Bruk av sky i offentlig sektor

Contents

Introduksjon

I en verden som stadig blir mer digitalisert er lagring og prosessering av data i offentlig sky et mer agilt, tidsbesparende, sikkert, miljøvennlig og kostnadseffektivt enn andre alternativer.

Det er et klart behov for offentlig sektor å digitalisere seg raskere. Utfordringer, bekymringer, tvetydighet og mangel på kunnskap rundt lovgivning og tekniske løsninger har ført til at digitalisering i offentlig sektor gått noe saktere enn andre sektorer. Samtidig ser vi at aktører som "knekker koden" på digitalisering kan ta ledende posisjoner, og Norge er et land som kan skryte av sterke fagmiljøer og innovative løsninger som plasserer oss som en av de ledende nasjonene innenfor digitalisering, digital innovasjon og digital transformasjon. Den desentraliserte organiseringen vi har i Norge legger til rette for innovasjon, men kan samtidig skape noen utfordringer for aktørene med mindre ressurser og kompetanse.

Bruk av offentlig sky krever en interdisiplinær tilnærming over både det juridiske og det tekniske domenet. Juridiske tiltak kan ikke løse alle tekniske utfordringer, og tekniske tiltak kan ikke løse alle juridiske utfordringer - men vår påstand er at man kan nå en tilstrekkelig grad av risikoreduksjon gjennom forståelse og avveininger på tvers av domenene.

Derfor ønsker vi å legge til rette for et åpent samarbeide i å utvikle malverk som skal fasilitere for bruk av skytjenester i offentlig sektor. Vi gjør dette i en "open-source ånd", og inviterer alle interesserte parter i å bidra. Microsoft og noen utvalgte partnere og domeneeksperter har tatt på seg å lede an i dette arbeidet, men vi er til slutt avhengig av en åpen og konstruktiv debatt og bidrag fra langt flere enn kjerneteamet for å kunne lage løsninger som vil bli allment akseptert.

I første omgang har vi definert skopet til dette prosjektet som kommunal sektor i Norge. Målgruppen for dette dokumentet er både beslutningstagere og operasjonelle IKT-ressurser som skal legge til rette for og gjennomføre prosjekter i sky.

Målet for dette prosjektet er å kunne gi en solid forståelse av hva skyteknologi er, og hvordan man benytter konkrete tjenester, produkter, og teknologier for å sikre en stabil og sikker drift av applikasjoner i skyen.

Helt konkret er målet å levere både referansearkitekturer og verktøy for raskt å kunne bygge såkalte "landingssoner" for ulike risiko og/eller klassifiseringsdomener for bruk av IaaS og PaaS tjenester.[1]

Det er viktig å påpeke at hver organisasjon må gjøre sin egen risikovurdering og er selv ansvarlig for juridiske betraktninger og ibruktakelse.

[1] Vi tar ikke med SaaS-tjenester i dette prosjektet, da ansvarsforholdet er annerledes og dermed er det behov for en noe annerledes diskusjon, samt at det allerede er ganske god forståelse av hva dette betyr og hvordan det må håndteres i markedet.

Dette prosjektet kan også ha verdi for andre aktører i både offentlig og privat næringsliv, og vi har som mål å kunne utvide skopet til andre aktører etter hvert som prosjektet modnes.

Oslo, 29 april 2022

Målbilde

Vi ønsker å tegne et målbilde for hva skyteknologi kan hjelpe kommunal sektor med.

Nedenfor finner du en liste over felles utfordringer vi hører for offentlig sektor - og noen betraktninger på hvordan sky kan hjelpe å kontre noen av disse utfordringene.

- Teknisk gjeld
- Mangel på ressurser (Personell)
- Mangel på kompetanse
- IT Support
- Utdaterte systemer (Og da usikre eller lite fleksbile systemer)
- Sikkerhet & Forensic
- Mangel på alternativer
- Tradisjonell sonemodell/IT infrastruktur vs moderne sky-miljø
- Mangel på standardisering (duplikater av fellestjenester, mangel på tjenestekataloger++)
- GDPR & Data Governance
- Kommunesammenslåing
- Kost
- Tilknytting til Helsenett

Hva er sky?

Hva er et datasenter

I informasjonsteknologiens spede barndom var det en gjengs oppfattning at verden kun ville trenge et begrenset antall datamaskiner. Vi kan kalle dette "stormaskinens tidsalder", og de fleste som benyttet en datamaskin jobbet gjennom en terminal som gav tilgang til data og regnekraft som befant seg i en sentral datamaskin. Disse stormaskinene befant seg typisk i datarommet til en organisasjon eller bedrift - en fysisk sikret lokasjon hvor kun autorisert personnel hadde tilgang.

Etterhvert som avhengigheten til datasystemer økte, ble det satt større og større krav til fysisk sikring og redundans for slike datarom, og det ble etterhvert både vanskelig, upraktisk og ulønnsomt å etterleve disse kravene for hver enkelt organisasjon og bedrift. Samtidig fikk vi ny og raskere nettverksteknologi som gjorde det mulig å flytte både stormaskiner, servere og data lengre unna brukerne. Dette la grunnlaget for en ny industri: datasenterindustrien.

Idag er datasenterindustrien en sentral komponent i vår digitale infrastruktur. Dedikerte datasenterleverandører leverer redundante tilkoblinger til nettverk- og elektrisitetsnett, nød-aggregater som holder datasenteret igang selv gjennom lange perioder med strømbrudd, og strenge tiltak for fysisk sikring for å hindre uautorisert tilgang.

I dag vil de aller fleste organisasjoner velge å benytte en profesjonell datasenterleverandør fremfor å bygge sitt eget datarom.

Fra datasenter til skytjenester

Hva er så sky, og hvordan skiller skyleverandører seg fra datasenterleverandører?

Idag bærer stort sett alle rundt på både mere regnekraft og lagringsplass en vi trenger. (Faktisk har en moderne smarttelefon mer regnekraft enn hele land hadde tilgang til for bare tiår siden. TODO: Kilde) På samme måte har de fleste datarom mer regnekraft og lagringsplass enn organisasjonen som eier det trenger. Vi overdimensjonerer systemene våre for å kunne ta unna for perioder med intens bruk - tenk 8-timers arbeidsdag for de fleste organisasjoner og bedrifter, black-friday og julehandel for varehandelen, og frist for innlevering av skattemeldingen for alle norske borgere. Dette fører til at vi har mange enkeltsiloer av overdimensjonerte systemer - dette er både dyrt og har store miljøimplikasjoner. Datasenterindustrien er i ferd med å bli en av verdens mest energikrevende bransjer. (TODO: Kilde)

Med skyteknologi så endres måten man kan kjøpe regnekraft og lagringsplass seg dramatisk. Organisasjoner kan nå kjøpe bare det de har behov for, når de har behov for det. En bedrift i varehandelen kan skalere opp før black-friday, og ned igjen etterpå. De kan til og med designe systemet sitt slik at det autoskalerer

med bruk. Finn.no har for eksempel XX% av besøkene sine innenfor lunsj-perioden på hverdagene (TODO: Kilde). Resten av tiden trenger de bare en brøkdel av regnekraften - som så kan frigis av skyleverandøren og selges til andre kunder, for eksempel forskningsorganisasjoner som kjører store jobber som ikke er tidskritiske - og derfor kan kjøpe kapasitet rimeligere, siden deres jobber kan aktivieres når det er mindre behov i markedet. Store skyleverandører vil også flytte om på workloads for kunder, slik at servere, racks, eller til og med hele datasentre kan skrus av for å spare energi i perioder med lav etterspørsel.

En annen forskjell på en datasenterleverandør og en skyleverandør er tjeneste-spekteret. Mens en datasenterleverandør er som en avansert utleier av fysisk plass, er en skyleverandør også en programvare- og driftsleverandør av hundrevis av avanserte tjenester som gjør det mulig å bygge digitale systemer raskere og bedre.

Hva er hybrid?

...

Fysisk og logisk sikring av datasentre

slik som perimetersikring kombinert med videoovervåking og døgkontinuerlig bemanning.

Ansvarsmodellen for offentlig sky

Azure i Norge

Sky og bærekraft

Hvordan gjennomføre et skyprosjekt?

...

Risikovurdering for bruk av sky

- Brudd på fiberkabler (Datasenter eller hel region)
- Strømbrudd (Datasenter)
- Tjeneste(r) går ned (oppgradering, patching)
- Leverandør går konkurs
- Ikke tilgjengelig kapasitet
- Myndigheter ber om innsyn
- Hacker(e) får tilgang (Storage, compute)
- Korrupt ansatt (internt)
- Korrupt ansatt (vendor/tredjepart)
- Korrupt ansatt (tjenesteleverandør (datasenter eller skyleverandør)
- Myndigheter klarer å få digital tilgang til datasentere
- Fysisk tilgang til utstyr
- FISA 702

Nyttige definisjoner og terminologi

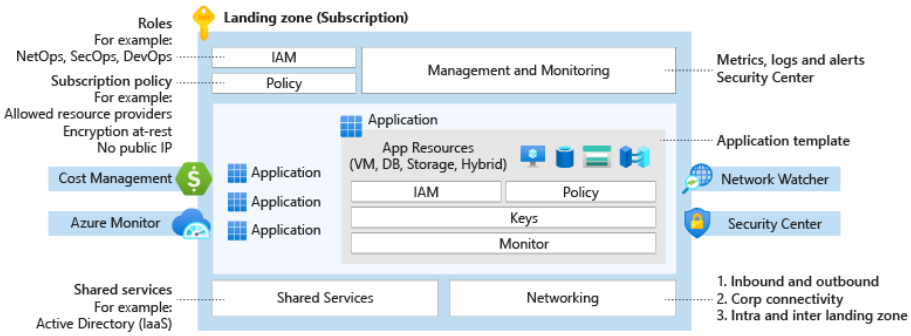
Landingssoner

Landingssoner i Azure består av flere abonnementer (subscriptions) i satt opp på en skalerbar måte og som samtidig ivaretar sikkerhet og tilhørende tjenester som nettverk og identitet.

Landingssoner muliggjør migrering, modernisering og innovasjon i stor-skala i Azure - samtidig som man kan rapportere på compliance (eller etablerte styringsregler man har satt for sin organisasjon).

Sonene som etableres tar høyde for alle plattformressurser som er nødvendig for å understøtte en bedrift's applikasjons-portefølje og differensierer ikke mellom infrastruktur som tjeneste og plattform som en tjeneste.

Generelt kan vi se på en landingssone slik:



En målarkitektur for offentlig sektor må ta høyde for både on-prem (/edge) og public cloud og styringgsett må understøtte dette holoistisk.

Tilgjengelighet (SLA)

- Høy tilgjengelighet (E.g - Konsumenttjeneste) 99.99 eller 99.95% oppetid. Noe nedetid (minutter) per år aksetabelt. Redundante server(e) og lagringskopier - men ikke på tvers av datasentere.
- Meget høy tilgjengelighet (e.g. pasientsystem) 99.99% eller høyere. Redundante servere og kopier av data på tvers av datasentere (med mer enn 10 km avstand).
- Unntakssituasjon (Disaster scenario) En hel region går ned og blir utilgjengelig.
- Fullstendig suverenitet/autonomitet (autonomity/soveriginity) Skyleverandør går konkurs, Norge mister all kommunikasjon med omverden, systemer som må fungere uavhengig av skyleverandør.

Referansearkitektur

Rent overordnet kan man se på en helhetlig arkitektur hvor vi bør skille på hva som lovmessig må ligge i egne datasentere/edge (lovmessig reguleringer og krav eller sammfunnskritisk) og hvordan vi klassifiserer ulike applikasjoner som kan plasseres i sky, edge eller on-premises.

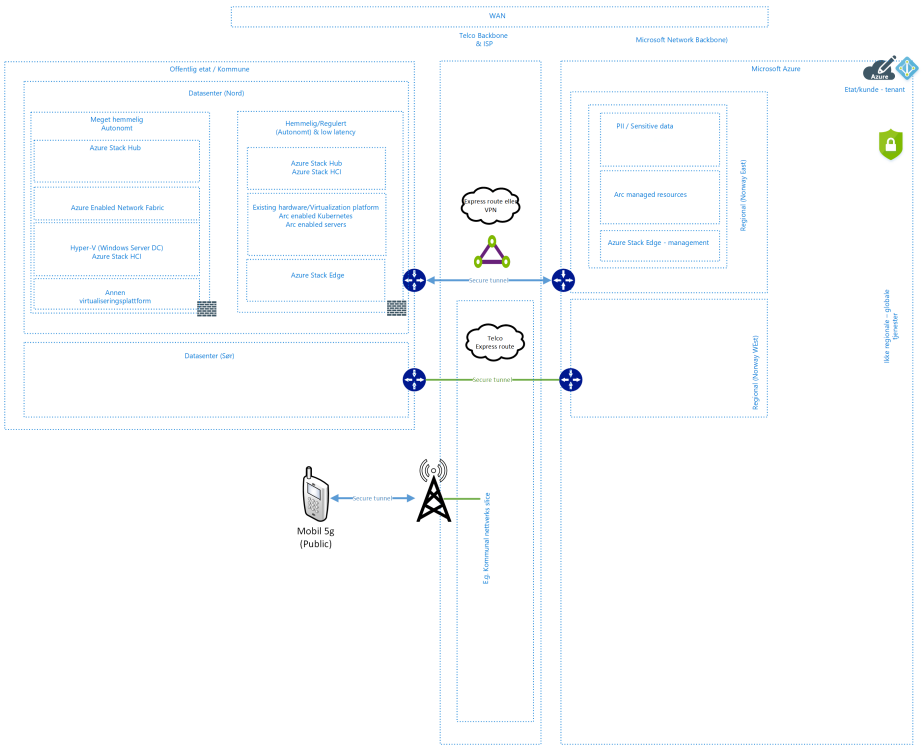


Figure 1: High-level

// TODO: Bør vi ha en forenklet modell for 'most common' scenarios? Iom. at det er få offentlige som er underlagt sikkerhetsloven?

`Eks. MVP 1 kommune med e.g.: Sykehus /sykehjem + x antall avdelinger/publikumstjenester, int`

// END TODO

Klassifiseringmatrise for applikasjoner

Her er et forsøk på hvordan vi kan tenke rundt klassifisering/skille av applikasjoner:

- Publikumstjeneste/Applikasjon (Internett eksponert)
- Intern applikasjon (interne ansatte)

- Ikke PII/sensitivt
- PII/Sensitivt
- Begrenset (Sikkerhetsloven)
- Konfidensielt (Sikkerhetsloven)
- Ikke sammfunnskritisk (tåler noe nedetid)

// TODO ikke i scope for v1.0 - Hemmelig (Sikkerhetsloven) - Strengt hemmelig (Sikkerhetsloven) - Særskilte lover / krav *(Eks. EKOM) - Sammfunnskritisk - delte tjenester (nasjonale) // End todo

Sammfunnskritiske tjenester som må kjøre og være tilgjengelig som er delt på tvers av lokasjoner/uavhengig av lokasjon.

Sluttbrukere eller systemer - bruker internet (VPN eller MPLS) eller telefoni for å nå tjenester.

- Sammfunnskritiske - lokale tjenster (edge & hybrid) Sammfunnskritiske tjenester må fungere i nødssituasjon hvor deler faller ut og tåler lite/eller ingen nedetid eller er svært sensitive til latens.

Sluttbrukere/systemer befinner seg lokalt (e.g. et sykehus/sykebil) mm.

// TODO - Klarer vi å lage en visualisering/ decision tree? # Matrise

On-premises

Dette er servere (virtualisert eller bare-metal) du har i dine egne datasentere hvor du kan drifte deler av applikasjonsporteføljen.

Nettverk

Du kan sikkert knytte ditt kontor til Azure ved hjelp av f.eks Site-to-Site VPN eller Azure Express Route.

Dersom det er behov for svært mange klienter tilknyttet et virtuelt nettverk og/eller det er mange kontorer som skal tilknyttes - så bør man vurdere å kombinere dette med Azure Virtual WAN.

Sikring av nettverk

I Azure finnes det mange aspekter av nettverkssikkerhet. På mange måter kan man designe en nettverkstopolgi som ligner et tradisjonelt datasenter med segmentering mm.

Man kan sikre trafikkflyt og nettverk i Azure med blant annet NSGs (Network security groups), Application Security groups, Brannmurer (Azure Firewall - eller tredjeparter slik som Barracuda, BigIp/F5 mm.).

I tillegg bør du basere sikkerhetsmodellen din på en “Zero Trust” modell (Se Zero trust in Azure her).

Tekniske komponenter for sikring og compliance

- Azure Datasenter sikring
- Customer Lockbox
- Confidential computing
- Azure Policy
- Customer managed Keys (Kryptering og Bring-Your-Own-Key)
- Azure Dedicated HSM
- Azure ARC
- Azure Dedicated Hosts

Utvalgte sikkerhetselementer

- Security baseline
- Security baseline (Azure Stack Edge)
- Security baseline (Azure Stack HCI)
- Azure Active Directory : Conditional access
- Azure Active Directory : Privileged identity management (PIM)
- Microsoft Defender for Cloud
- Azure DDOS Protection

Krisesituasjoner

I en særskilt krisesituasjon bør vi stille oss følgende spørsmål:

- Hvor lang tid tar det før ditt eget utstyr begynner å feile (on-premises utstyr)?
- Hvilke 'skjulte' avhengigheter har dine systemer? (eks. DNS/CA mm)
- Hvordan skal sluttbrukere nå applikasjoner som er eksponert på internett?

Særskilte norske lover, krav og anbefalinger(som man bør ta stilling til)

- Arkivloven: *"Arkivloven inneholder ingen bestemmelser som direkte regulerer lagring av arkiv i skytjenester, og er i utgangspunktet ikke til hinder for bruk av slike løsninger. Det følger likevel av arkivloven § 9 b at arkivmateriale ikke kan «førast ut or landet, dersom dette ikkje representerer ein naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta." Når det er lagt til grunn at den fysiske lagringsplassen avgjør hvor data er å finne, følger det naturlig av denne bestemmelsen at overføring av arkivmateriale til servere i utlandet bryter med forbudet mot å føre arkiv ut av landet."*

Bokføringsloven

// TODO - Noen skrive noe smart rundt bokføringsloven ### Sikkerhetsloven // TODO - Noen skrive noe smart rundt sikkerhetsloven ### NKOM // TODO

- Noen skrive noe smart rundt NKOM ### NSM - Råd og anbefalinger for IKT sikkerhet

NSM har en rekke råd og anbefalinger for IKT sikkerhet. Grunnprinsipper for IKT-sikkerhet 2.0 er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet og er inspirert av mange av disse.

Tekniske tiltak fra grunnprinsippper for IKT-sikkerhet kan knyttes mot Azure Policies for en automatisert overvåkning og rapportering av compliance på tvers av hele virksomhetens digitale eiendom. Azure har over 700 eksisterende innebygde policies for IaaS, PaaS og hybrid i tillegg til muligheten for å lage egne tilpassede policies. En samling av Azure policies som er gruppert etter et felles formål kalles en Policy Initative. Tilsvarende samlinger av Azure policies finnes og vedlikeholdes av Microsoft for anerkjente internasjonale regelverk som: ISO 27001:2013 og CIS 1.3.0.

Under vises et skjermbilde fra Azure Policy sin compliance oversikt hvor utvalgte NSM prinsipper er knyttet inn. Merk at dette kan gi en oversikt på tvers av tjenester og infrastruktur, med Azure Arc kan man også evaluere policy tilstand mot hybrid og multisky.

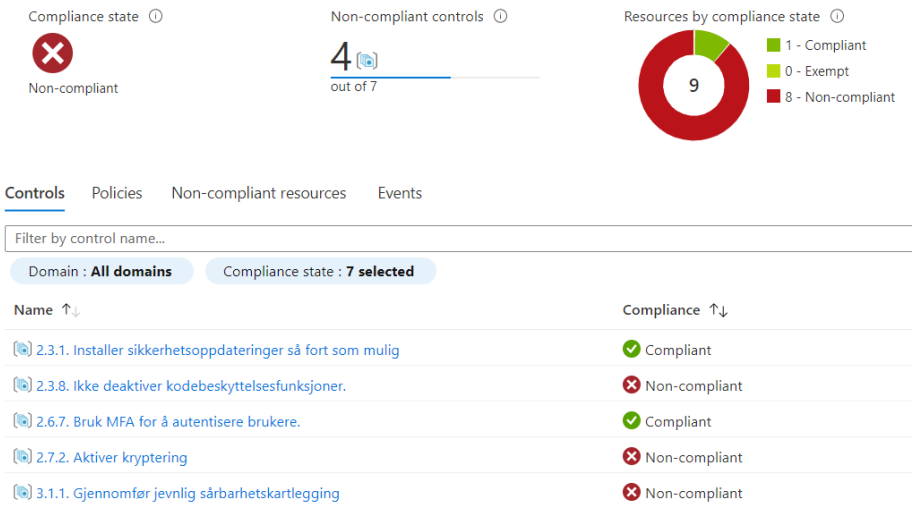


Figure 2: Policy initative

Compliance i Azure Policy viser tilstanden for de spesifikke policy definisjonene man har knyttet opp og det vil sjeldent være et en-til-en forhold mellom en kontroll i et rammeverk og en policy. Et rammeverk eller en standard vil også inneholde prosess og organisatoriske tiltak som ikke kan knyttes opp mot en teknisk policy. Derfor vil compliance mot feks NSM grunnprinsipper, ISO 27001:2013 eller CIS 1.3.0 i Azure

Policy kun gi en delvis oversikt over det totale bildet.

Under vises et eksempel på sikkerhetstiltak fra ulike kategorier i NSM grunnprinsipper som er knyttet mot relevante Azure Policies. Et sikkerhetstiltak kan ha flere Azure Policies for en bredere dekning og eksempelet viser muligheten for kombinasjon på tvers av IaaS, PaaS i Azure og hybrid/multisky. ### Eksempel: NSM grunnprinsipper for IKT-sikkerhet 2.0 policy initiative

Sikkerhetstiltak	Grunnprinsipp	Kategori	Azure Policy referanse	Kommentar
2.3.1 Installer sikkerhetsoppdateringer så fort som mulig.	2.3 Ivareta en sikker konfigurasjon	2. Beskytte og opprettholde	System updates should be installed on your machines	IaaS i Azure
2.3.8 Ikke deaktiver kodebeskyttelsesfunksjoner.	2.3 Ivareta en sikker konfigurasjon	2. Beskytte og opprettholde	Windows Defender Exploit Guard should be enabled on your machines	IaaS i Azure eller hybrid- og multisky med Azure Arc
2.5.1 Styr dataflyt mellom nettverks-soner.	2.5 Kontroller dataflyt	2. Beskytte og opprettholde	Subnets should be associated with a Network Security Group	Azure nettverk

Sikkerhetstiltak	Grunnprinsipp	Kategori	Azure Policy referanse	Kommentar
2.6.7 Bruk MFA for å autentisere brukere.	2.6 Ha kontroll på identiteter og tilganger	2. Beskytte og opprettholde	MFA should be enabled on accounts with write permissions on your subscription	Azure AD
2.7.2 Aktiver kryptering i de tjenestene som tilbyr slik funksjonalitet.	2.7 Beskytt data i ro og i transitt	2. Beskytte og opprettholde	Storage accounts should have infrastructure encryption	PaaS i Azure
2.7.2 Aktiver kryptering i de tjenestene som tilbyr slik funksjonalitet.	2.7 Beskytt data i ro og i transitt	2. Beskytte og opprettholde	Transparent Data Encryption on SQL databases should be enabled	PaaS i Azure

Sikkerhetstiltak	Grunnprinsipp	Kategori	Azure Policy referanse	Kommentar
3.1.1 Gjennomfør jevnlig sårbarhetskartlegging.	3.1 Oppdag og fjern kjente sårbarheter og trusler	3. Oppdage	A vulnerability assessment solution should be enabled on your virtual machines	IaaS i Azure eller hybrid- og multisky med Azure Arc
3.1.1 Gjennomfør jevnlig sårbarhetskartlegging.	3.1 Oppdag og fjern kjente sårbarheter og trusler	3. Oppdage	Vulnerability assessment should be enabled on SQL Managed Instance	PaaS i Azure
3.1.3 Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare).	3.1 Oppdag og fjern kjente sårbarheter og trusler	3. Oppdage	Endpoint protection should be installed on your machines	IaaS i Azure eller hybrid- og multisky med Azure Arc

CSA Cloud Controls Matrix (CCM)

Cloud Security alliance og (https://cloudsecurityalliance.org/research/cloud-controls-matrix/)[CCM mapping]er vanlig brukt for benchmarking mot ulike sertifiseringer og i kravspesifikasjoner rettet mot skyleverandør.

Microsoft har en omfattende mapping på hvordan dere skyløsning mappes mot

CCM kontrollere.

Se full rapport her mot ulike kontroller fra f.eks CIS/NIST/PCI/ISO mm: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Vedlegg

Azure i Norge

- 2 datasentere i Norge
- Datalagring i Azure
- Availability Zones in Norway
- Mission Critical workloads in Norway

Rapporter, audit, innsyn

Klareringssenter inneholder hundrevis av rapporter, innsyn og tredjepart audits for Microsoft sine tjenester i sky. Her kan du finne alt fra linker rundt overholdelse av regler og standarder, personvern, datainnsyn mm.

Alternativt kan du også gå inn her for å finne rapporter direkte: https://servicetrust.microsoft.com/ ## Schrems-II - EU Data Boundry - EU Data Boundry - FAQ

GDPR

Som kunde opprettholder du eierskap til kundedata – innhold, personlige kundedata og andre data du leverer til lagring og drifting i Azure-tjenestene. Du har også kontroll over eventuelle andre geografiske områder der du bestemmer deg for å rulle ut løsningene eller replikere dataene dine.

Der en tjenestes funksjonalitet krever global datareplikering, er detaljene tilgjengelige her.

Linker

- Protecting privacy in Microsoft Azure
- Microsoft EU Data Boundary
- Trusted Cloud
- Datalagring i Azure
- Microsoft Azure SOC Rapporter
- Online Services Terms for Microsoft Azure

Verktøy

- Azure Advisor
- Microsoft Defender for Cloud
- Azure Policy
- Azure Optimization Engine