

NOKIOS 2019:



#påtide-påtvers: Transformasjon for bærekraft

Trondheim
29. - 31. okt.



accenture

ARKIVVERKET

basefarm

bouvet

Brønnøysundregistrene

Capgemini

computas

EVRY

Forskningsrådet

Kantega



sopra steria

telenor

tieto

Difi

NTNU

Kurs 5:

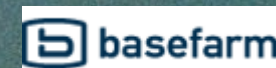
Skyanskaffelser og informasjonssikkerhet

Hvordan oppnå sikre tjenester i skyen fra dag 1 og hele veien videre?

1. Eirik Thormodsrud
Sopra Steria



2. Arvid Grøtting
Basefarm



Introduksjon



Eirik Thormodsrud er leder for Cyber Security Advisory i Sopra Steria. Eirik har lang fartstid med sikkerhets- og samsvarsrevisjoner, sikkerhetsarkitektur og sikkerhetstesting. Skytjenester er en av de områdene som Eirik har jobbet mest med de siste årene.



Arvid Grøtting er sikkerhetssjef (CISO) i Basefarm. Han er utdannet informatiker fra Universitetet i Oslo og har jobbet teknisk med blant annet programmering, drift og nettverk før en glidende overgang til sikkerhetsledelse.

Praktisk

Vi ønsker:

- Åpen diskusjon
- Spørsmål og kommentarer underveis
- Deling av erfaringer
- Tidsstyring (vi holder i det)
- Mobiler på lydløs

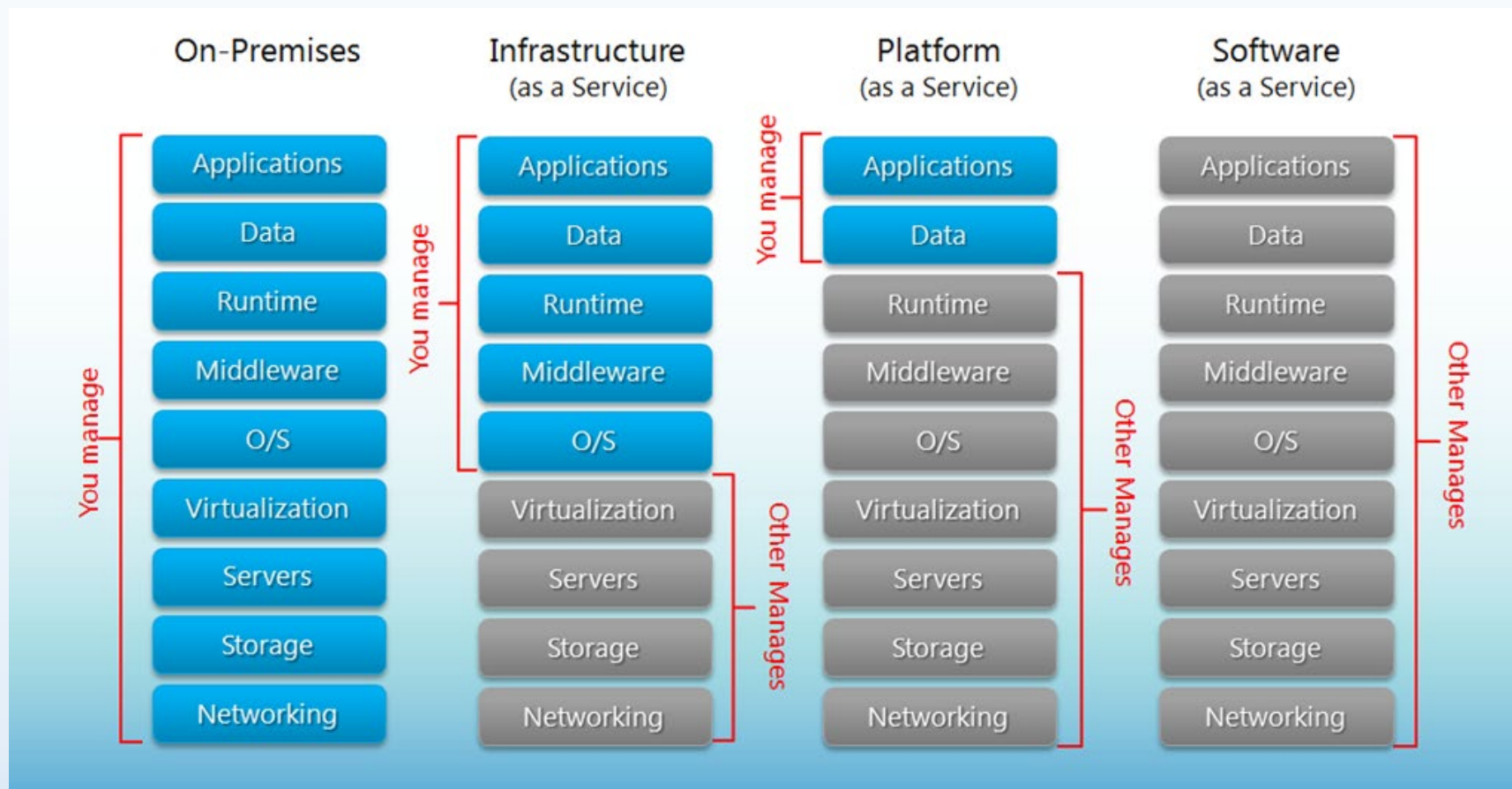
Case (for oppgaver)

Etaten har 1000 ansatte og jobber med å levere transporttjenester i alle store norske byer. Det er en spennende tid med introduksjon av bysykler, elsparkesykler, egen bilpark med delingsbiler samt lokale trikker og bussruter. Etaten er underlagt Departementet og har ansvar for å følge opp de overordnede føringene gjennom tildelingsbrevet. Etaten har gjennom mange år bygget opp en portefølje med applikasjoner som understøtter et sett med forretningsprosesser som er avgjørende for å kunne levere trygg og effektiv transport i norske byer. Disse applikasjonene driftes på egen teknisk infrastruktur i datarom i Porsgrunn og Ålesund. Egen IT-avdeling har alltid hatt ansvaret for å holde infrastruktur og applikasjoner tilgjengelig for både egne ansatte og publikum som bruker etatens tjenester via nett. Egne kunderegistre er etter hvert opprettet for abonnements tjenester og betaling. Her ligger blant annet kundenenes navn, adresse og betalingshistorikk.

IT-sjefen har tenkt på skytjenester en liten stund og har bestemt seg for at de bør vurdere å bruke skyen både til kapasitetstjenester og standardiserte applikasjoner for bl.a. kundepleie og kontorstøtte. Det kan skape rom for å fokusere ytterligere på tjenesteinnovasjon og kundetilfredshet. Han har samlet sammen noen kolleger for å diskutere hvordan de går i gang og hva de bør tenke på for å lykkes på kort og lang sikt. Rundt bordet sitter sikkerhetssjefen, driftssjefen, innkjøpssjefen, etatsjuristen og den nye lederen for tjenesteutvikling.

Praten går livlig.....

Skymodeller og ansvar



Skymodeller

SaaS

NETFLIX

 Office 365

PaaS

 **amazon**
web services

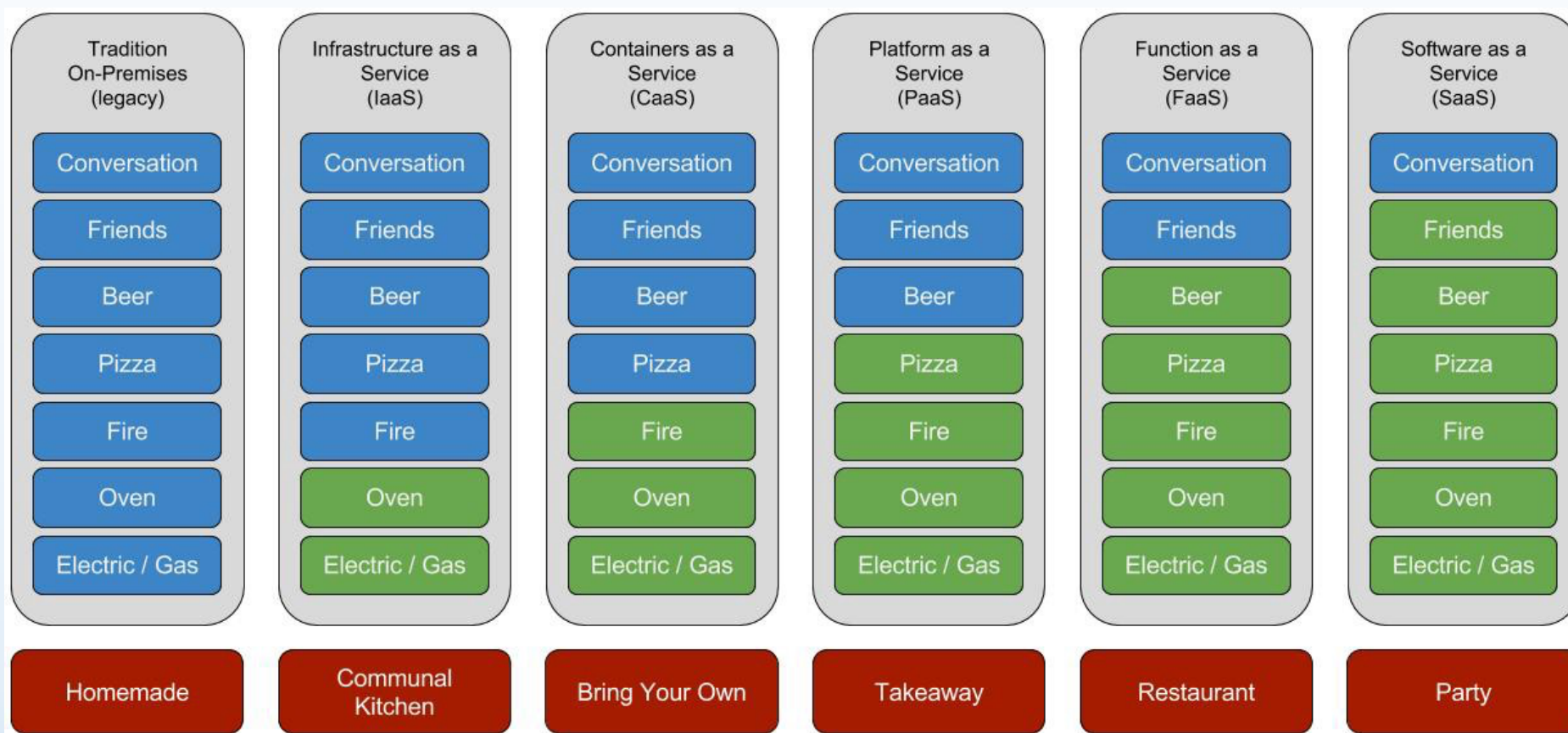
 Microsoft
Azure

IaaS

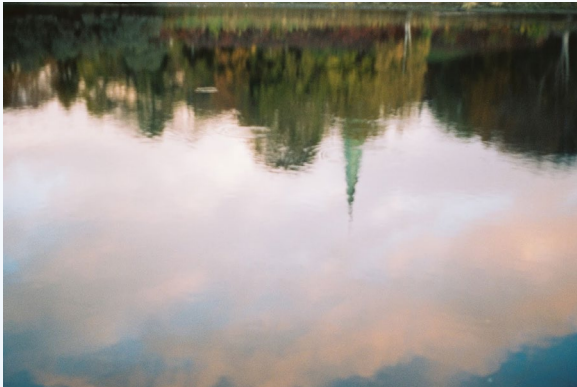
 **amazon**
web services™ **EC2**

 Microsoft
Azure

Skymodeller – analogi



Eierskapsmodeller



- **Privat:** Eid eller betalt av kun en organisasjon, og benyttes utelukkende for denne organisasjonen
- **Fellesskap:** Delt av flere organisasjoner som typisk har fellestrekk eller –interesser. Typisk organisasjoner med felles kravsett, eksempelvis helse eller andre deler av offentlig sektor.
- **Offentlig:** Eid av en organisasjon som selger tjenester til offentligheten eller til spesifikke grupper av organisasjoner
- **Hybrid:** Kombinasjon av flere skytyper, typisk offentlig og privat

Involverte parter

- **Cloud Service Provider:** Selskapet som byr på skytjenesten
- **Cloud Customer:** Selskapet som kjøper skytjenesten
- **Cloud Reseller:** Selskap som selger CSP sin skytjeneste, vanligvis med egne tjenester på toppen
- **Managed Service Provider:** Selskap som tar seg av administrasjon og drift av applikasjoner og tjenester på vegne av et annet selskap
- **Cloud Access Security Broker:** Selskap som leverer uavhengig Identity and Access Management (IAM) til skyløsninger
- **Regulators:** Statlige aktører

Krav i skyleveranser

Leveransemodell setter mulighetsrom for kravstilling

- Direktekjøp fra skyleverandør = velge standardiserte tjenester
 - Fordel -> mye å velge i
 - Ulempe -> liten mulighet til å tilpasse enkeltkomponenter
 - Må bygge selv
- Kjøp via managed leverandør
 - Fordel -> leverandør tilpasser basert på standardtjenester
 - Kravstille løsning
 - Ulempe -> kan muligens ikke velge underliggende tjenester

Unødvendig spesifikke krav driver pris! Hva er godt nok?

Hvor tør du lagre i skyen?



Må du ha en sky i Norge? I EU/EØS? I et EU-godkjent tredjeland?
Hva er sikkerhetstruslene, hva er risikoen, og hvilke lovkrav gjelder?

Oppgave 1: Krav og behov

Hvilke sikkerhetskrav må Etaten stille til en skyleveranse?

- Risiko: Hva kan gå galt?
- Behovsmessige krav?
- Lover / regulatoriske krav?

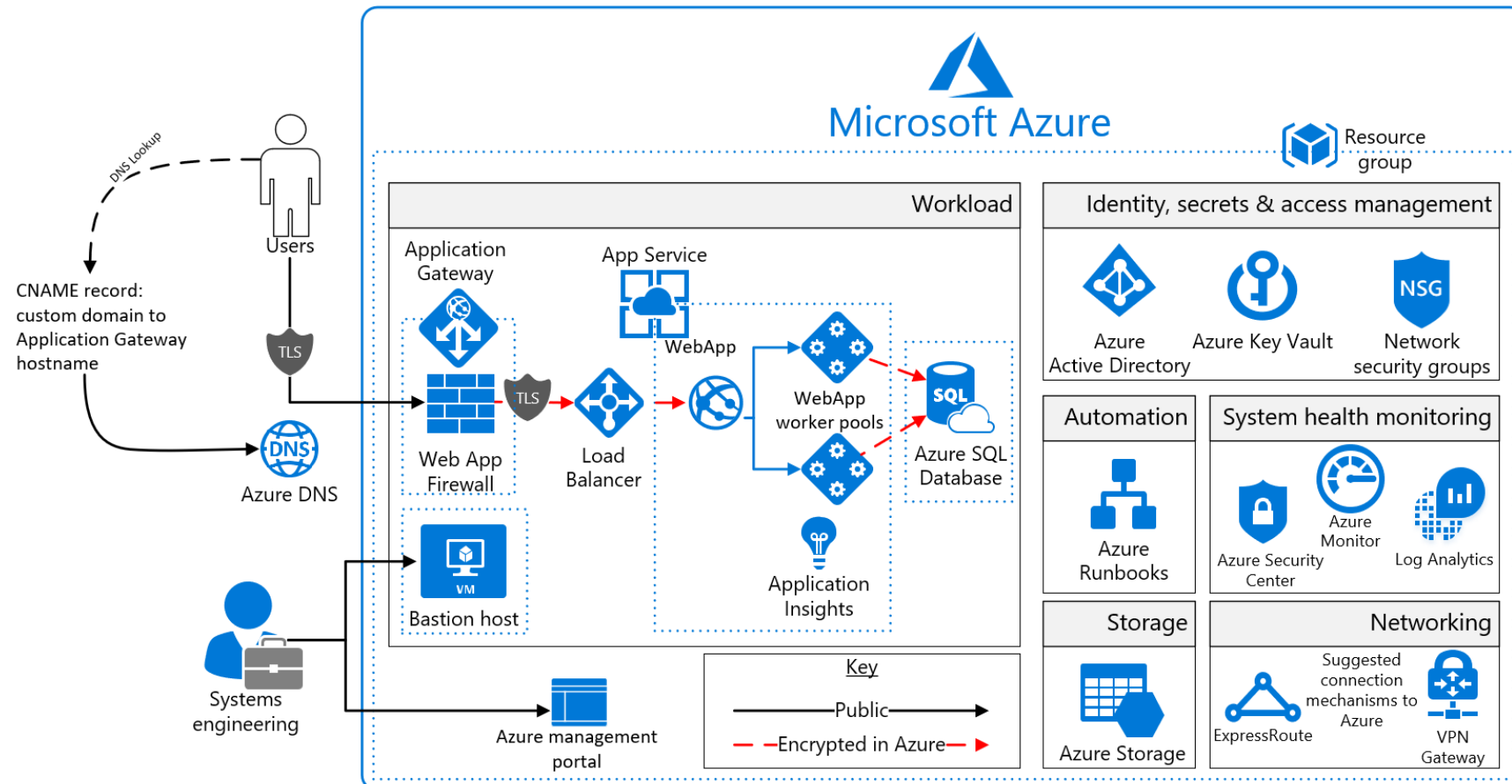
Hvilke behov har virksomheten for sikkerhet?

Hvordan kan kravene stilles?

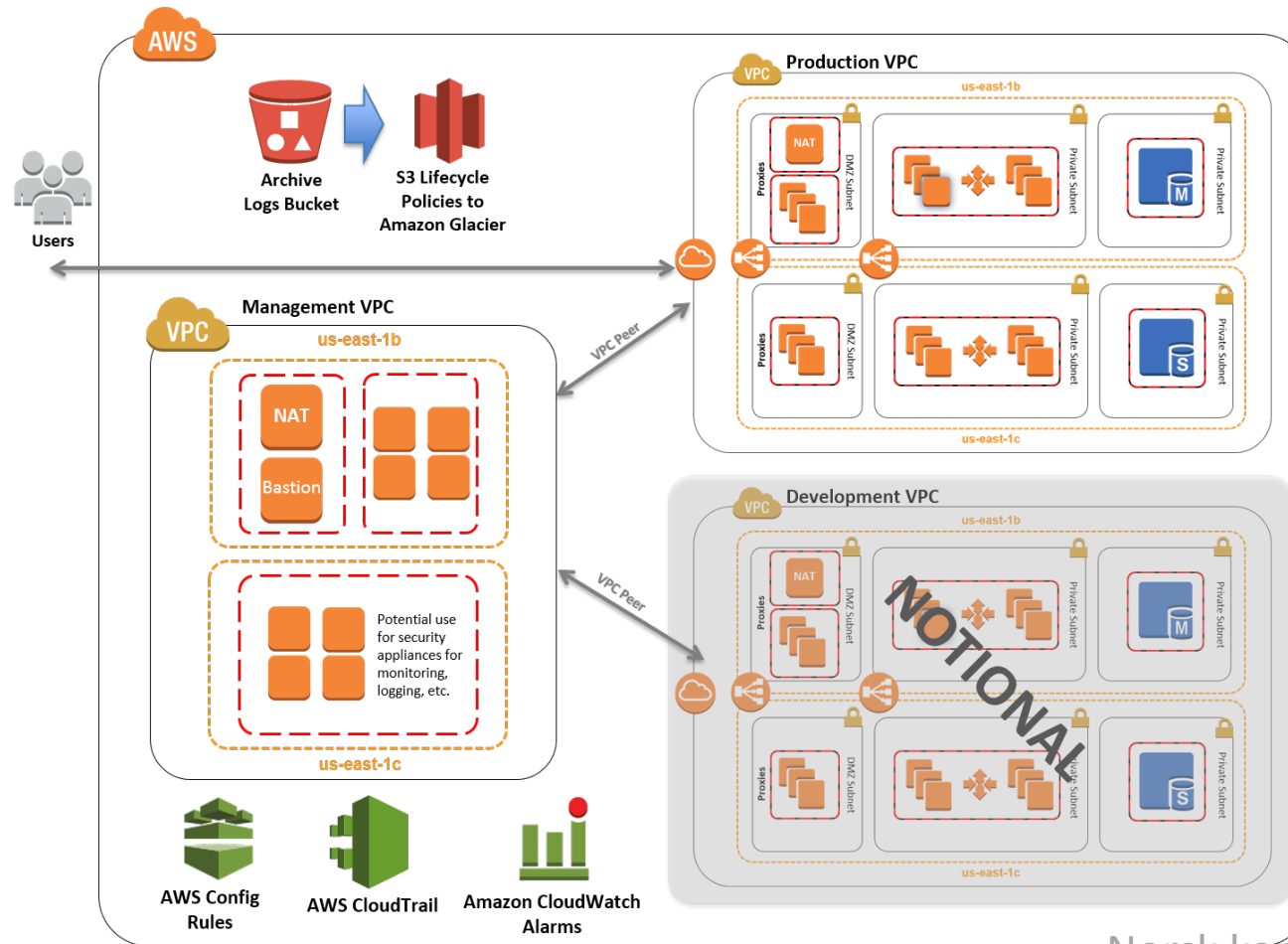
Nyttige verktøy

- Litteratur:
 - Cloud Security Alliance: <https://cloudsecurityalliance.org/>
 - <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
 - NIST Cloud Computing Reference Architecture 500-292
 - NIST Definition of Cloud Computing 800-145
- Verktøy:
 - Leverandørenes løsninger:
 - Microsoft Azure: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/>
 - Amazon AWS: <https://aws.amazon.com/architecture>
 - Google Cloud: <https://gcp.solutions/>
 - Netflix (Amazon AWS)
 - Security monkey: <https://netflix.github.io/>
 - Spotify (Google Cloud)
 - Google Cloud Security Toolbox: <https://labs.spotify.com/>

Referansearkitektur Azure



Referansearkitektur AWS



Kurs 5:

Skyanskaffelser og informasjonssikkerhet

PAUSE

1. Eirik Thormodsrud
Sopra Steria



2. Arvid Grøtting
Basefarm



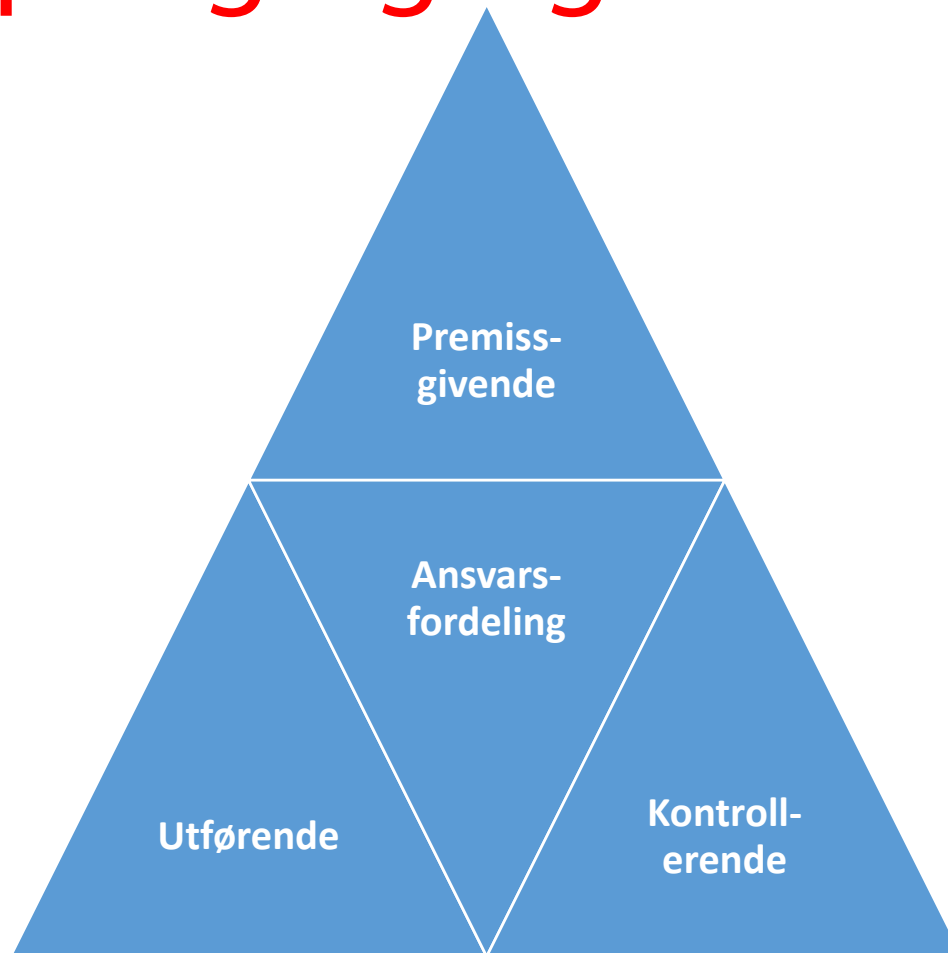
Oppgave 2: Kompetanse

Hva trenger dere av kompetanse selv?

Hva må dere beholde selv?

Hvilke faktorer spiller inn for behov for kompetanse?

Oppfølging og vedlikehold



Oppfølging

Status – hvor ble det av driftsmøtet?

- Ved direktekjøp må man selv følge med
- Ved kjøp gjennom leverandør kan man kreve mer av leverandør
- Nødvendig med vurdering av kost vs nytte vs kompetanse

Livssyklus

- Skyleverandørene ønsker standardiserte tjenester
 - Ønske om færrest supporterte versjoner
 - Fokus på ny funksjonalitet
- Utfordringen er å designe løsningen modulært
 - Bør/må kunne oppgradere og endre komponenter på kort tid
- Fordel er at man tvinges til å holde seg oppdatert.
 - Legacy vil ofte koste mer i sky
- Politiske og eksterne føringer kan komme fort og ha påvirkning
 - Enkelte land/leverandører kan bli uønsket
 - Lovverk o.l. kan påvirke hva man kan ha hvor

Etterlevelse (compliance)

- Skyleverandørene ønsker å være relevant for alle
 - Designer da tjenester mot de fleste sikkerhetskrav
 - Tilgjengeliggjør revisjonsrapporter og bevis
- Krever kompetanse til å tolke rapporter og underlag
- Leverandører kan avlaste tolkning
- Risikoen og ansvaret eies uansett av organisasjonen!

Avsluttende diskusjon

“There is no cloud. It's just someone else's computer.”

Chris Watterston



Norsk konferanse for IKT i offentlig sektor