

# AWS Accounts and OUs Best Practices

# Balancing the needs of builders and central cloud IT

**Builders:**  
Stay agile



Innovate with the speed and  
agility of AWS

**Cloud IT:**  
Establish governance



Govern at scale with  
central controls

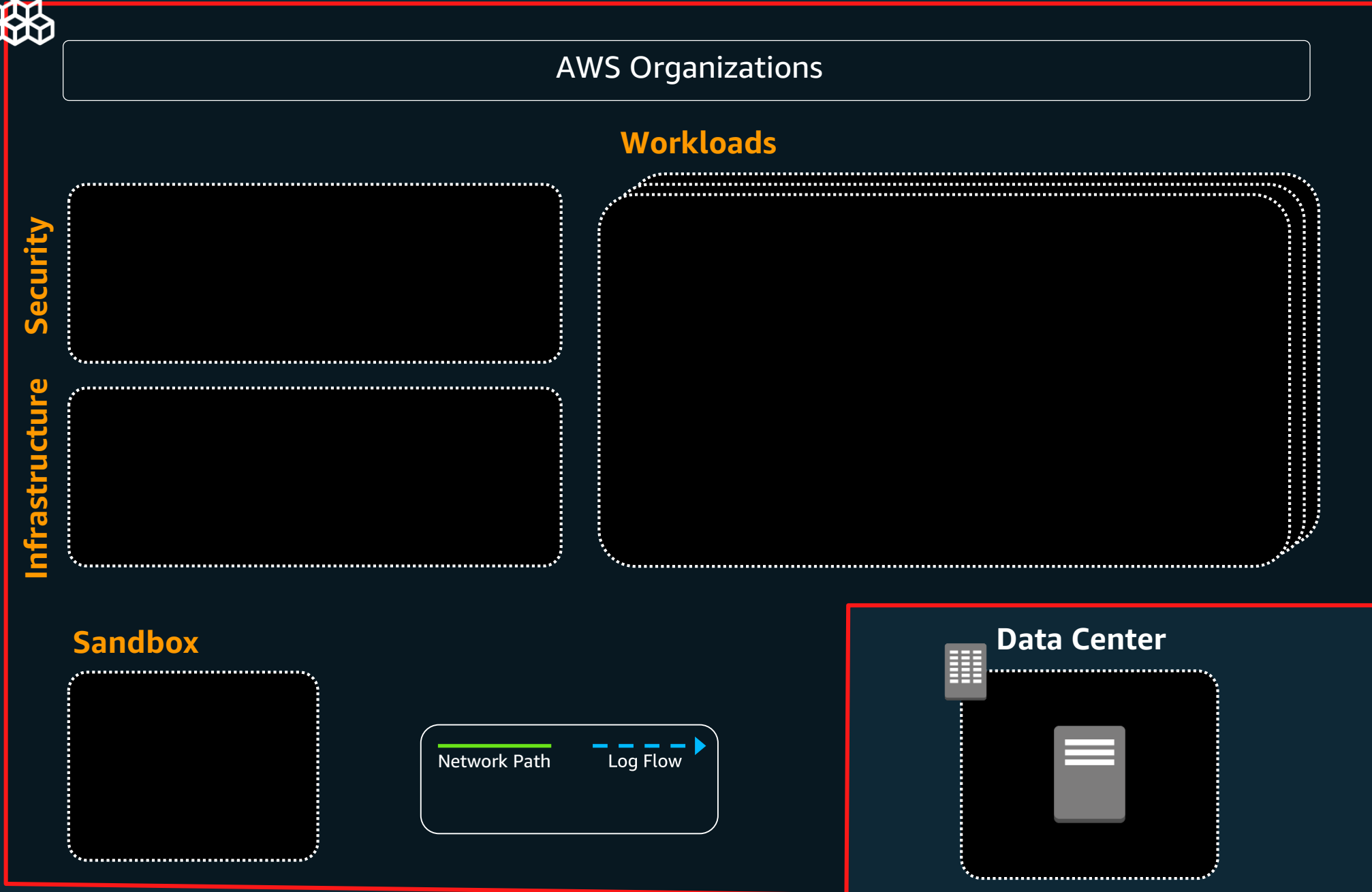
# Account Strategies: 4 common view points

- Financial
  - Determining how resource utilization and consumption is measured, reported and recharged
- Business
  - Considering Service provider model, Merger & Acquisition possibilities, financial responsibility and autonomy
- Governance
  - Determining what services are permitted, how are they secured, controlled and audited
- Operational
  - Considering Operating model, operational integration, networking and cloud provider limits

# Ideas and guidance // Multi-account Strategy

- Service control policies strategies and recommendations
- Identify Federation best practices and details
- Steps to migrate into a multi-account environment
- Networking recommendations (Transit gateway, Shared Amazon VPC, Private Link, peering, etc.)
- Security specific tooling and where to run/how e.g. Firewalls, IDS/IPS
- Alerting and alarming recommendations
- Forensics landing zone
- QA/Staging landing zone
- Backup/disaster recovery recommendations at account level
- Cost implications of many accounts vs. few
- CI/CD in a multi-account environment

# Multi-account approach



**Orgs:** Account management

**Log Archive:** Security logs

**Security:** Security tools, AWS Config rules

**Shared services:** Directory, limit monitoring

**Network:** AWS Direct Connect, TGW

**Dev Sandbox:** Experiments, Learning

**Dev:** Development

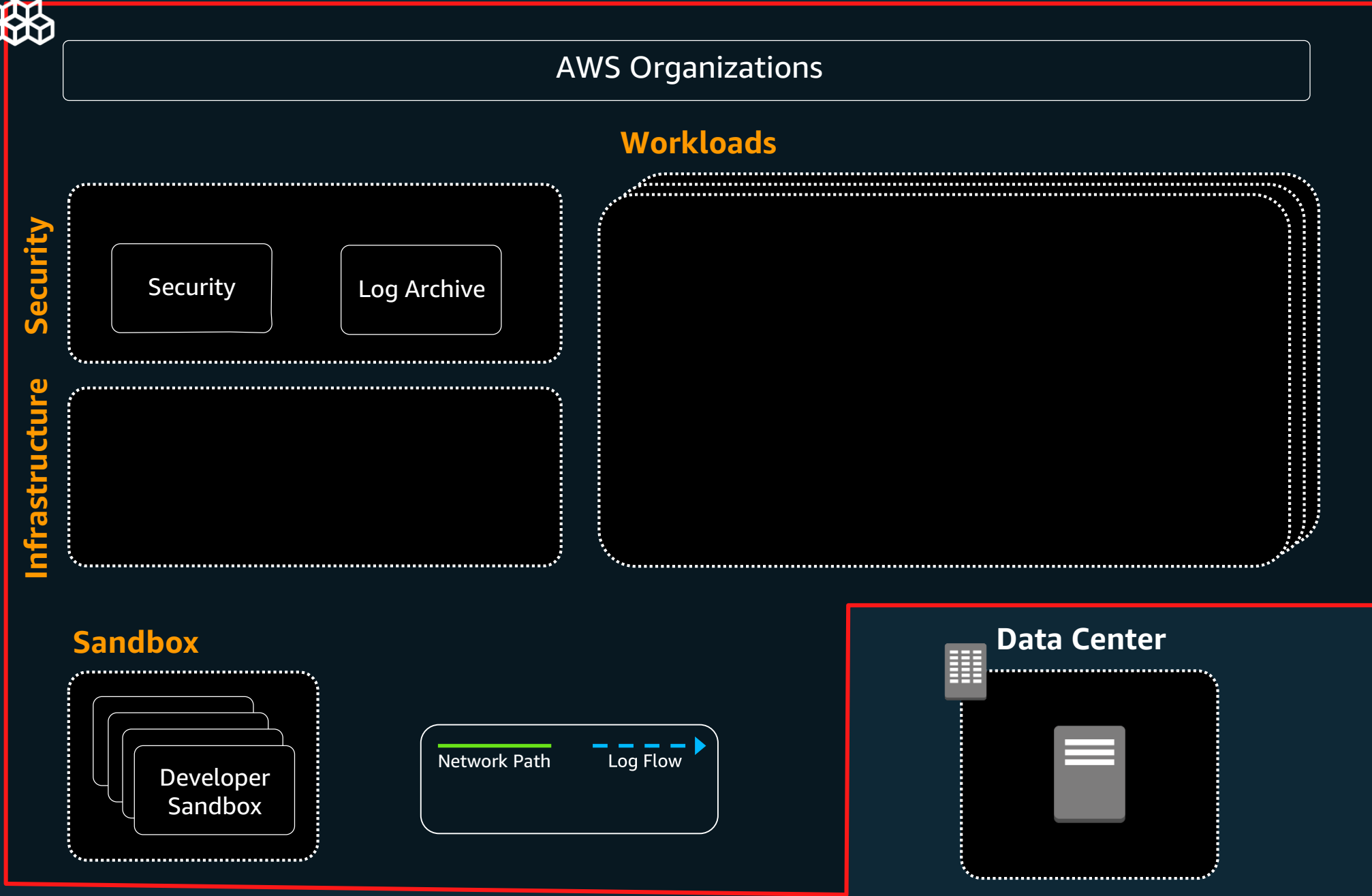
**Pre-Prod:** Staging

**Prod:** Production

**Team SS:** Team Shared Services, Data Lake



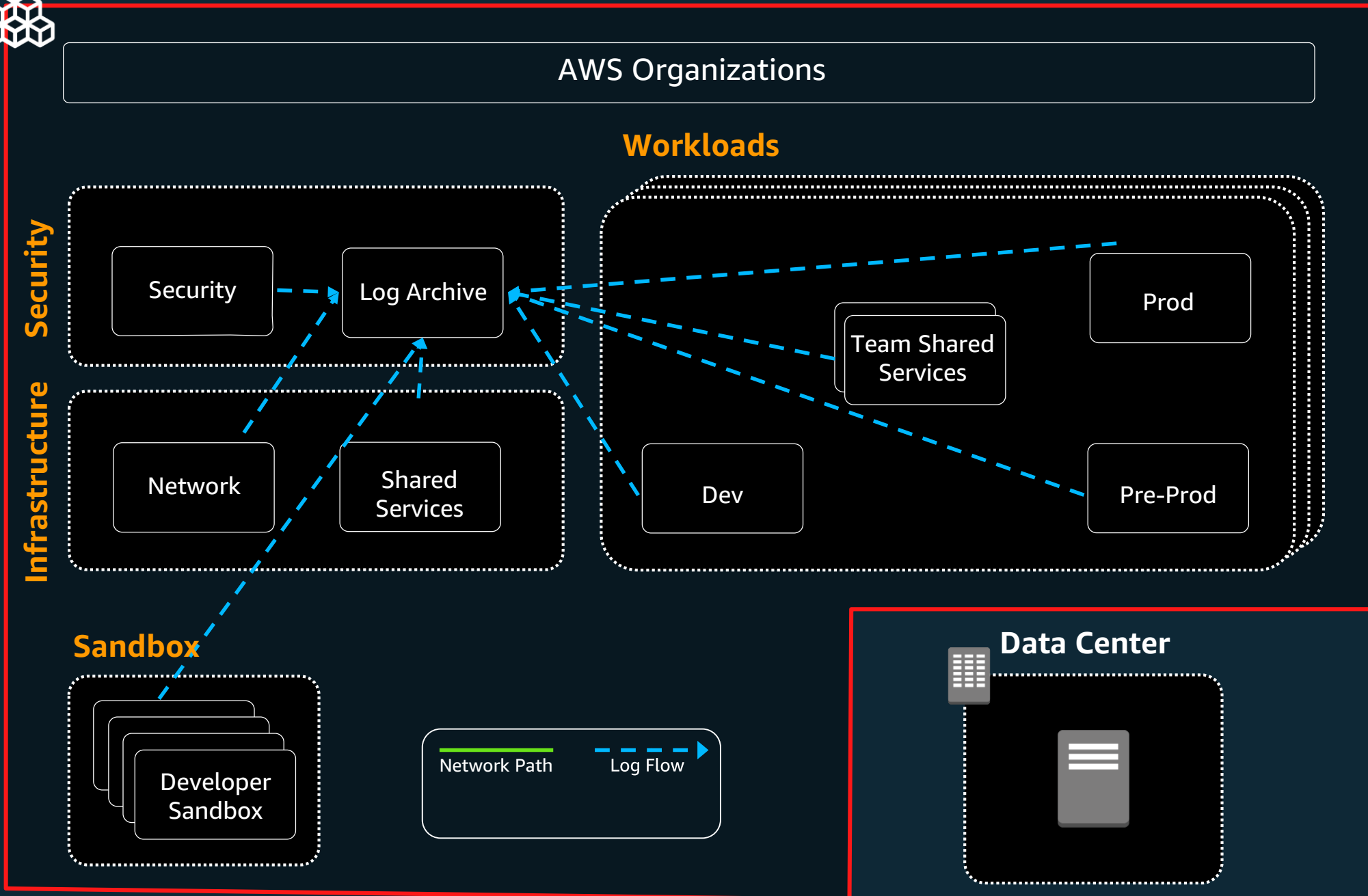
# Multi-account approach



- Orgs:** Account management
- Log Archive:** Security logs
- Security:** Security tools, AWS Config rules
- Shared services:** Directory, limit monitoring
- Network:** AWS Direct Connect, TGW
- Dev Sandbox:** Experiments, Learning
- Dev:** Development
- Pre-Prod:** Staging
- Prod:** Production
- Team SS:** Team Shared Services, Data Lake



# Multi-account approach // security log flow



**Orgs:** Account management

**Log Archive:** Security logs

**Security:** Security tools, AWS Config rules

**Shared services:** Directory, limit monitoring

**Network:** AWS Direct Connect, TGW

**Dev Sandbox:** Experiments, Learning

**Dev:** Development

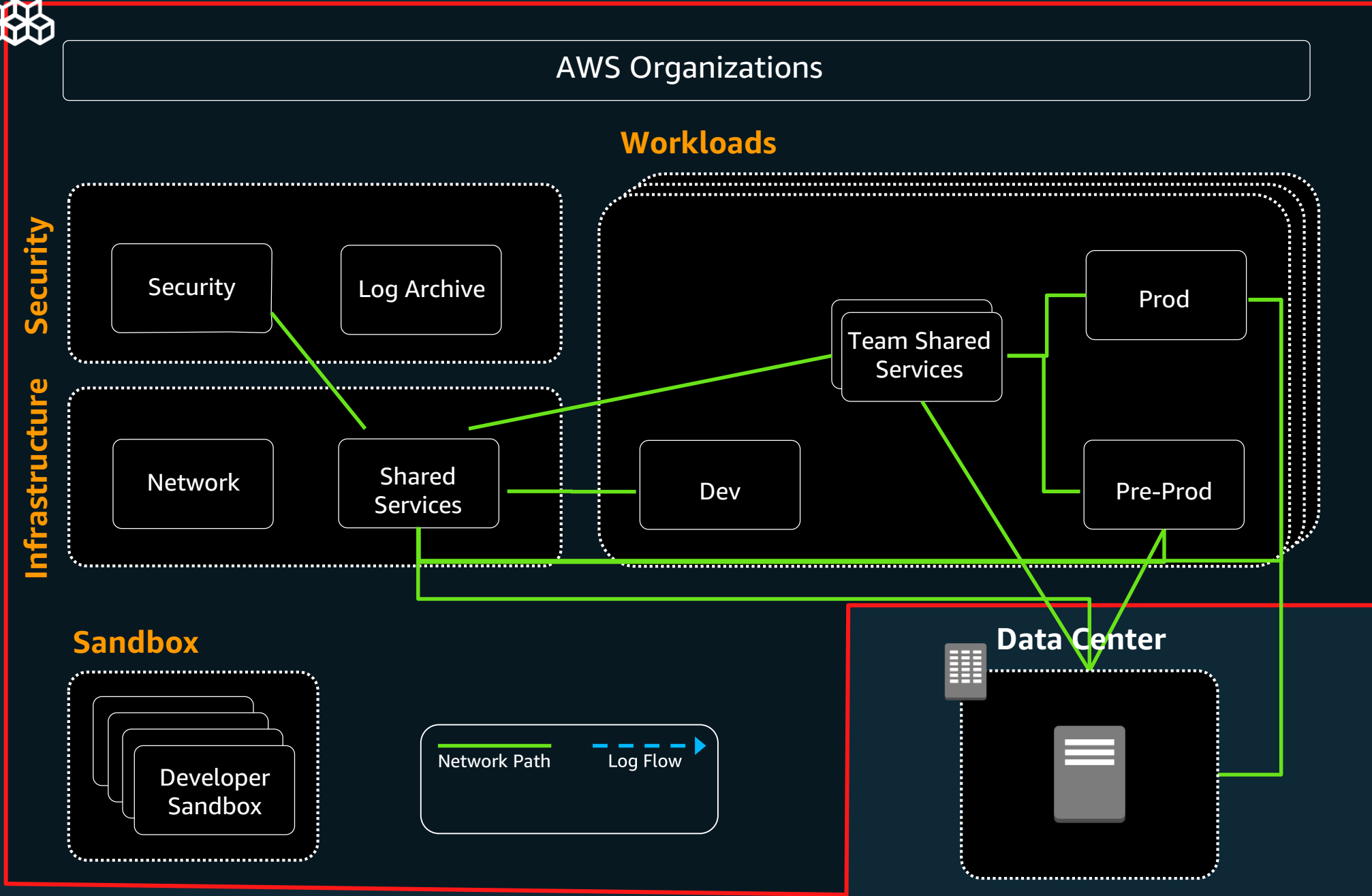
**Pre-Prod:** Staging

**Prod:** Production

**Team SS:** Team Shared Services, Data Lake



# Multi-account approach // network connectivity



- Orgs:** Account management
- Log Archive:** Security logs
- Security:** Security tools, AWS Config rules
- Shared services:** Directory, limit monitoring
- Network:** AWS Direct Connect, TGW
- Dev Sandbox:** Experiments, Learning
- Dev:** Development
- Pre-Prod:** Staging
- Prod:** Production
- Team SS:** Team Shared Services, Data Lake





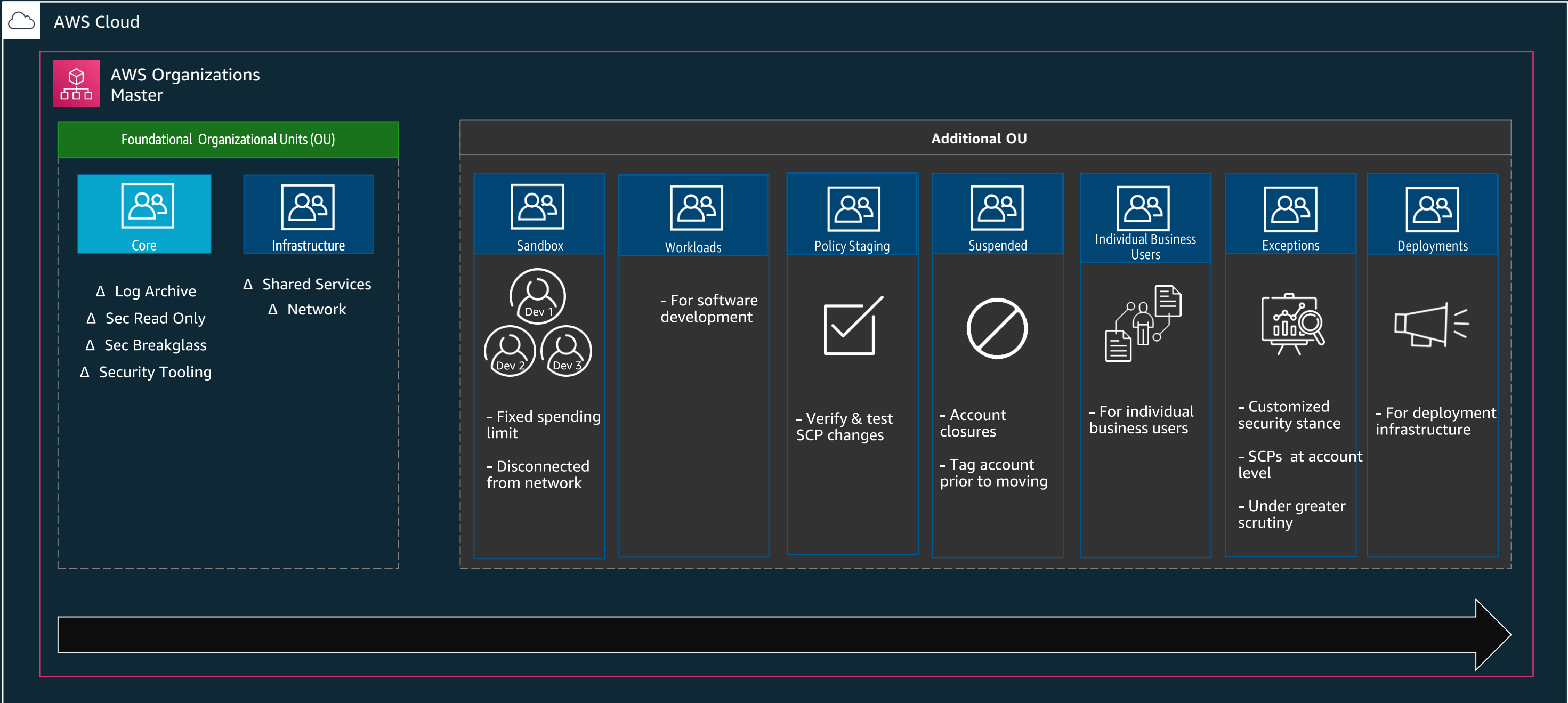
# Organizational Units

# Organizational Units

- Grouping of AWS Accounts
- Service Control Policies (SCP) to the groups / accounts
- Tagging policies to the groups / accounts
- Use permission grouping (NOT corporate structure)

How likely is the group to need a set of similar policies?

# High Level OU structure



# AWS Organizations Master



AWS Cloud



AWS Organizations  
Master



SCP



OU

No connection to DC

Organizational Units

Service control policies

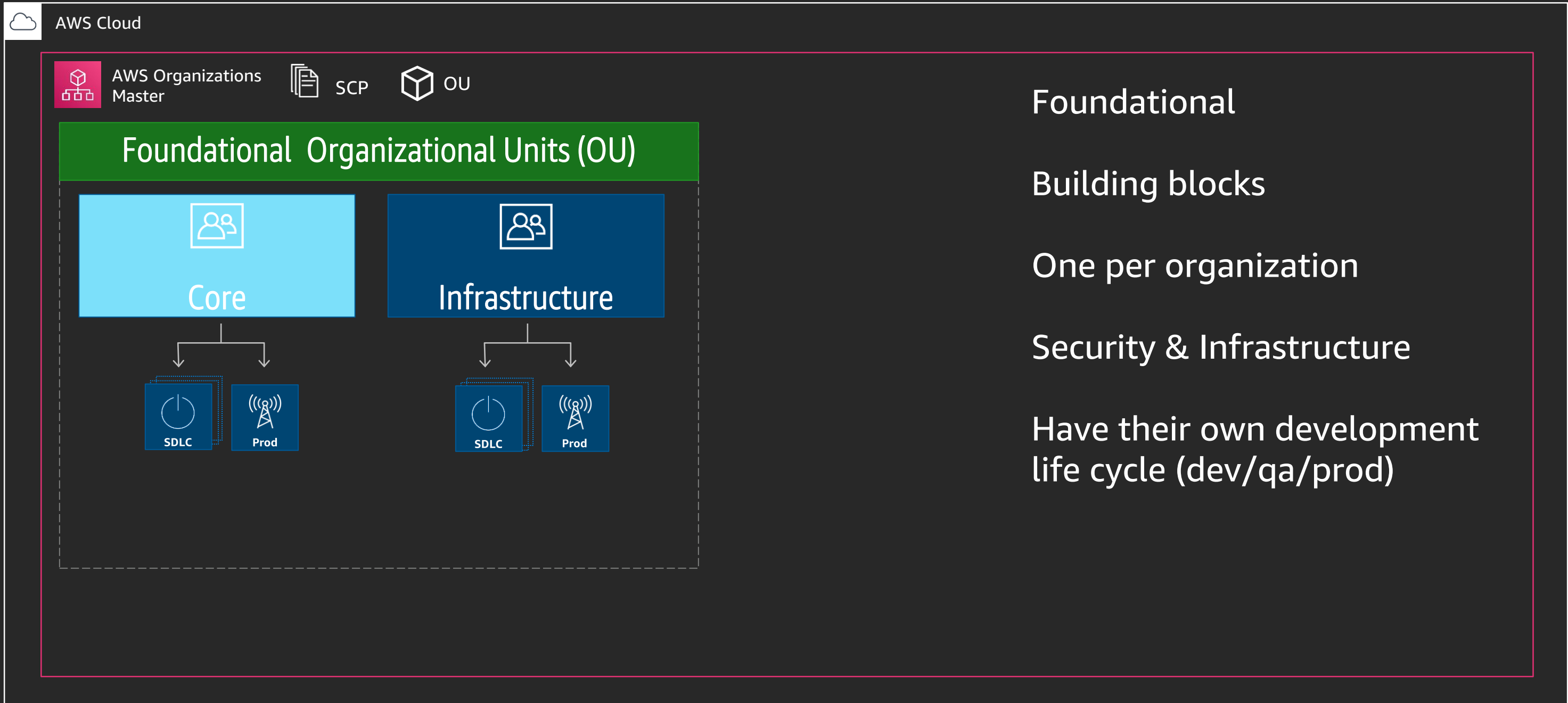
Consolidated billing

Minimal resources

Limited access

Restrict Orgs role!

# Foundational OUs



Foundational

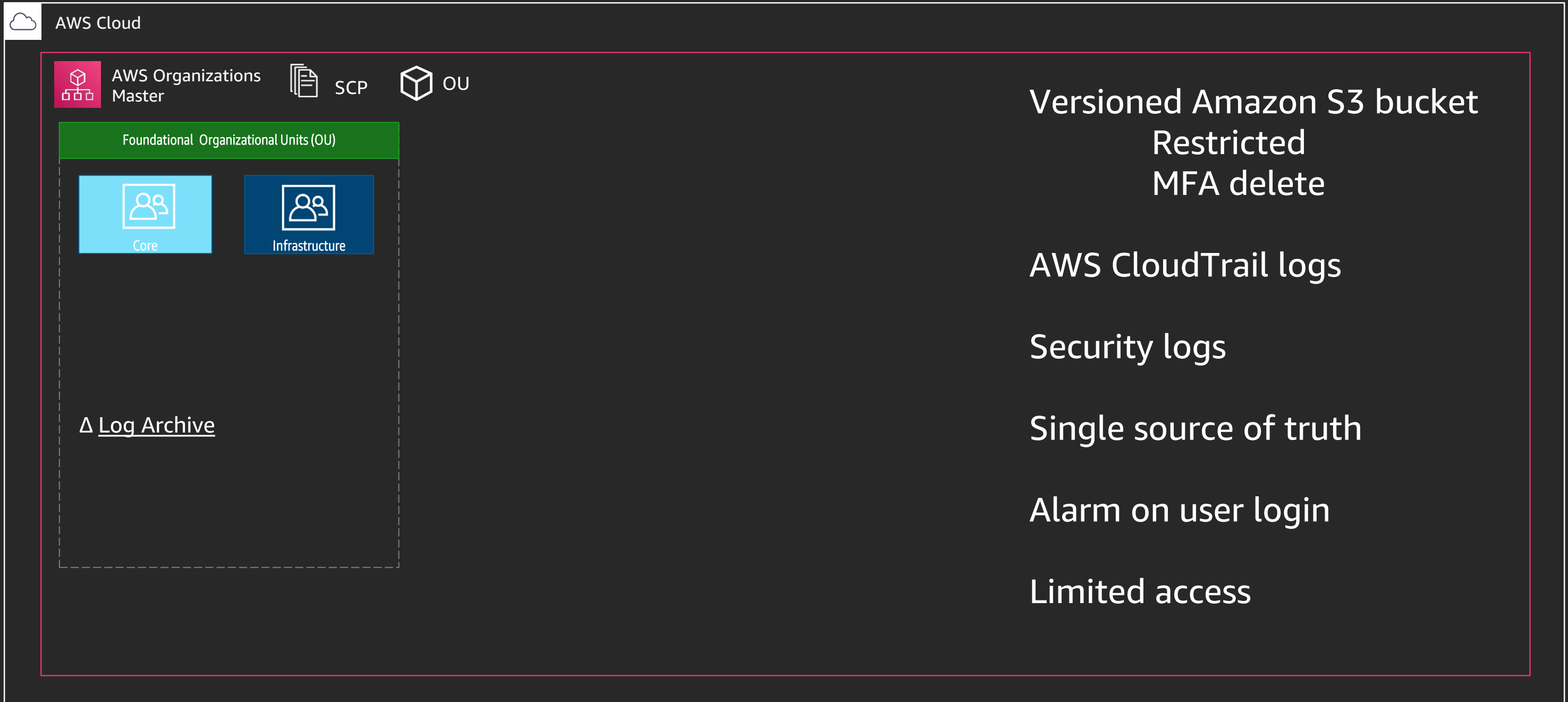
Building blocks

One per organization

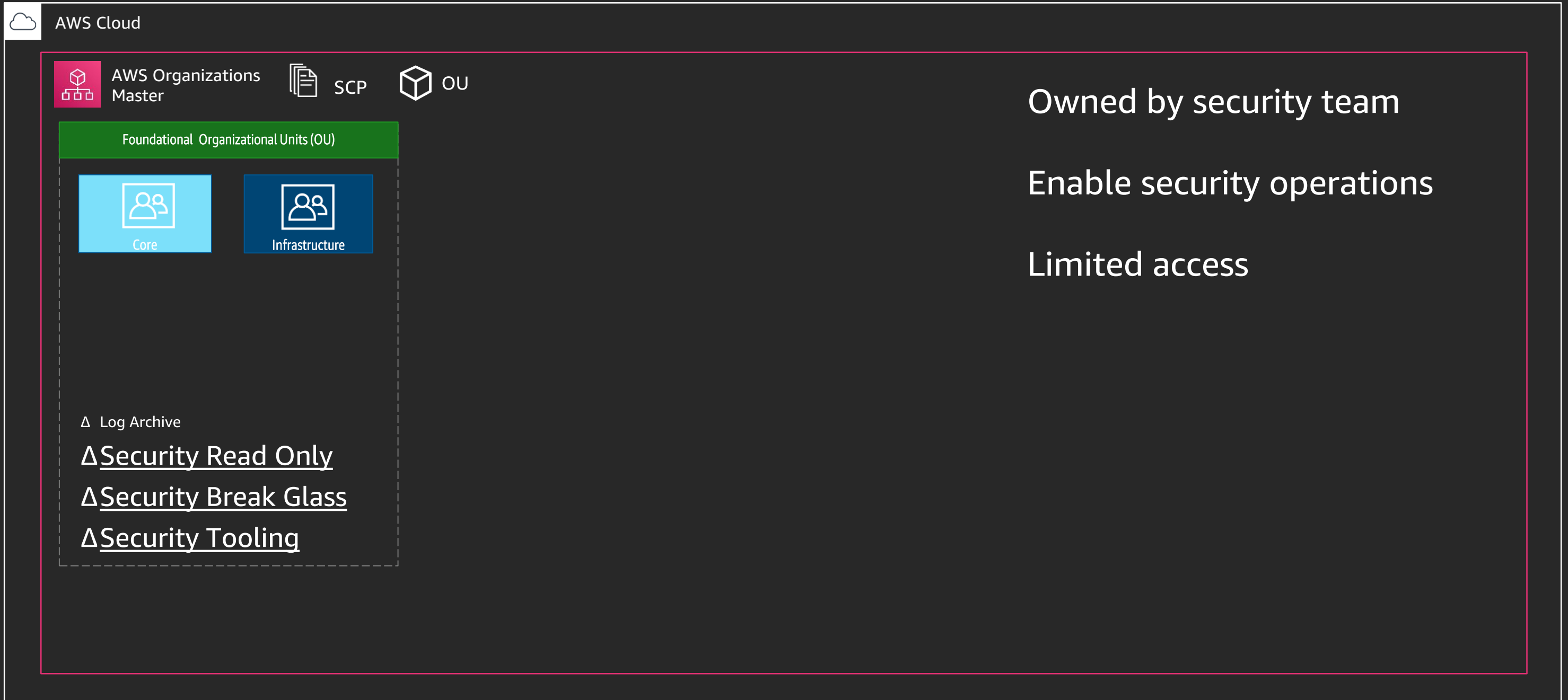
Security & Infrastructure

Have their own development life cycle (dev/qa/prod)

# Log Archive



# Security Accounts



# Security Accounts // Read Only

The screenshot shows the AWS Organizations console interface. At the top, there is a navigation bar with the AWS Cloud logo and the text 'AWS Cloud'. Below this, there are three main navigation items: 'AWS Organizations Master' (with a tree icon), 'SCP' (with a document icon), and 'OU' (with a cube icon). The main content area is titled 'Foundational Organizational Units (OU)' and contains two organizational units: 'Core' (light blue) and 'Infrastructure' (dark blue). Below these units, there is a list of permissions: 'Log Archive', 'Security Read Only', 'Security Break Glass', and 'Security Tooling'. The 'Security Read Only' permission is highlighted with a dashed red box.

View/Scan resources in other accounts

Exploratory Security Testing

Cross account read-only (security Auditor)

Limited access



# Security Accounts // Break Glass

The screenshot shows the AWS Organizations console interface. At the top, there is a navigation bar with the AWS Cloud logo and the text 'AWS Cloud'. Below this, there are three main sections: 'AWS Organizations Master' (indicated by a red icon), 'SCP' (Service Control Policies, indicated by a document icon), and 'OU' (Organizational Units, indicated by a cube icon). A green header bar labeled 'Foundational Organizational Units (OU)' contains two blue boxes: 'Core' and 'Infrastructure', each with a person icon. A dashed white box highlights a list of permissions for the 'Core' OU: 'Log Archive', 'Security Read Only', 'Security Break Glass' (underlined), and 'Security Tooling'. To the right of the screenshot, four lines of text provide context: 'Alert on login', 'Response in case of an event', 'Should almost never be used', and 'Extremely Limited access'.

Alert on login

Response in case of an event

Should almost never be used

Extremely Limited access

# Security Accounts // Tooling

The screenshot shows the AWS Organizations console interface. At the top, there is a navigation bar with the AWS Cloud logo and the text 'AWS Cloud'. Below this, there are three main navigation items: 'AWS Organizations Master' (with a tree icon), 'SCP' (with a document icon), and 'OU' (with a cube icon). The main content area is titled 'Foundational Organizational Units (OU)' and contains two organizational units: 'Core' (light blue) and 'Infrastructure' (dark blue). Below the OUs, there is a list of items with expandable triangles (Δ): 'Log Archive', 'Security Read Only', 'Security Break Glass', and 'Security Tooling' (which is underlined).

Security tools and audit

Amazon GuardDuty

AWS Security Hub

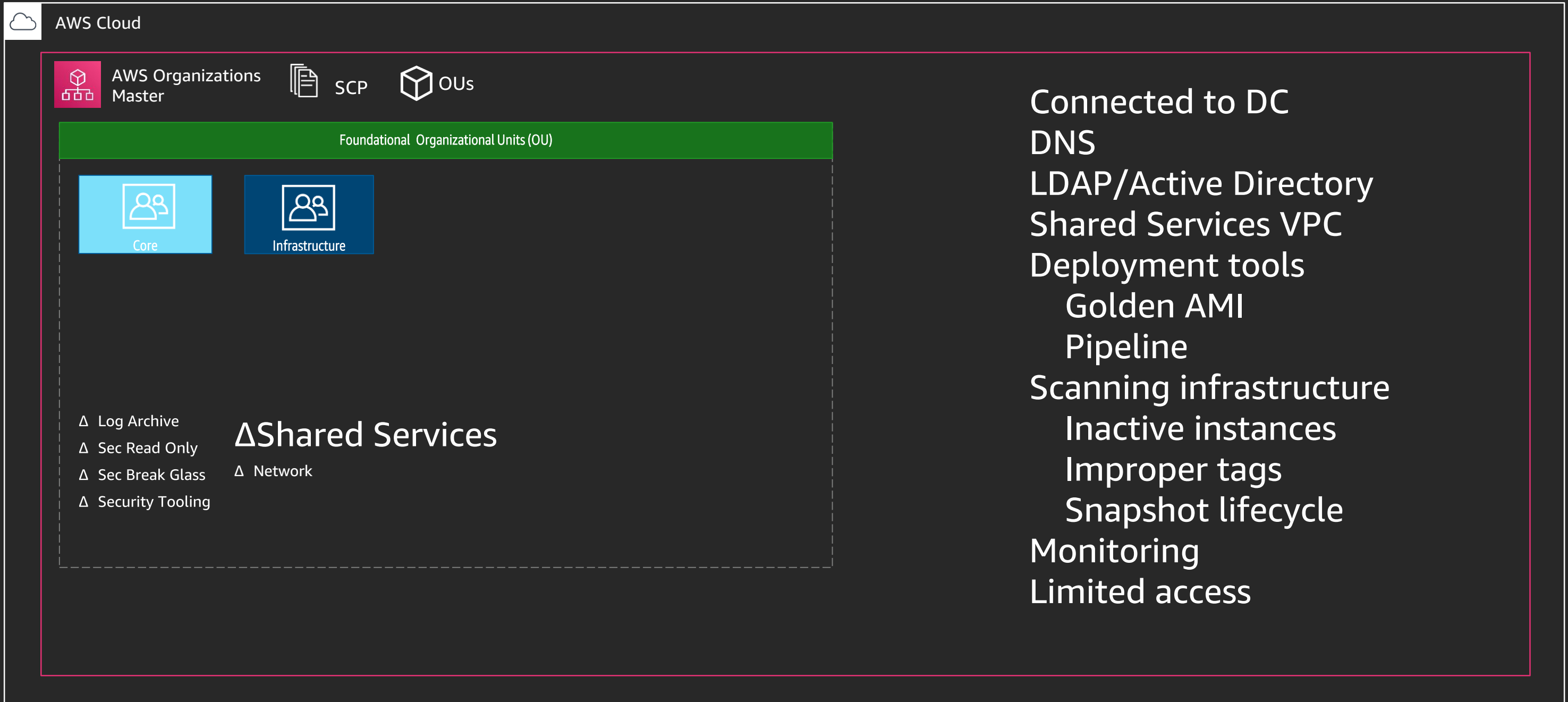
AWS Config Aggregation

Cross-account roles

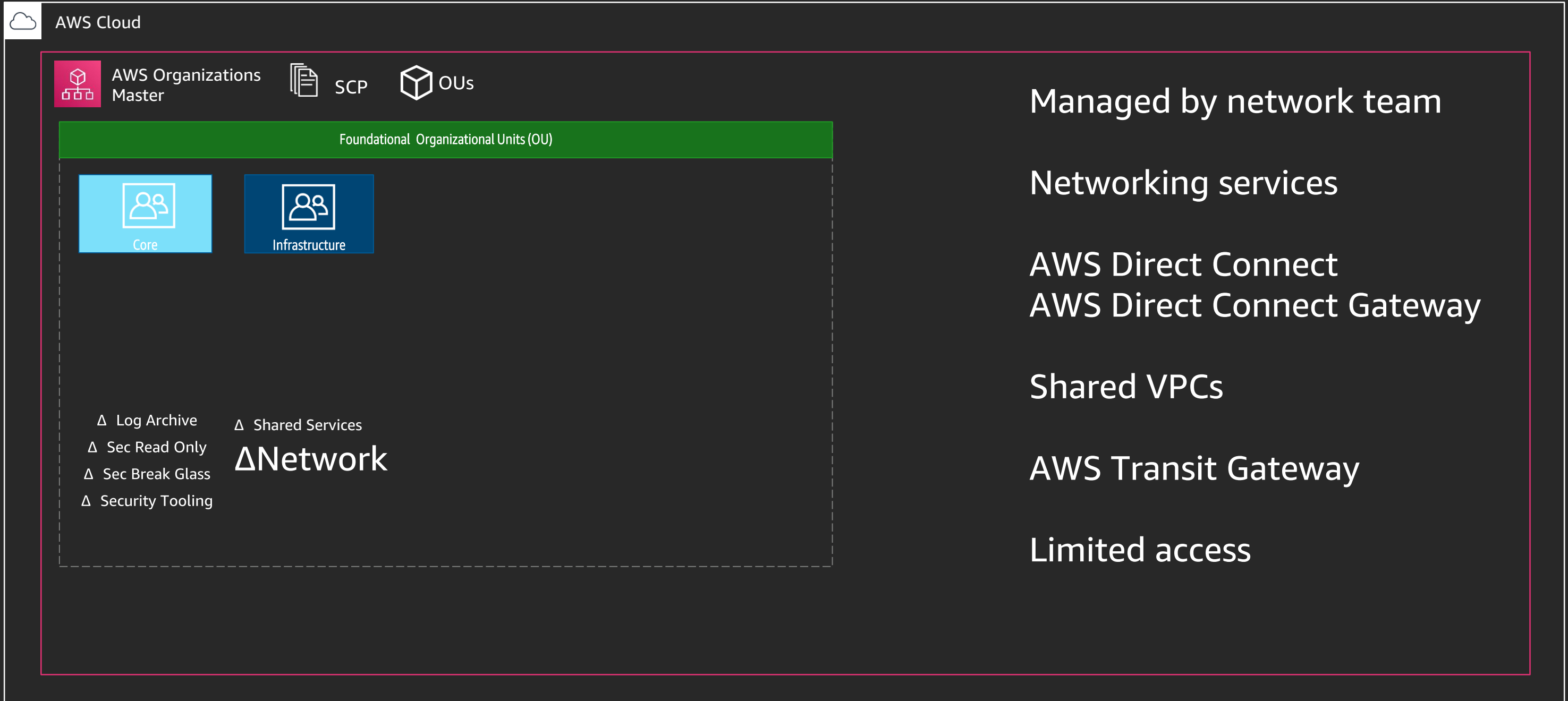
Automated Tooling

Automations, not humans

# Shared Services



# Network



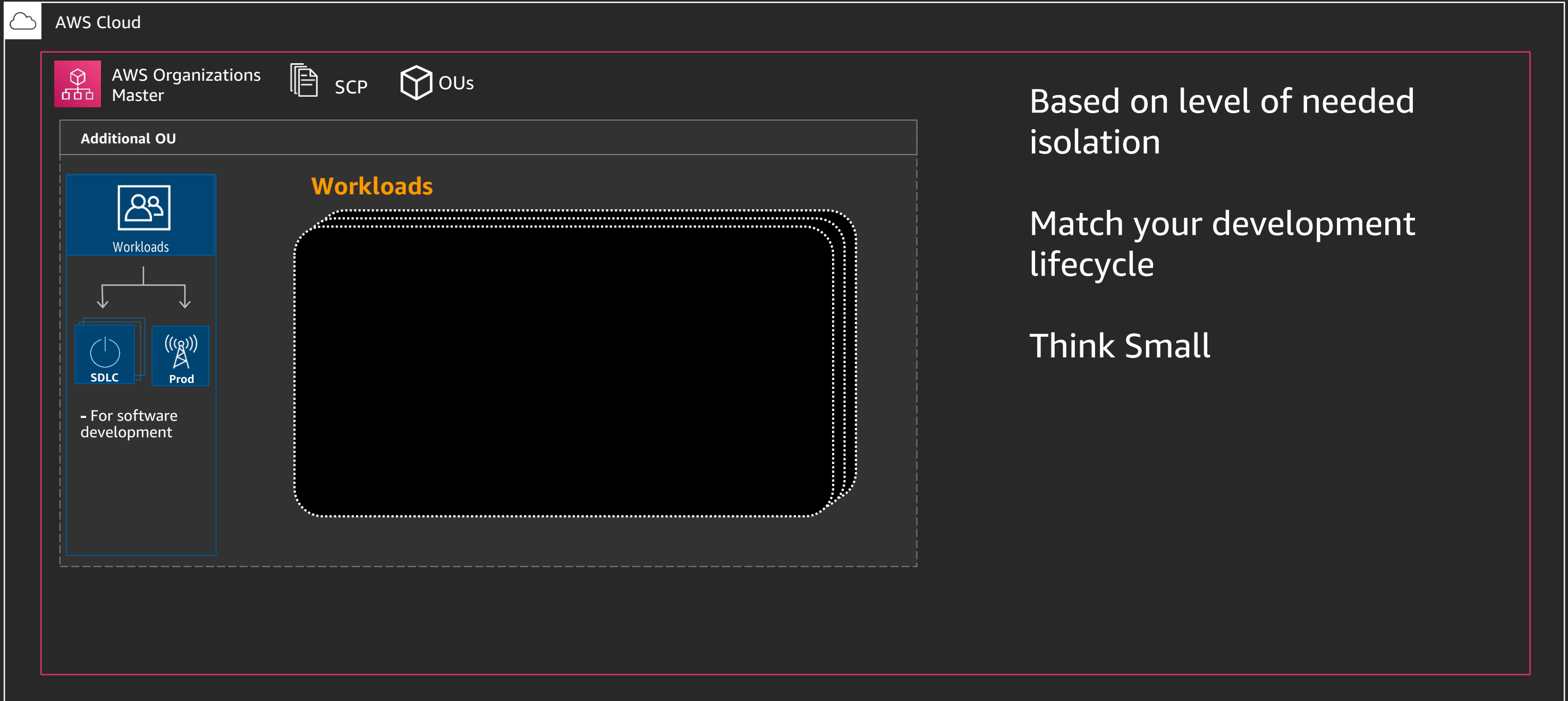
# Additional Organizational Units

# Developer Sandbox

The screenshot shows the AWS Organizations console interface. At the top, there's a navigation bar with the AWS Cloud logo and the text 'AWS Cloud'. Below this, there are three main sections: 'AWS Organizations Master' (with a tree icon), 'SCP' (with a document icon), and 'OUs' (with a cube icon). The 'OUs' section is expanded to show a list of 'Additional OU'. One of these OUs is highlighted in blue and labeled 'Sandbox'. This 'Sandbox' OU contains three individual developer accounts, labeled 'Dev 1', 'Dev 2', and 'Dev 3'. Below the developer accounts, there are two bullet points: '- Fixed spending limit' and '- Disconnected from network'. To the right of the console screenshot, there is a list of characteristics for the Developer Sandbox:

- No connection to DC
- Individual Dev Accounts
- Innovation space
- Fixed spending limit
- Autonomous
- Experimentation

# Workloads

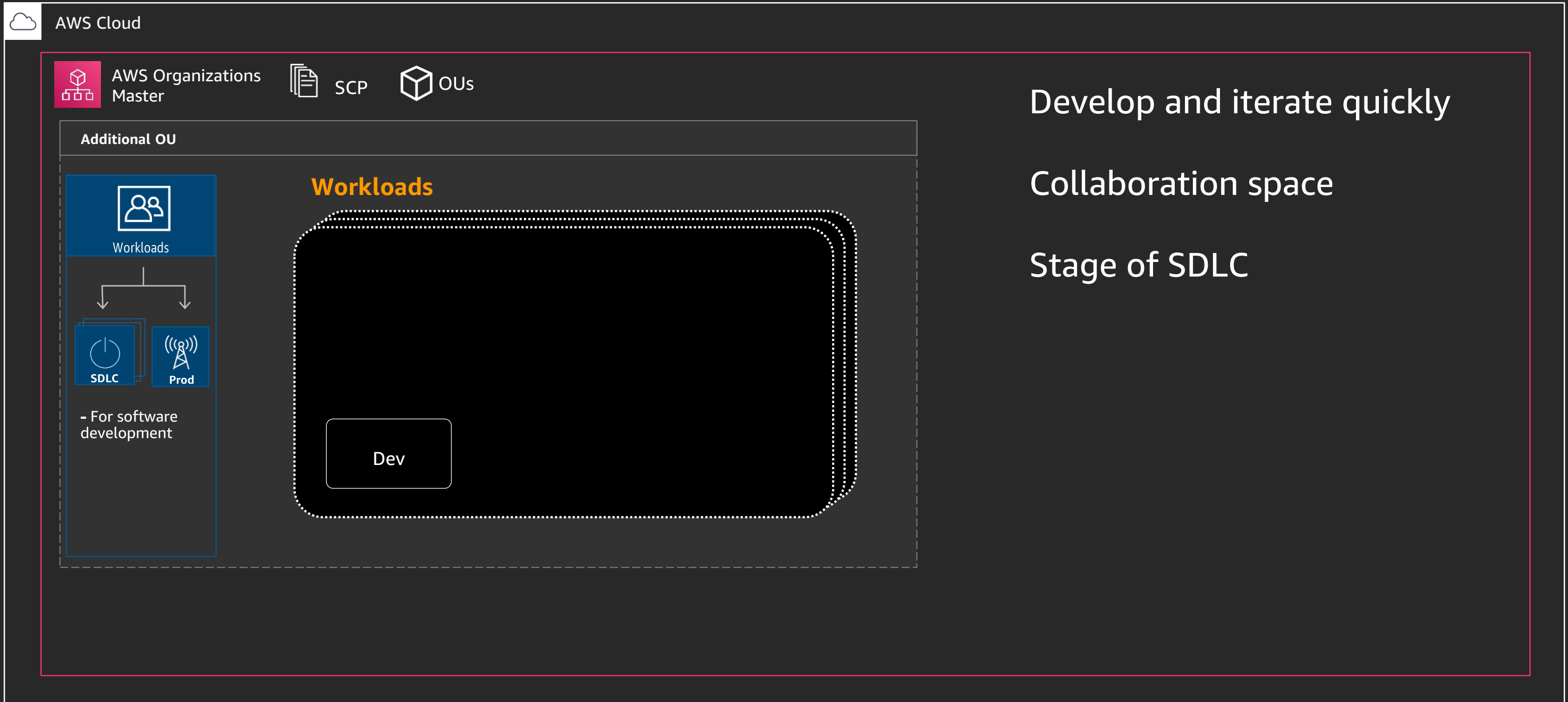


Based on level of needed isolation

Match your development lifecycle

Think Small

# Workloads // Dev



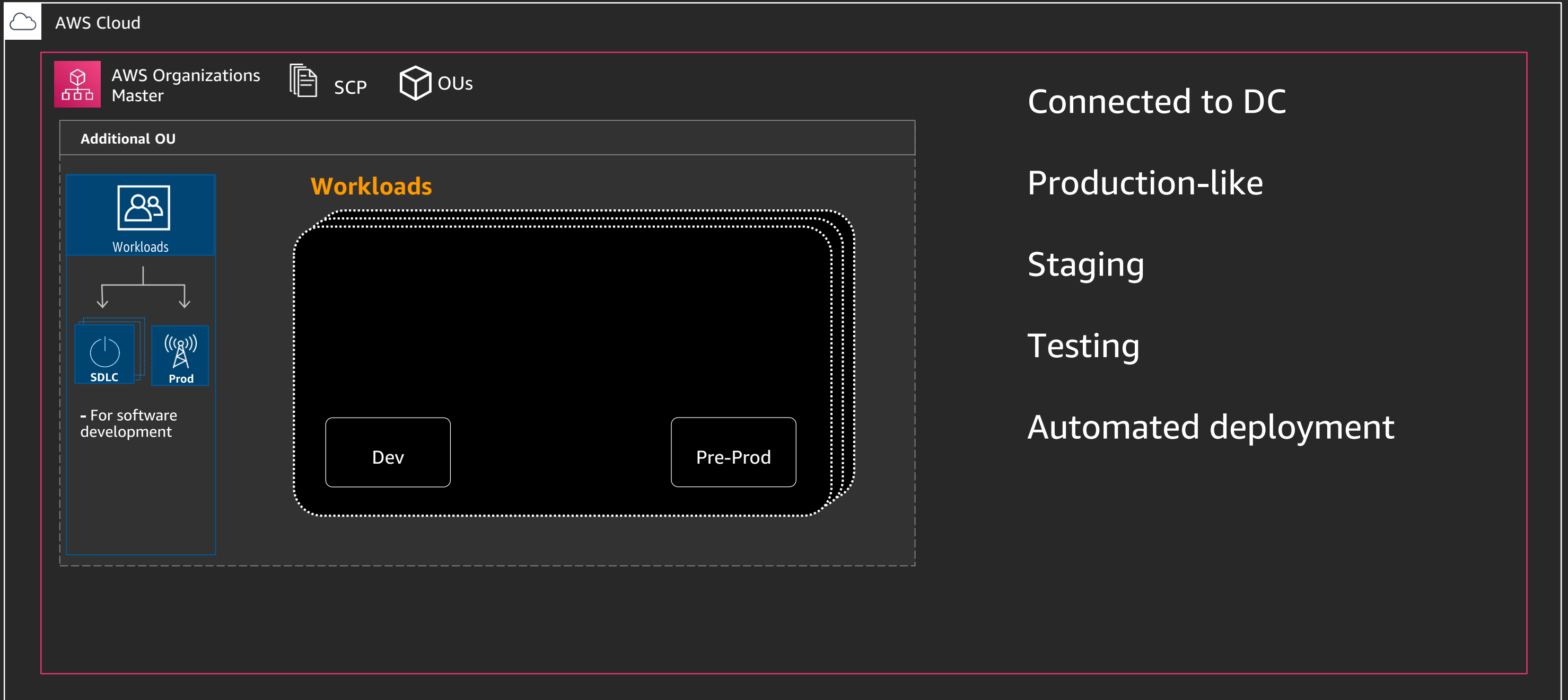
Develop and iterate quickly

Collaboration space

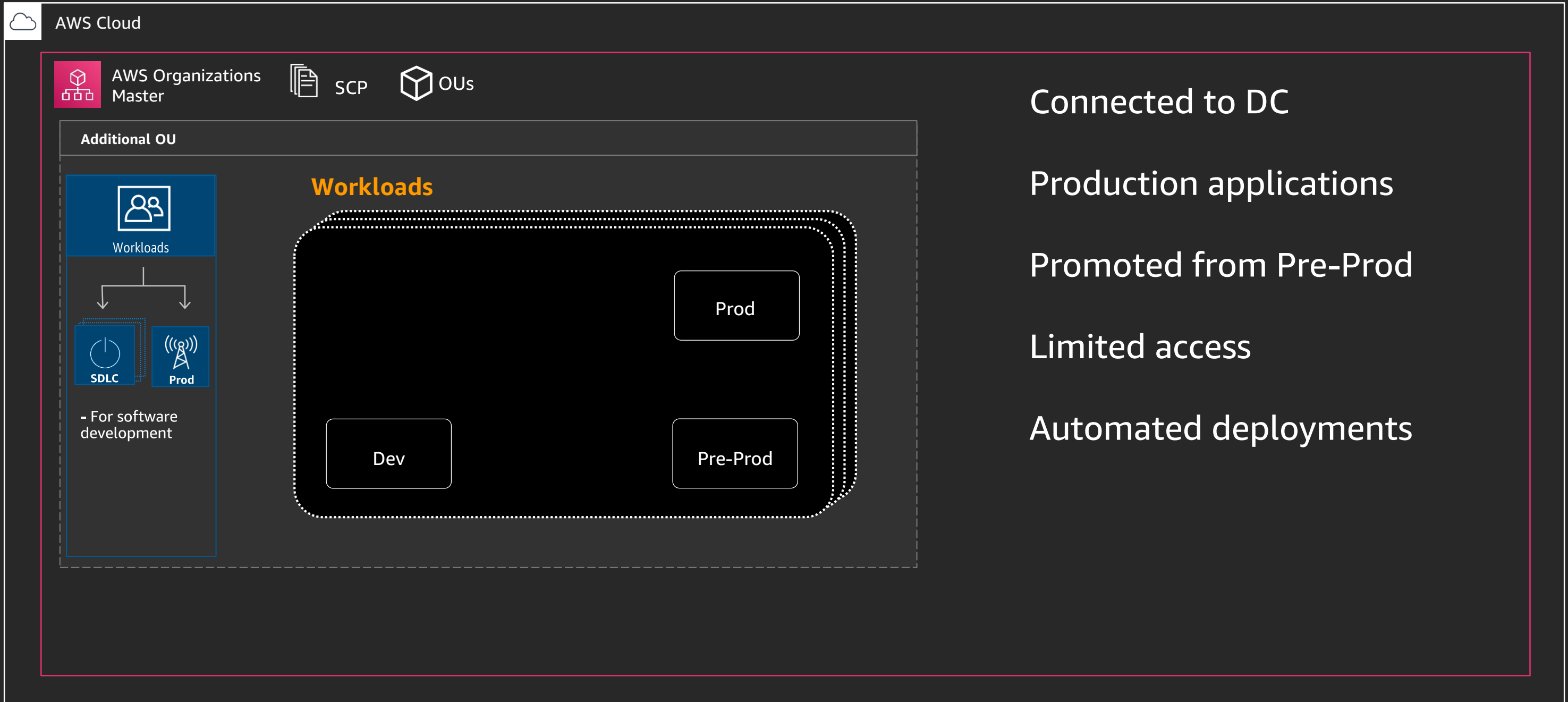
Stage of SDLC



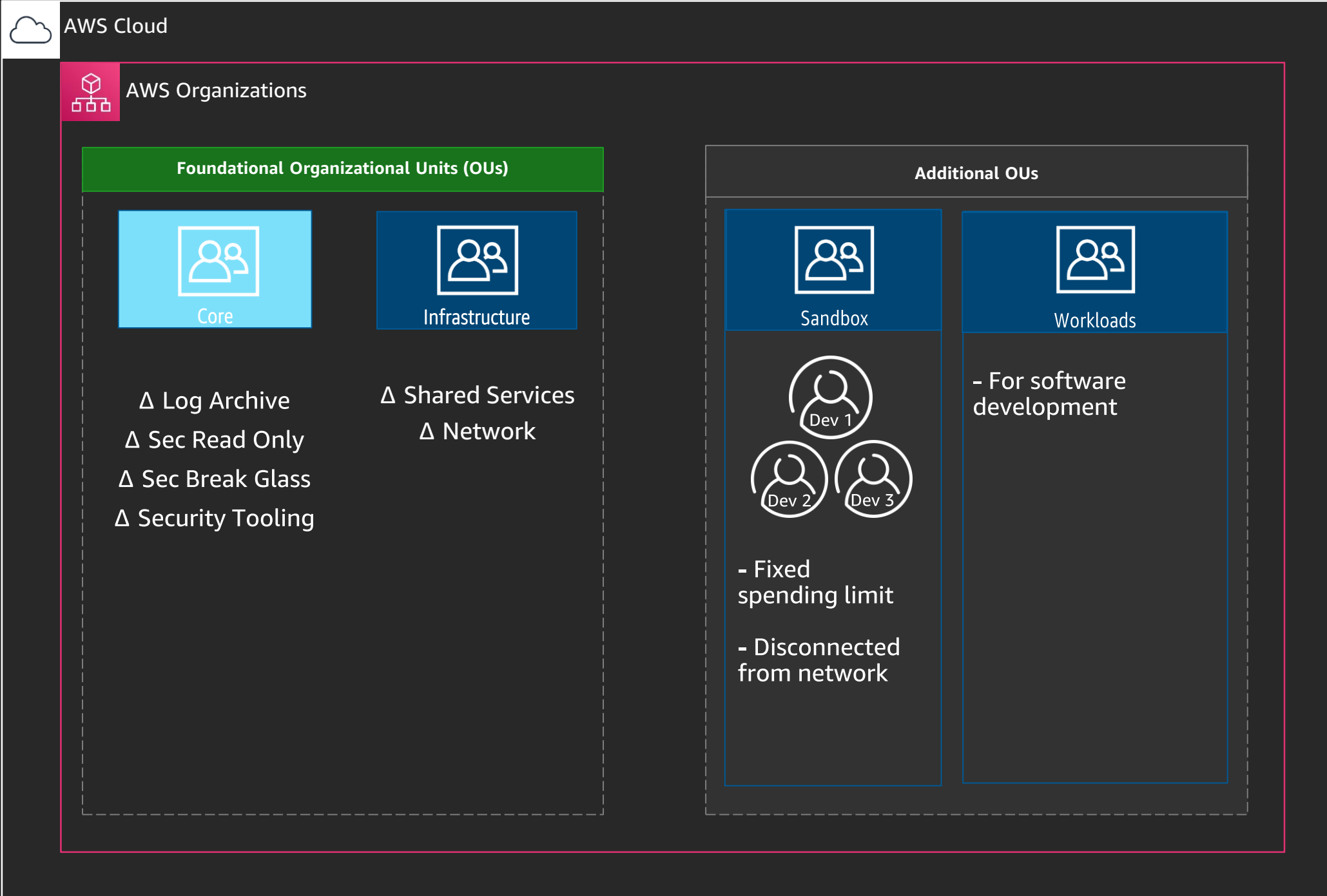
# Workloads // Pre-Prod



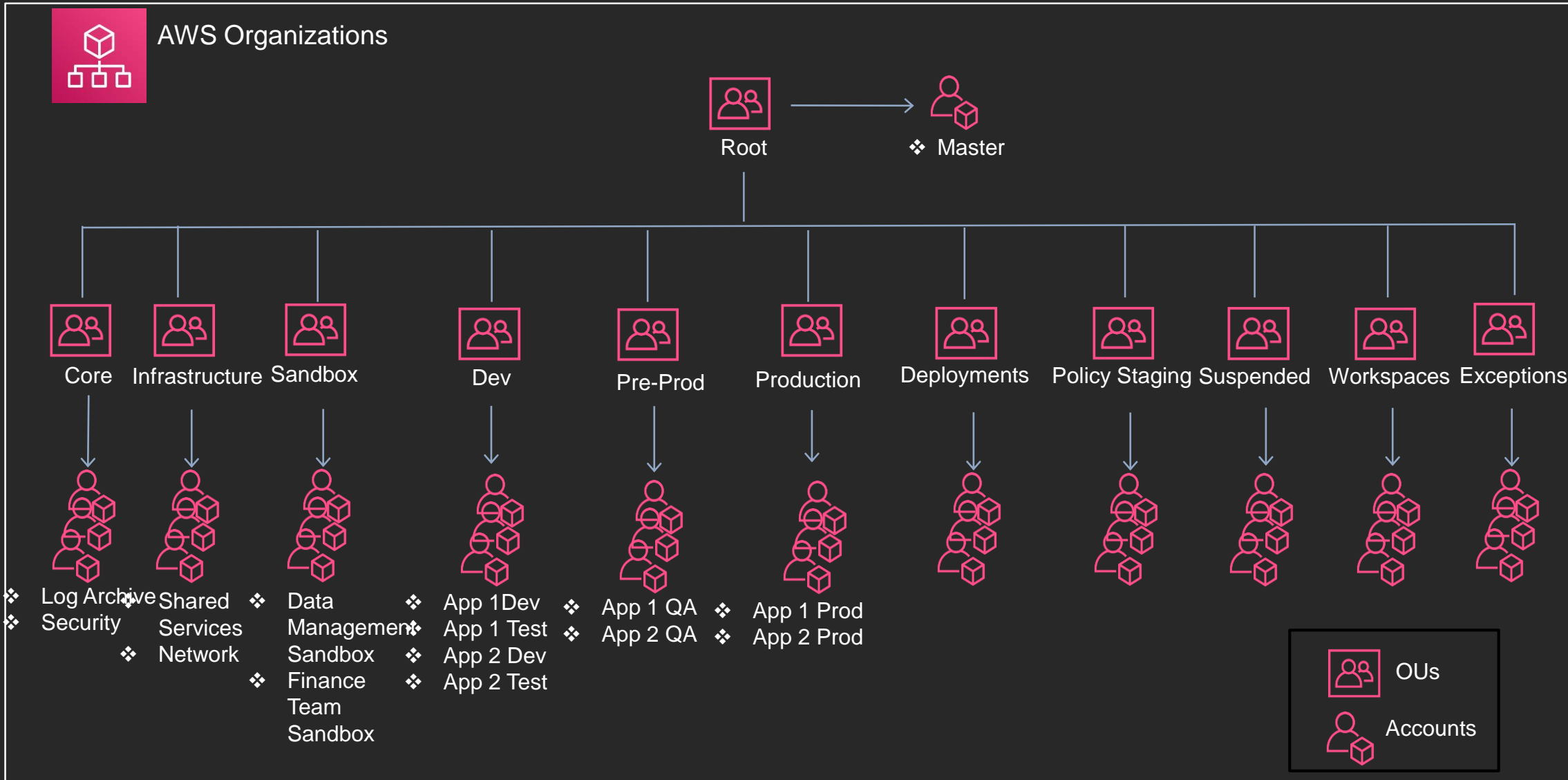
# Workloads // Prod



# Starter AWS multi-account framework



# OU Chart – Customer Example



- Core
  - Audit Logs (Flow log, cloud trail)
  - Log Correlation (Splunk)
  - Audit Tools

- Infrastructure
  - Directory services, DNS
  - Deployment Tools
  - Log aggregation tools (Splunk)

- Sandbox
  - POC env / Developers Playground
  - Fixed spending, time bound
  - No access to DC

- Dev
  - Collaboration space
  - Develop and iterate quickly
  - Stage of SDLC

- UAT
  - Connected to DC
  - Production like
  - Staging/Testing

- Production
  - Connected to DC
  - Production applications
  - Promoted from ore-prod

- Deployments
  - Build pipelines (CI/CD)
  - One account per each workload
  - Highly secured
  - Extremely limited access

- Policy Staging
  - Safely test policies
  - Promote to an OU
  - Promote to final target OU

- Suspended
  - De-commissioned accounts will stay in this OU for sometime before permanently deleted

- Exceptions
  - Applications that require deviations from common policies

- Workspaces
  - AWS Workspace accounts

Questions?