Mastering Multi-Account Strategy with AWS Control Tower

Simplifying Cloud Governance

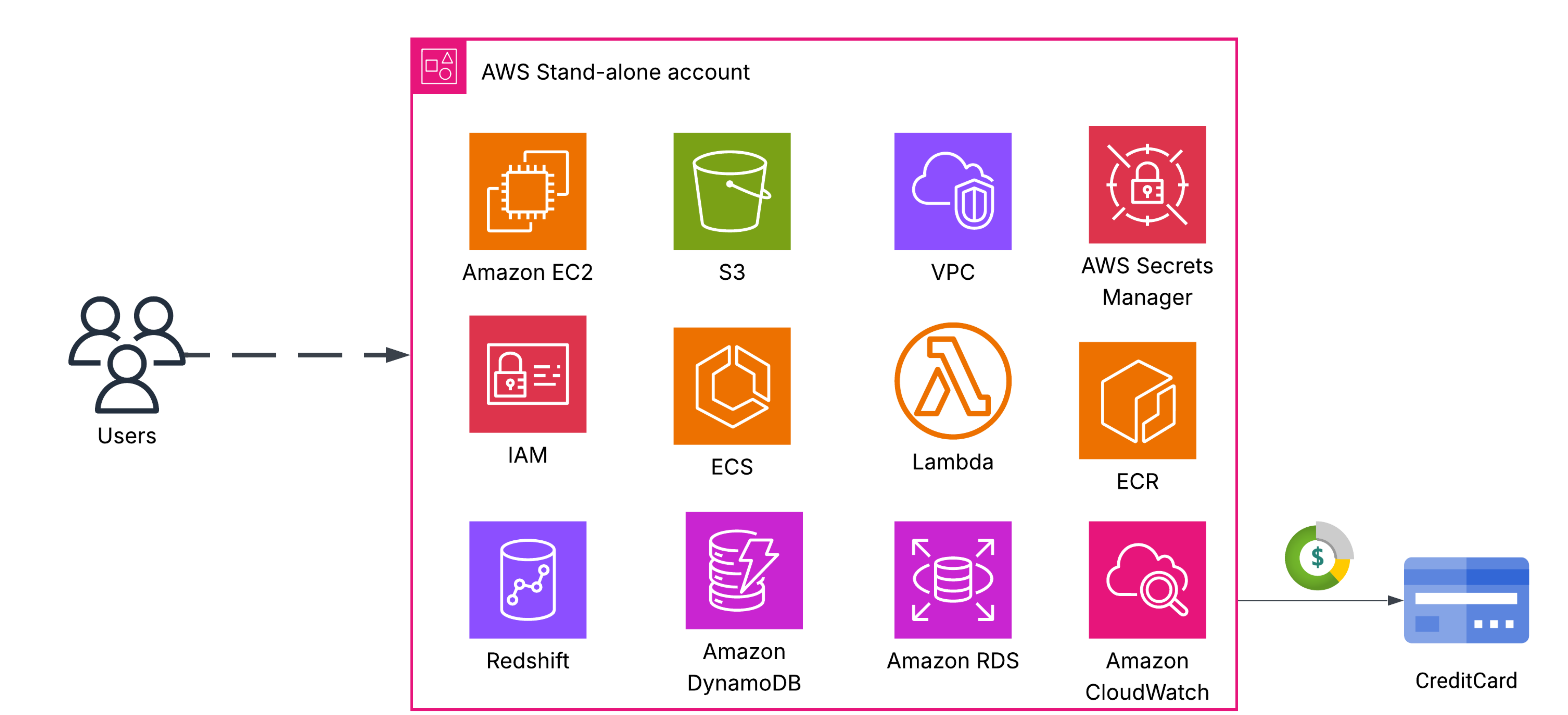
Srinivasan
Cloud Architect - PwC

What we will cover today:

- *AWS Account*
- *A View from Enterprise Lens*
- *AWS Landing Zone*
- *AWS Control Tower(deep-dive)*
- *Demo*
- *Key Takeaways*
- *Career Path*
- *Q & A*

AWS Account:

Logical permissions boundary within AWS Ecosystem.



Enterprise Lens:

- *Reduced Blast Radius*
- *Single sign-on capability*
- *Centralized Security Management*
- *Centralized Logging*
- *Organizational standards*
- *Unified Billing, Cost Management*

Blast Radius

Single Sign-On

Security Lens

Logs

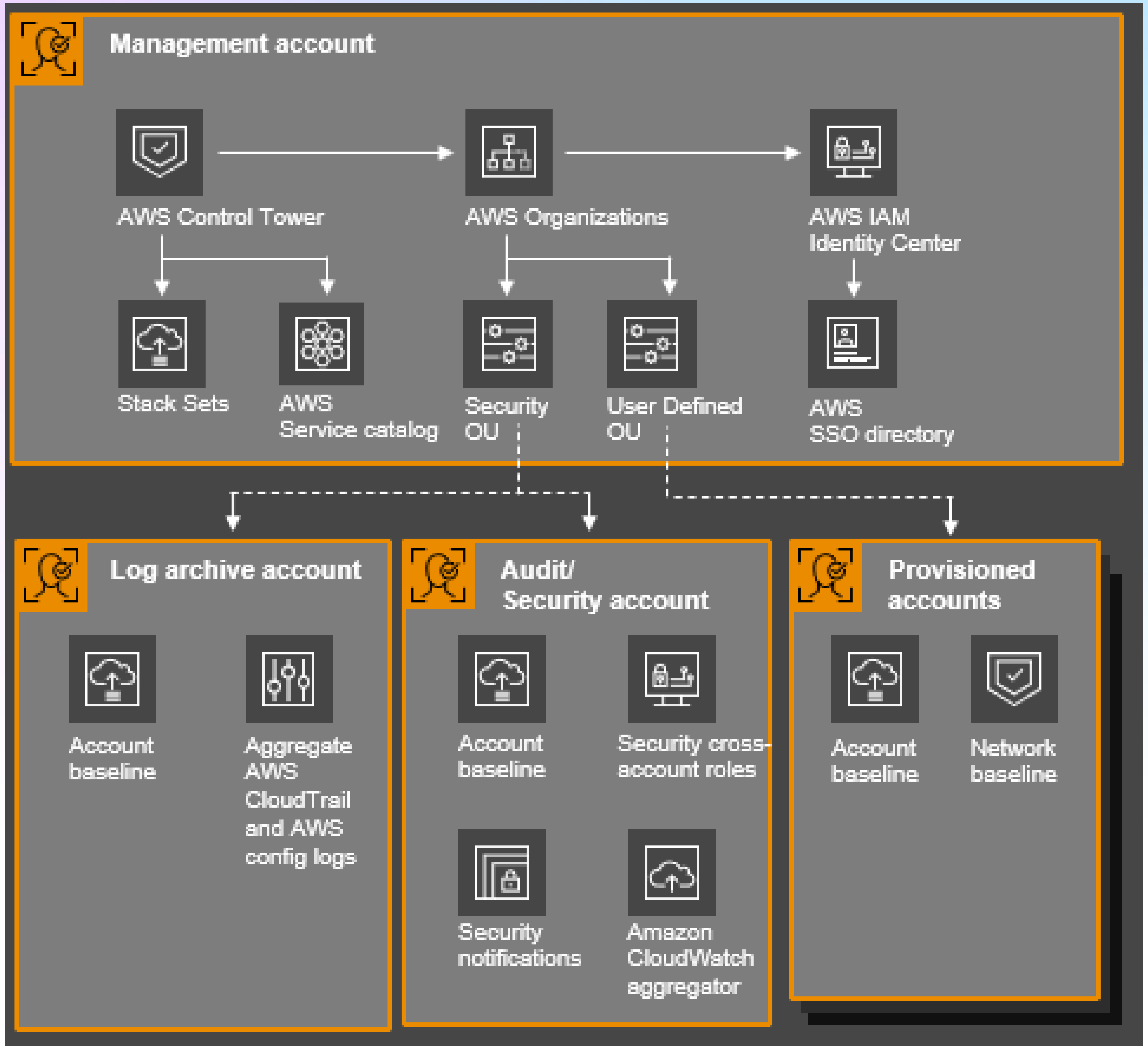
Organizations Standards

Cost Management and Billing

AWS Landing Zone

Setup that is configurable, secure, scalable, multi-account AWS environments based on AWS best practices

- *Management account*
- *Log-archive account*
- *Security account*
- *Workload accounts(1..n)*



*AWS Deprecated this in 2020***

Why use AWS Control Tower?

AWS Control Tower

AWS Organizations

Set up a well-architected AWS Landing Zone in a few clicks

Standardized account provisioning with Infrastructure-as-Code (CloudFormation or Terraform)

Centralized policy management

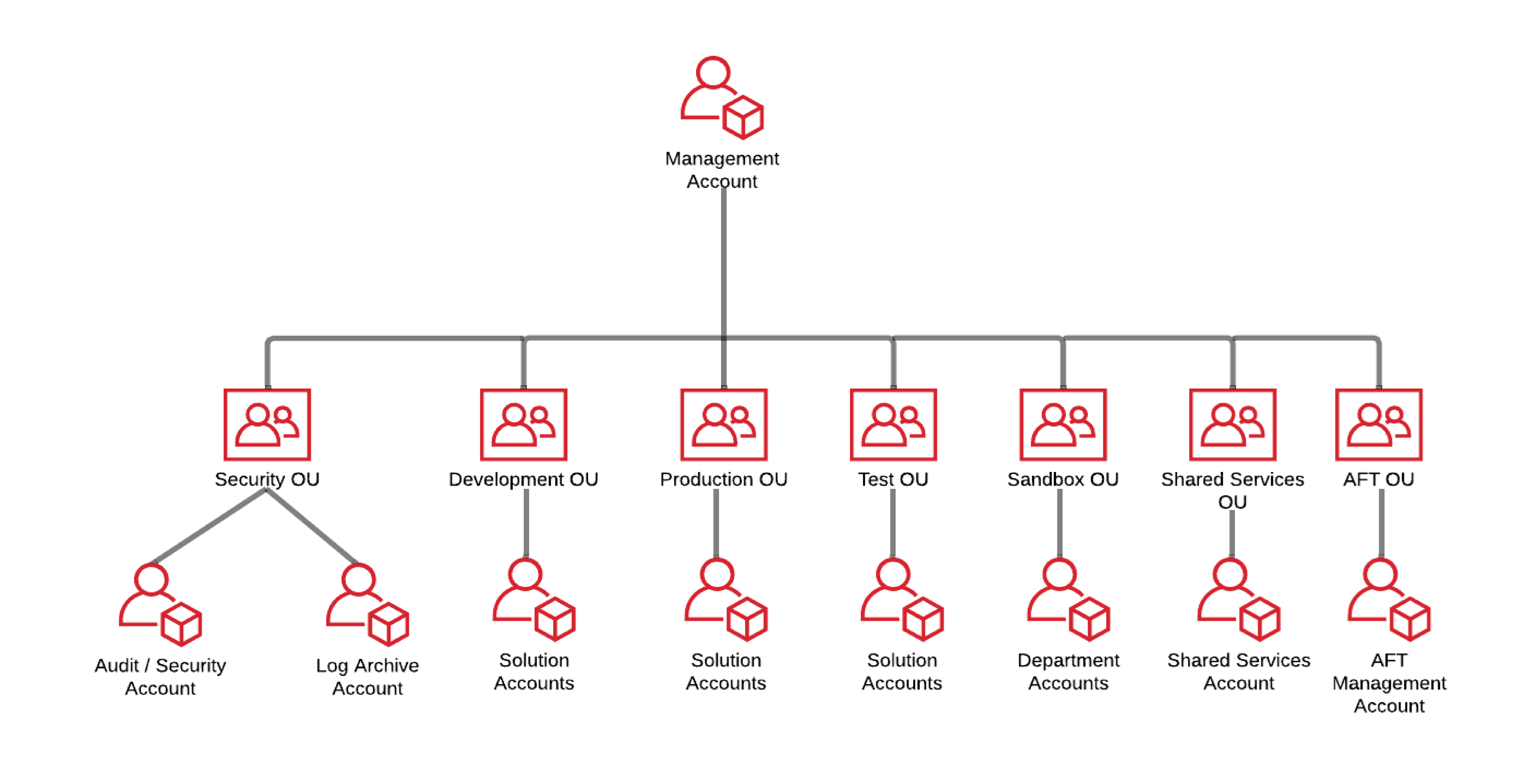
Enforce governance and compliance proactively

Enable end-user self-service

Get continuous visibility into your AWS environment

Gain peace of mind

Enterprise OU Structure:



Policy Enforcements:

Mandatory controls

- *Disallow configuration changes to CloudTrail*
- *Enable CloudTrail in all available regions*
- *Enable integrity validation for CloudTrail log file*
- *Disallow configuration changes to AWS config*
- *Enable AWS config in all available regions*

Strongly recommended controls

- *Disallow creation of access keys for the root user*
- *Disallow actions as a root user*
- *Detect whether MFA for the root user is enabled*

Elective controls

- *Disallow changes to replication configuration for Amazon S3 Buckets*
- *Detect whether MFA is enabled for AWS IAM users*
- *Detect whether versioning for Amazon S3 Buckets is enabled*

Centralized Identity and Access Management

Single Sign-On

AWS Organizations

AWS IAM Identity Center provides default directory for identity.

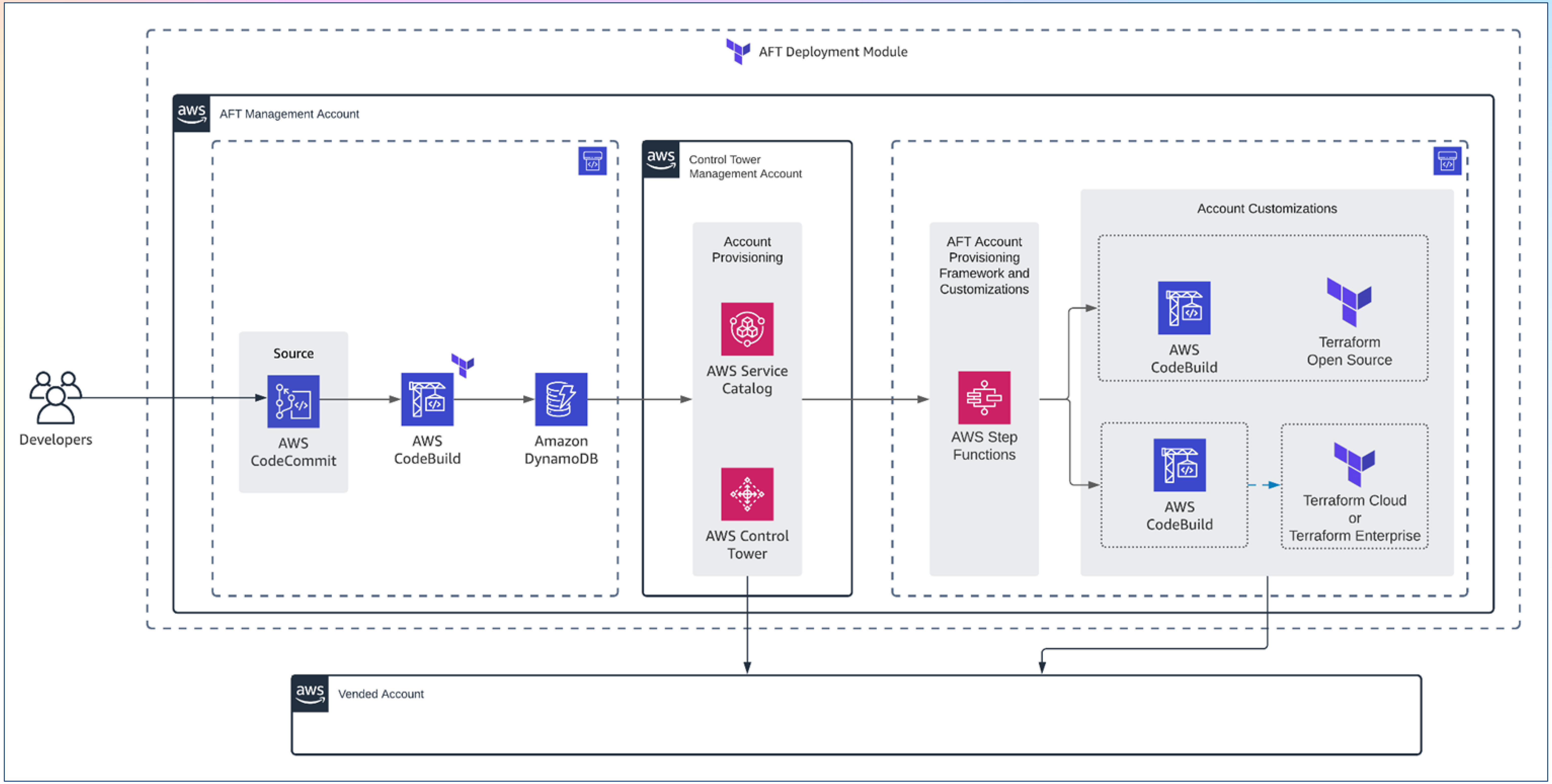
Enables federated access management across all accounts in your organization. Integrates with third party tools like Okta, ADFS etc.,

Preconfigured IAM groups

Preconfigured permission sets (e.g., admin, read-only, write).

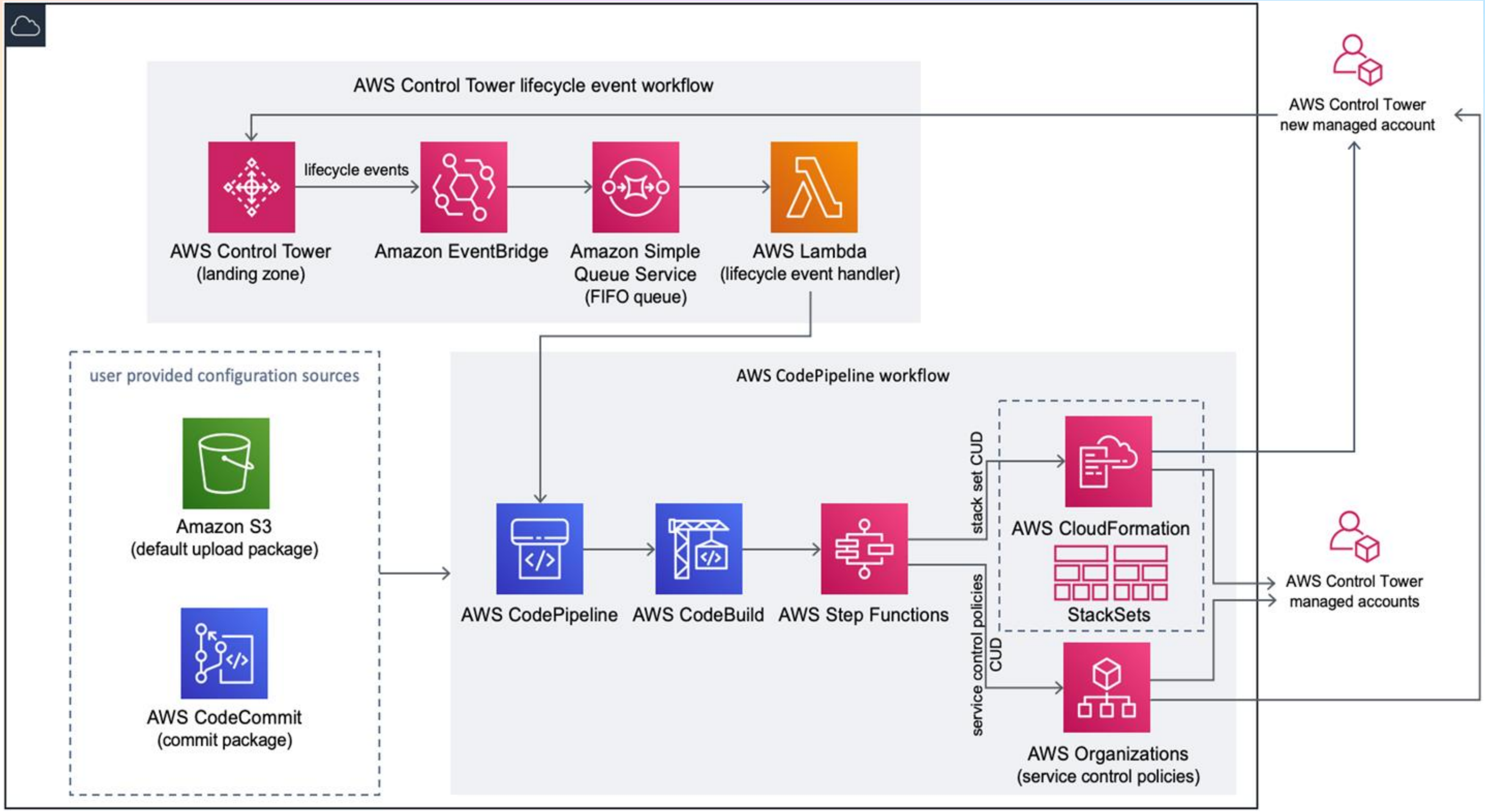
Account Factory: Terraform

Account requests, customizations are done through terraform configurations from SCM



Account Factory: Cloud Formation

Account requests, customizations are done through Cloud Formation templates



Demo

Key Takeaways:

- *Use Control Tower features to Simplify your Cloud Governance*
- *Create OU’s as per the business requirements*
- *Build Secure Foundations with Controls library*
- *Always follow IaC best practices*
- *Always visualize solution from Enterprise Lens*

Career Path:

- *Cloud Architect - Designs secure multi-account AWS environments*
- *DevOps Engineers – Automates provisioning via Account Factory*
- *Cloud Administrators – Manages users, access, budgets*
- *Cloud Security Engineers - Implements Controls & compliance*

Q & A

THANK YOU FOR ATTENDING!

Have queries/ideas later, Connect with me on LinkedIn