

# Naviger trygt på rejsen til Public Cloud

Mikkel Ramlov, Conscia Cloud  
Conscia 14. september, 2021





## Få indsigt i....

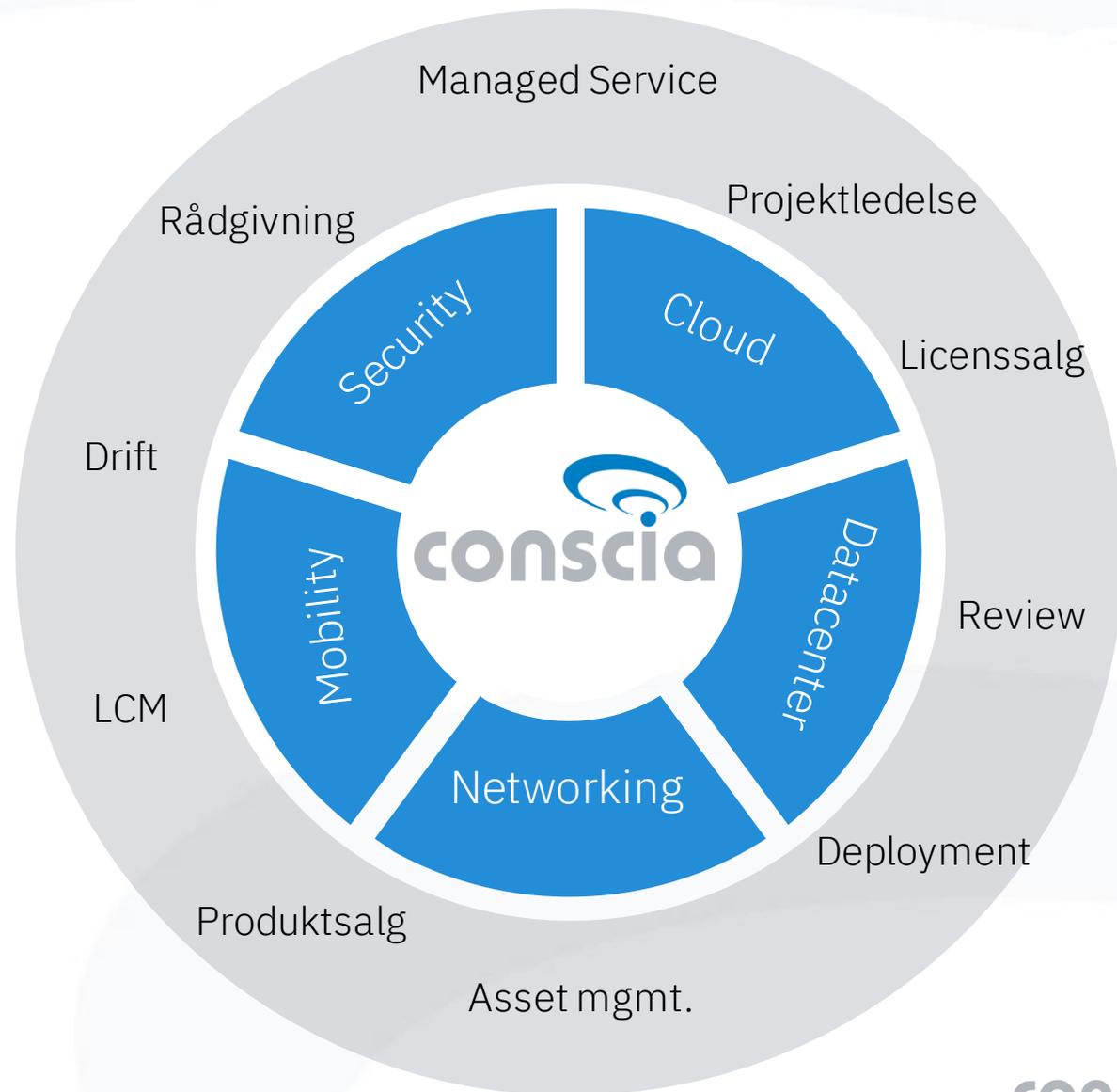
---

- ✓ Ansvarsfordelingen på Public Cloud
- ✓ Effektiv beskyttelse af din Cloud
- ✓ Kom sikkert i skyen

# Hvem er jeg....



**Mikkel Ramlov**  
AWS Lead Architect





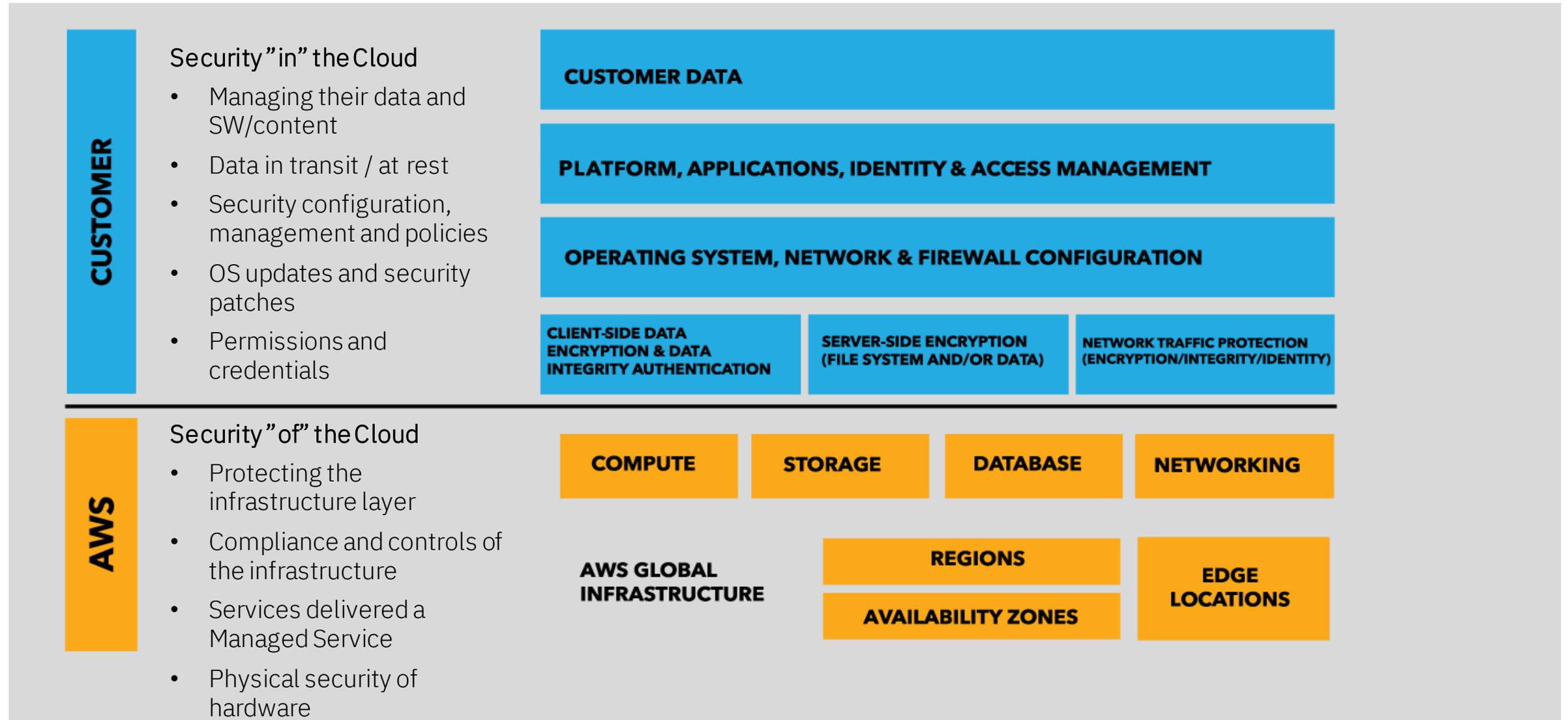
## Få indsigt i....

---

- ✓ Ansvarsfordelingen på Public Cloud
- ✓ Effektiv beskyttelse af din Cloud
- ✓ Kom sikkert i skyen

# Shared responsibility model

Kundens ansvar er bestemt af de valgte Public Cloud service





## Få indsigt i....

---

- ✓ Ansvarsfordelingen på Public Cloud
- ✓ Effektiv beskyttelse af din Cloud
- ✓ Kom sikkert i skyen

# Effektiv beskyttelse med AWS

## De 3 hovedkategorier

### Protect

Definer adgangspolitikker og handlingspolitikker på konto, bruger og asset niveau.



### Detect

Få indsigt i virksomhedens sikkerheds/compliance-tilstand gennem event/planlagt overvågningscyklus.



### Respond

Automatiseret event drevne respons og mitigerering. Fokus på event klassificering og *root cause* analyse



# Effektiv beskyttelse af data

Public Cloud (AWS) udbydere har et bredt udvalg af Sikkerhedsservices

## Protect

- Network
  - AWS Network Firewall
  - AWS Shield (Advanced)
  - AWS WAF
  - AWS FW Manager
  - AWS Certification Manager
- AWS Services
  - AWS IAM / SSO
  - AWS Organizations
- Data
  - AWS KMS
  - AWS CloudHSM
  - AWS EC2 Nitro Virtualization
  - Resource based policies

## Detect

- AWS Services
  - AWS CloudTrail
  - AWS Security Hub
  - AWS Config
  - AWS CloudWatch
  - AWS Trusted Advisor
  - AWS GuardDuty
- Data at rest
  - AWS Macie
- Data in transit
  - AWS GuardDuty
- Application
  - AWS Inspector
  - AWS IOT Device Defender

## Respond

- Incident log
  - AWS CloudWatch
  - AWS Detective
- Handling
  - AWS System Manager
    - Incident Manager
  - CloudEndure Disaster Recovery

# Segmenterings strategi

Klar adskillelse mellem ansvar og miljøer – Environment as a Service

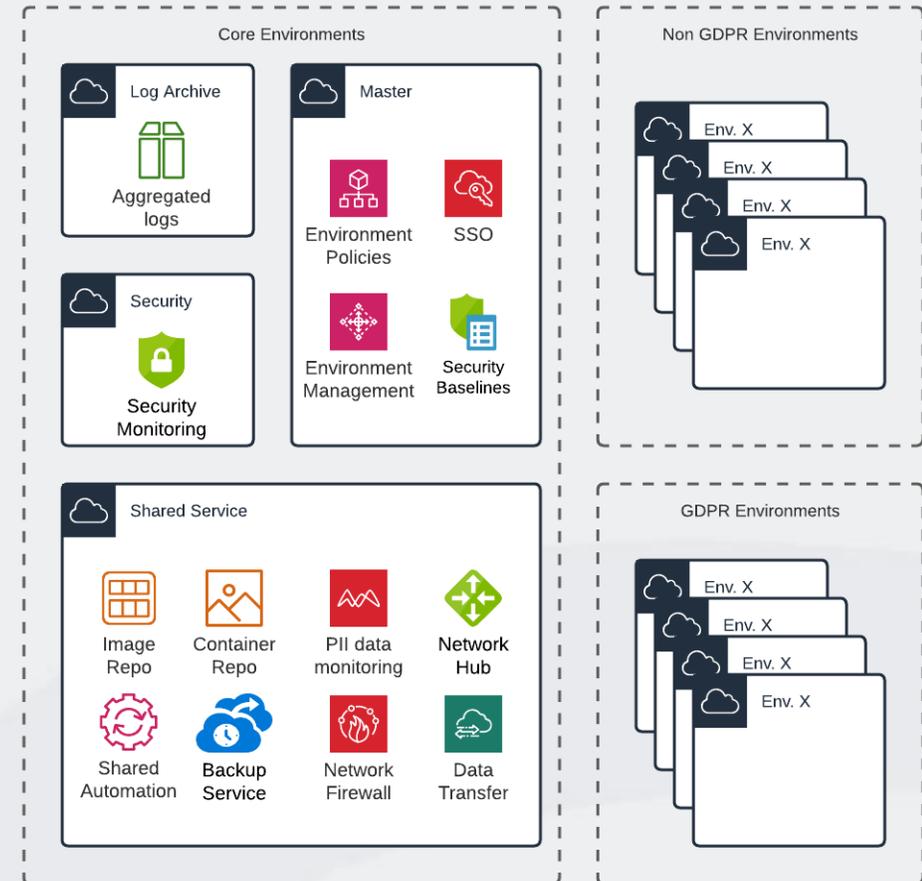
Article 25 of the GDPR states that the controller “shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed”.

Article 30 of the GDPR states that “...each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility”.

Article 32 of the GDPR states that “...the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: [...]

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; [...]

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.”





## Få indsigt i....

---

- ✓ Ansvarsfordelingen på Public Cloud
- ✓ Effektiv beskyttelse af din Cloud
- ✓ Kom sikkert i skyen

# Fra strategi til praksis

Assess

Prepare

Deploy

Optimize

- Kortlæg IT portefølje
- Udarbejd en TCO/BC
- Fastlæg workload strategi
- Indsaml data om eksisterende workloads (dependency mapping, OS's, cpu, RAM osv.)
- Klassificér data

# Fra strategi til praksis

Assess

Prepare

Deploy

Optimize

- Skab klar ansvarsfordeling på bl.a. disse områder
  - Ejerskab
  - Budget og cost optimering
  - Sikkerhed og compliance
  - Drift og udvikling
  - ...
- Opstil compliance krav til nye Cloud workloads
- Definer målbare KPI'er for Cloud protection

# Fra strategi til praksis

Assess

Prepare

Deploy

Optimize

- Etabler en centralt styret AWS platform som kan skalere med veldefinerede regler og overvågning på plads.
- Anvend best practices indenfor automation.
- Re-design workload så den udnytter Cloud native services, (nitro, S3, lamda, elastic storage m.fl.)
- Automatiser Cloud deployment, workload installation og konfiguration.
- Klassificer data og data containers

# Fra strategi til praksis



- Optimeringstiltag
  - Kør PII data discovery tool.
  - Dataklassificér ubestemt data
  - Anvend IAM adgangsanalyse værktøjer for indskærpet adgang på kritisk data.
  - Test/Vedligehold dataoprydnings procedurer

# Spørgsmål?

Kontakt Conscia Danmark, hvis du gerne vil drøfte  
hvorledes du får succes med Public Cloud

