
aws
SUMMIT
LONDON | APRIL 27, 2022

CO-04

Building the foundation for cloud governance

Sharique Kamal (He/Him)
AWS Technical Instructor
AWS TnC

Agenda

1. Well-Architected Principles
   - *Operating your workloads*
   - *Account Management Separation*
2. Multi-Account Strategy
   - *Organizing your environment*
   - *Organizational Structure*
3. More
   - *Centralized Billing*
   - *AWS Budgets*
   - *Organization policies*
   - *Controls & Guardrails*

What does an ideal environment look like?

Ready to support highly available and scalable workloads

Configurable to support evolving business requirements

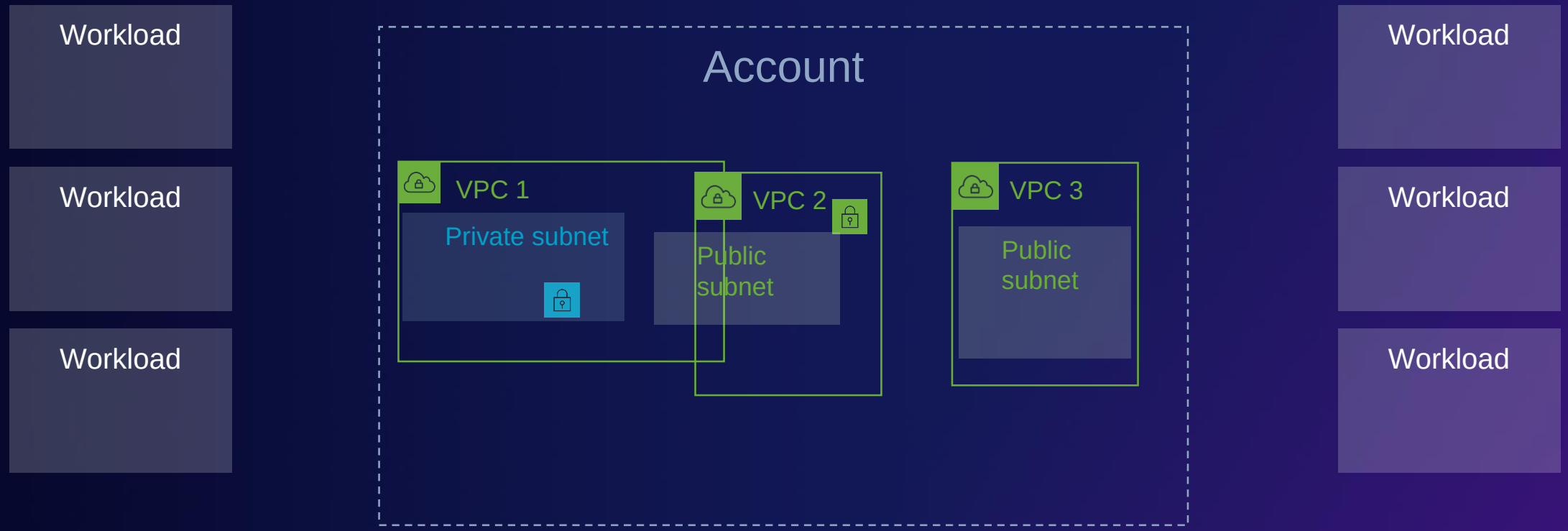
Meets the organization's security and auditing requirements

Workloads

- Level of Isolation
- Customized Development Lifecycle
- Isolate Risk
- Think Big; Start Small

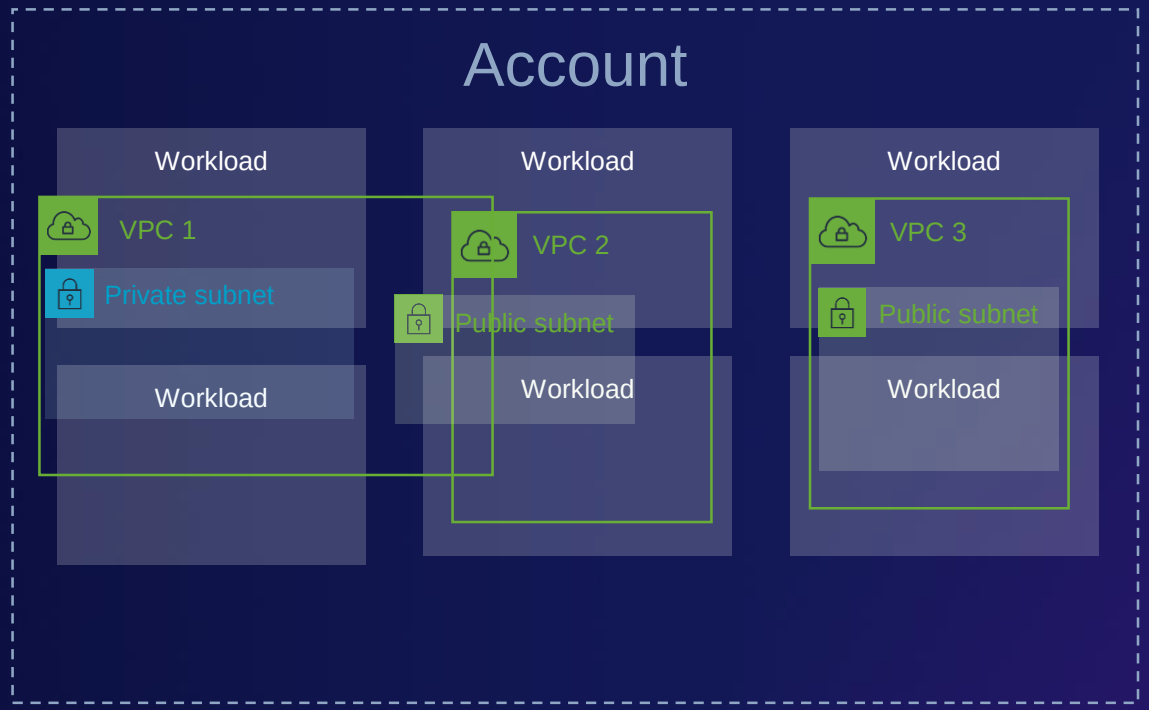
Customer: Acme, Inc

- INITIAL APPROACH



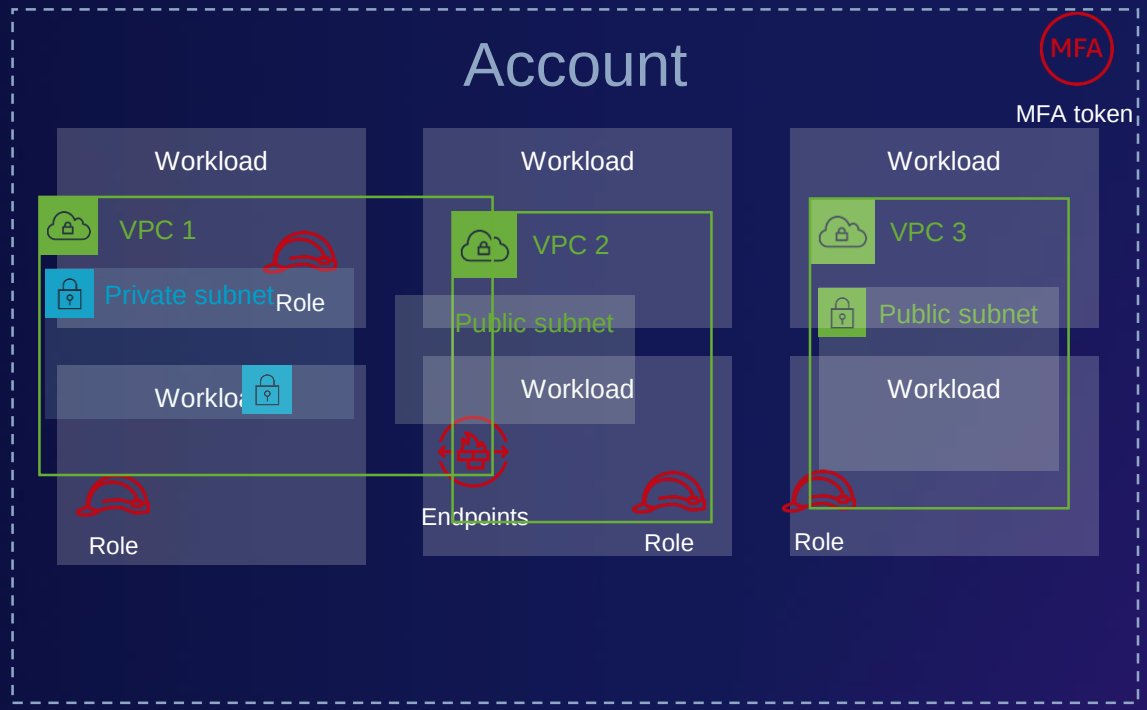
Customer: Acme, Inc.

- INITIAL APPROACH



Customer: Acme, Inc.

- INITIAL APPROACH



Securely operating your cloud environment at scale

- Identify and prioritize risks using a threat model
- Identify and validate control objectives
- Keep up to date with security threats
- Keep up to date with security recommendations
- Evaluate and implement new security services and features regularly
- Automate testing and validation of security controls in pipelines

Multi-Account Benefits

Benefits

Centrally provision accounts and resources

Share resources and control access to accounts, regions, and services

Optimize costs and identify cost-saving measures

Secure and audit your environment for compliance

Use Cases

Many teams

Rapid innovation with resources provisioned quickly and exclusively for each team

Business process

Organize AWS accounts to reflect business processes with different operational, regulatory, and budgetary requirements

Billing

Simplify billing where resources used within an AWS account can be allocated to the business unit that is responsible for that account

Isolation & security

Tight security boundaries enforced by built-in isolation between accounts, and consolidation for workloads with similar risk profiles

AWS Account Management and Separation

- Separate workloads using accounts
- Secure AWS account
- Manage accounts centrally
- Set controls centrally
- Configure services and resources centrally

AWS Organizations & AWS Control Tower

- **ENABLE CONTROL**

Manage and govern centrally across AWS Accounts implementing your AWS multi-account environment

Manage and define your organization and accounts

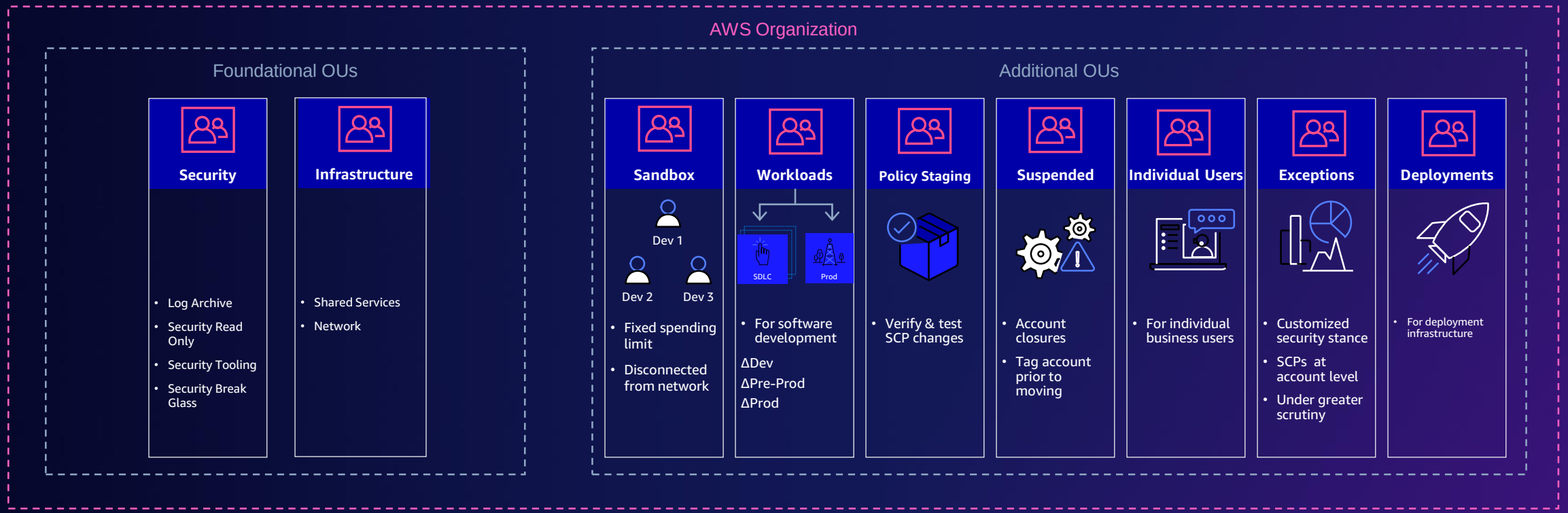
Control access and permissions

Audit, monitor, and secure your environment for compliance

Share resources across accounts

Centrally manage costs and billing

Structure your multi-account environment



Foundational OUs

Infrastructure

Security

Infrastructure OU Accounts

Security OU Accounts

Security Tooling

Log Archive

Security Read Only

Security Break Glass

Workloads OU

DEV

- Develop quickly
- Collaboration Stage
- Prepare to deploy to Staging

STAGING

- Production Like
- Testing
- Automated Deployment
- Promotion to Prod

PROD

- Production Workloads
- Restricted Access
- Promoted from staging
- Automated Deployments

Sand Box OU

- Drive Innovation
- Budgets
- Isolation of Resources
- Not connected to the corporate network

More Governance features

- AWS Budgets
- Organizational Policies
- Cost Anomaly Detection
- AWS Backup
- StackSet Integrations
- S3 Storage Lens

AWS Budgets

- Pro-actively Monitor Spending
- Tags
- Accounts
- Resources

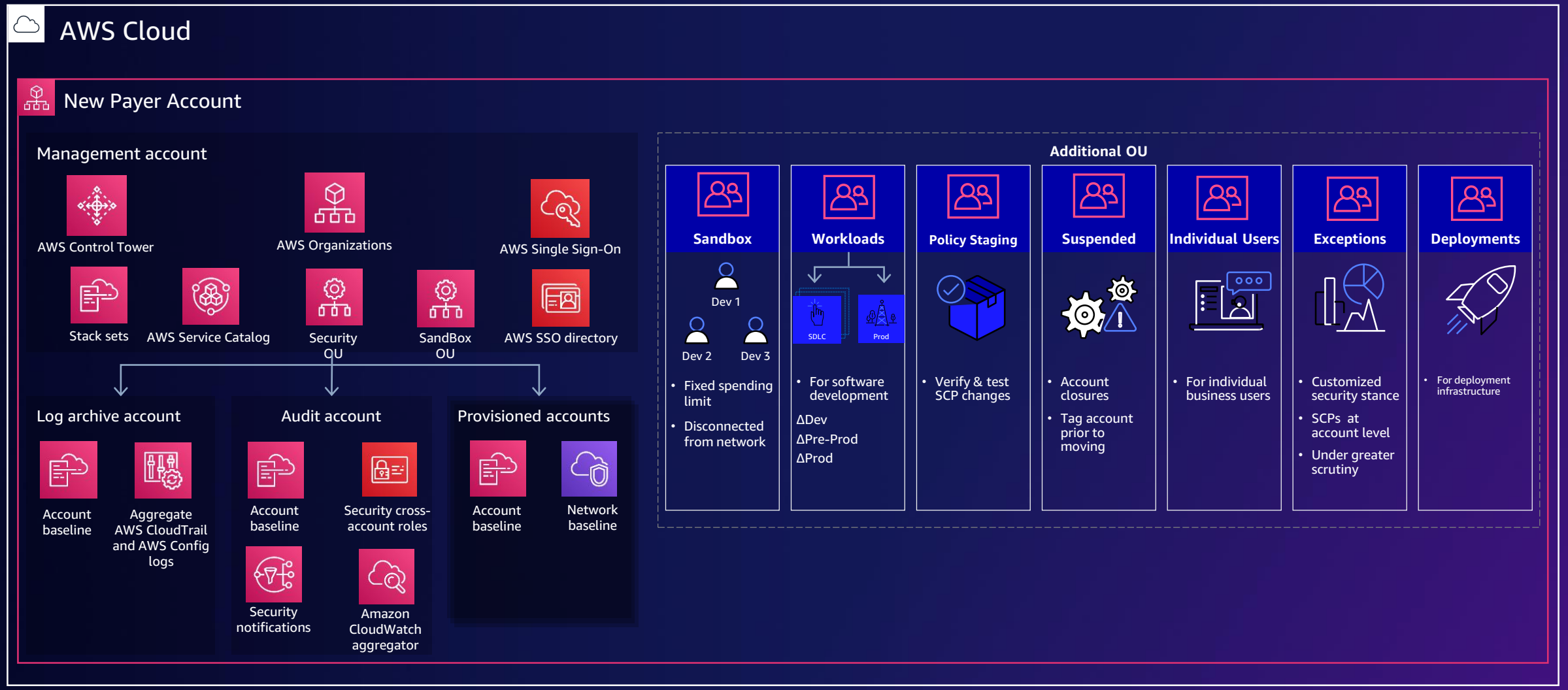
Organizational Policies

- Service Control Policies (SCP)
- Tagging policies
- AI/ML Policies
- Backup Policies

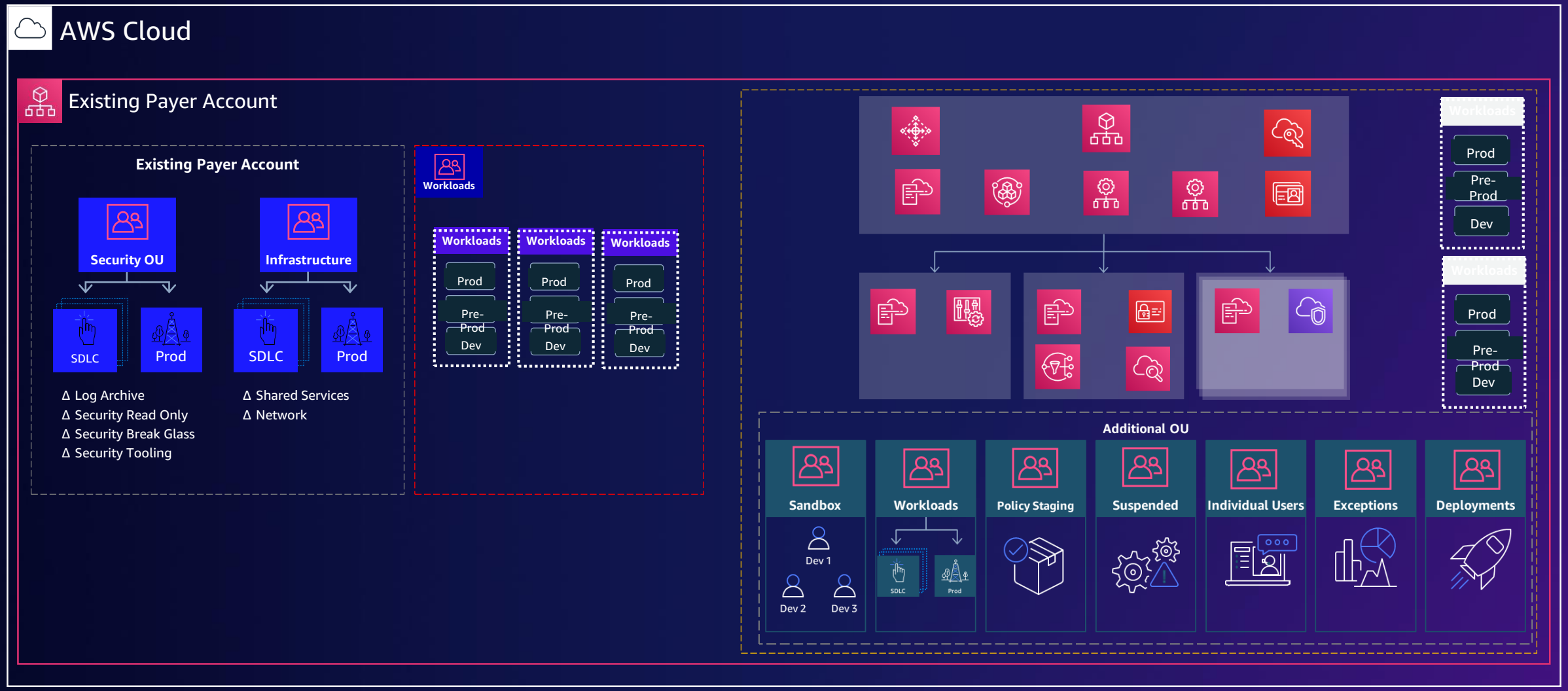
AWS Organizations (SCP Template)

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Deny",
      "Action": ”<Insert service to block here>:*",
      "Resource": "*”,
      "Condition": {…}
    }
  ]
}
```

New Customer Journey



Existing Customer Journey



Extend central governance with AWS Organizations

Centrally provision account & resources

Share resources and control access to accounts, regions, and services

Optimize costs and identify cost-saving measures

Secure and audit your environment for compliance

Extend central governance with AWS Organizations

Centrally provision account & resources

- AWS CloudFormation
- AWS Systems Manager
- AWS Service Catalog

Share resources and control access to accounts, regions, and services

- AWS Personal Health Dashboard
- AWS Resource Access Manager
- AWS Backup & Backup Policies
- Tag Policies

Optimize costs and identify cost-saving measures

- AWS Trusted Advisor
- AWS Compute Optimizer
- AWS Cost Explorer
- AWS License Manager
- S3 Storage Lens

Secure and audit your environment for compliance

- AWS Audit Manager
- Amazon GuardDuty
- Amazon Cloud Directory
- AWS Firewall Manager
- Amazon Macie
- AWS Security Hub
- AWS IAM Access Analyzer
- AI/ML Policies

Learn more about Cloud Governance and Control Tower

AWS Well Architected Labs

Collection of **Hands-on labs** to help you learn, measure and build using architectural best practices.

The labs are categorized into levels, where 100 is introductory, 200/300 is intermediate and 400 is advanced.

Access the **labs** here

AWS Control Tower Workshops

Collection of **Control Tower** workshops on Multi-account provisioning, Account Factory and different tasks within Control Tower.

Work with different aspects of **Control Tower** implementation such as Provisioning, Authentication and Authorization, Security and Compliance etc.

Access the **Workshop** here

Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

Thank you!

Sharique Kamal


linkedin.com/in/shariquekamal/


@sharique12k

Please complete the session survey