#MPS | Skyforum | 02-25

10. april 2025

Norwegian agency for public and financial management

Agenda

- Markedsplassen for skytjenester
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- Hva kan vi lære av finansnæringen? DNB
- Pause
- Cloud R&A
- CIPS
- CyberX
- FinOps

Generell informasjon for møtet

Helene Stunes, førstekonsulent MPS

Norwegian agency for public
and financial management

Agenda

- **Markedsplassen for skytjenester**
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- Hva kan vi lære av finansnæringen? DNB
- Pause
- Cloud R&A
- CIPS
- CyberX
- FinOps

Markedsplassen for skytjenester

Gisle Elgsaas Vada, juridisk seniorrådgiver

Norwegian agency for public
and financial management

STATUS

	Ansvarlig PL	Nåværende aktivitet	Plan fremover
Programmet	Sverre	• Programledelse • Styringsgruppe • Tjenesteeiermøte • KS/KS Digital	• Skyforum: DPF • **Innretning 2030** • Referansegruppe/interessentarbeid • Teknisk løsning («Digital»)
Juridisk	Gisle	• ITT CIPS • ITT v2 • Veiledningsarbeid • Kontrakter	• **CIPS-kontrakter** • SaaS-kontrakter • Partners/resellers • Norden/Baltikum
Infrastruktur- og plattformer	Ingrid	• ITT CIPS • Evaluering • Avropsprosjekt	• Veiledningsarbeid • CIPS 2.0 • **Tildeling**
Kostnads-optimalisering	David	• Sertifisering • Behovsanalyse • RFI • Strategi for FinOps	• Lansering/utprøving • IaaS/PaaS/SaaS • ITT FinOps/Rammeverk • **Veiledningsarbeid/landingsside**
Kunstig intelligens	David	• Strategi RAG AI • RFI RAG-AI • Open source lisensvilkår	• Landingsside • ITT RAG-AI • **Veiledningsarbeid**
Informasjons-sikkerhet og personvern	Kristina	• CRS kick-off/forvaltning • Veiledningsarbeid • 9 RFIs/tilslutning • Avklaring krav til personvern	• ITT SAT/3PMT: forhandlinger • Fase 2a/2025 • Veiledningsarbeid • **Kunngjøring Threat Intel**
Ekspertbistand	Helene	• Markedsanalyse • Behovsanalyse • Strategi Cloud R&A	• Markedsdialog • ITT • **Forhandlinger**
Digitale tjenester	Ann Kristine	• Funksjoner • Strategi • Plan for arbeidet	• **Behovsvurdering** • Effektanalyse • Retning avklart: enkel bestillings-løsning • Pilotering

#MPS | NOEN UTVALGTE ELEMENTER

KS/KS Digital

Innledet et samarbeid med KS/KS Digital. Velkommen 371 kommuner!

Referanse-arkitektur

Oppdatert og publisert

Utprøving SaaS

Iverksatt

3 pre-kvalifiseringer

Security Awareness & Training, Third Party Privacy Management, Cloud Research & Advisory

4 kunngjøringer

Governance, Risk & Compliance, Web Appliction Firewalls, Cyber Threat Intelligence,

#MPS | NESTE STEG

CIPS

Evaluering og tildeling

Porteføljen blir til

Fire forhandlinger, fire kunngjøringer, veiledninger og annet oppdatert materiale

Geopolitisk risiko

Re-etablering av koordineringsarbeidet i staten

Spørsmål

Agenda

- Markedsplassen for skytjenester
- **Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig**
- Hva kan vi lære av finansnæringen?
  DNB
- Pause
- Cloud R&A
- CIPS
- CyberX
- FinOps

Overføring av personopplysninger til USA

Skyforum, 10. april 2025

Partner Thomas Olsen

simonsen vogtwiig

Oversikt overføringsreglene

GDPR kap. V

Overføring ut av EØS er forbudt, med mindre det foreligger et overføringsgrunnlag

1. "Beslutning om tilstrekkelig vernenivå" fra Kommisjonen
2. Nødvendige garantier fra behandlingsansvarlig og databehandler
3. Unntak for særlige situasjoner (svært snever adgang/ad-hoc)

«Overføring» (EDPB Guidelines 5/2021 v2.0):

1. En behandlingsansvarlig eller databehandler (dataeksportør) er underlagt GDPR
2. Dataeksportøren tilgjengeliggjør personopplysninger til en annen behandlingsansvarlig eller databehandler (dataimportør)
3. Dataimportøren er i et land utenfor EØS

simonsen vogtwiig

Bakteppet – Schrems I og II

- Klage fra Max Schrems til det irske datatilsynet vedr. Facebooks overføring til USA
- Schrems I (2015): **Safe Harbour** kjent ugyldig
- Schrems II (2020):
  - Gir **Privacy Shield** og EU SCC tilstrekkelig vern gitt amerikansk etterretningslovgivning?
    - FISA 702: pålegg til "electronic communications providers"
    - E.O. 12333: monitorering av datatrafikk
  - Domstolen:
    - Privacy Shield underkjent med umiddelbar virkning
    - EU SCC fremdeles gyldige, men krav om konkrete vurderinger av overføringen

Gjeldende status overføringsgrunnlag

GDPR kap. V

1. **"Beslutning om tilstrekkelig vernenivå" fra Kommisjonen**
   - **"Godkjente land":** Andorra, Argentina, Kanada (kommersielle organisasjoner), Færøyene, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Storbritannia, Sør-Korea, Sveits og Uruguay
   - **10. juli 2023: EU-US Data Privacy Framework**
2. **Nødvendige garantier fra behandlingsansvarlig og databehandler, herunder**
   - **EUs standardavtaler (EU SCC) – Schrems II: krav om Transfer Impact Assessment (TIA)!**
   - **Bindende konsernregler (BCR) – Schrems II: krav om TIA!**
3. **Unntak for særlige situasjoner (svært snever adgang/ad-hoc)**
   - Samtykke
   - Oppfylle/inngå avtale
   - Fastsette, gjøre gjeldende eller forsvare rettskrav

simonsen vogtwiig

Transfer impact assessment (TIA)

EDPB Recommendation 01/2020 v. 2.0

1. Kartlegg overføringer

2. Identifiser overføringsgrunnlag

3. EU SCC/BCR: Gir overføringsmekanismen effektiv vern i lys av regler og praksis i tredjelandet?

   - Partene må innestå for at de ikke har noen grunn til å tro at lovgivning og praksis hindrer dem fra å etterleve forpliktelsene, sett hen til
     - formål, typen aktører, sektor, kategorien opplysninger, lagring/fjerntilgang, dataformat og videreoverføring
     - Lovgivning og praksis i tredjelandet
     - Relevante kontraktuelle, tekniske og organisatoriske tiltak

4. Tekniske, organisatoriske og kontraktuelle *tilleggstiltak*
   - *Kundestyrt kryptering*
   - *Anonymisering*

5. (Formelle prosessuelle skritt)

6. Følg med på utviklingen og gjør nye vurderinger ved endringer

simonsen vogtwiig

Data Privacy Framework (DPF)

- Rettsikkerhetsgarantier og begrensninger i am. myndigheters tilgang til personopplysninger
- Kan overføre uten ytterligere vurderinger til virksomheter som er selvsertifisert og står oppført på Data Privacy Framework List
- Virksomhetene i USA må etterleve DPF prinsippene
- Tiltakene som USA har innført gjør det enklere også å overføre på grunnlag av EU SCC eller BCR
  - Datatilsynet: Kan basere seg på Kommisjonens vurderinger, også med hensyn til ikke-sertifiserte virksomheter
- Se veiledning «Overføring av personopplysninger til USA» på markedsplassen for skytjenester

Tiltak fra Trump-administrasjon

Adekvansbeslutningen og de relevante amerikanske lovene gjelder fortsatt, men:

- E.O. vedr. «Ensuring Accountability for All Agencies»
  - Krav om at alle føderale enheter legger frem regulatoriske tiltak for «presidential review»
  - Kan påvirke Federal Trade Commission sin uavhengighet i håndhevingen av DPF-prinsippene
- Avsatt tre demokratiske medlemmer i Privacy and Civil Liberties Oversight Board (PCLOB)
  - Fører kontroll med at etterretningen ikke krenker enkeltpersoners rettigheter
  - Intensjon om å utpeke nye medlemmer, men p.t. ikke beslutningsdyktig

Uttalelser fra tilsynsmyndighetene i NO, SV og DK

- *Utskiftning i PCLOB først utfordring dersom det trekker ut i veldig lang tid å få på plass nye medlemmer*
- *Adekvansbeslutning gjelder inntil den blir opphevet av EU-kommisjonen eller EU-domstolen*
- *Regner med at reglene før eller siden utfordres for EU-domstolen*
- *Viktig å ha exit-strategi*
- *Også bruk av amerikanske skytjenester på europeisk jord kan påvirkes negativt dersom adekvansbeslutningen oppheves*
- Agendapunkt på EDPBs møte 8. april 2025

simonsen vogtwiig

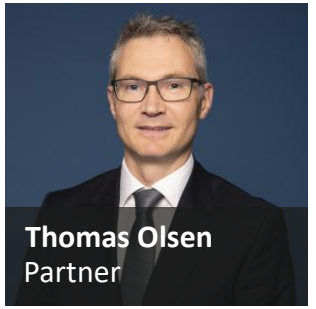
Hva bør virksomhetene gjøre?

- Følge utviklingen nøye
- Kartlegg overføringer til USA
- Få på plass eller vær beredt til å etablere alternativt overføringsgrunnlag til DPF, f.eks. EU SCC
- Vurder behovet for å revidere gjennomførte TIA-er som følge av endringer i USA og/eller underkjennelse av DPF
  - Fremdeles mulig å støtte seg på vurderingene som Kommisjonen har gjort mht. DPF?
  - Tiltak som ikke lenger står seg og/eller muligheter for tilleggstiltak?
- Exit-strategi: i mangel av effektive tilleggstiltak kan det være nødvendig å bytte leverandør

simonsen vogtwiig

Takk for oppmerksomheten!

Spørsmål?



Thomas Olsen
Partner

922 56 404
tol@svw.no

Simonsen Vogt Wiig

Filipstad Brygge 1
Post boks 2043 Vika
0125 Oslo

+47 21 95 55 00
post.oslo@svw.no

simonsen vogtwiig

www.svw.no

Agenda

- Markedsplassen for skytjenester
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- **Hva kan vi lære av finansnæringen? DNB**
- Pause
- Cloud R&A
- CIPS
- CyberX
- FinOps

Hvordan styre leverandørrisiko og få til en kontrollert avslutning av tjenester?

Skyforum / DFØ 10. april 2025

Ellen-Karine Hektoen – Group Technology
Odd Kleiva – Group Legal

Hva skal vi snakke om?

- Hva er DORA?
- Hva er styring av leverandørrisiko?
- Hvordan få til en kontrollert avslutning av tjenester?

DORA?
Robusthet – stabil og sikker drift

Digital Operational Resilience Act (DORA) er finansbransjens versjon av digitalsikkerhetsloven

Digital motstandsdyktighet er avgjørende for å opprettholde sikker og stabil drift og dermed tillit hos kundene

Forordningen tydeliggjør bl.a. hvordan banker og andre deltakere i det finansielle systemet skal forholde seg til tredjeparter (leverandører) og hvordan en skal styre leverandørrisiko

DORAs fem pilarer

IT risiko og styring

- Utvidede og detaljerte krav for IT risikostyring
- Styringsstruktur for alle relevante områder
- Krav til styret og CEO

Hendelses-rapportering

- Krav til når, hva og hvordan det skal rapporteres til myndigheter og kunder

Testing av motstandsdyktighet

- Systematisk og sammenhengende testregime
- Planer og rapporter
- TLPTer

Risikostyring av tredjeparter (TPRM)

- Leverandører og underleverandører
- Hovedfokuset i dag

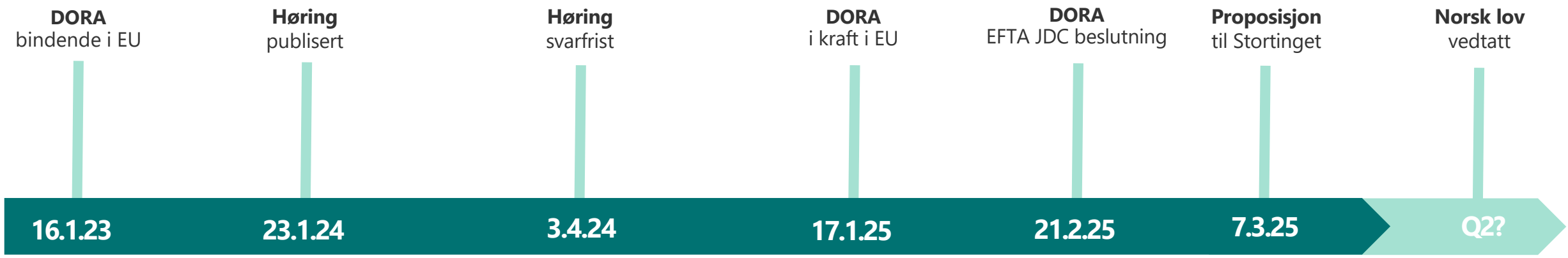
Informasjonsdeling om cybertrusler

Nivå 1, 2 og 3 regulering

- Nivå 1: DORA forordningen
- Nivå 2: RTSer og ITSer
  - ESAene skriver utkast ellers følger en prosedyren for henholdsvis delegerte rettsakter og gjennomføringsrettsakter
- Nivå 3: Q&Aer og retningslinjer
  - Ikke formelt bindende, men “make every effort” for å etterleve

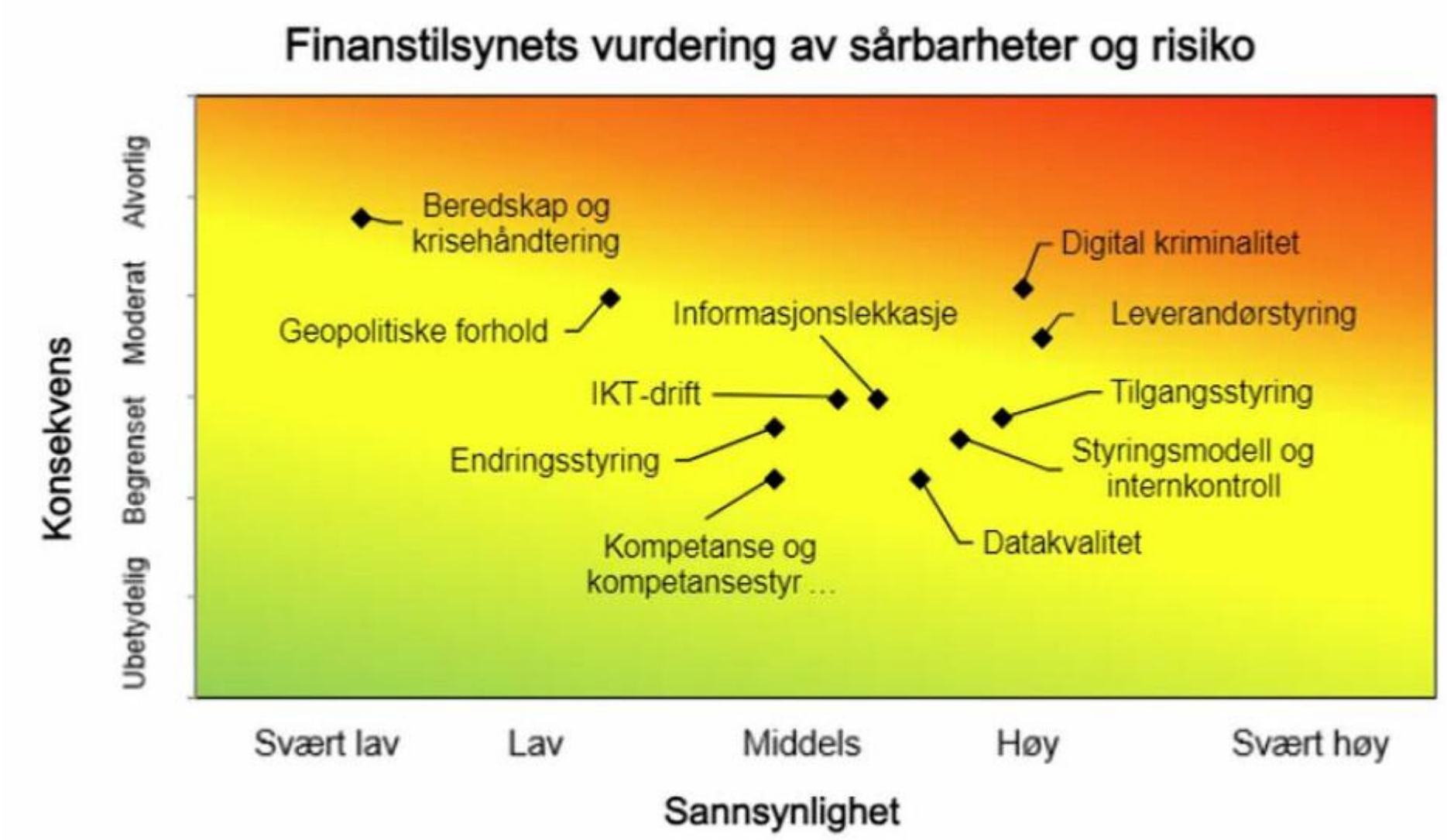
RTS: Regulatory Technical Standard
ITS: Implementing Technical Standard

DORA tidslinje



- De første signalene var samtidig implementering i Norge og EU
- De siste signalene er juli 2025.

Hvordan styre leverandørrisiko?



- Komplekse leverandørkjeder
- Krevende samhandlings-modeller
- Mangel på kompetanse på oppfølging av leverandører

Kilde: Risiko- og sårbarhetsanalyse (ROS) 2024 - Finanstilsynet.no

Styring av leverandørrisiko

- DORAs fjerde pilar

Strategi, policy, roller og rapportering

Register over IT leverandører og under-leverandører

Kritikalitet

Konsentrasjons-risiko

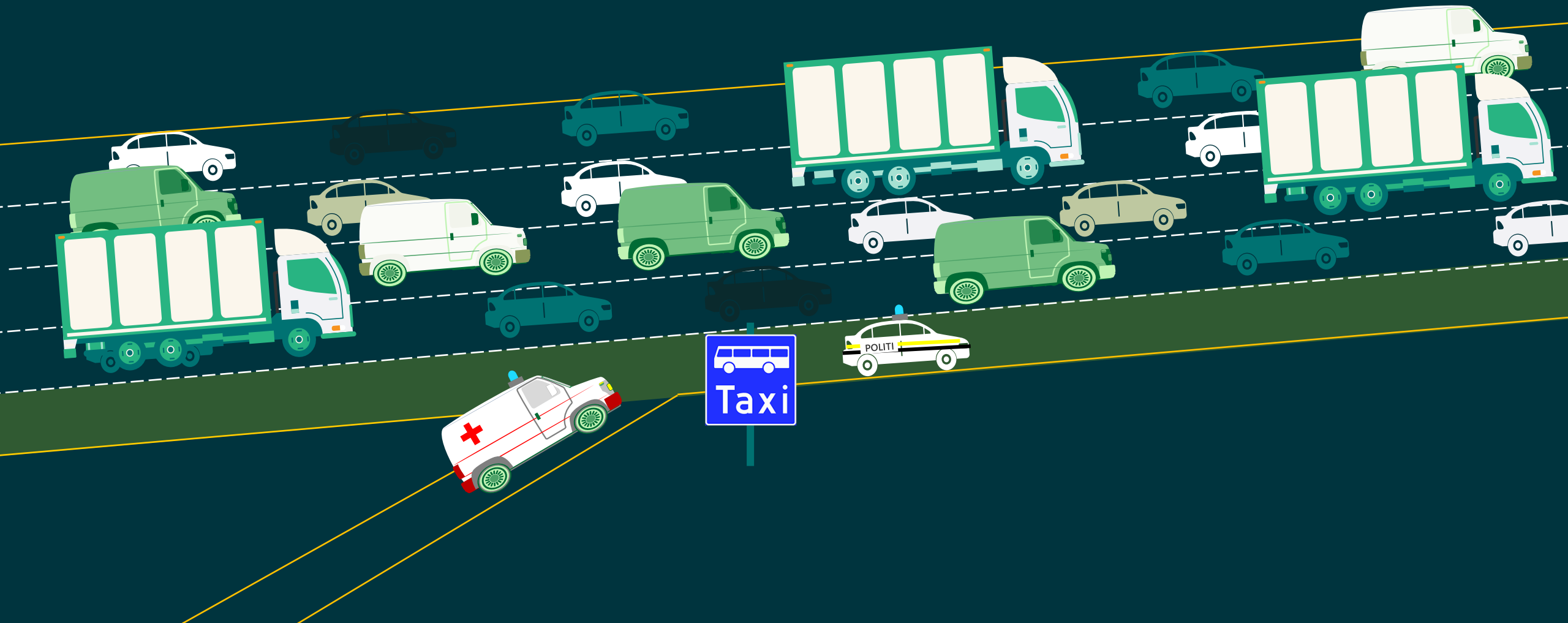
Kontrakts-vilkår

Vendor due diligence og løpende oppfølging (inkl. revisjoner)

Avslutning av tjenester («exit»)

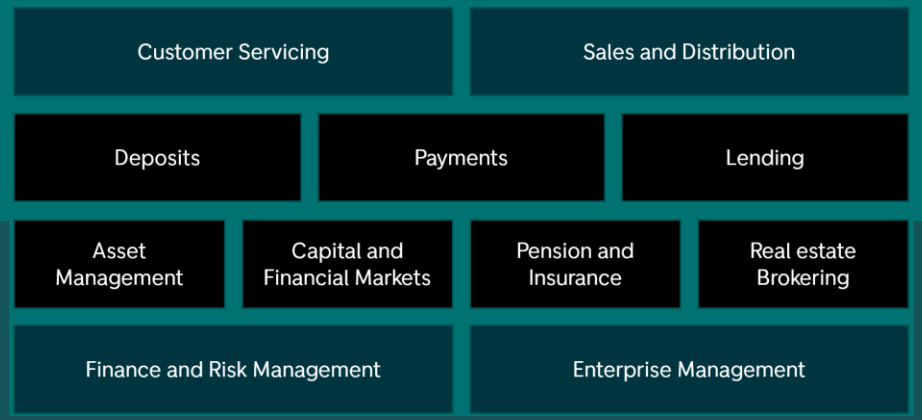
Hvorfor er kritikalitet viktig?

DORA art 3(22) og 243 andre steder i DORA



BIA - Business Impact Analysis – DORA art. 11.5 & ISO 22317

Hva skjer ved bortfall av forretningsfunksjonen i f.eks. 72 timer?



En forretningsfunksjon beskriver *hva* et selskap kan levere

men beskriver ikke *hvordan* det er levert

Konsentrasjonsrisiko

- EU ønsker at vi forstår og begrenser risiko knyttet til bruk av:
  - samme leverandør (eller nært relaterte leverandører) som leverer IT som understøtter flere kritiske funksjoner, og
  - leverandører som ikke er lett utbyttbare

- Sektorkritiske leverandører
  - Blir direkte regulert under DORA
  - Skyleverandører som Microsoft Azure, AWS, Google Cloud, men listen er ikke klar enda

Tung: alle bør ha en exit-strategi klar

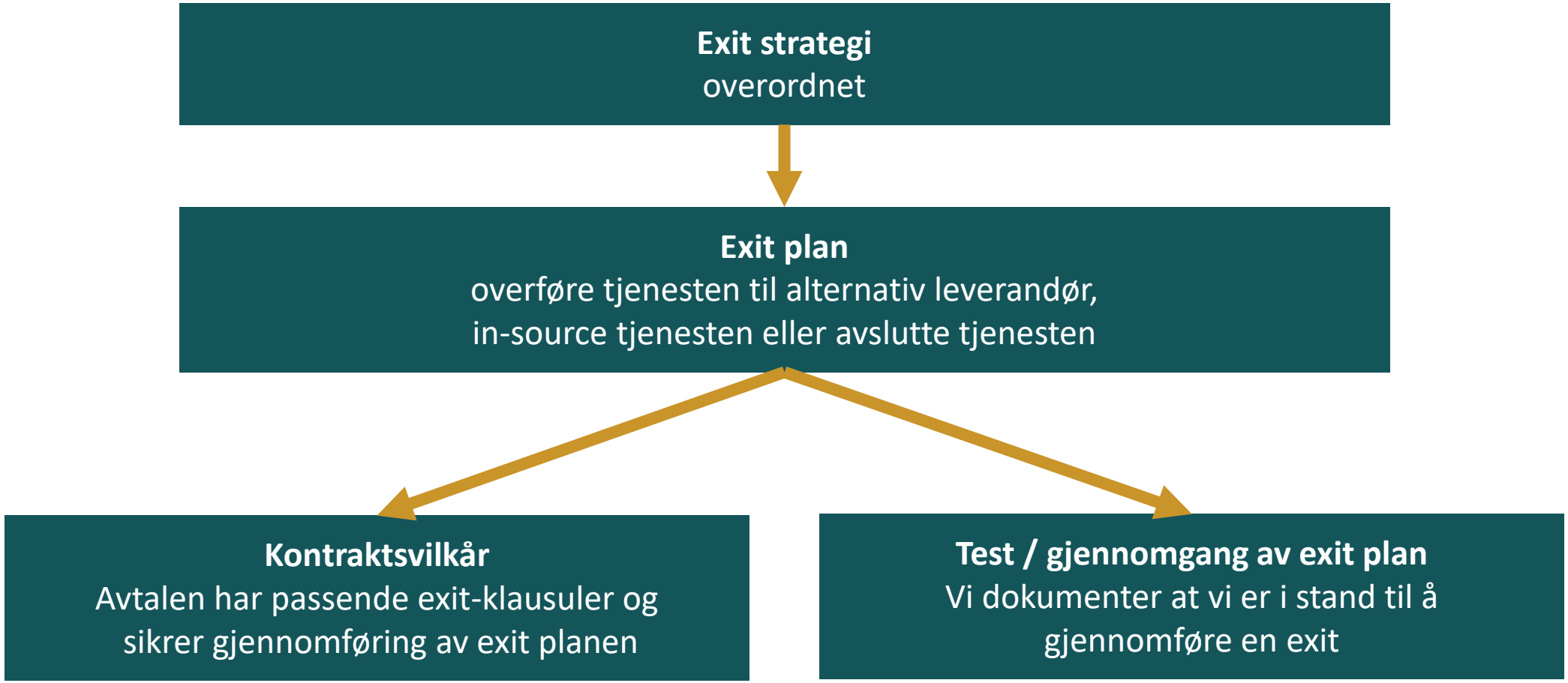
Hvordan få til en kontrollert avslutning av tjenester? (exit)

Avslutte avtalen?

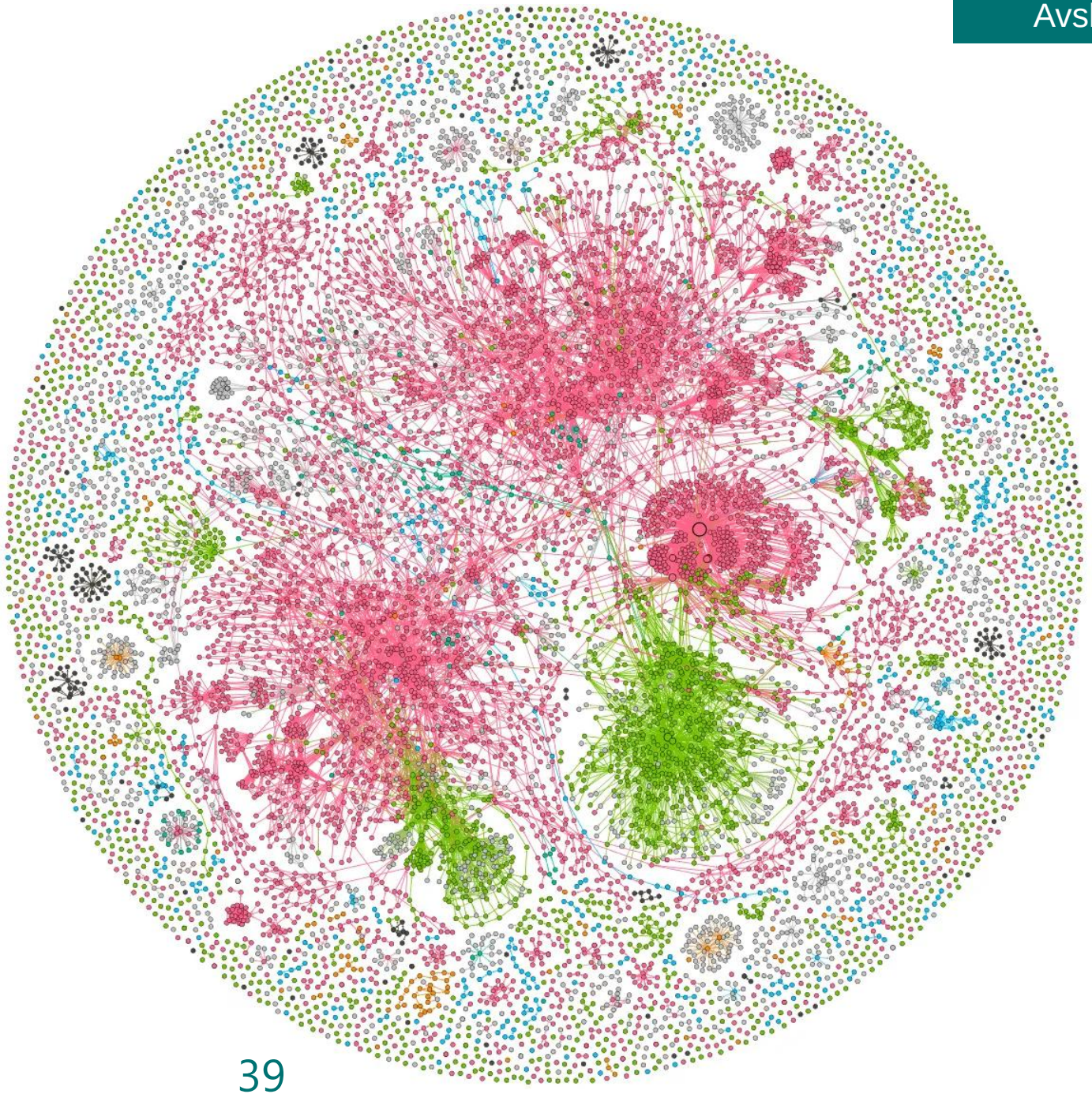
- Ulike situasjoner som krever at avtalen avsluttes

- Noen situasjoner skyldes forhold hos
  - leverandøren, f.eks. dårligere leveranser, sikkerhetsbrudd, regulatoriske brudd
  - kunden, f.eks. nye «sære» krav
  - andre forhold, f.eks. leverandøren blir solgt til en av uakseptabel eier eller sanksjoner

Avslutning av avtalen (exit)



Jobber på stormaskinen



Sky-strategier

- Hos store europeiske banker er ca. 80% av IT kontraktene skykontrakter (SaaS + CSP)

- **Sky native vs sky-agnostisk utvikling**
  - Fordeler med skyagnostisk: Portabilitet, kostnadsoptimering og unngå lock-in (avhengighet)
  - Utfordringer: Kompetanse, kompleksitet og tap av tilgang til leverandørspesifikk funksjonalitet

- **Én sky vs multi-sky og hybrid-sky**
  - Fordeler med multi-sky: Kvalitet, pris, risiko, redusere lock-in
  - Utfordringer: Kompetansekrevende, komplekst
  - Aktiv-aktiv

- EU Cloud and AI Development Act & EuroStack

Google Cloud

SaaS: Software as ae – skybaserte applikasjoner
CSP: Cloud Service Providers – f.eks. AWS, Azure og Google Cloud

Forskjellige senarioer

Klassisk drift /
Privat sky

Sky

On-prem drift på egen hardware	**IaaS** Infrastructure as a Service	**PaaS** Platform as a Service	**SaaS** Software as a Service
Applikasjon	Applikasjon	Applikasjon	Applikasjon
Data	Data	Data	Data
Operativsystem	Operativsystem	Operativsystem	Operativsystem
Virtualisering	Virtualisering	Virtualisering	Virtualisering
Server	Server	Server	Server
Lagring	Lagring	Lagring	Lagring
Nettverk	Nettverk	Nettverk	Nettverk
Mennesker	Mennesker	Mennesker	Mennesker
Data senter	Data senter	Data senter	Data senter

= kundens ansvar

= skyleverandørens ansvar

Hva kan vi ønske å flytte?

Applikasjon	Lisenser og vedlikeholdsavtaler, kompatibilitet	«konfigurasjonsbeskrivelser, script og lignende» (SSA-D) «kildekode til integrasjoner eller spesialutviklede moduler» og informasjon i Forvaltningsdokumentet (SSA store-sky) Backup
Data	Eksport og konvertering	
Operativsystem		
Virtualisering		
Server	Overføring av utstyr	
Lagring		
Nettverk		
Mennesker	Kompetanse, rutiner, ansatte / innleide	Tilganger
Data senter	Leieavtale	

Avhengigheter til andre systemer etc.

Avslutning i Statens Standardavtaler (SSA)

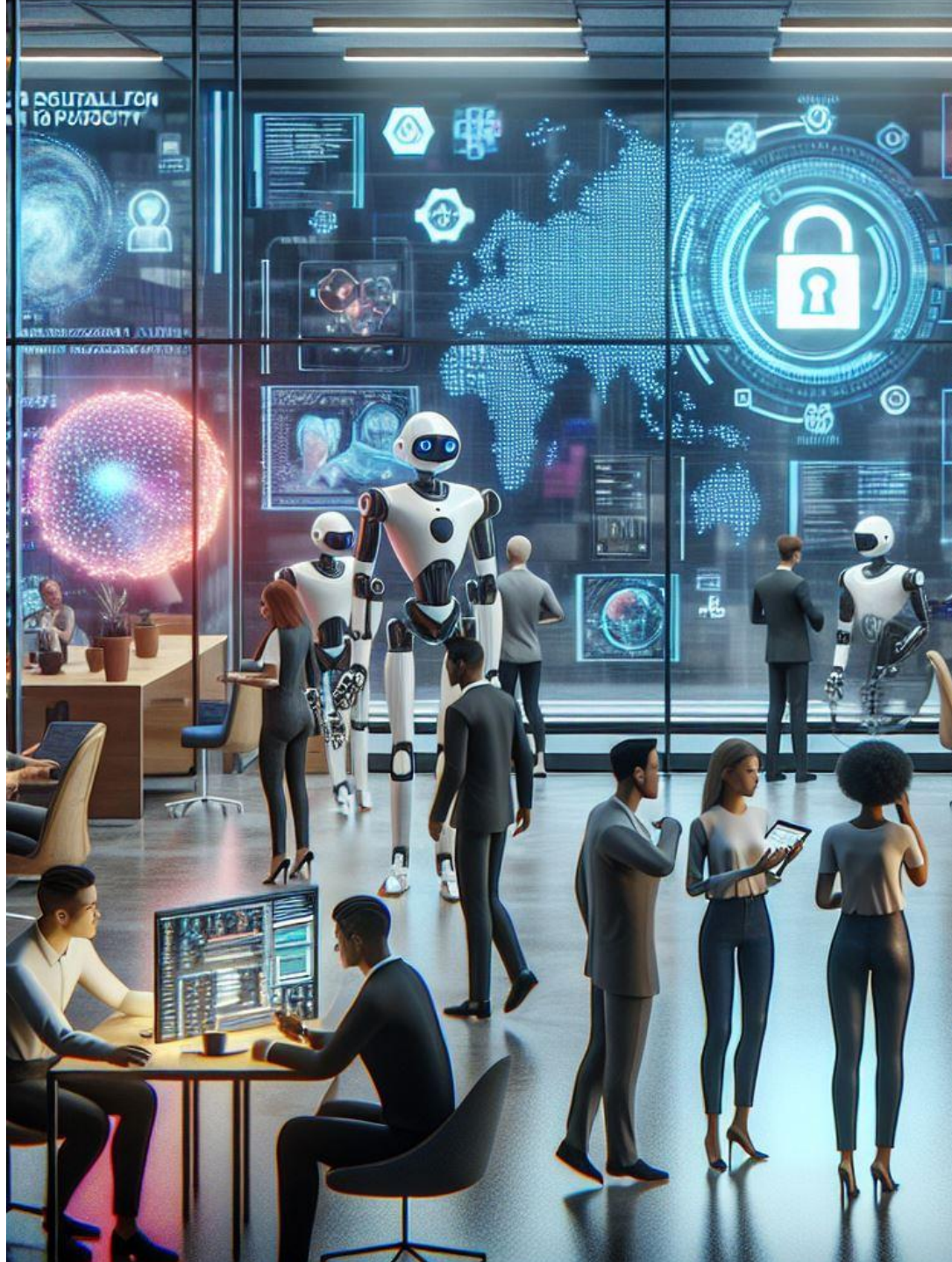
- **SSA-D (for on-prem drift) kapittel 2.5**
  - **I begynnelsen av avslutningsperioden** legger kunden frem avslutningsplanen og leverandører supplerer.
  - Rett til **bistand** fra leverandør for å gjennomføre overføring til ny leverandør eller reintegrering
  - Retten til bistand varer til tjenesten er etablert hos ny leverandør + stabiliseringsperiode (60 dager)
  - Forsøker å hindre **opportunistisk opptreden** i avslutningsperiode
    - Låser pris og kompetansenivået hos resursene
    - Krever at gammel leverandør samarbeider med eventuell ny leverandør

- **SSA-store sky kapittel 2.4**
  - Overordnet plan skal lages **ved etablering** av leverandøren basert på kundens føringer (i bilag 1 og 2)
  - Detaljert plan lages ved varsel om exit
  - Rett til bistand fra leverandør

- **SSA-lille sky kapittel 2.6**
  - Bistand fra leverandør avtales som tilleggstjeneste

Oppsummering

- DORA
- Risikostyring av leverandører
- Avslutning av tjenester (“exit”)



Spørsmål?

Pause (10 min)

Følg MPS på LinkedIn →

Norwegian agency for public and financial management

Agenda

- Markedsplassen for skytjenester
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- Hva kan vi lære av finansnæringen? DNB
- Pause
- **Cloud R&A**
- CIPS
- CyberX
- FinOps

Cloud Research & Advisory

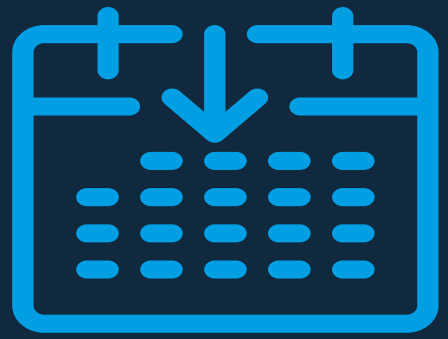
Helene Stunes, prosjektleder

Norwegian agency for public
and financial management

Cloud R&A | Avtaleinformasjon

Database for artikler / forskningsmateriell

Tilgang på analytikere/rådgivere



Konferanser / arrangementer

Cloud R&A | Avtaleinformasjon

Area of service

Cloud transformation	Cloud migration and deployment	Digitalisation	Cloud infrastructure
Change management	Cloud virtualisations	Cloud platforms	Hybrid cloud
Artificial intelligence / machine learning	Cloud operation	SaaS in general	SaaS ERP
Cloud cost optimisation/ FinOps	Cloud cyber security	Cloud GDPR	Cloud procurement

Cloud R&A | Avtaleinformasjon

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)

Cloud R&A | Tidsplan

- Kunngjøring og prekvalifisering
- Tilbudsfasen
- Forhandlingsfasen
- Kontraktsignering

Cloud R&A | Tidsplan

Kunngjøring og prekvalifisering

- → 01. mars — Spørsmålsfrist prekvalifisering
- → 10. mars — Søknadsfrist prekvalifisering
- → 12. mars — Sendt invitasjon til tilbudsfasen

Tilbudsfasen

Cloud R&A | Tidsplan

Tilbudsfasen

- → 31. mars — Spørsmålsfrist tilbudsfasen
- → 14.04 25 — Tilbudsfrist
- → April 25 — Gjennomgang av tilbud

Forhandlingsfasen

Cloud R&A | Tidsplan (tentativ)

Forhandlingsfasen

- → April/mai/juni Forhandlinger/evaluering
- → Mai/juni Tildeling av kontrakt

Kontraktsignering

Tentative tidsplaner

Cloud R&A | Fordeler med avtalen

Mål Cloud R&A

- Tilgang til oppdatert markedsinnsikt
- Tilgang til strategisk rådgivning med lavt volum
- Tilgang til forum med spesialistkompetanse

Mål MPS

- Betydelig bedre priser/enhetskostnad
- Balanserte kommersielle vilkår
- Effektiv bestillingsmekanisme
- Forbedret informasjonssikkerhet
- GDPR-kompatible driftsmodeller
- Fleksibilitet og et bredt spekter av tjenester
- Redusert miljøavtrykk

Spørsmål

Agenda

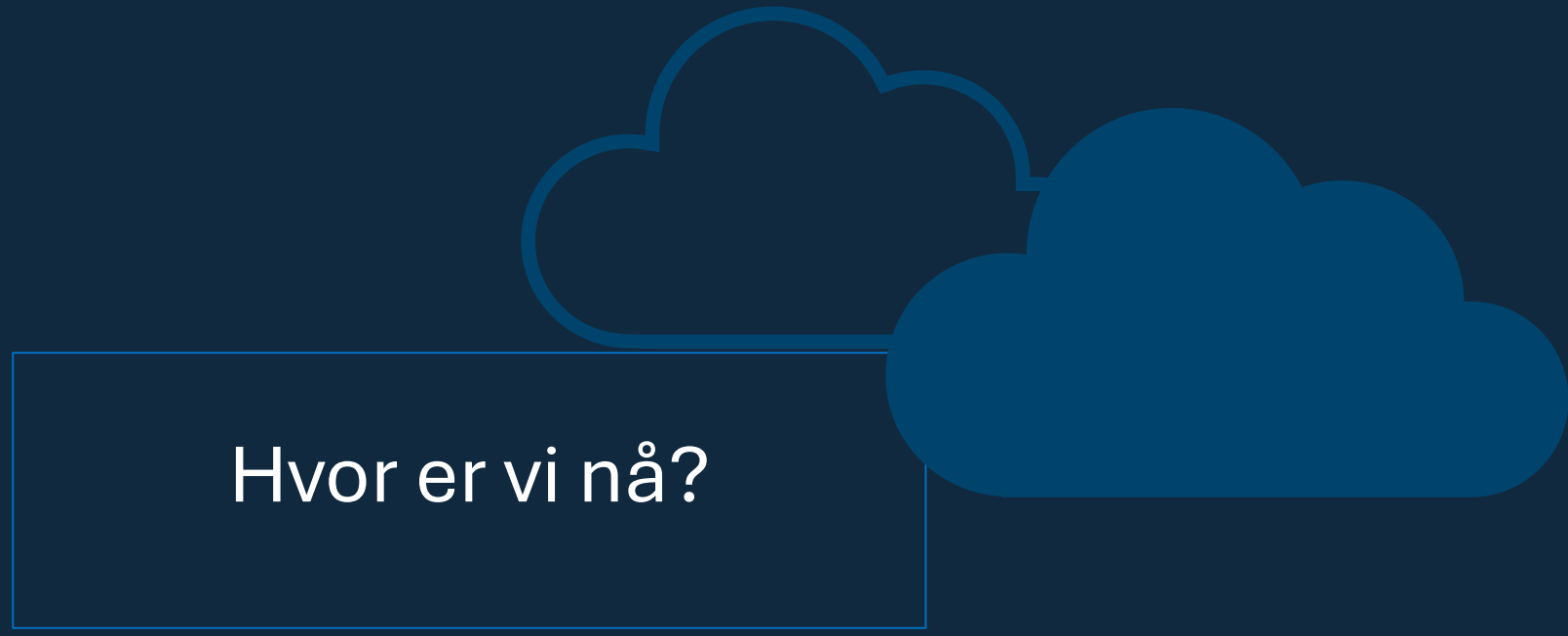
- Markedsplassen for skytjenester
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- Hva kan vi lære av finansnæringen? DNB
- Pause
- Cloud R&A
- **CIPS**
- CyberX
- FinOps

CIPS

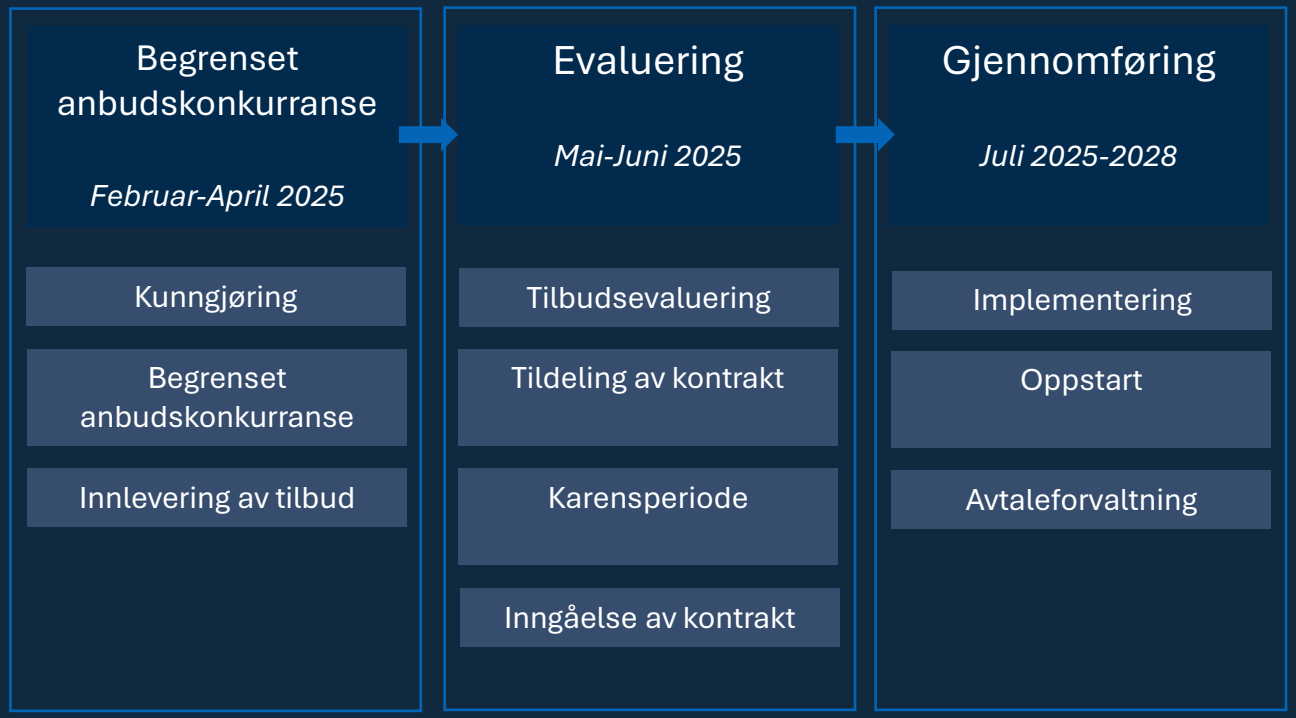
Ingrid Sørensen, prosjektleder

Norwegian agency for public and financial management

CIPS



CIPS | Anskaffelsesprosess



CIPS | Avropsprosessen

- Arbeidsgruppe
- Beskrivelse av avropsprosessen
- Mal for mini-konkurranse
- Jobbet med case

Spørsmål

Agenda

- Markedsplassen for skytjenester
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- Hva kan vi lære av finansnæringen? DNB
- Pause
- Cloud R&A
- CIPS
- **CyberX**
- FinOps

CyberX

Kristina Nikolajeva, prosjektleder

Per Jakobsen, seniorrådgiver

David Behrens, seniorrådgiver

Norwegian agency for public and financial management

CyberX | Status pågående anskaffelser

Kunngjort	• 05.02.2025 • **«Information security and data protection training and awareness» (T&A)** • SaaS-basert løsning for grunnleggende opplæring og bevisstgjøring innen informasjonssikkerhet og personvern
Kunngjort	• 05.02.2025 • **«Third party data protection compliance management» (TPP)** • En skybasert tjeneste som skal bidra til etterlevelse av GDPR og redusere personvernrisiko hos tredjeparter/i leverandørkjeden.

T&A og TPP | Tentativ tidsplan

- Kunngjøring og prekvalifisering
- Tilbudsfasen
- Forhandlingsfasen
- Kontraktsignering

T&A og TPP | Tentativ tidsplan

Kunngjøring og prekvalifisering

- → 03. mars — Spørsmålsfrist prekvalifisering
- → 10. mars — Søknadsfrist prekvalifisering
- → mars — Sendt invitasjon til tilbudsfasen

Tilbudsfasen

T&A og TPP | Tentativ tidsplan

Tilbudsfasen

→ 22. april	Spørsmålsfrist tilbudsfasen
→ 30.04.2025	Tilbudsfrist
→ Primo mai 2025	Gjennomgang av tilbud

Forhandlingsfasen

T&A og TPP | Tentativ tidsplan

Forhandlingsfasen

- → mai/juni — Forhandlinger/evaluering
- → Juni — Tildeling av kontrakt

Kontraktsignering

Tentative tidsplaner

CyberX | Planlagte anskaffelser – Tilslutningsprosess

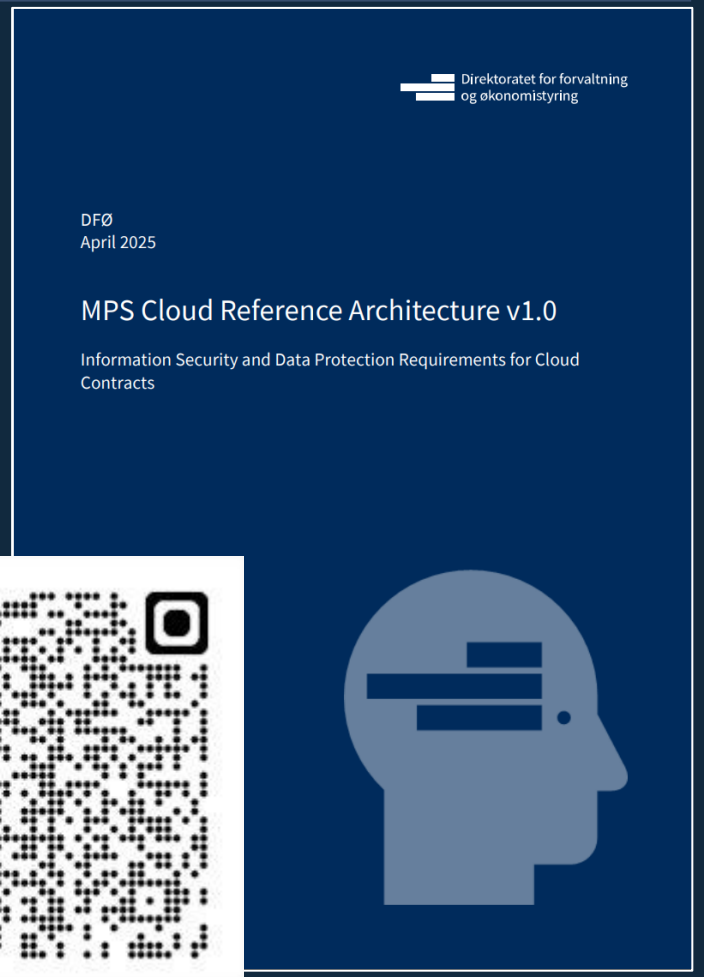
Under arbeid	• Information security and data protection – Governance Risk & Compliance (GRC) • Tentativ kunngjøring Q2
Under arbeid	• Web Application and API Protection (WAAP) • Tentativ kunngjøring Q2
Under arbeid	• Vulnerability management (VM) • Tentativ kunngjøring Q3-4
Under arbeid	• Cyber Threat Intelligence platform • **Kunngjøring april 2025**

Mer informasjon om tilslutning

#mps

CyberX | Lansering - Referansearkitektur - krav til informasjonssikkerhet og personvern

Prinsipielle krav	**Overordnede krav til kontraktsmessige forhold**
Basiskrav	**Obligatoriske krav til cybersikkerhet**
Tilleggskrav	**Leverandørens forslag til cybersikkerhetsarkitektur basert på kundens behov**



#mps

CyberX | Struktur og metodikk

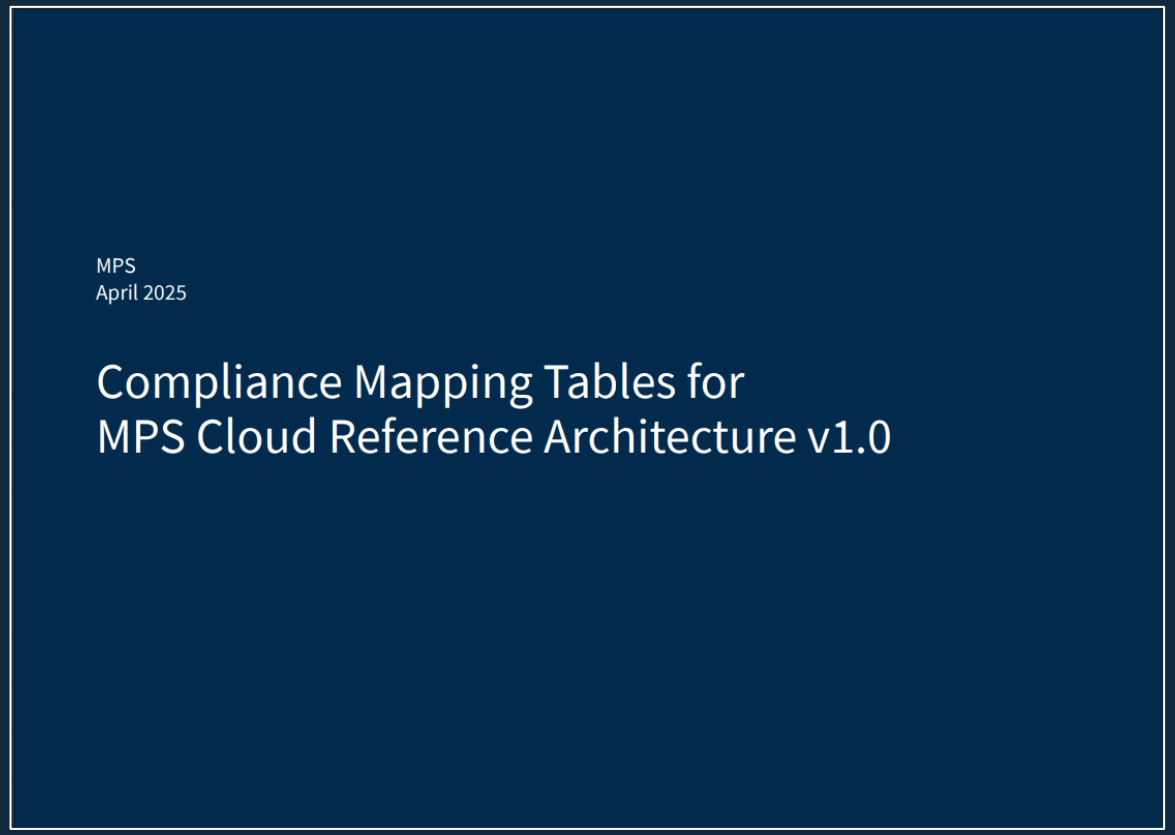
Prinsipielle krav: Overordnede krav til informasjonssikkerhet og personvern som skal inkluderes i hovedkontrakten for avtaler om skytjenester.

Basiskrav: Et omfattende sett med krav til informasjonssikkerhet som skal inkluderes som et sikkerhetsvedlegg i avtaler om skytjenester.

Tilleggskrav: Et sett med valgfrie krav til informasjonssikkerhet som er ment å støtte norsk offentlig sektor med «sikkerhet i skyen», støttet av leverandørens referansearkitektur, spesifikke nasjonale krav og andre sikkerhetsrelaterte tjenester.

CyberX | Mapping av informasjonssikkerhetskrav mot standarder

- Hjelp til mapping av kravene i referansearkitekturen til etablerte standarder og rammeverk
- Tabellene vil bli utvidet med ytterligere standarder og rammeverk i fremtidige versjoner
- Mapping er ment som veiledning, og er ikke nødvendigvis komplett.



CyberX | Formålet med referansearkitekturen

Et viktig formål med referansearkitekturen er å oppnå bedre sikkerhet ved bruk av skytjenester, hvor leverandøren tar et tydeligere ansvar for sikkerhet og personvern:

- Bidra til å styrke informasjonssikkerheten og personvern i offentlig sektor
- Standardiserte krav til støtte ved anskaffelser og forvaltning av skytjenester
- Inkluderer krav til leverandørens forpliktelser for sikkerhet i den leverte tjenesten *og*
- virksomhetens egen risikohåndtering ved bruk av tjenesten

CyberX | Om utvikling av referansearkitekturen

- Utviklet av MPS siden 2023
- Utgangspunkt i etablerte standarder og rammeverk
- Innspill fra offentlige virksomheter basert på faktiske anskaffelser og erfaring
- Innspill fra Markedsplassens CyberX ekspertgruppe
- Innspill og tilbakemeldinger fra leverandører
- Innspill fra relevante myndigheter
- Testet i markedsplassens egner anskaffelser
- Videreutvikles kontinuerlig basert på tilbakemeldinger fra markedet, nye lovkrav og Markedsplassens egne erfaringer

CyberX | Engelsk versjon med norske kommentarer

Eksempel på krav med norsk kommentar:

Overordnede prinsippkrav

#	Krav (engelsk)	Norsk kommentar
A.1	The Supplier acknowledges that information security is of critical importance to the Norwegian government and Customers under this Agreement.	Ved avtaler som gjøres for norsk offentlig forvaltning er det nødvendig å sikre at leverandøren har grunnleggende forståelse for trusselbildet og de høye krav til sikkerhet som gjelder for offentlig sektor. Dette er viktig for å etablere god tillit til leverandøren.

CyberX | Eksempler

Principal Security Requirements		
A.8	Governance	The Supplier shall appoint a security responsible at an executive level as a counterpart to the Customer, who is responsible for strategic security meeting places, reporting, and follow-up of material risks, incidents, and Vulnerabilities
A.6	Notification	In the event of a serious security incident or significantly increased threat to the information security relating to the provisioning of the Services, the Supplier shall provide an initial notification in writing or by phone directly to the Customer within 24 hours and a report of the incident within 72 hours. This equally applies to compromises of personal information.

Cloud Enablement Security Requirements		
C.7	Cryptography	The Supplier should provide mechanisms / services for encryption to enable effective encryption of Customer data at rest and in transit with customer-managed / customer-owned cryptographic keys. The Supplier should document its roadmap to ensure that cryptographic algorithms used in the Service are quantum resistant, in accordance with, e.g., CNSA 2.0 ("Commercial National Security Algorithm Suite 2.0"), NIST standards for post-quantum cryptography, “NSMs veileder for kvantemigrering”, “NSMs kryptografiske anbefalinger (utkast 2024)”, or similar.

CyberX | Målgruppe for referansearkitekturen

Norsk offentlig sektor

- Virksomhetsledere
- IT ansvarlige
- Sikkerhetsansvarlige
- Personvernombud
- Innkjøpere
- Kontraktsforvaltere
- Leverandører av skytjenester

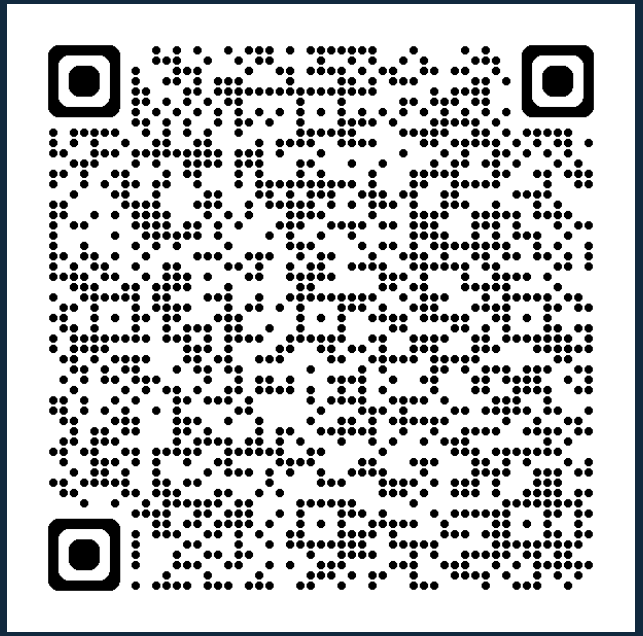
Cloud Reference Architecture v1.0

Gi oss gjerne tilbakemeldinger
om innhold og/eller hvordan dere har
benyttet referansearkitekturen!

E-post: markedsplassen@dfo.no

CyberX | Cyber Threat Intelligence

- Basert på erfaringer fra utprøving og RFI
- Tjenesten skal bistå offentlige virksomheter med å identifisere, analysere og respondere på sikkerhetstrusler
- Viktige momenter vil blant annet være datakilder, analyse/fremstilling og integrasjonsmuligheter
- SaaS-løsning



Sluttrapport: Utprøvingsprosjekt trusseletterretning

CyberX | Cyber Threat Intelligence

- Siste mulighet for kommuner til å melde seg på!
- Frist tirsdag 15. April
- Frivillig og ikke eksklusiv avtale

Påmeldingsskjema for kommuner

Spørsmål

Agenda

- Markedsplassen for skytjenester
- Data Privacy Framework og overføringer til USA, Simonsen Vogt Wiig
- Hva kan vi lære av finansnæringen? DNB
- Pause
- Cloud R&A
- CIPS
- CyberX
- **FinOps**

FinOps

David Behrens, prosjektleder

Norwegian agency for public
and financial management

FinOps | Utprøvingsprosjekt SaaS-lisenser

- Lisenshåndteringssystem
- God respons (23 søknader)
- Gjennomført Kick-off med deltakerne (5 stk)
- Oppstart etter påske
- Varighet 3 måneder

Spørsmål

Neste Skyforum

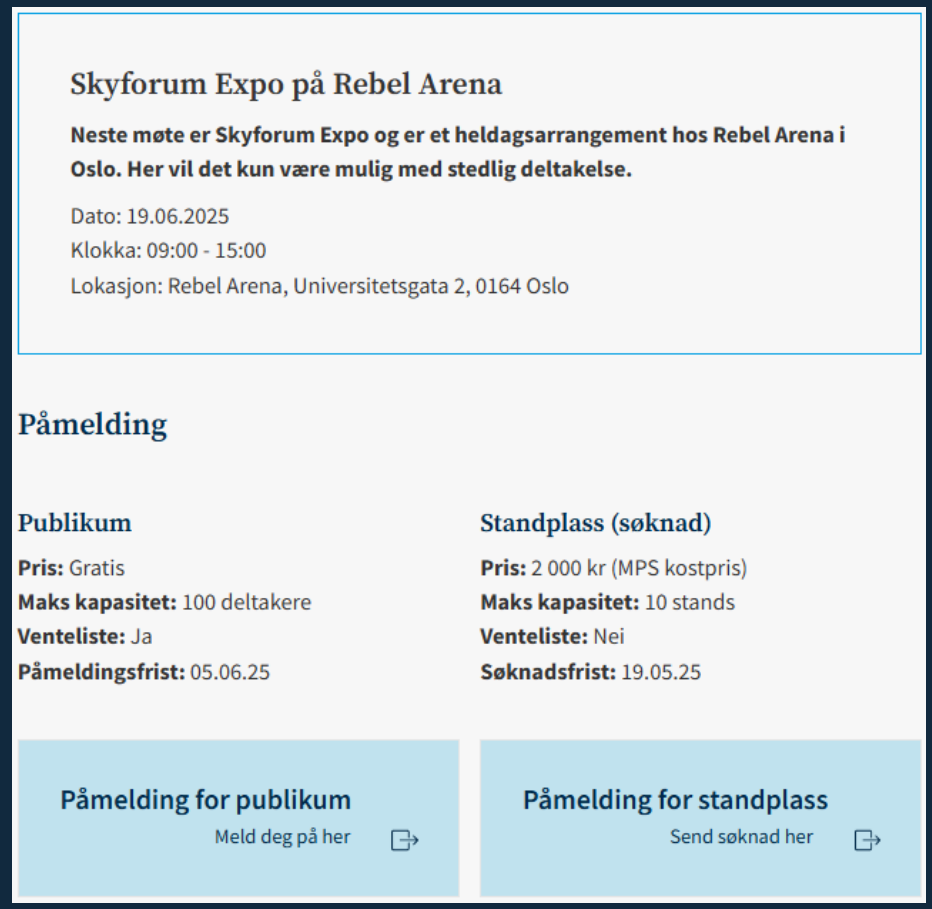
Skyforum Expo

19. juni 2025

Det blir ikke livestream under arrangementet.
Vi legger ut opptak i ettertid.

#mps

Neste Skyforum



Skyforum Expo på Rebel Arena

Neste møte er Skyforum Expo og er et heldagsarrangement hos Rebel Arena i Oslo. Her vil det kun være mulig med stedlig deltakelse.

Dato: 19.06.2025
Klokka: 09:00 - 15:00
Lokasjon: Rebel Arena, Universitetsgata 2, 0164 Oslo

Påmelding

Publikum

Pris: Gratis
Maks kapasitet: 100 deltakere
Venteliste: Ja
Påmeldingsfrist: 05.06.25

Standplass (søknad)

Pris: 2 000 kr (MPS kostpris)
Maks kapasitet: 10 stands
Venteliste: Nei
Søknadsfrist: 19.05.25

Påmelding for publikum
Meld deg på her

Påmelding for standplass
Send søknad her

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

Kontaktinformasjon

Ann Kristine Halvorsen
MPS Digital
annkristine.halvorsen@dfo.no

David Behrens
FinOps / AI (Threat Intel)
david.behrens@dfo.no

Gisle Elgsaas Vada
MPS Juridisk
gisle.elgsaasvada@dfo.no
+47 916 97 432

Halvord Vinger
CyberX
halvord.vinger@dfo.no

Helene Stunes
Cloud R&A / Skyforum
helene.stunes@dfo.no

Ingrid Elisabeth Sørensen
CIPS
ingridelisabeth.soerensen@dfo.no

Kristina Nikolajeva
CyberX
kristina.nikolajeva@dfo.no

Per Jakobsen
CyberX
per.jakobsen@dfo.no

Sverre Christian Stoltz
programdirektør
sverre.stoltz@dfo.no
+47 920 45 300


#MPS | THANK YOU!
markedsplassen.anskaffelser.no
Norwegian agency for public
and financial management