#mps | Skyforum | 04-24

18. september 2024

Norwegian agency for public and financial management

Generell informasjon for møtet

Helene Stunes, førstekonsulent MPS

Norwegian agency for public
and financial management

Agenda

- Markedsplassen for skytjenester
- Føyen AS om Risiko med ulike avtalemodeller i skyen
- CIPS
- FinOps / AI
- Cloud R&A
- CyberX

Agenda

- **Markedsplassen for skytjenester**
- Føyen AS om Risiko med ulike avtalemodeller i skyen
- CIPS
- FinOps / AI
- Cloud R&A
- CyberX

Markedsplassen for skytjenester

Sverre Chr. Stoltz, programdirektør #MPS

Norwegian agency for public
and financial management

#MPS | STATUS: HØY AKTIVITET

Programmet	Kontrakter	CIPS	FinOps/AI	CyberX	Cloud R&A	Digital
På plan	På plan	På plan	På plan	Foran plan	På plan	Bak plan
• Nasjonal strategi • Ny innkjøps-løsning/Markeds-plass for skytjenester	• ITT CIPS • ITT v2 • Veiledningsarbeid • Kontrakter	• ITT CIPS	• Sertifisering • Behovsanalyse • Markedsanalyse • Strategi for FinOps • Strategi RAG AI	• CRS kick-off • Veiledningsarbeid • 9 RFIs	• Markedsanalyse • Behovsanalyse • Forbereder ITT	• Funksjoner • Strategi
• Skyforum • Innretning 2030 • Referansegr. • Neste steg	• CIPS-kontrakter • SaaS-kontrakter • Partners/resellers • MoUs • Open source	• Forhandlinger • Veiledningsarbeid	• Lansering Utprøving • 2 RFIs • ITT FinOps • ITT (RAG) AI? • Veiledningsarbeid	• ITT PMT • Fase 2 • Veiledningsarbeid	• Markedsdialog • Kunngjøring	• Behovsvurdering • Effektanalyse • Plan videre/KGV • Retning: bestillings-løsning
Sverre	Gisle	Ingrid	David	Kristina	Helene	Charlotte

FORRETNINGSMÅL					
Balanserte vilkår	Pris/kostnad	Effektive avrop	Kostnads-optimalisering, klima og miljø	Cybersikkerhet og GDPR	Fleksibilitet

TREDOBLING I BRUK AV SKYTJENESTER I OFFENTLIG SEKTOR

- Alle bruker skytjenester: 20 MRD
- 60-70% mangler strategi/plan

- Forretningsplan for virksomheten
- IT-strategi (som itereres med:)
- Strategi for bruk av skytjenester, lisenser og finans

- Ikke sky → Lite → Mye → Alt i sky
- On-prem, hybrid, privat, allmenn

BRUK AV VÅRE KONTRAKTER OG VEILEDNINGER

- Digtale reguleringer i EU
- Overføring av personopplysninger
- Referansearkitektur for informasjonssikkerhet
- Kick-off for måling av informasjonssikkerhet på internet
- Avtalene er frivillige og ikke-eksklusive
- Tilpassede veiledninger for virksomhetene
- **Verdiøkningen ligger i oppfyllelse av MPS forretningsmål**
- Mer endring og omstilling → bruk av skytjenester

SKYENS MODELL: FORVENTNINGER

- Skyens kommersielle modell (konsumbasert), SaaS, kunde-plassering
- Krever endring og omstilling/kapasitet: skyen er en del av digitaliseringen av offentlig sektor
- Stegvis tilnærming: basiskontrakter omsluttet av informasjonssikkerhet/GDPR
- Virksomheten som data-eier: kan ikke og bør ikke videreføres/delegeres
- Fra det kommersielle bildet til risiko: bruk av skyløsninger
  - Informasjonssikkerhet
  - Personvern/konfidensialitet
  - Kostnadskontroll, klima og miljø
  - Exit (avslutning av sky-kontrakten, teknisk, funksjonelt, rettslig, bortfall)
  - Kontrakter

Spørsmål

Agenda

- Markedsplassen for skytjenester
- **Føyen AS om Risiko med ulike avtalemodeller i skyen**
- CIPS
- FinOps / AI
- Cloud R&A
- CyberX

FØYEN

Risiko med ulike avtalemodeller i skyen

Oslo, 18. september 2024 | Partner/advokat Lars Folkvard Giske

FØYEN

Ulike avtalemodeller ved kjøp av skytjenester

Direkteavtale

Kjøp via forhandler

Indirekte kjøp

XaaS, som også inkluderer tredjepartsky

FØYEN

Hva bør man være oppmerksom på i skytjenestevilkårene – direkte kjøp?

- Manglende prissikring, fortsatt komplekse «lisensmodeller»
- Korte abonnementsperioder/varighet
- Korte oppsigelsesfrister og ekstraordinære muligheter for skyleverandør til å si opp med enda kortere frister i visse situasjoner, f.eks. i vanhjemmelssituasjoner eller ved endrede myndighetskrav

- Manglende varslingsfrister ved endringer i og/eller bortfall av tjenester
- Lav terskel for suspensjon
- Vilkår for heving ofte uten vesentlighetsterskel, eller ved ethvert betalingsmislighold (stort som lite), uten mulighet for å rette misligholdet før heving skjer

- Heving på dagen, og ingen «overgangsperiode». Hva med tilgang på data?
- Vilkårene kan endre seg
- Lovvalg og verneting langt utenfor Norges grenser.

- MVA risikoen tilligger kunden

- Dvs. «As- Is» leveranser, mange plikter og få rettigheter
- Manglende forutsigbarhet er fellesnevneren i skyvilkår
- Vilkårene hensyntar ikke at bytte ikke kan gjøres fra en dag til neste.
- Helt ok for mange skytjenester, men kanskje ikke greit at leveransesikkerhet understøttes for virksomhetskritiske/samfunnskritiske løsninger?

FØYEN

Så hva bør en gjøre?

- En kan velge å .....

- Eller dersom løsningen er virksomhets/samfunnskritisk, og en er opptatt av forretningskontinuitet og/eller gode kommersielle betingelser o.l så:
  - Sørg for konkurranse når du anskaffer
  - Lag en evalueringsmodell for «godheten» i skyvilkårene, i tillegg til det kommersielle
  - Vurder å inngå bindende abonnement
  - Ikke tro at du ikke kommer noen vei!
  - (i tillegg til å sikre regulatorisk compliance)

FØYEN

Kjøp gjennom forhandler

- ulike avtalemodeller som kan påvirke risikoen/leveransesikkerhet

Eksempel Microsoft

Program som innebærer direkteavtale mellom Microsoft og Kunde:

- Entreprise Agreement (direkte med MS)
- Microsoft Customer Agreement (MC), (direkte med MS, men kan også inngås gjennom forhandler)
- Microsoft Online Services Agrement (MOSA), (direkte med MS)

Program som ikke innebærer direkteavtale mellom Microsoft og Kunde:

- Customer Solution/Hosting exception
- Managed Services exception

Eksempel Amazon

Program som innebærer direkteavtale mellom Amazon og Kunde:

- Entreprise Agreement
- Amazon Customer Agreement (direkte med AWS)
- End Customer Account Model (kjøp gjennom forhandler)

Program som ikke innebærer direkteavtale mellom Microsoft og Kunde:

- Solution Provider Account Model (kjøp gjennom forhandler)

FØYEN

Kjøp gjennom forhandler

- ulike leveransemodeller, hvordan påvirker dette risikoen/leveransesikkerhet?

Aksept av skytjenestevilkår

– etablerer en direkte avtale med Skyleverandør

Konsekvensen er at skyvilkårenes rettigheter og forpliktelser kan håndheves direkte mellom sluttkunden og skytjenesteleverandør. Da er rettigheter og plikter slik den følger av abonnementsbetingelsene

Aksept av skytjenestevilkår

– etablerer ikke direkteavtale

Konsekvensen er mange fallgruver som:

- Manglende compliance
- Risiko for **domino effekt** (en annen kundes mislighold kan medføre stans eller opphør også mot deg som kunde)
- Manglende vanhjemmels «dekning»
- Manglende erstatningsrett ved brudd på GDPR, taushetsplikt m.v
- Relasjonen til forhandler skaper tilleggsrisiko
- +++

FØYEN

Indirekte kjøp - ulike avtalemodeller for SaaS leverandører som hoster løsningen hos en hyperscaler

Er Kunde selv

Dvs. inngå abonnementsavtale om IaaS/PaaS tjenester med en hyperscaler (evt. gjennom en forhandler).

Innebærer som regel at Saas-leverandøren må akseptere skytjenesteleverandørens standardvilkår.

Tenant tilhører SaaS leverandøren.

Avtalemodellen brukes ofte som modell hvor SaaS-leverandøren ønsker å etablere multitenant løsninger.

INNEBØRER HØY RISIKO for SaaS-leverandør

Er forhandler

Dvs. SaaS-leverandøren inngår en forhandleravtale som gir rett til å videreselge IaaS/PaaS tjenester hos en hyperscaler.

Tenant tilhører da kunden det videreselges til (og samtidig leverer SaaS-tjenester til).

Fordrer installasjon i miljøet/kontoen til den enkelte kunde, og vil kunne være mer kostnadskrevende.

Men vi ser at enkelte skyleverandører har tjenester som sikrer massedistribusjon til mange kundetenants samtidig. For eksempel MS Partner Shared Services.

LAV RISIKO for Leverandør

Kunden tegner direkteavtale

Kunden hoster SaaS-tjenesten selv og gir programvareleverandøren tilgang til kontoen hos en hyperscaler.

Fortsatt høy risiko for kundene ved forretningskritiske/samfunnskritiske løsninger pga manglende vern/forutberegnlighet.

P.T LAV RISIKO for Leverandør, fortsatt høy for Kunden

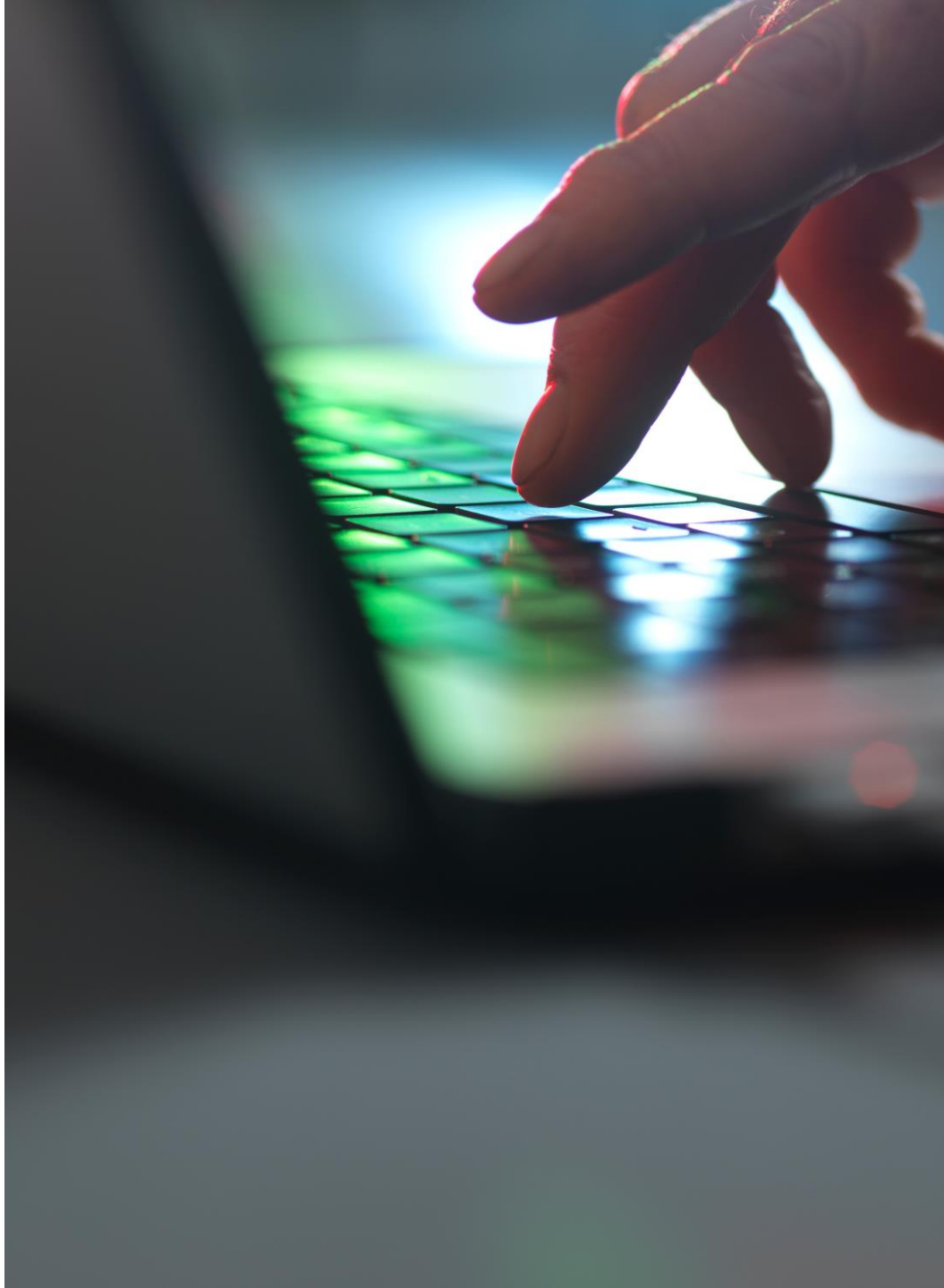
FØYEN

Indirekte kjøp, kundeperspektivet, eksempel Microsoft

Microsofts utgangspunkt i Microsoft Customer Agreement er at en kun kan bruke online tjenestene:

«solely for Customer's own use and business purpose and are non-transferable and you are not entitled to distribute, subslicense, rent, lease or lend any Online services, in whole or in part, or use them to offer hosting services to a third party»

Men unntak (for SaaS):
"create and maintain a Customer Solution and, despite anything to the contrary in Customer's volume licensing agreement, combine Microsoft Azure Services with Customer Data owned or licensed by Customer or a third party, to create a Customer Solution using the Microsoft Azure Service and the Customer Data together. Customer may permit third parties to access and use the Microsoft Azure Services in connection with the use of that Customer Solution. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer's volume licensing agreement are met by that use



FØYEN

Indirekte kjøp, kundeperspektivet, eksempel Microsoft, forts.

- Når SaaS leverandøren er kunde av Microsoft, får ikke sluttkunden noen DPA med Microsoft – viktig at GDPR likevel sikres i verdikjeden, inkl. Art. 32 risiko vurdering
- Om Microsoft bryter DPA (mellom SaaS leverandør og MS), vil eventuell erstatning ikke dekke krav fra sluttkundene. Problem?
- Når SaaS leverandøren er kunde av Microsoft, får ikke sluttkundene vanhjemmelsbeskyttelse av Microsoft. Problem?
- Når SaaS leverandøren er kunde av Microsoft, får ikke sluttkundene erstatning av Microsoft ved brudd på taushetsplikt. Problem?
- Når SaaS leverandøren er kunde av Microsoft, får ikke sluttkundene krav på SLA bøter av Microsoft ved SLA brudd. Problem?
- Siden SaaS leverandøren er ansvarlig for mislighold av Microsofts skytjenestevilkår som en sluttkunde forårsaker, vil slike tilfeller i verste fall kunne føre til suspensjon eller heving mot SaaS leverandøren. **# Risiko for domino effekt**
- Vil kundene akseptere dette for virksomhetskritiske løsninger, eller vil de kreve tiltak?

FØYEN

Indirekte kjøp, risiko om SaaS leverandøren er **forhandler** av IaaS/PaaS miljøet

- Alt er relativt trygt og greit hvor forhandlermodellen innebærer at det inngås en direkteavtale mellom IaaS/PaaS leverandøren og den enkelte sluttkunde. Dvs applikasjonen installeres på kundens konto.
- Ved kjøp gjennom forhandler er det likevel viktig å ha en klar avtale med forhandler/SaaS leverandør hvordan forbruk optimaliseres, endringer initieres, pricelock o.l.
- For Microsoft til eksempel, så bortfaller risikoene nevnt på forrige slide.
- Microsoft Shared Services gjør det mulig å massedistribuere oppdateringer til flere kundeinstallasjoner samtidig.
- Ulemper – SaaS leverandøren må ofte inngå separat avtale må inngås med en distributør (av MS). Må også hensyntas i eventuelle risikovurderinger.
- En ulempe sett fra kundeperspektivet er at de fortsatt må leve med Microsoft Customer Agreement, og manglende «forutberegnelighet». Ref. slide 3.

FØYEN

Indirekte kjøp, risiko om SaaS-leverandøren får tilgang til kundens tenant

- Et tredje alternativ er at leverandøren får tilgang til kundens tenant
- Dvs kunden tegner selv direkteavtale med Microsoft om bruk av Azure
- For Saas Leverandøren så blir da risikoen lik som i CSP tilfellet = forsvinner
- En ulempe sett fra kundeperspektivet er at de fortsatt må leve med Microsoft Customer Agreement, og manglende «forutberegnelighet». Ref. slide 3.

FØYEN

Kontakt

Advokatfirmaet Føyen AS
Dronning Eufemias gate 8
0191 Oslo
Tlf: +47 21 93 10 00
foyen.no

Følg oss i sosiale medier:
Nyhetsbrev / LinkedIn
Instagram / Facebook

Lars Folkvard Giske
Partner
92 41 88 01
lars.giske@foyen.no

Meld deg på Føyens nyhetsbrev her:

https://form.apsis.one/kqQPxbsu4Dq9

Eller via vår nettsideFoyen.no

Agenda

- Markedsplassen for skytjenester
- Føyen AS om Risiko med ulike avtalemodeller i skyen
- **CIPS**
- FinOps / AI
- Cloud R&A
- CyberX

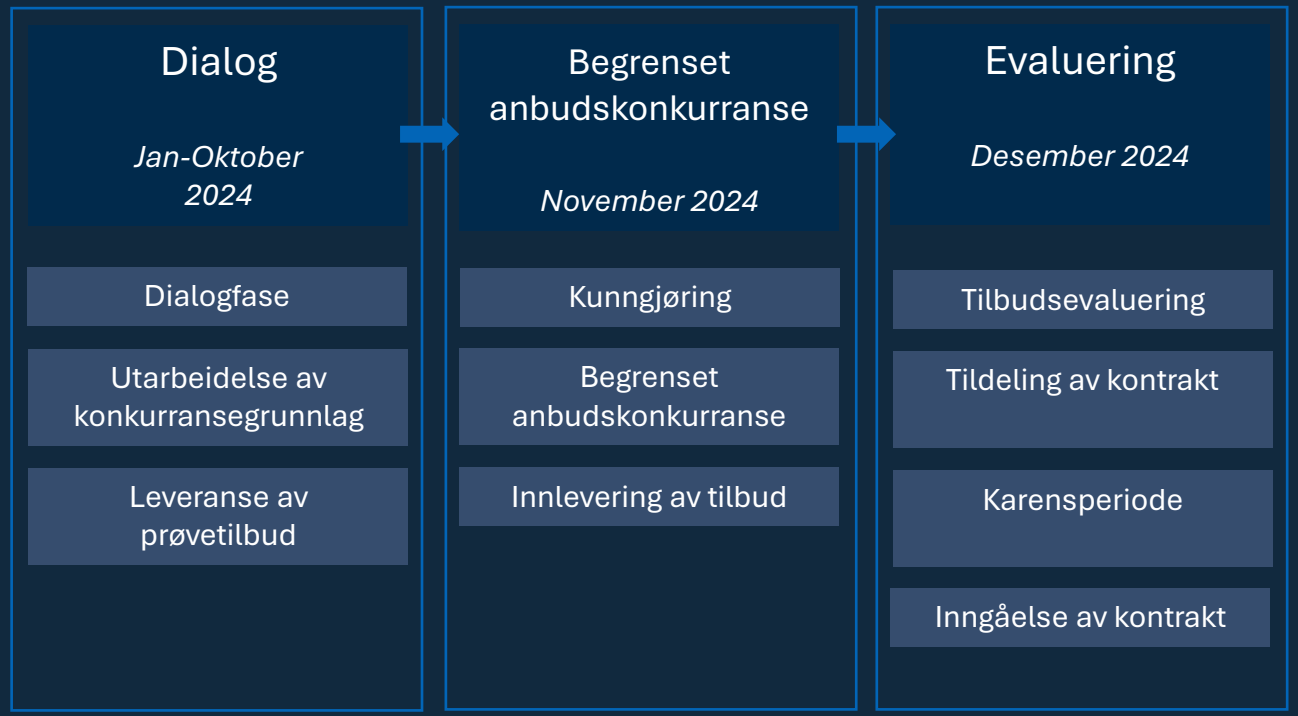
CIPS

Ingrid Sørensen, prosjektleder

Norwegian agency for public and financial management

CIPS | Status

- Pågående anskaffelsesprosess
- Konkurransepreget dialog
- 6-8 leverandørkandidater
- Tildeling 2-4 kontrakter



CIPS | Avropsmekanismer

Direkte

‘Skrivebord’

Mini-konkurranse

CIPS | Kundens perspektiv

Løsning

Definere behov

Avrop CIPS

Implem entering

Konfigurering

Drift

Vedlikehold

Spørsmål

Agenda

- Markedsplassen for skytjenester
- Føyen AS om Risiko med ulike avtalemodeller i skyen
- CIPS
- **FinOps / AI**
- Cloud R&A
- CyberX

FinOps / KI

David Behrens, prosjektleder

Norwegian agency for public
and financial management

FinOps | Status utprøvingsprosjekt

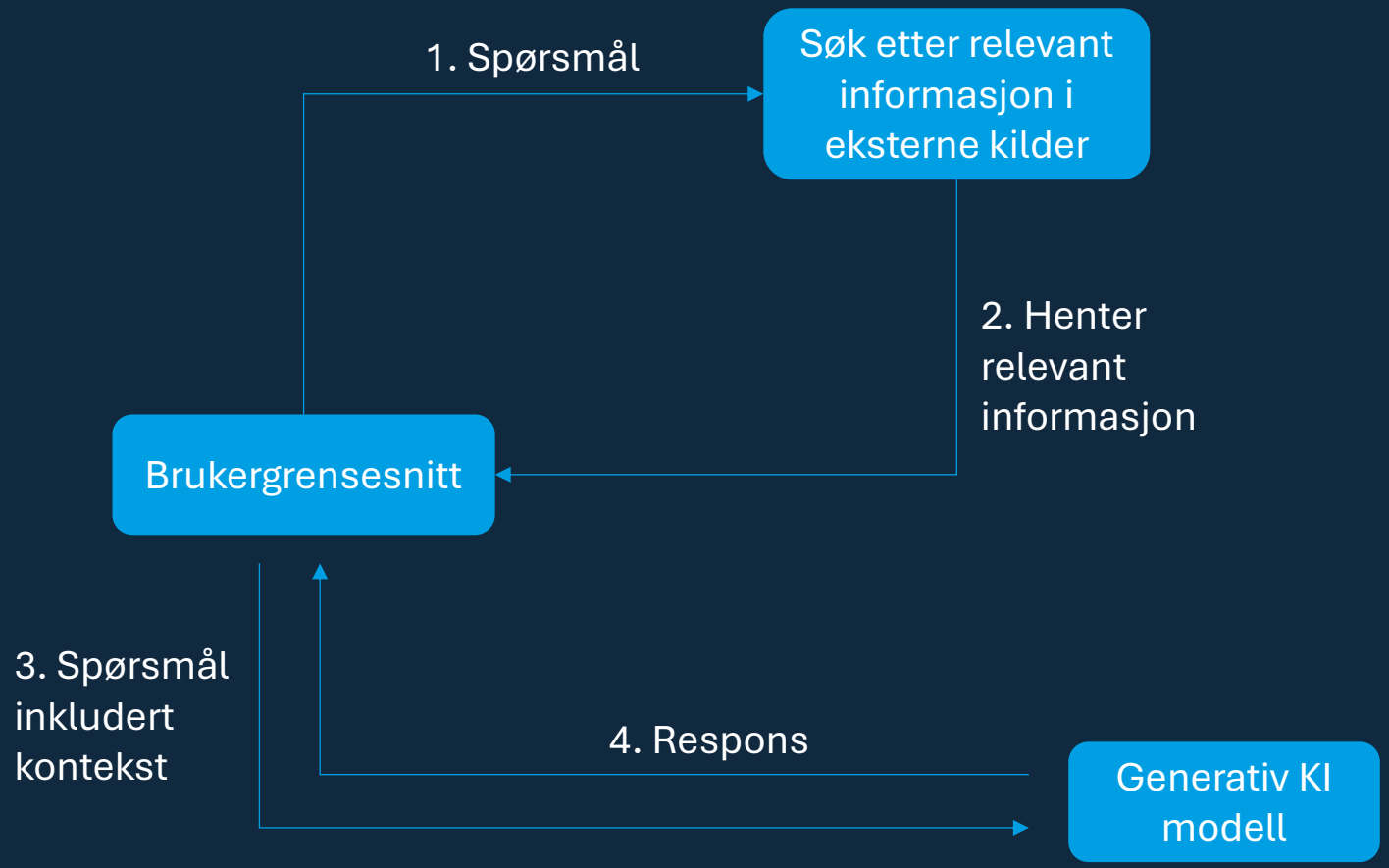
- Snart i gang med første utprøvingsprosjekt på FinOps: Fokus er på IaaS og PaaS spend
- Frist for å søke om å delta utløp 10. september
- Har mottatt flere relevante søknader
- Vurderer søknadene nå og kommer til å sende ut invitasjoner til oppstartsmøte veldig snart

RAG AI | RFI

- Retrieval-Augmented generation (RAG)
- RFI Publisert på Doffin og TED
- Frist for å svare utløp 1. september
- God respons spesielt fra plattformleverandører
- Savner leverandører av generative KI modeller
- Dialogmøter pågår denne og neste uke

RAG AI | Hva er det?

- RAG er en teknikk for å øke nøyaktigheten og påliteligheten til generativ KI ved å hente data fra eksterne kilder (Rick Merritt, 2023)



RAG AI | Hvorfor RAG?

Økt relevans

Kontroll

Referanser og sporbarhet

RAG AI | Hva ser vi på?

- Ser på ulike produkter og leveransemodeller
- Open source versus closed source
- Fleksibel deployering
- Generelt bruksområde
- Støtte for ulike dataformater
- Multimodal
- Støtter flere KI modeller
- Sikkerhet, opphavsrett
- Språk

Spørsmål

Agenda

- Markedsplassen for skytjenester
- Føyen AS om Risiko med ulike avtalemodeller i skyen
- CIPS
- FinOps / AI
- **Cloud R&A**
- CyberX

Cloud Research & Advisory

Helene Stunes, prosjektleder

Norwegian agency for public
and financial management

Cloud R&A | Formål

- Rammeavtale for leverandøruavhengige forsknings- og rådgivningstjenester relatert til produkter og tjenester innen skyteknologi

Cloud R&A | Kartlegging

Markedsundersøkelse

Behovsanalyse

Ekspertgruppe

Cloud R&A | Kartlegging

Markedsundersøkelse

Behovsanalyse

Ekspertgruppe

- Besvarelser fra 10 leverandører
- Kjennskap til det norske markedet/tilstedeværelse
- 50 % tilbyr alle tre hovedområder
  - Artikkeldatabase/forskningsmateriell
  - Tilgang på analytikere/rådgivere
  - Konferanser/arrangementer

Cloud R&A | Kartlegging

Markedsundersøkelse

Behovsanalyse

Ekspertgruppe

- Frist: 20. september 2024 kl. 13:00

Vil du også besvare behovsanalysen?

Ta kontakt med prosjektleder via e-post: helene.stunes@dfo.no

Cloud R&A | Kartlegging

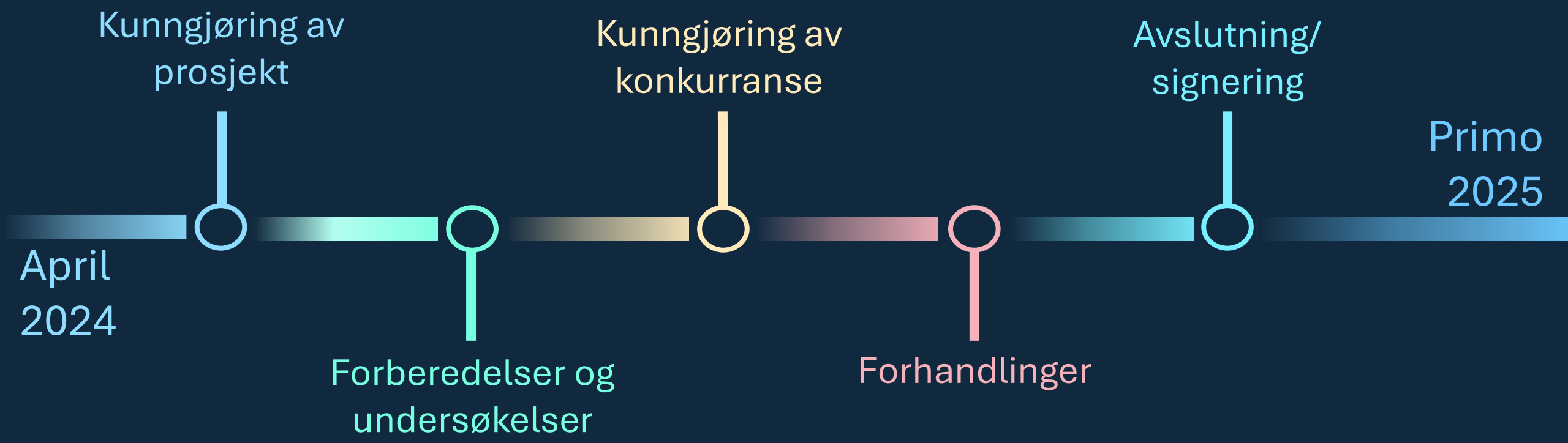
Markedsundersøkelse

Behovsanalyse

Ekspertgruppe

- Representer fra ulike offentlige virksomheter
- Arbeidsoppgaver
  - Kvalitetssikring
    - Strategi
    - Konkurransedokumenter

Cloud R&A | Veien videre



prosjekt

konkurranse

signering

Primo 2025

April 2024

Forberedelser og undersøkelser

Forhandlinger

- Behovet er tilstede
- Leverandørene er interesserte

→

- Analysere svar fra behovsundersøkelse
- Sette opp utkast til avtaledokumenter
- Dialog med ekspertgruppe

Spørsmål

Pause (10 min)

Følg MPS på LinkedIn →

Norwegian agency for public and financial management

Agenda

- Markedsplassen for skytjenester
- Føyen AS om Risiko med ulike avtalemodeller i skyen
- CIPS
- FinOps / AI
- Cloud R&A
- **CyberX**

CyberX

Per Jakobsen, seniorrådgiver

Norwegian agency for public
and financial management

Cloud Security Reference Architecture

Referansearkitektur for sikkerhet i skyavtaler med norske kommentarer

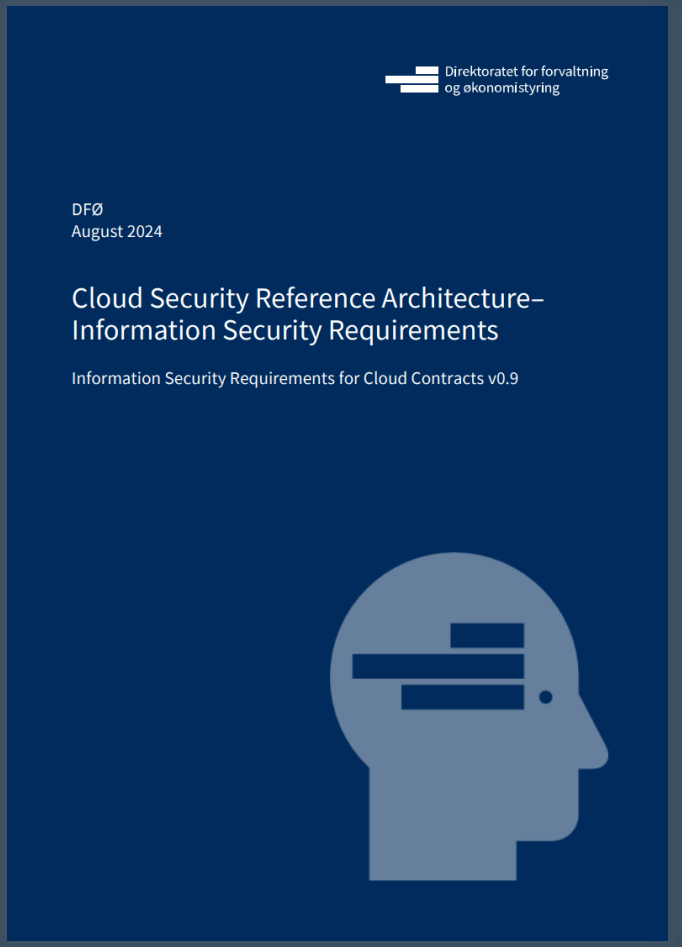
CyberX | Referansearkitektur for sikkerhet i skyavtaler -overordnet

Informasjonssikkerhetskrav for skytjenester utviklet av MPS

Utdypet med norske kommentarer som veiledning til kravene

Verifiserbare krav til sikkerheten i skytjenester
ved anskaffelse og forvaltning

Vektlegger sikker bruk av skytjenester «security in the cloud»



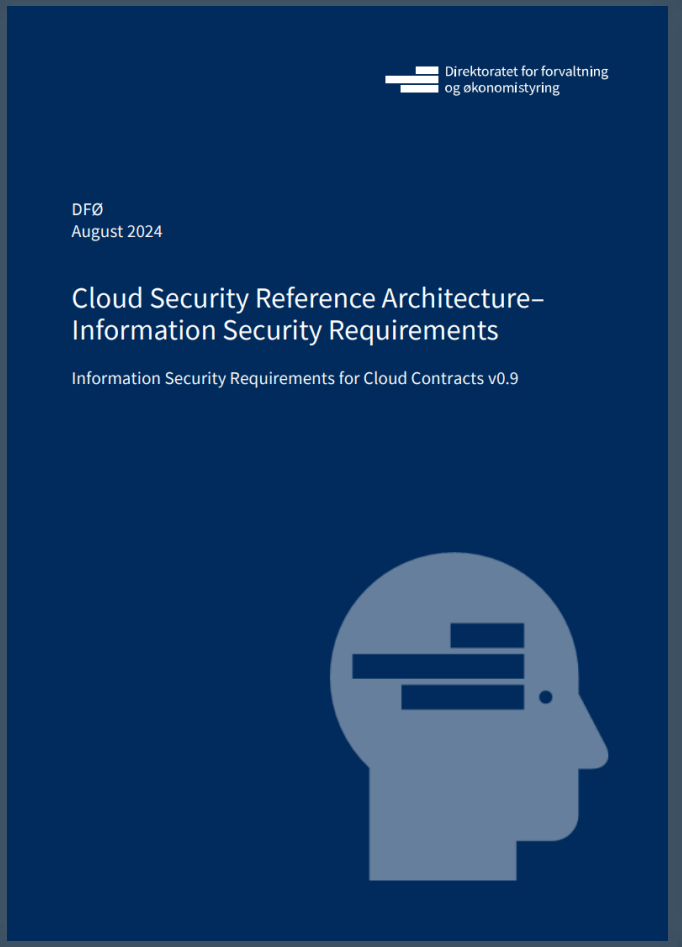
CyberX | Referansearkitektur for sikkerhet i skyavtaler - grunnlag

Utviklet i perioden 2022 – 2024 i dialog med brukere i offentlig sektor - stat, fylkeskommuner og kommuner

Internasjonale standarder og rammeverk inkludert ISO 27001 og NIST Cyber Security Framework v2.0

Norske standarder og rammeverk inkludert NSM Grunnprinsipper og Normen

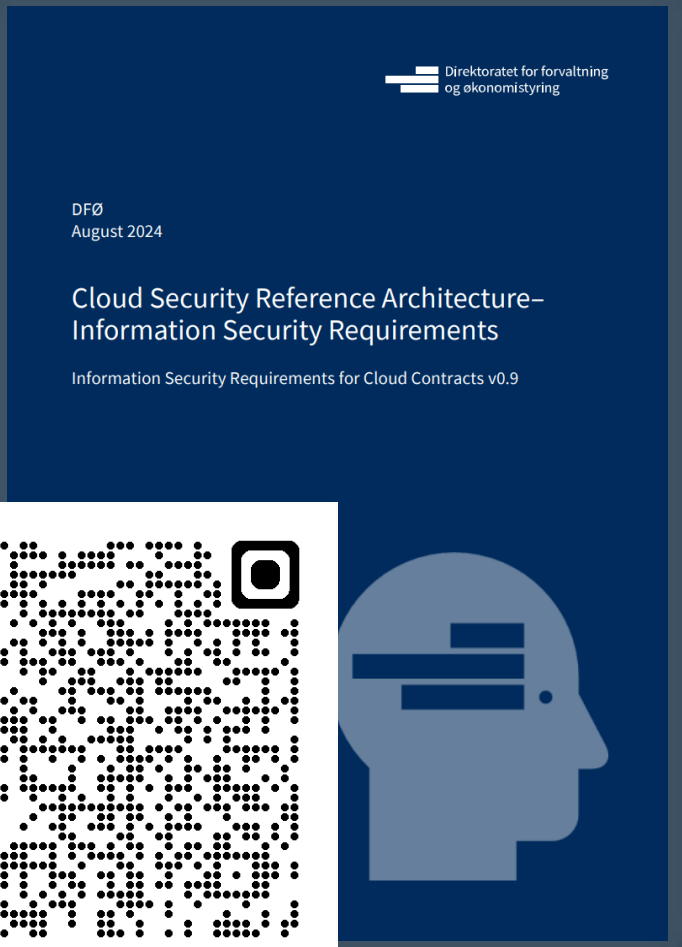
Juridiske krav og rammeverk inkludert GDPR, NIS2, Sikkerhetsloven og loven om digital sikkerhet.



#mps

CyberX | Referansearkitektur for sikkerhet i skyavtaler - struktur

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



#mps

CyberX | Referansearkitektur – kommentarer på Norsk
Eksempelkrav - I hvilken grad beskriver veiledningen aktiviteter/prosesser for ledelsesstyring?

Eksempel:

Krav på engelsk	Norsk kommentar
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.	Det er viktig at leverandøren utpeker en sikkerhetsansvarlig på et høyt nok nivå som motpart til kunden, fordi dette sikrer at strategiske sikkerhetsspørsmål får nødvendig oppmerksomhet og håndtering på høyeste nivå i organisasjonen. En slik rolle er avgjørende for effektiv kommunikasjon og samarbeid om sikkerhetsstrategi, rapportering, og oppfølging av vesentlige risikoer, hendelser og sårbarheter. Dette bidrar til en helhetlig og proaktiv tilnærming til sikkerhet, som igjen styrker tilliten mellom leverandøren og kunden, og sikrer bedre håndtering av potensielle trusler.

CyberX | Referansearkitektur - Status og videre utvikling

Lansert på Sikkerhetsfestivalen v0.9:
Cloud Security Reference Architecture,
overordnede prinsipper, metoder og krav

Under utarbeidelse v1.0:

- «Mapping» til juridiske/regulatoriske krav og sikkerhetsstandarder/rammeverk
- Krav til personvern
- Innspill fra brukermiljøer og evalueringsskjemaer

Hjem / Fagområder / Cybersikkerhet / Krav til informasjonssikkerhet i skyavtaler - referansearkitektur

Krav til informasjonssikkerhet i skyavtaler - referansearkitektur

DFØ ved Markedsplassen for skytjenester (MPS) har utarbeidet krav til informasjonssikkerhet i skyavtaler i form av en referansearkitektur med grunnleggende krav til sikkerhet (publiseres her som et utkast i versjon 0.9). Kravene er ment å være en støtte innen krav til sikkerhet i arbeidet med anskaffelser av skytjenester for offentlige virksomheter og er basert på MPS anskaffelser/skyavtaler. Virksomhetene må selv vurdere hvilke krav som er relevante og eventuelt stille egne tilleggskrav ut over sikkerhetskravene i rammeverket. MPS jobber fortløpende med å videreutvikle referansearkitekturen basert på innspill fra offentlig sektor og leverandører, og versjon 1.0 vil publiseres i løpet av 2024.

Dette er en norsk veiledning til MPS "Cloud Security Reference Architecture - information security requirements v0.9". Referansearkitekturen i original (PDF, engelsk) kan lastes ned her:

Cloud_Contract_Security_Reference_Architecture_v09.pdf
PDF 380.95 KB

Digitale reguleringer innen EU

Veiledning på MPS

CyberX | Digitale reguleringer innen EU – veiledning på markedsplassen

Krevende landskap av reguleringer innen personvern og cybersikkerhet

Oversikt over ulike lover som er relevante å sette seg inn i med hensyn til cybersikkerhet og personvern:

NIS2-direktivet
Cyber Resilience Act (CRA)
Lov om Digital operasjonell motstandsdyktighet (DORA)
Data Act (DA)
Lov om digitale tjenester (DSA)
Lov om digitale markeder
Artificial Intelligence Act (AI/KI loven)

Digitale reguleringer i EU

I 2024 må virksomheter navigere et stadig mer krevende landskap av reguleringer innen personvern og cybersikkerhet. I denne veiledningen presenterer vi en oversikt over aktuelle digitale reguleringer og forskrifter fra EU, sammen med en kort forklaring på status i Norge.

Del I. Cybersikkerhet

NIS2-direktivet

Oversikt

NIS2-direktivet[1] er den nyeste EU-lovgivningen som regulerer cybersikkerhet. NIS2-direktivet er den offisielle etterfølgeren til nettverks- og informasjonssikkerhetsdirektivet (NIS), som ble introdusert i EU i 2016.

NIS2 har som hovedmål å etablere et høyt felles nivå for cybersikkerhet i hele EU. Det setter også et krav om at EUs medlemsland øker cybermotstanden til offentlige og private virksomheter som opererer i kritiske sektorer. Dette gjør NIS2-direktivet til en av de viktigste rettsaktene knyttet til cybersikkerhet i EU. Direktivet legger frem spesifikke tiltak for risikostyring av cybersikkerhet og etablerer obligatoriske rapporteringskrav for flere kritiske sektorer.

NIS2-direktivet trådte i kraft 16. januar 2023. EUs medlemsstater har imidlertid frist til 17. oktober 2024 med å innarbeide NIS2 i nasjonal lovgivning og sørge for nødvendig offentliggjøring. Dermed vil NIS2-direktivet gjelde og håndheves fra 18. oktober 2024.

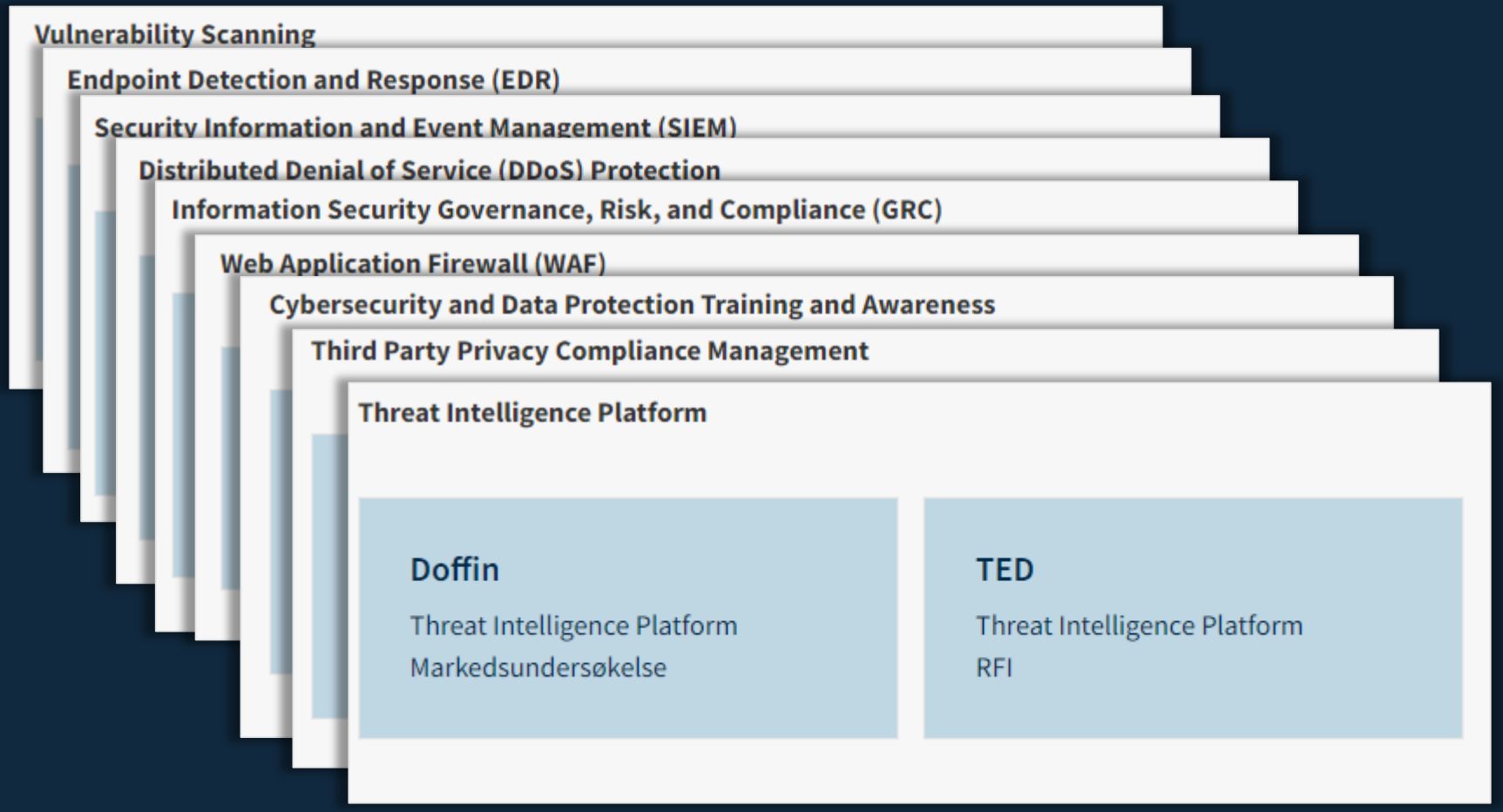
Avsnittene under gir en oversikt over NIS2-direktivet, endringene det medfører, og oppsummerer implikasjoner for virksomheter.

Innholdsfortegnelse

Kommende kontrakter på MPS

Veiledning på MPS

CyberX | veiledninger på markedsplassen utvikles for kommende kontrakter



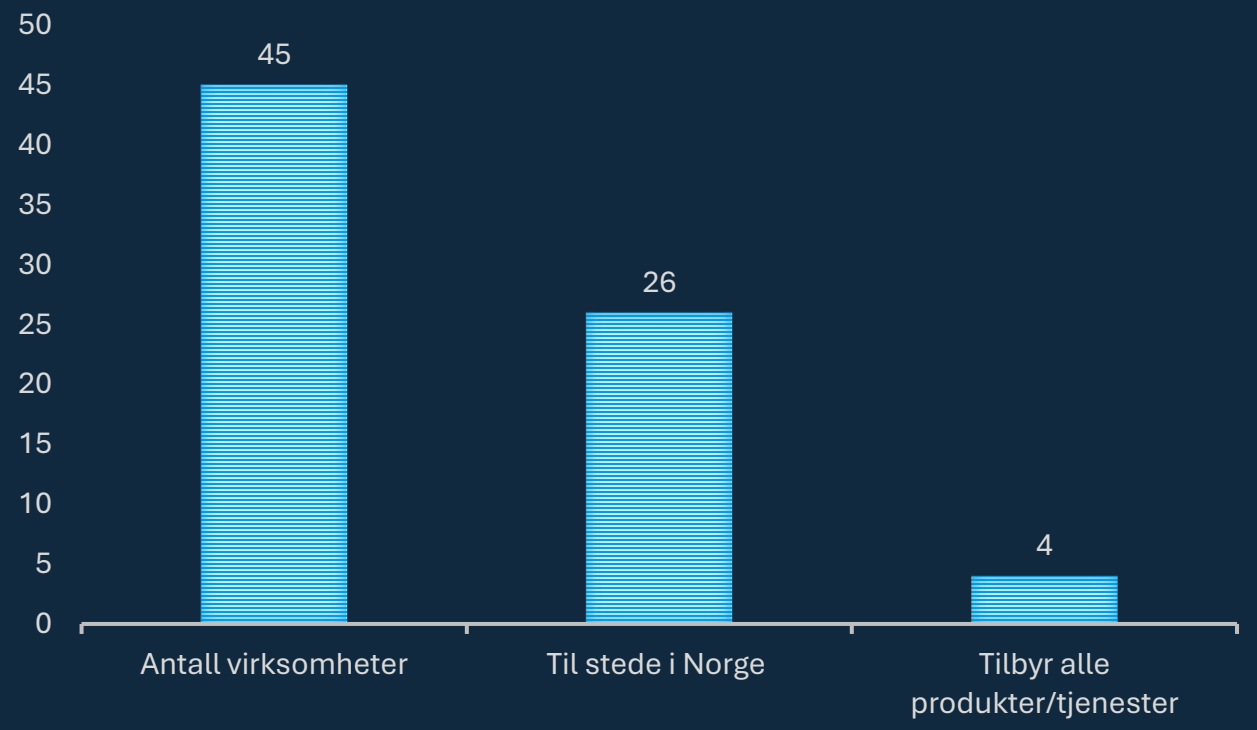
CyberX

Kristina Nikolajeva, prosjektleder

Norwegian agency for public and financial management

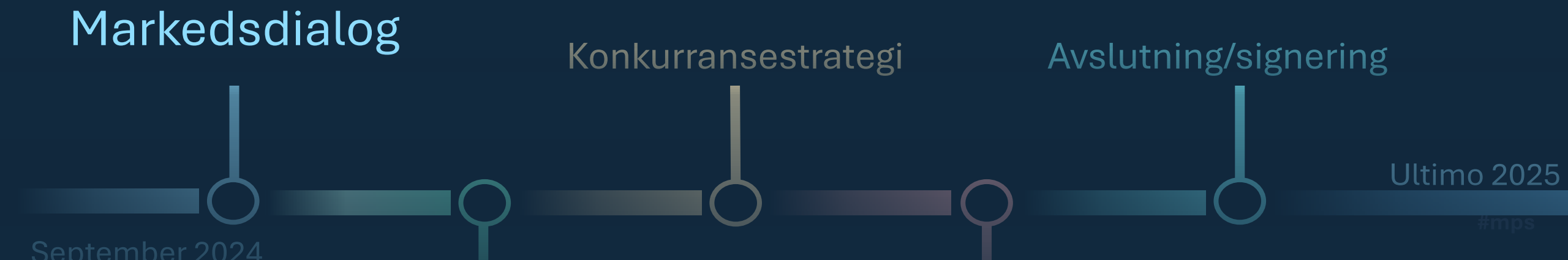
CyberX | Markedsundersøkelser: Cybersecurity and data protection - frist 22/8

- **Cybersecurity and Data Protection Training and Awareness**
- Distributed Denial of Service (DDoS) Protection
- Endpoint Detection and Response (EDR)
- **Information Security Governance, Risk, and Compliance (GRC)**
- Security Information and Event Management (SIEM)
- Third Party Privacy Compliance Management
- Threat Intelligence Platform
- **Vulnerability Scanning**
- Web Application Firewall (WAF)



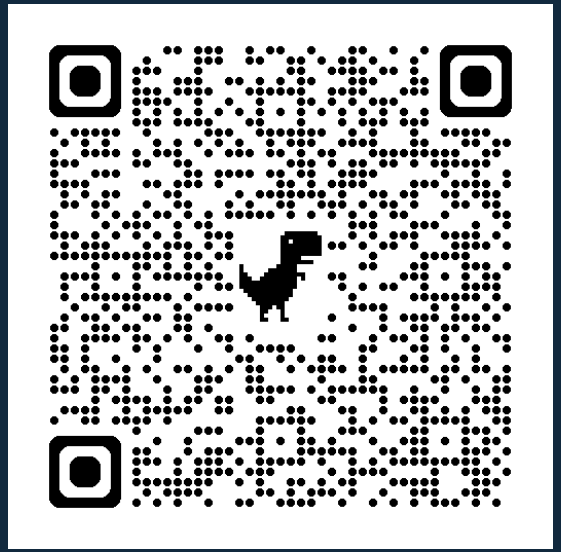
CyberX | Markedsundersøkelser | Veien videre

CyberX | Markedsundersøkelser | Veien videre



CyberX | Cyber Risk Score | Avtale

- MPS sin første avtale er inngått!
  - Utprøvingsprosjekt
  - Konklusjon
- Rammeavtalen er ikke-eksklusiv og frivillig å bruke
- Rammeavtalen gjelder i to år fra **1.september 2024**
- **Avropskontrakt varer i 15 måneder (3+12 måneders lisens)**



- Øk din informasjonssikkerhet ved bruk av

RiskRecon by Mastercard

Leverandør: KPMG AS

CyberX | Cyber Risk Score | Avtale

- Prøveperiode

  3 måneder gratis prøveperiode

- Roller/ansvar
  - MPS
  - Virksomhetene
  - Leverandøren

- Avrop

  cyberriskscore@kpmg.no

dfø

markedsplassen for skytjenester

En del av Anskaffelser.no

Hjem / Avtaler / Cyber Risk Score - Informasjon om rammeavtalen

Cyber Risk Score - Informasjon om rammeavtalen

Dette dokumentet[1] gir virksomhetene retningslinjer for hvordan avtalen bør brukes. Riktig bruk av tjenestene og avtalen er sentral for virksomhetenes realisering av forbedret informasjonssikkerhet ved bruk av Cyber Risk Score.

Om rammeavtalen

Direktoratet for forvaltning og økonomistyring (DFØ) ved Markedsplassen for skytjenester (MPS) har inngått avtale om måling av informasjonssikkerhet på internett med **KPMG AS** som leverer skytjenesten **RiskRecon** by Mastercard.

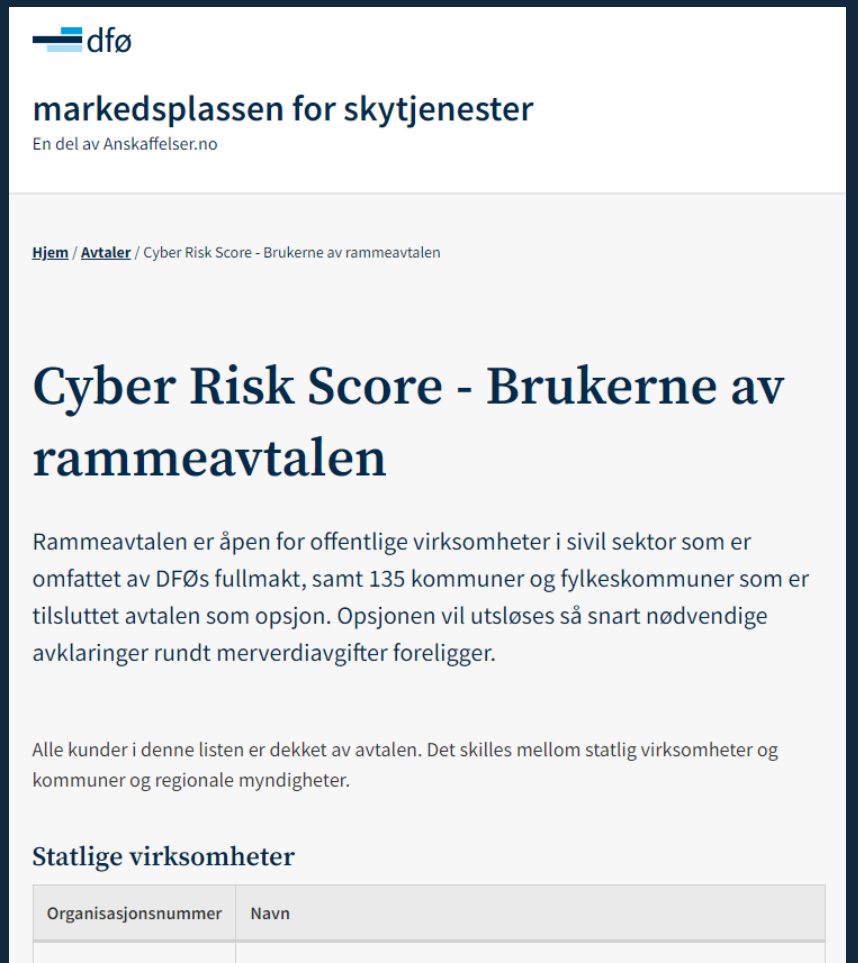
Rammeavtalen er ikke-eksklusiv og frivillig å bruke for virksomheter i sivil sektor som er omfattet av DFØs fullmakt[2].

CRS Framework Agreement documents Les mer →

#mps

CyberX | Cyber Risk Score | Avtale

- Brukerne av rammeavtalen



dfø

markedsplassen for skytjenester

En del av Anskaffelser.no

Hjem / Avtaler / Cyber Risk Score - Brukerne av rammeavtalen

Cyber Risk Score - Brukerne av rammeavtalen

Rammeavtalen er åpen for offentlige virksomheter i sivil sektor som er omfattet av DFØs fullmakt, samt 135 kommuner og fylkeskommuner som er tilsluttet avtalen som opsjon. Opsjonen vil utsløses så snart nødvendige avklaringer rundt merverdiavgifter foreligger.

Alle kunder i denne listen er dekket av avtalen. Det skilles mellom statlig virksomheter og kommuner og regionale myndigheter.

Statlige virksomheter

Organisasjonsnummer	Navn

CyberX | Cyber Risk Score | Avtale

- Kontrakten er publisert på vår nettside

dfø

markedsplassen for skytjenester

En del av Anskaffelser.no

Hjem / Avtaler / Cyber Risk Score Framework Agreement

Cyber Risk Score Framework Agreement

The Framework Agreement between DFØ (MPS) and KPMG AS for the delivery of a Cyber Risk Score Software-as-a-Service from RiscRecon by Mastercard is effective September 1, 2024.

Note that we are working on publishing the Framework Agreement in a more user friendly way and format.

Also note that we have redacted/removed a total of four -4- pages from the publicly available documents as they contain confidential information such as pricing information, cf. the Norwegian Freedom of information Act, section 13, cf. the Norwegian Public Administration Act section 13 first paragraph number 2and Section 23 (Norwegian: Offentleglova §13, jf. Forvaltningsloven § 13 første ledd nr. 2).

CRS Framework Agreement

CyberX | Cyber Risk Score | Avtale

- Cyber Risk Score er et verdifullt verktøy for virksomheter som ønsker å styrke sin evne til å identifisere, vurdere og håndtere cybertrusler.

cyberriskscore@kpmg.no

dfø

markedsplassen for skytjenester

En del av Anskaffelser.no

Hjem / Avtaler / Hvordan virksomheter kan dra nytte av Cyber Risk Score

Hvordan virksomheter kan dra nytte av Cyber Risk Score

I dagens digitale verden er cybertrusler en kontinuerlig utfordring for virksomheter. Teknologiske fremskritt har gjort det mulig for angripere å utnytte sårbarheter og påføre betydelig skade på organisasjoner. Derfor er det avgjørende for virksomheter å ha effektive strategier og verktøy for å identifisere og håndtere cybertrusler. Én slik strategi som har vist seg å være svært nyttig er bruk av Cyber Risk Score.

Hva er Cyber Risk Score?

Cyber Risk Score er en metode for å kvantifisere og vurdere en virksomhets eksponering for cybertrusler sett fra internett. Det er en numerisk verdi som reflekterer den totale risikoen for en virksomhet basert på ulike faktorer, for eksempel sårbarheter i infrastrukturen, historiske data om sikkerhetsbrudd og organisasjonens evne til å håndtere sikkerhetshendelser. Cyber Risk Score gir en helhetlig vurdering av sikkerhetsnivået sett fra internett og hjelper

Cyber Risk Score

Frank Horntvedt
Partner, Cyber & Security

Hva vet du i dag om organisasjonens eksponering på internett?

Vet du hvilke systemer/ressurser/tjenester virksomheten eksponerer på Internett og hvor de befinner seg i verden?

Hva er tilstanden for de eksponerte ressursene, samt endring over tid?

Hva med virksomhetens leverandører?

Hvilken risikoeksponering har de?

RISIKOEKSPONERING

CRS - Viser risikoeksponering på internett

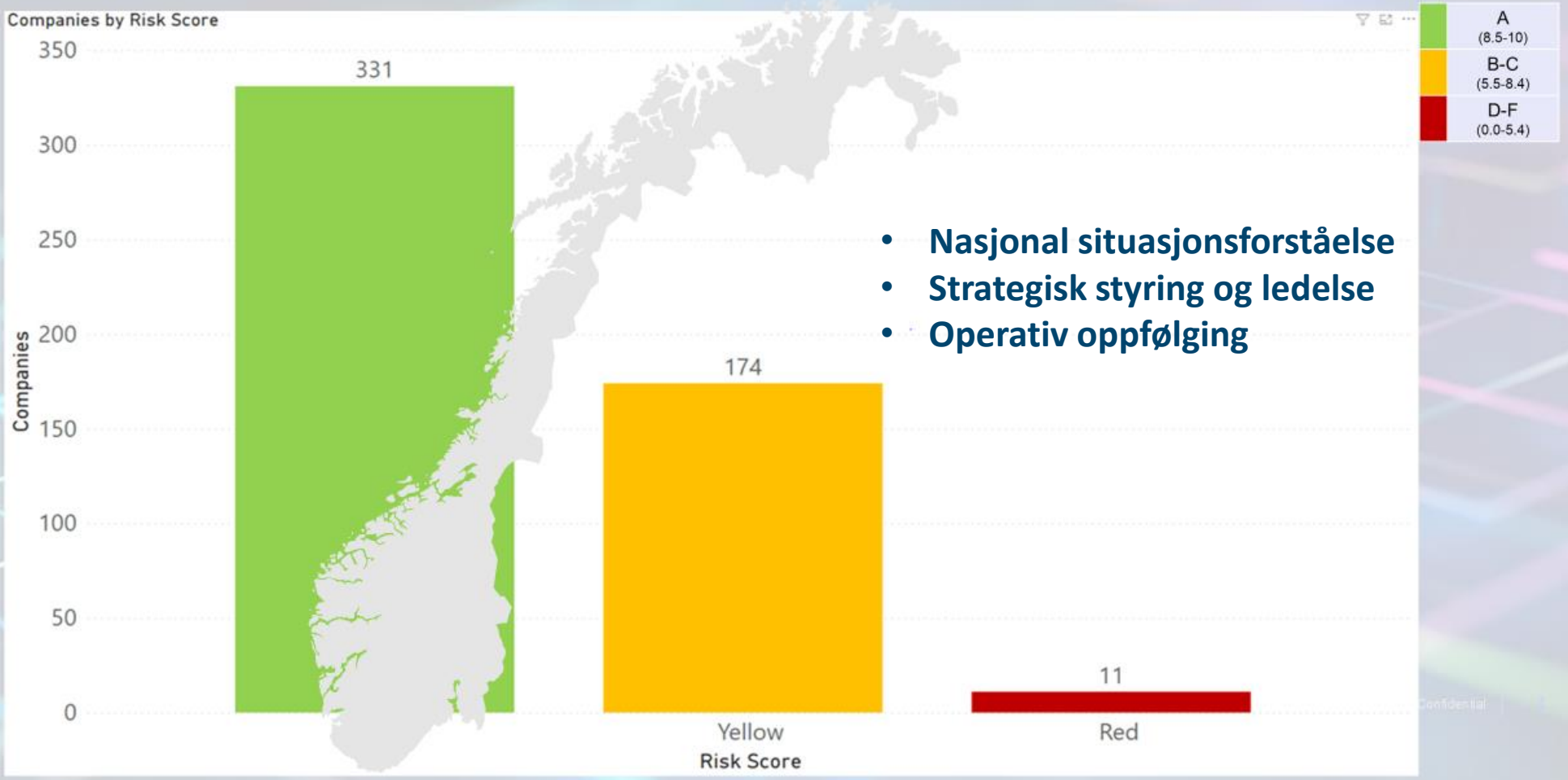
Identifisere

Vurdere

Håndtere

RISIKOEKSPONERING

Nåsituasjonen offentlig sektor Norge



- Nasjonal situasjonsforståelse
- Strategisk styring og ledelse
- Operativ oppfølging

Hva er Risk Recon?

Mastercard RiskRecon er et skybasert verktøy som kontinuerlig monitorerer både virksomhetens eksponerte ressurser, samt underleverandørers.

Risk Recon gjør ikke...

- Endring av parametere
- Injisering av kode
- Cross-site scripting (XSS) angrep
- SQL-injeksjon
- Forsøk på å forbigå autentiseringskrav
- Buffer Overflow-angrep
- Utfylling og innsending av skjema
- Passordgjetting
- Utnyttelse av sårbarheter
- Omgåelse av sikkerhetskontroller

Få kontroll over din cyberrisiko

Få detaljert og lett-forståelig oversikt over virksomhetens cyberrisko eksponert på internett.

Sett krav til leverandører

Tilgang til nødvendig vurderingsgrunnlag for å kunne sette krav til leverandører.

Lett-anvendelige rapporter

Tilpassede rapporter for et bredt spekter av bruksområder.

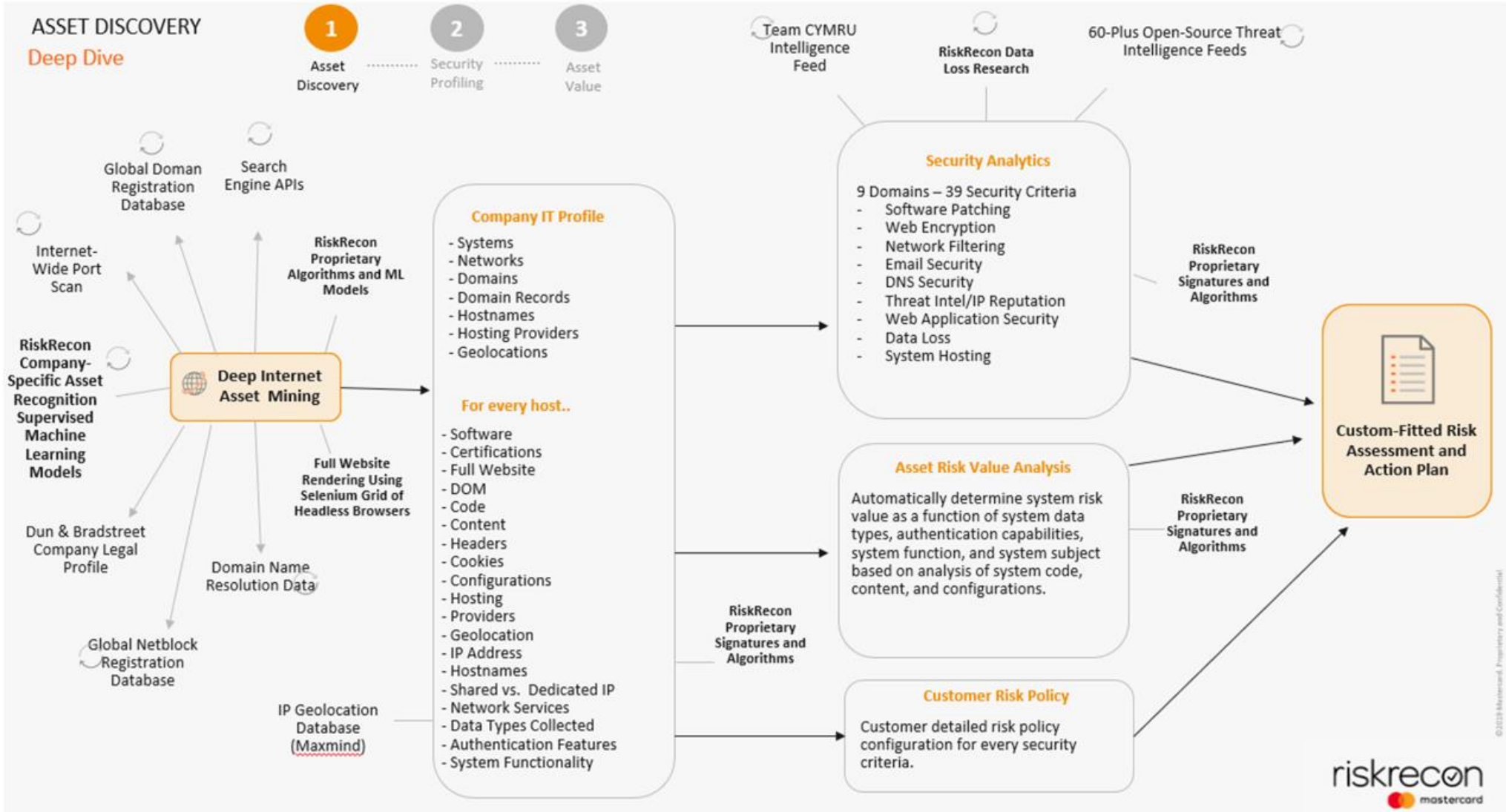
Sporbarhet over tid

Spor endringer i virksomhetens cyberrisiko over tid.

Årlig økning av cyberangrep som følge av digitale sårbarheter.

180%

For spesielt interesserte, innblikk i hvordan RiskRecon fungerer

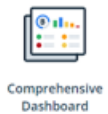


HVA INNGÅR I CYBER RISK SCORE KONTRAKTEN

CYBER RISK SCORE ABONNEMENT

3 måneder GRATIS prøveperiode

Portal med:



Omfattende og lettfattelig dashboard

Tilpassning til virksomhetens behov

Oversiktlig rapport til virksomhetens ledelse

Prioritering av tiltak ut fra virksomhetens risikoaksept

Verdikjederisiko

Indikatorer for samsvar med bl.a. ISO 27001 / NIS2

Detaljert information om sårbarheter pr. ressurs

Tiltaksplaner som kan deles med berørte, også leverandører

Forslag til korrigerende tiltak

Informasjon om egne og leverandørers sikkerhetsbrudd

Muligheter for filtrering av informasjon

Rapporter tilpasset ulike behov

TILLEGGSTJENESTER

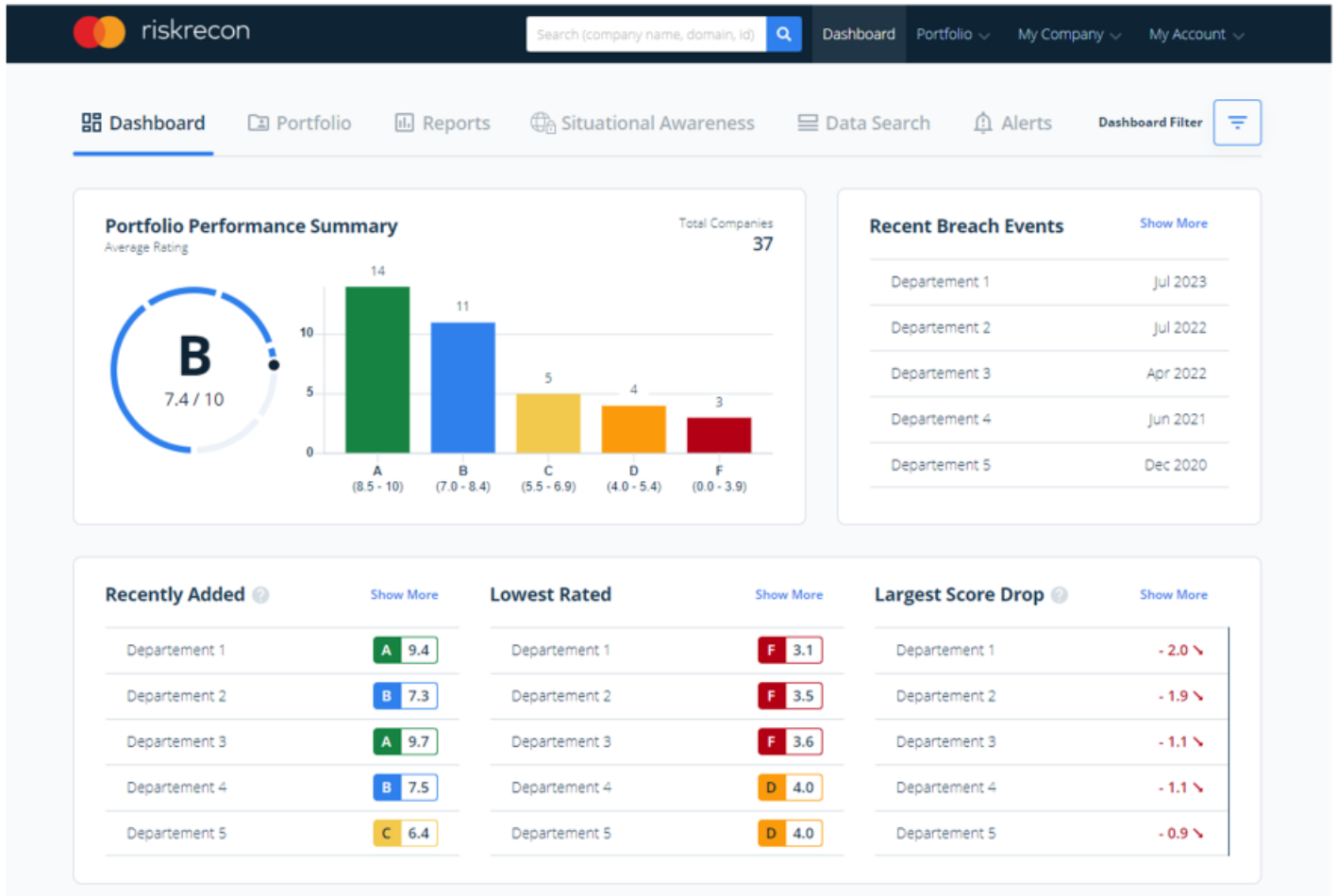
Kurs (gruppeundervisning eller virksomhetsintern)

- **Introduksjon til RiskRecon**
  Bruk av RiskRecon verktøyet og dens funksjoner
- **Styrk Cybersikkerheten din**
  Strategisk bruk av RiskRecon verktøyet for å styrke sikkerheten
- **Forstå cyberrisikoen din**
  Gir en grundig forståelse av cyberrisiko relatert til virksomheten
- **Avanserte funksjoner for avanserte brukere**
  Innføring i bruk av avanserte funksjoner i RiskRecon verktøyet
- **Systemintegrasjon**
  Innføring i integrasjon av RiskRecon med virksomhetens øvrige IT-systemer
- **Forstå og håndter tredjepartsrisiko med RiskRecon**
  Bruk av RiskRecon som verktøy for håndtering av verdikjederisiko

Rådgivningstjenester (Subject Matter Experts)

- Etablere veikart for Cybersikkerhet
- Optimalisering av RiskRecon verktøyet
- Verdikjederisiko
- Integrasjon med virksomhetsprosesser
- Systemintegrasjon

Oversiktlig Dashboard

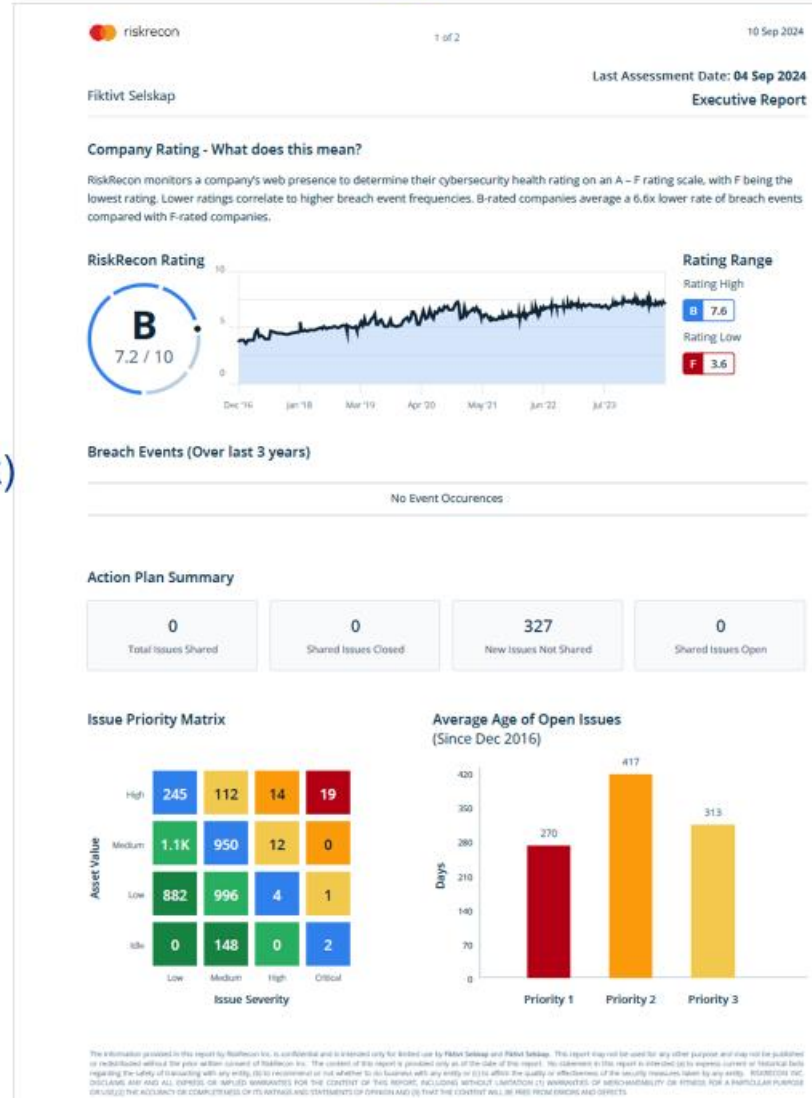


- Administrasjon av verktøyet
- Risikoprofil og monitorering
- Varsling, workflow og validering av standarder
- Rapportering og referansepunkter

Eksempel på ledelsesrapport

Standard rapporter

- Executive (ledelse)
- Sammendrag
  - (overordnet / teknisk)
- Detaljert (teknisk)



riskrecon 1 of 2 10 Sep 2024

Fiktivt Selskap

Last Assessment Date: **04 Sep 2024**
Executive Report

Company Rating - What does this mean?

RiskRecon monitors a company's web presence to determine their cybersecurity health rating on an A – F rating scale, with F being the lowest rating. Lower ratings correlate to higher breach event frequencies. B-rated companies average a 6.6x lower rate of breach events compared with F-rated companies.

RiskRecon Rating

B
7.2 / 10

Rating Range

Rating High
B 7.6

Rating Low
F 3.6

Breach Events (Over last 3 years)

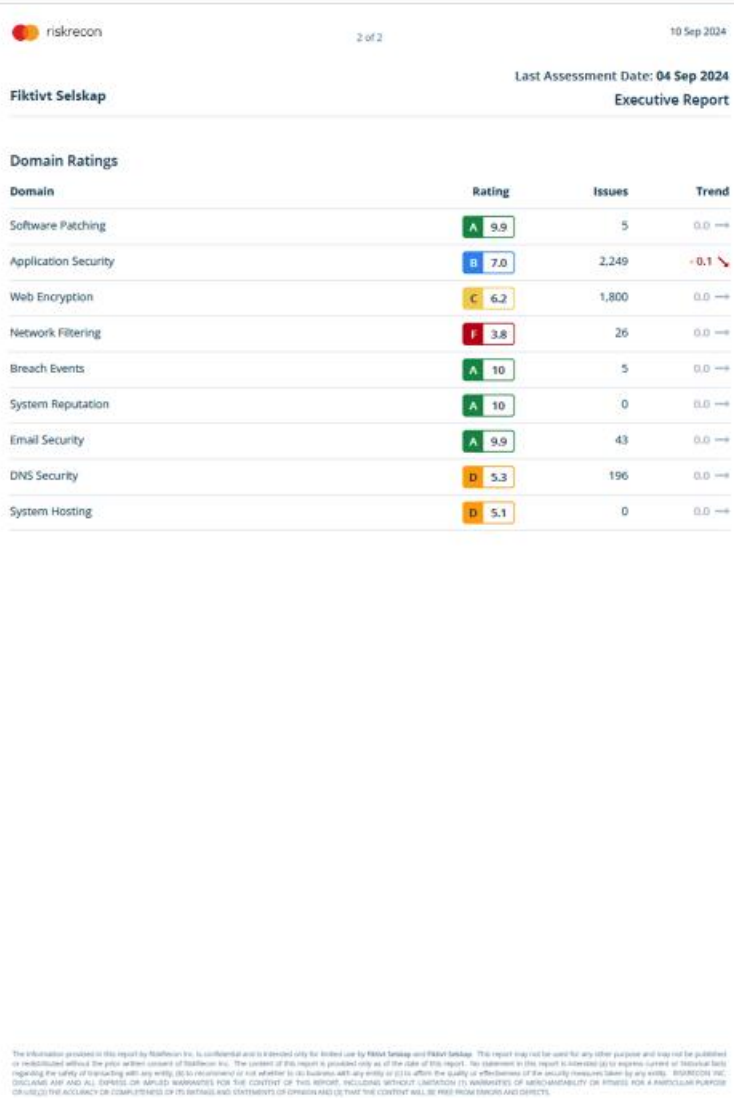
No Event Occurences

Action Plan Summary

0	0	327	0
Total Issues Shared	Shared Issues Closed	New Issues Not Shared	Shared Issues Open

Issue Priority Matrix

Average Age of Open Issues
(Since Dec 2016)



riskrecon 2 of 2 10 Sep 2024

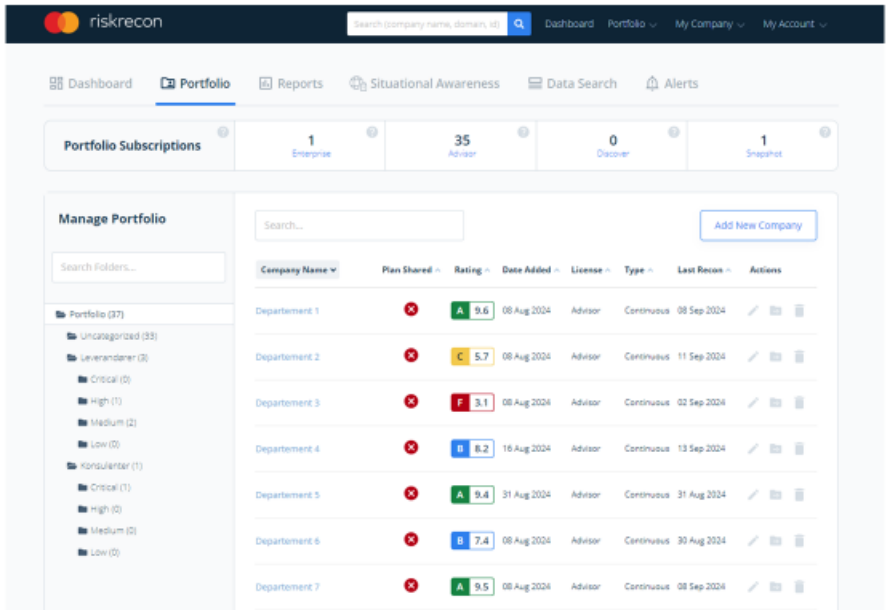
Fiktivt Selskap

Last Assessment Date: **04 Sep 2024**
Executive Report

Domain Ratings

Domain	Rating	Issues	Trend
Software Patching	A 9.9	5	0.0 →
Application Security	B 7.0	2,249	-0.1 ↘
Web Encryption	C 6.2	1,800	0.0 →
Network Filtering	F 3.8	26	0.0 →
Breach Events	A 10	5	0.0 →
System Reputation	A 10	0	0.0 →
Email Security	A 9.9	43	0.0 →
DNS Security	D 5.3	196	0.0 →
System Hosting	D 5.1	0	0.0 →

Oversikt Tredjeparter / Underleverandører



Eksempel på oversikt over tilstanden i verdikjeden og informasjon som er tilgjengelig ved valg av en leverandør

Onboarding Cyber Risk Score

Cyber Risk Score er tilgjengelig

Administrator administrerer tjenesten
3 måneder gratis prøveperiode starter

Administrator mottar velkomstmelding

Administrator følger anvisningene i mottatt epost og innrulleres i tjenesten.

RiskRecon oppretter portal

Kundens URL benyttes som basis for etablering av portal og utgangspunkt for skanning av virksomhetens eksponerte systemer.

RiskRecon sender innrulleringsepost til administrators epostadresse.

Kontakt KPMG på cyberriskscore@kpmg.no

Du mottar en informasjonspakke med veiledning, eksempel rapporter, priser, lenker etc.,
Fyll ut avropskontrakten, signer og send den tilbake som pdf.
Den som oppgis som administrator vil administrere tjenesten.

Avropskontrakt signert av KPMG returneres.

Informasjon om kundes URL og epost-adresse til administrator deles med RiskRecon.

Nye kunder må registreres i KPMGs systemer i samsvar med krav fastsatt av Finanstilsynet

dfø Skyforum – Kick-off

Hvorfor Cyber Risk Score?

Vet du at?
Virksomheter med god cybersikkerhetshygiene har **35 ganger lavere** frekvens av destruktive løsepengevirushendelser.

Hva får din virksomhet ut av tjenesten?

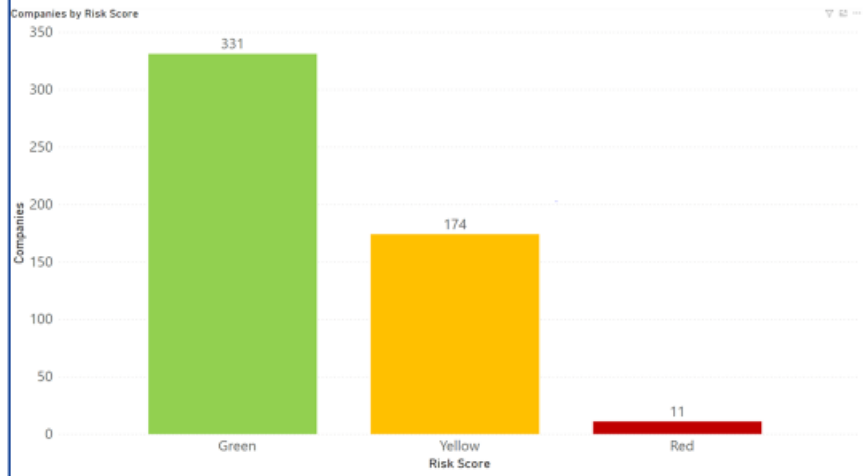
- **Oversikt over virksomhetens**
  - totale risikoeksponering på Internett
  - innsikt i verdikjederisiko
  - ressurser eksponert på Internett (volum/aktive og «glemte»)
- **Faktabasert grunnlag for virksomhets- og risikostyring**
- **Etterlevelse av regulatoriske krav**
- **Redusert risiko for Cyber hendelser**

Hva bidrar din virksomhet med?

- **Nasjonale og sektorvise sikkerhetsmyndigheter får oversikt over den totale risikoeksponering for alle offentlige etater**
  - Bedret risikoforståelse nasjonalt (NSM) og sektorvis (ulike CERT)
  - Grunnlag for nasjonale og sektorvise tiltak

Hvordan er din sikkerhetshygiene?

I hvilken gruppe ligger din virksomhet?



Vet du at?
Selskaper med cyberrisikovurdering på **'F' har 4 ganger større sannsynlighet** for å oppleve en datatapshendelse ifølge RiskRecon-analyser.

Kontaktinformasjon

E-post

cyberriskscore@kpmg.no

Hjemmesider

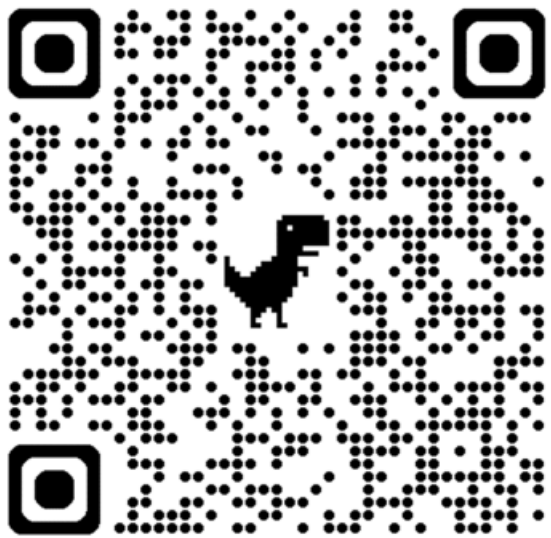
Nærmere informasjon om avtalen:

Cyber Risk Score - Informasjon om rammeavtalen

Hva er din Cyber Risk Score? - KPMG Norge

RiskRecon Manage Cyber Security Risks

Alle virksomheter som er omfattet av DFØs rammeavtale kan gjøre direkte avrop.



Spørsmål

Neste Skyforum

28. november 2024

Kontaktinformasjon

markedsplassen@dfo.no

Tema	Navn	E-post
CIPS	Ingrid Elisabeth Sørensen	ingridelisabeth.soerensen@dfo.no
FinOps	David Behrens	david.behrens@dfo.no
Cloud R&A	Helene Stunes	helene.stunes@dfo.no
CyberX	Kristina Nikolajeva	kristina.nikolajeva@dfo.no

#mps | Thank you!

markedsplassen.anskaffelser.no

Norwegian agency for public and financial management