Lov om offentlige anskaffelser (anskaffelsesloven) – Lovdata
Anskaffelsesforskriften: Forskrift om offentlige anskaffelser (anskaffelsesforskriften) - Lovdata

Anskaffelsesprosedyrer

Ett-trinns prosedyre

Anbudskonkurranse

Tilbudskonkurranse

m.m.

To-trinns prosedyre

Konkurranse med forhandling

Konkurranse med dialog

Digdir: Anskaffelser i gjennomføringsfasene | Prosjektveiviseren

m.m.

Anskaffelsesloven: Lov om offentlige anskaffelser (anskaffelsesloven) – Lovdata
Anskaffelsesforskriften: Forskrift om offentlige anskaffelser (anskaffelsesforskriften) - Lovdata

Konkurransebestemmelser og kontrakt

Published February 2025

dfø

Instructions to tenderers

Negotiated procedure with pre-qualification

for the procurement of Cloud Research & Advisory 24/576

Norwegian public sector cloud marketplace
Norwegian agency for public and financial management
Phone no.: 400 07 997
E-mail: markedsplassen@dfo.no
Business registration no.: 986 252 932

dfø

Framework Agreement for the provision of

Cloud Research & Advisory

Reference number: 24/576
Doffin reference: 2025-101743
Ted reference: 85691-2025

Signatures

The Contracting Authority	The Supplier
Date, place	16/9 OSLO Date, place
Nina Kulås *CEO, DFØ*	*Elin Ronesen* *MVP Legal Counsel, Gartner Norge AS*

Norwegian public sector cloud marketplace
Norwegian agency for public and financial management
Business registration no.: 986 252 932

Konkurransebestemmelser

- Formål og behov
  - Kunder
  - Varighet
  - Økonomiske rammer
  - Tilhørende dokumenter
- Instruksjoner og begrensninger
- Tidsplan for konkurranse
- Kvalifiseringskrav
- Evaluering
- Tildeling

Link ITT Cloud R&A: Cloud Research & Advisory (Cloud R&A) | markedsplassen for skytjenester

Cloud R&A | Anskaffelse

Omfang	• Artikkeldatabase/forskningsmateriell • Tilgang på analytikere/rådgivere • Konferanser/arrangementer
Type kontrakt	• Rammeavtale (ikke-eksklusiv og frivillig)
Parallelle avtaler	• 2 – 4 leverandører
Delkontrakter	• Nei
Verdi	• Estimert: 300.000.000 NOK • Maks: 550.000.000 NOK
Varighet	• 3 år *eller* • til maksverdi er nådd
Opsjoner	1. Utvidelse 1 (ett) år 2. Kommuner og fylkeskommuner
Kunder	• 303 (98 tilsluttede kommuner/fylkeskommuner)

Kvalifikasjonskrav

Eksempler på hva vi bruker som kvalifikasjonskrav for våre anskaffelser:

Krav til leverandørens registrering, autorisasjoner mv. (FOA § 16-2)

Leverandøren skal være et lovlig etablert foretak og være registrert i et relevant fag-, handels- eller foretaksregister i leverandørens opprinnelses- eller etableringsstat.

Økonomisk og finansiell kapasitet (FOA § 16-3)

Leverandøren skal ha tilstrekkelig økonomisk og finansiell kapasitet til å oppfylle kontrakten.

Tekniske og faglige kvalifikasjoner (FOA §16-5)

Leverandøren skal ha relevant erfaring. Med relevant erfaring menes levering av liknende tjenester.

Seleksjon

4.5 Selection criteria

The Contracting Authority's intention is to limit the number of otherwise qualified candidates to a number between three and five candidates, who will be invited to tender. The Contracting Authority reserves the right to continue the procedure even if fewer than three candidates are qualified.

The shortlist of qualified candidates will be reduced to between three and five candidates who will be invited to tender on the basis of the following criterion:

Nr.	Selection criterion	Documentation requirements
S1	The Supplier's quality, relevance and scope of the submitted references.	*QR3 sec. 4.4.3*

Notwithstanding the above, only participants representing distinct cyber threat intelligence solutions/services shall be selected among the participants. Furthermore, if there are two or more participants representing the same solution/service, the Contracting Authority reserves the right to select only the highest-ranked participant for further participation in the procurement process

Kravspesifikasjon i skyanskaffelser

to typer krav – ett beslutningsgrunnlag

Funksjonelle krav

Hva brukeren skal kunne gjøre.
Hvilke behov som dekkes.
Hvilke effekter som skapes.
Løsningsnøytrale.
Gir grunnlag for evaluering.

Tekniske krav

Arkitektur og sikkerhet.
Drift og tilgjengelighet.
Integrasjoner og API-er.
Etterlevelse og standarder.
Må fungere i standard sky.

Kravspesifikasjonen skal fremheve forskjeller – ikke låse løsninger

Evalueringskrav

- Sammenlikne tilbudene
- Helhetlig vurdering
- Kvalitet i fokus
- Risiko som eget kriterium: kontrakt, SLA, skyvilkår, personvern og sikkerhet
- Reell leveranseforståelse gjennom forhandlingene

The framework agreement will be awarded on the basis of the tender with the best price-quality - risk ratio according to the following criteria:

Award criteria	Weight	Assessment areas	Documentation
Quality	50 %	▪ Functional requirements; and ▪ Technical requirements as further described in clause 5.3.2 below	▪ Appendix 1 (Service)
Price	30 %	▪ Total price as further described in clause 5.3.3 below	▪ Attachment 2.1 Price matrix All prices exclusive of VAT
Risk	20 %	▪ Contractual agreement documents, hereunder terms relating to information security and data protection as further described in clause 5.3.4 below	• Attachment 7 Contractual clauses • Attachment 8 Compliance information security and data protection • Appendix 4.5 Supplier's Terms & Conditions including service level agreement (SLA) and limitations and reservations

Absolutte krav

Ja/nei-krav

Disse kravene er enten oppfylt eller ikke. Manglende oppfyllelse innebærer avvsiningsplikt

Når burde du stille absolutte krav?

Krav som er så viktige at du ikke kan akseptere tilbudet uten.

Forbehold det til krav som er ufravikelige.

Redusert handlingsrom

Absolutte krav låser prosessen tidlig og reduserer fleksibiliteten

Fallgruve: «for sikkerhetsskyld»

Ofte benyttes begreper som «krav», «skal» eller «må» i konkurransedokumentene uten at det er ment å innebære at kravet er absolutt, presiser dette i konkurransedokumentene.

Sikkerhetskrav –absolutte krav?

«Secure by Design»: sikkerhet er innebygd i løsningen fra start

"MFA (Multifaktorautentisering): Løsningen *skal* støtte MFA for alle brukere, og *skal* kunne integreres med kundens IdP (f.eks. MS Entra ID/ID-porten).

SSO (Single Sign On):

Løsningen *skal* støtte moderne autentiseringsprotokoller (SAML 2.0 / OIDC).

Logging: Kunden *skal* ha tilgang til revisjonslogger (audit logs) som viser hvem som gjorde hva og når. Loggene må kunne eksporteres via API til kundens SIEM-system.

Ingen standardpassord:

Løsningen skal ikke leveres med forhåndsdefinerte passord.

Hvordan vi håndterer sikkerhetskrav

Sikkerhet forankres i kontrakten
Hovedtyngden av sikkerhetskravene ligger i kontrakten, ikke i kravspesifikasjonen. Kravspesifikasjonen knyttes primært til løsning og funksjonalitet, og inneholder derfor begrenset med sikkerhetskrav.

Reelle og etterprøvbare kontraktskrav
Gjennom et eget informasjonssikkerhetsbilag stilles detaljerte krav til leverandørens styring, prosesser og sikkerhetspraksis over tid.

Strukturert og transparent sikkerhetsoppfølging
Leverandøren må eksplisitt redegjøre for etterlevelse av hvert krav (ja / delvis / nei). Dette gir tydelighet rundt avvik, modenhet og forbedringsbehov, og muliggjør systematisk oppfølging av sikkerhet gjennom hele kontraktsperioden.

Gruppearbeid: Burde sikkerhetskrav være absolutte krav?

- **Bør sikkerhetskrav være absolutte krav i offentlige anskaffelser?**

Når gir det mening å gjøre et sikkerhetskrav absolutt (må-krav)?

Når gir absolutte sikkerhetskrav mindre verdi – eller skaper utfordringer?

Ta gjerne utgangspunkt i:

- Security by Design
- MFA (multifaktorautentisering)
- SSO (Single Sign-On)
- Logging
- Ingen standardpassord

- **Tips**: Sertifiseringer (ISO 27001) er ofte bedre som kvalifikasjonskrav enn som tildelingskriterier. Eller?

Kahoot!

DEL 3

Pause

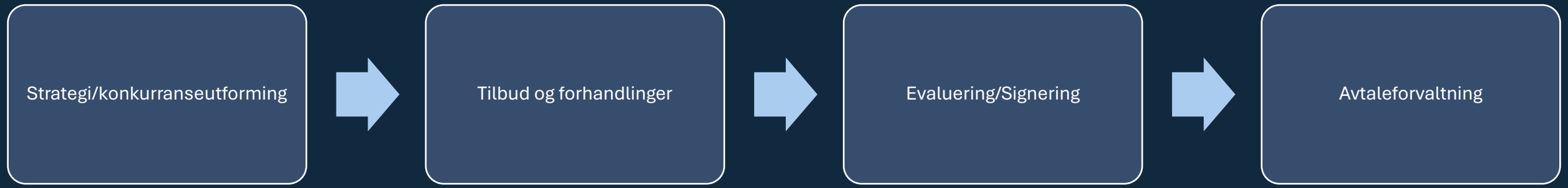
Følg MPS på LinkedIn →

Norwegian agency for public and financial management

Fra forhandling til forvaltning

Sverre Stoltz, Kristina Nikolajeva og Helene Stunes

Norwegian agency for public
and financial management


Strategi/konkurranseutforming
Tilbud og forhandlinger
Evaluering/Signering
Avtaleforvaltning

Strategi og konkurranseutforming

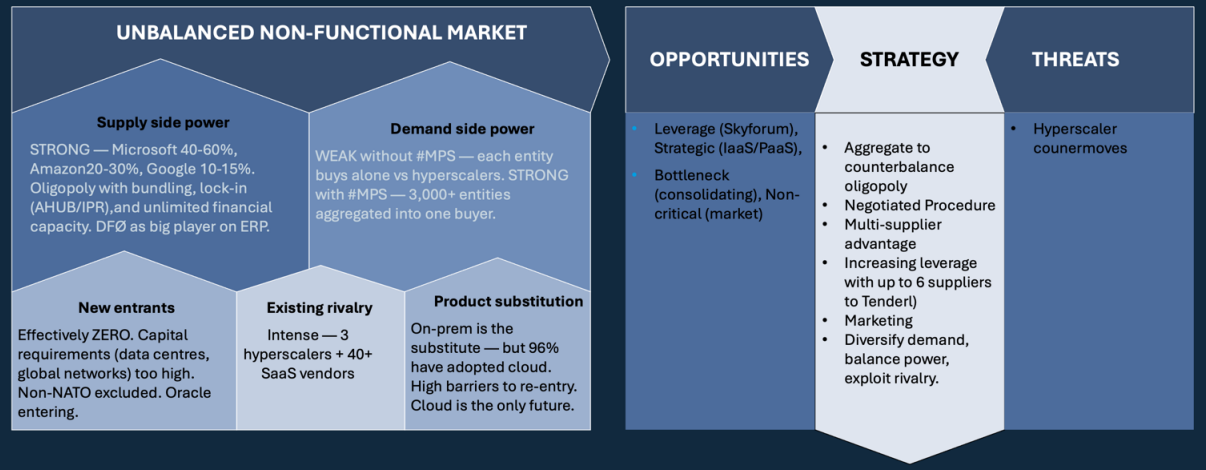
- Strategi er ikke en plan
- Valg som foretas før planen lages
- Skal vi lage det selv eller anskaffe?
- Dekke alle behovene eller noen?
- Når?
- Hva kjennetegner markedet?
- Hvordan er leverandørene?
- Hvordan produseres tjenenesten?
- Hvilken strategi har leverandørene?
- Er det et fungerende marked?

- Porter’s Five Forces
- SWOT
- Porter’s Four Corners
- Porter’s Supply Chain
- Ansoff Diversification
- Kralijic/Gelderman Matrix

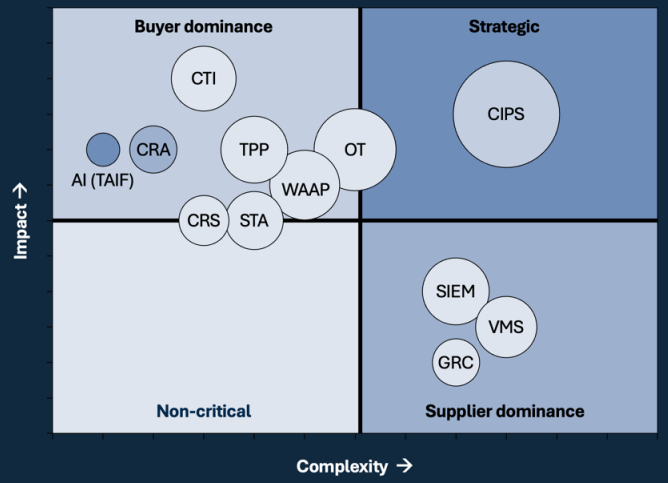
- Øke forståelse
- Strategi
- Forhandlinger

Limited use of normal market mechanisms

The competitive landscape of the Norwegian public sector shows an ubalanced cloud market with parts monopoly/parts oligopoly with Microsoft and DFØ as the main players.



Current supply positioning



##	Short-name	Long-name
1	CIPS	Cloud infrastructure & platform services
2	SIEM	Security incident and event management
3	VMS	Vulnerability management services
4	GRC	Governance, risk & compliance
5	CTI	Cyber threat intelligence
6	CRA	Cloud research & advisory
7	TPP	Third-party privacy management
8	STA	Security training & awareness
9	CRS	Cyber risk score
10		

Eksempel

Strategy development model

01 Foundation (Steps 1-2) | 02 Choices (Steps 3-4) | 03 Selection (Step 5) | 04 Implementation (Step 6) | 05 Monitor (Step 7)

	Step	Description	Key considerations	Outcome
①	**Vision & mission**	Clear and inspiring picture of the desired future state	Align with mission and resonantes with stakeholders	Direction and motivation for strategic initiatives
②	**Objectives**	SMART	Cascades from vision, support to overall strategy	Guides decision making
③	**Analysis**	Assessment, data-driven	Intern/external, building stratetic depth	Developing alternatives
④	**Alternatives**	Range of courses of action	Exploring alternatives, resources, risk appetite	Informed choice, strategic flexibility
⑤	**Selection**	Chosen path	Balance objectives, feasibility, alignment with vision/mission	Guide resource allocation and prioritisation of efforts
⑥	**Implementation**	Execution through defined actions	Commitment across organisation	Actionalbe tasks, initiating innovation and progress
⑦	**Monitoring & control**	Performance assessments, adjustments	Metrics, review and feedback loops	Ensure alignment with strategic intent

#mps

Growth vectors

Four paths to 50% market share and a dominant posision by 2030 includes NBC2, cloud enablement, hardened public cloud, SaaS, FA and governance deepening.

Market development **Three-pronged approach** • Nordic-Baltic Cloud Connect • Health sector probe • Cloud Enablement	**Diversification** **We do not expect difersification** • RAG-AI (Sovereign AI) • OT Security (New domain) • Cloud Enablement (New domain)
Market penetration **Deepen governance** • FA participation from 318 → 500 • Grow Skyforum to 5.000 p/y • CIPS governance deepening	**Product development** **Expand current offerings** • SaaS/Project-M (Menon) • CyberX Phase 3 (MDR) • Hardened public cloud (HSM)

#mps

Hva kan forhandles?

- Pris
- Kontraktsvilkår
- SLA
- DPA
- Kvalitet
- Sikkerhet

Plan og forberedelser

- Definere mål og ønsket resultat
- Etablere tidsplan og møtefrekvens
- Sikre nødvendige ressurser
- Forberede teamet (roller, ansvar, felles forståelse)
- Være godt forberedt
- Forberede leverandørene

God forberedelse legger grunnlaget for en god forhandling – og øker sannsynligheten for å oppnå ønsket resultat.

Eksempel: Fem – steg forhandlingsplan

Evalueringfasen

- Tildelingskriterier
- Vurdering av tilbud
- Risiko og etterlevelse
- Ansvar og struktur
- Dokumentasjon

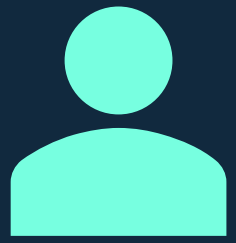
Tildeling og signering

- Meddelelsesbrev til leverandører
- Debrief (erfaring og tilbakemelding)
- Protokoll og dokumentasjon
- Karensperiode
- Kontraktsignering

Onboarding

Leverandører

- Strategi for call-offs
- Møtevirksomhet og oppfølgning
  - Governance-møter



Kunder

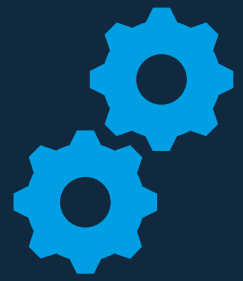
- Kommunikasjon til virksomhetene
  - Oppstartsmøte
- Markedsføring
- Veiledning
- Kontraktstilgang til kunder

Internt

- Forvaltningsplan

Avrop og implementering

- Avrop
  - Fordelingsnøkkel
  - Minikonkurranse
  - M.m.



Implementering

- Tilgang
- Hjelp fra leverandørene
- Kurs og kompetanse ved bruk av løsninger
- Interne ressurser

Leverandøroppfølging

- Møter – frekvens
- Tydelig roller og ansvar

DFØ peer role	Responsibility	Supplier peer role	Responsibility
MPS' Category Manager	Contact person for reporting and daily activities. Not authorised to make changes to the contract. Responsible for the agreement		
MPS' Security Officer	Following up security incidents, monitoring security level		
MPS' Authorised Representative	Authorised representative. Authority to amend, change the Framework Agreement.		
MPS' Program director	Responsible for the performance of MPS. Escalation points, settling disputes.		
Head of MPS	Escalation point. Settling disputes		

Agenda

- Eksempler

Main topic	Elements within topic
Parties' overall performance	1. Utilisation, including implementation, of the services 2. Customer success - status 3. Areas of improvement 4. Commercial development 5. Legal developments 6. Data protection developments 7. Performance indicators, performance and content 8. Management Information report
Company update and strategic risk	1. Company update and strategic risk 2. Road map
Information security risks	1. Information security risks and vulnerabilities 2. General security situation 3. Special security situation for Norway 4. Evolving the security reference architecture to accommodate changes in the cybersecurity threats and risk landscape 5. Information security incidents
Social and environmental	Status and forecast 1. Social requirements 2. Environmental requirements

Rapportering

- Frekvens
- Templet

Area	Response from Supplier
List of new Call-Off Contracts concluded preceding month together with name of Customers, duration and packages with additions.	
Total number of Call-Off Contracts together with name of Customers and total charges invoiced, including types of services/modules applicable for each contract.	
Statistical utilisation of the Services for all Call-Off Contracts, including number of users, IP addresses, domains and how often the system is used per Customer	
Material risks and issues	
Average availability of the Services previous month. Service credits offered to the Customer due to breach of Service Level Agreement, in total and for each Customer.	
Number of support cases from the Customers, in total and for each Customer.	
Number of unwanted incidents under the delivery of Services such as loss of data, downtime, abuse, etc.	

Avslutning og veien videre

- **Oppsummering:** De 5 viktigste suksesskriteriene

  - **Involver sikkerhet før utlysning og bruk standarder:** Sikkerhet og personvern kan ikke "drysses på" til slutt. Når må være absolutte krav i kravspesifikasjonen, og når kan det være bør-krav. Len deg på anerkjente rammeverk (NIST, C5, Normen, Cloud Reference Architecture) fremfor å finne opp egne, sære krav. Bruk MPS konkurransegrunnlag så langt det passer.

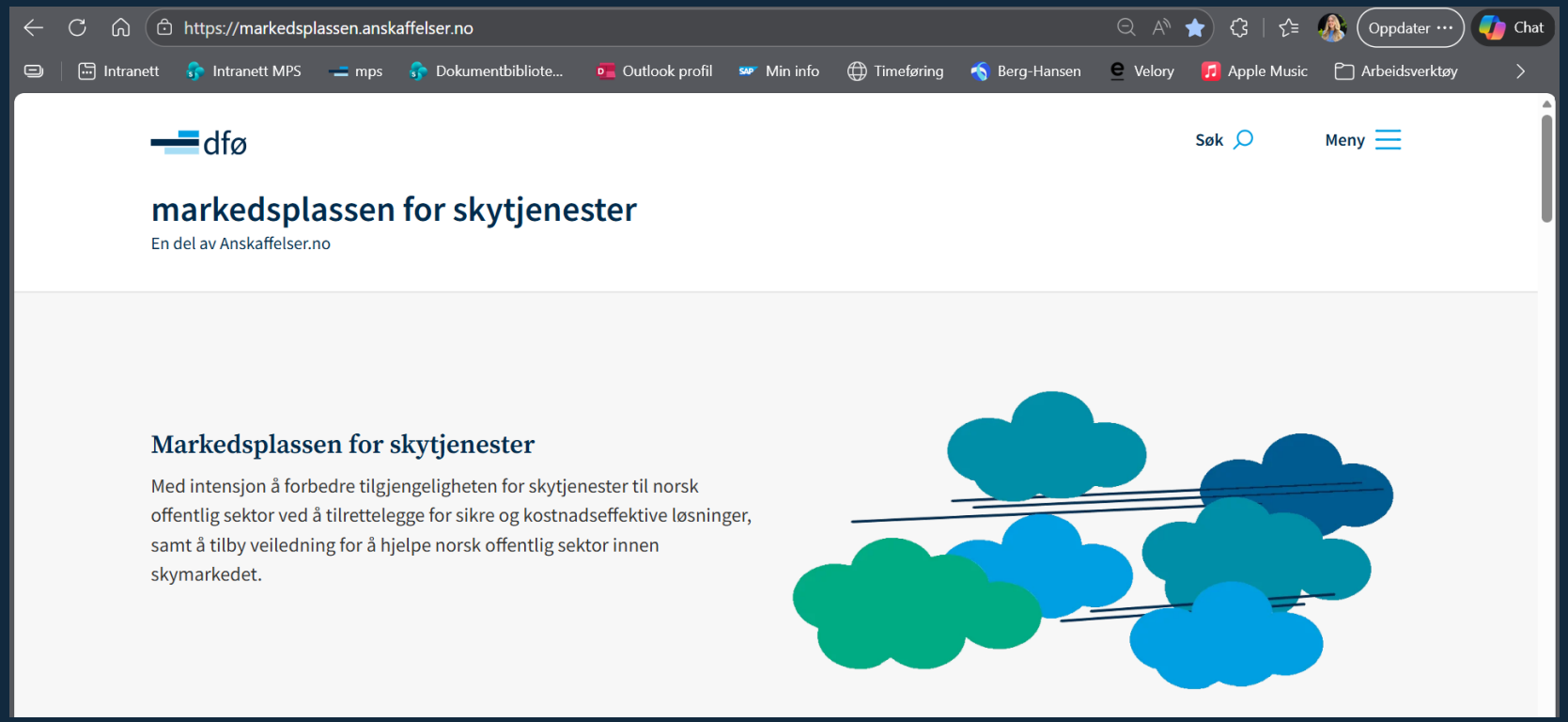
  - **Kjenn din data:** Du kan ikke sikre det du ikke vet du har. Dataklassifisering avgjør valget av løsning.

  - **Exit-strategi er obligatorisk:** Vit nøyaktig hvordan du får dataene dine ut *før* du signerer kontrakten.

  - **Skyen er ferskvare:** Sikkerhetsarbeidet starter ved implementering. Krever løpende oppfølging av både leverandør og egne konfigurasjoner.

  - **Markedsdialog:** Snakk med leverandørene – de kjenner til løsningen best!

Her finner du presentasjonene



https://markedsplassen.anskaffelser.no/aktuelt/presentasjoner

Neste Skyforum

Skyforum

23. april 2026

https://markedsplassen.anskaffelser.no/aktuelt/skyforum

Gjerne gi oss tilbakemelding på dagens foredrag!

https://svar.dfo.no/LinkCollector?key=7Q7ATZ3YU2CN

#mps

Kontaktinformasjon

Tema	Navn	E-post
Infrastruktur og plattformer	Ingrid Elisabeth Sørensen	ingridelisabeth.soerensen@dfo.no
Skykontrakter	Hanna Hjertås	hanna.hjertas@dfo.no
Skyadopsjon	Helene Stunes	helene.stunes@dfo.no
Cybersikkerhet	Kristina Nikolajeva	kristina.nikolajeva@dfo.no

Kahoot!

DEL 4

#mps | Thank you!

markedsplassen.anskaffelser.no

Norwegian agency for public and financial management