AWS Organizations

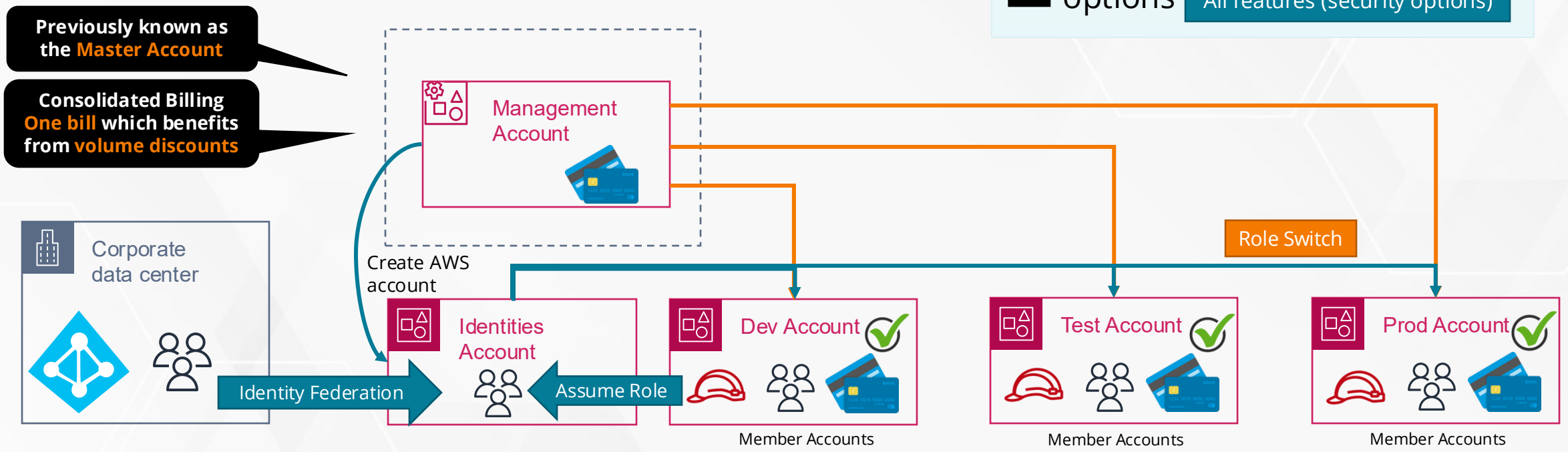
Managing multiple AWS accounts with AWS Organizations

ACADEMY

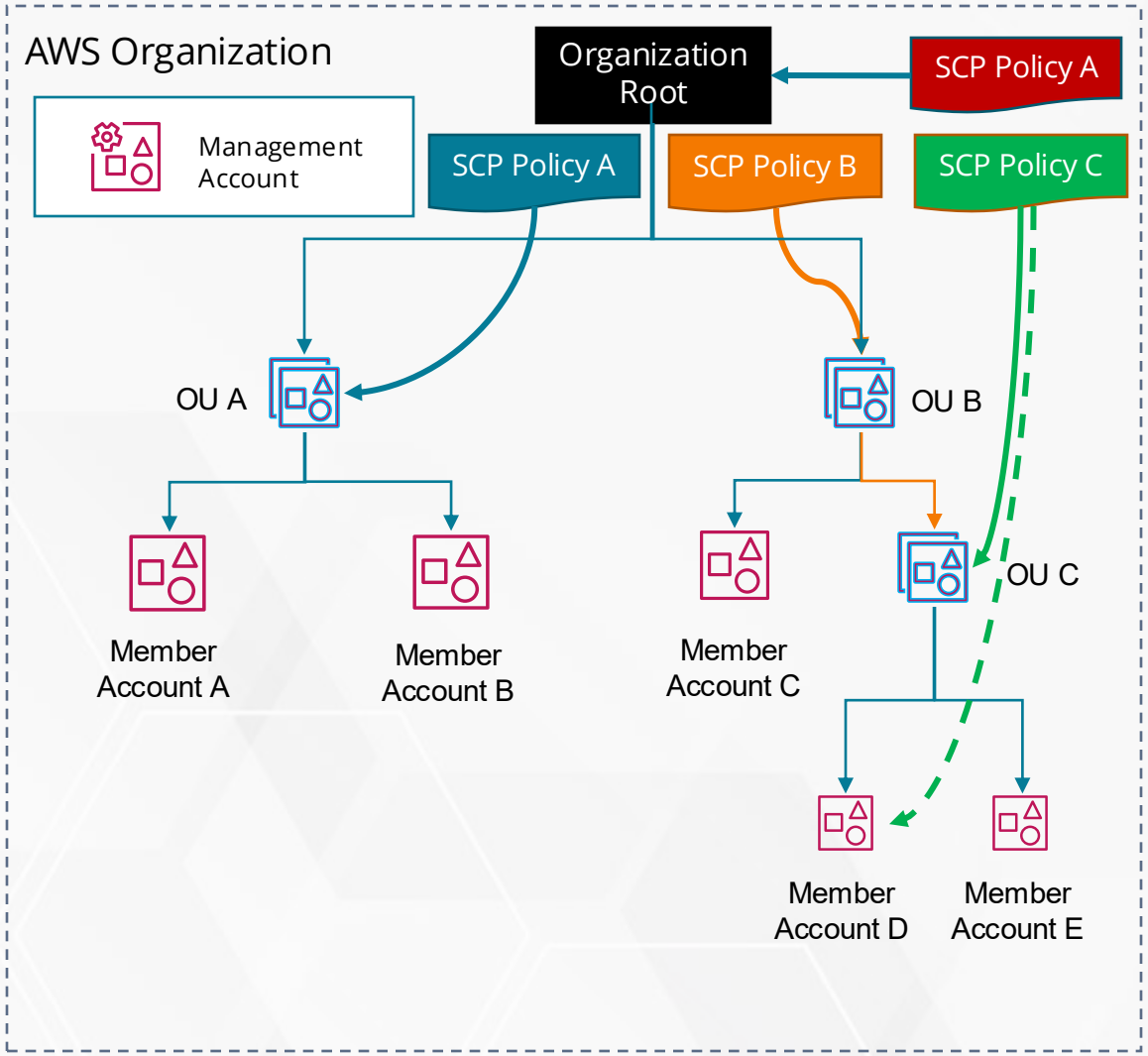
Introducing AWS Organizations

AWS Organizations is a management and governance service that enables you to centrally manage multiple AWS accounts for your business.

2 feature options
- Consolidated Billing feature
- All features (security options)



Managing Accounts with Organization Units (OUs)



An AWS organization consists of:

- A management account
- Zero or more organizational units (OUs)
  - Can have nested OUs
- Zero or more member accounts
- Zero or more policies

Benefits of OUs:

- Group similar accounts based on function using AWS Organization Units (OUs)
- Apply common policies with Service Control Policies (SCPs)
- Share common resources, e.g., Resource Access Manager (RAM)
- Provision and manage common resources
- Manage costs and benefit from volume discounts with Consolidated Billing

Organizational Units (OU) Design Principles

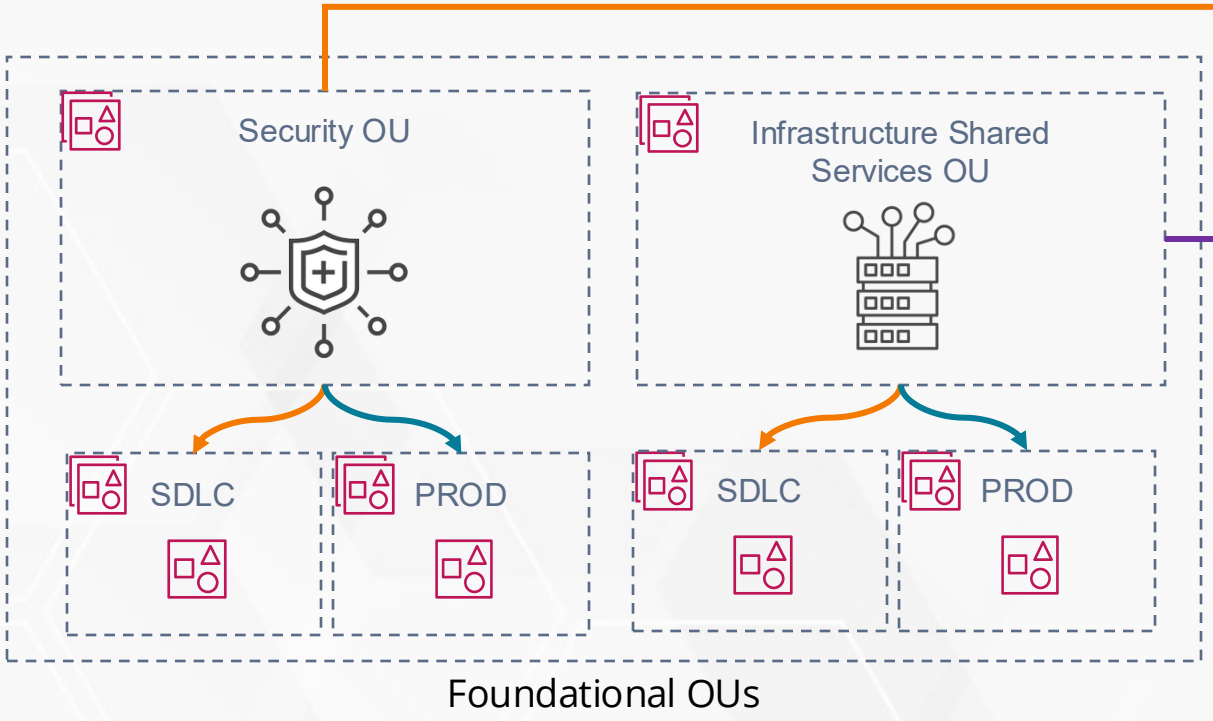
1. Organize based on security and operational needs
2. Apply security guardrails to OUs rather than accounts
3. Avoid deep OU hierarchies
4. Start small and expand as needed
5. Avoid deploying workloads to the organization's management account
6. Separate production from non-production workloads
7. Assign a single or small set of related workloads to each production account
8. Use federated access to help simplify managing human access to accounts
9. Use automation to support agility and scale

Recommended OU Architecture

Production and Non-Production (SDLC) OUs and Accounts

- Use nested OUs to separate non-production (SDLC) accounts from production (prod) accounts
- Enforce different policy configurations for non-production OUs vs prod OUs
- For commercial off-the-shelf (COTS) applications, have separate OUs – one for production accounts and another for staging accounts

Define OUs for Foundational Accounts



Log Archive Accounts – CloudTrail Logs, VPC Flow Logs, Config Logs.

Security Tooling Accounts – Detection, Data Protection and Infrastructure Protection

Security ReadOnlyAccess Accounts. - Enabling the security team to access compromised accounts with read-only access

Security Break Glass – Provide authorized security administrators with write-access to compromised accounts

Infrastructure Shared Services – Designed to host centralized resources for your organization as a whole such as DNS services, Amazon VPC endpoints, shared VPCs and subnets. Other shared services could also include Amazon Route 53 resolver endpoints for hybrid DNS and directory services.

Recommended OU Architecture

Additional OUs

Sandbox Accounts	Workloads Accounts	Policy Staging Accounts	Deployments Accounts
			
Sandbox Project A Sandbox Project B	Customer Services A Customer Services B Shared Data Lake		Customer Services A CICD Customer Services B CICD
Designed for experimentation efforts	Designed to host business and end user apps	Design to allow testing of organization wide policy changes	Design to allow critical roles played by your CI/CD tools
Used by dev teams with enforced spend limits	Workloads may include shared apps used by other workloads	Not necessary for workloads specific policies	Run CI/CD activities from Deployment accounts, not workloads environments

and more...

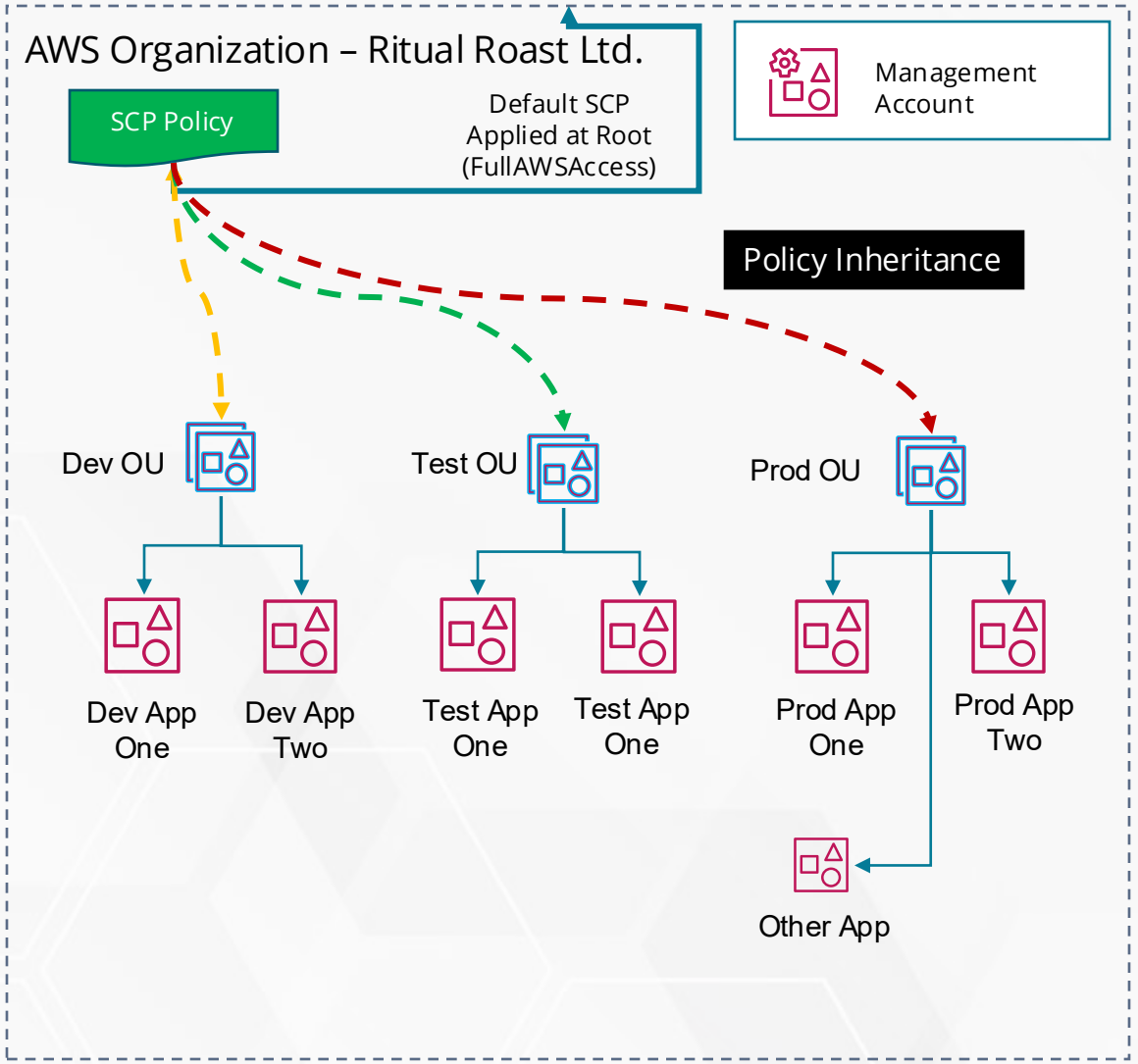
https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/organizing-your-aws-environment.html

Service Control Policies (SCPs)

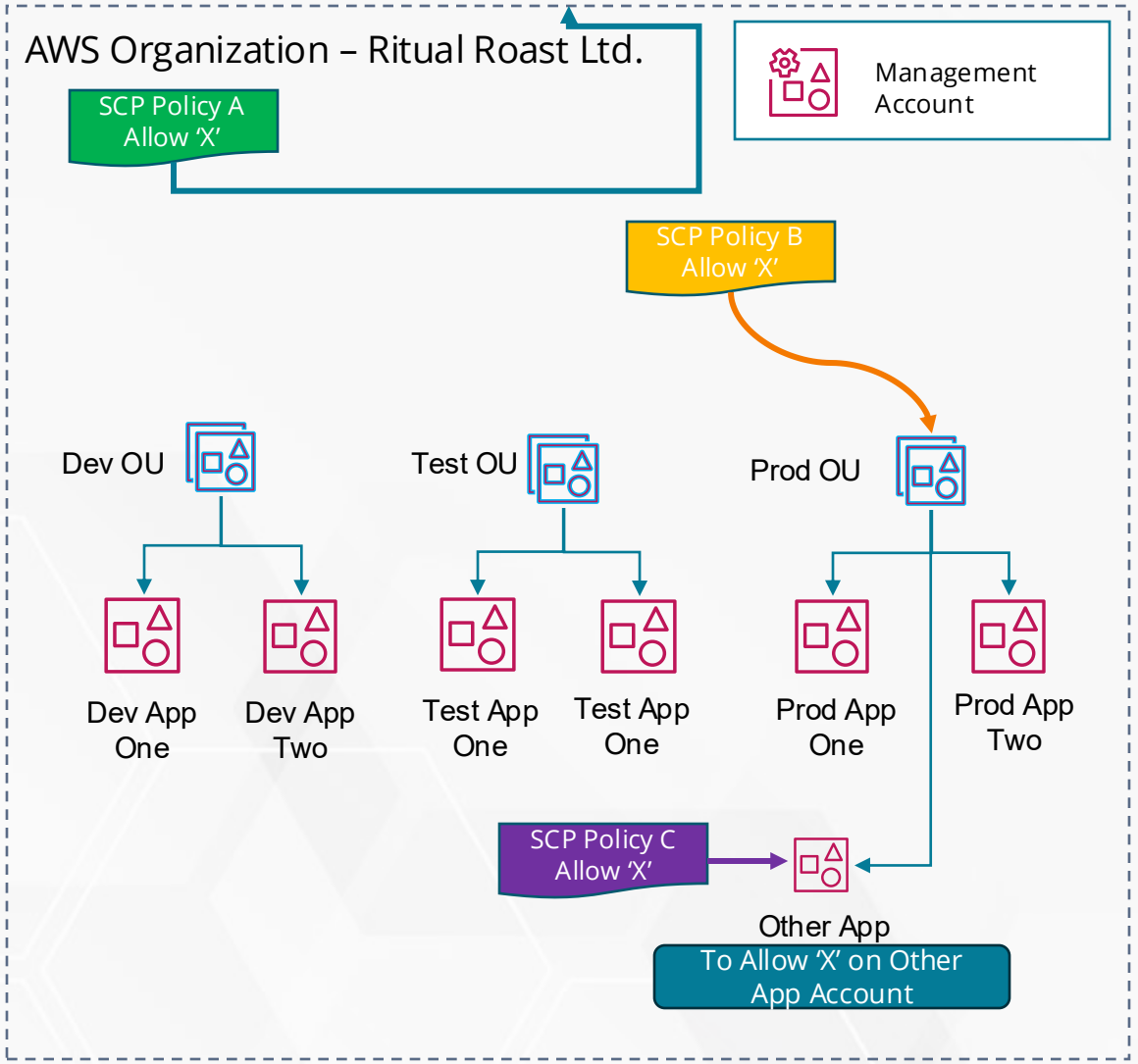
Securing your AWS accounts with Service Control Policies

IAAS ACADEMY

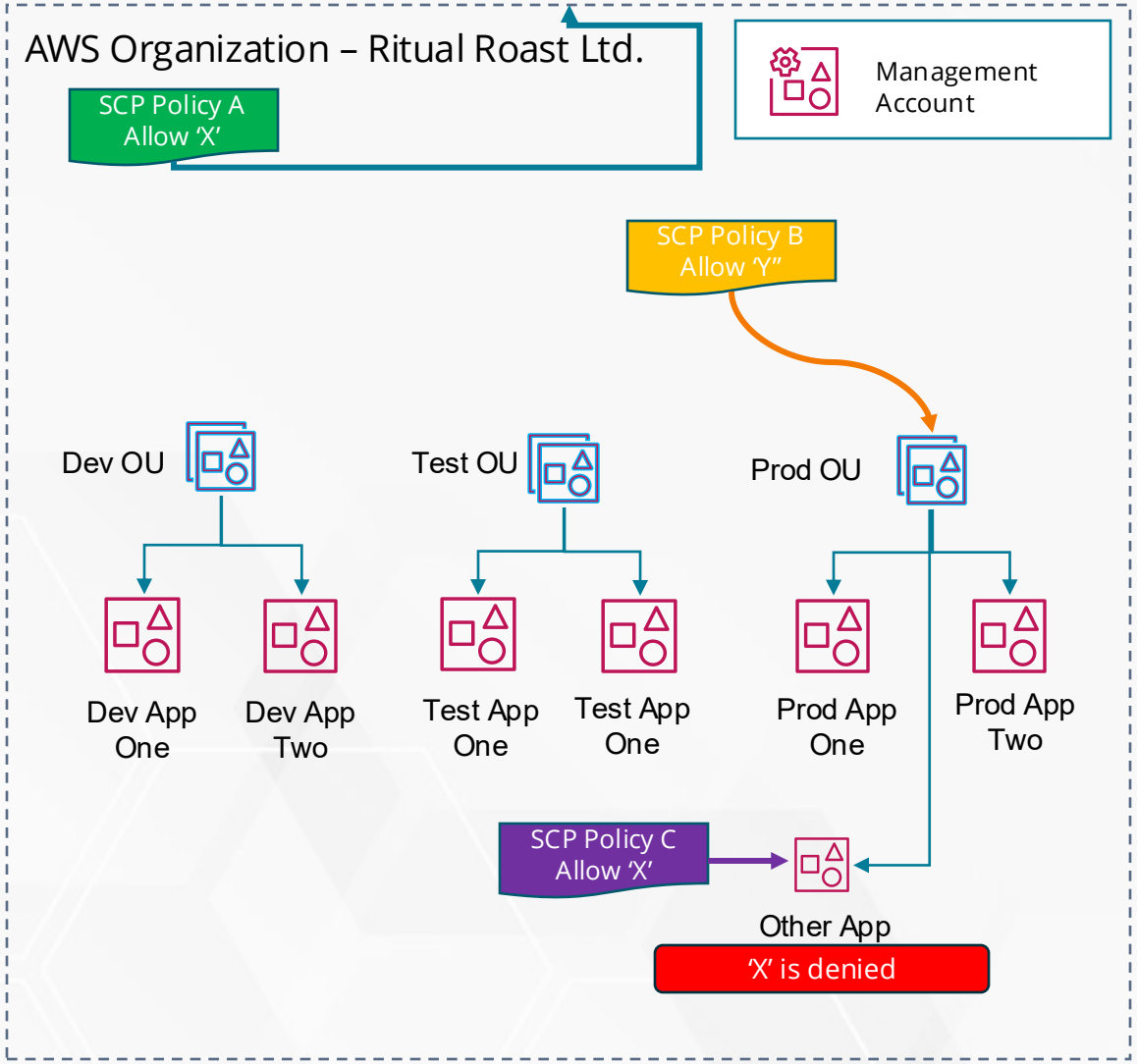
Introduction to Service Control Policies (SCPs)



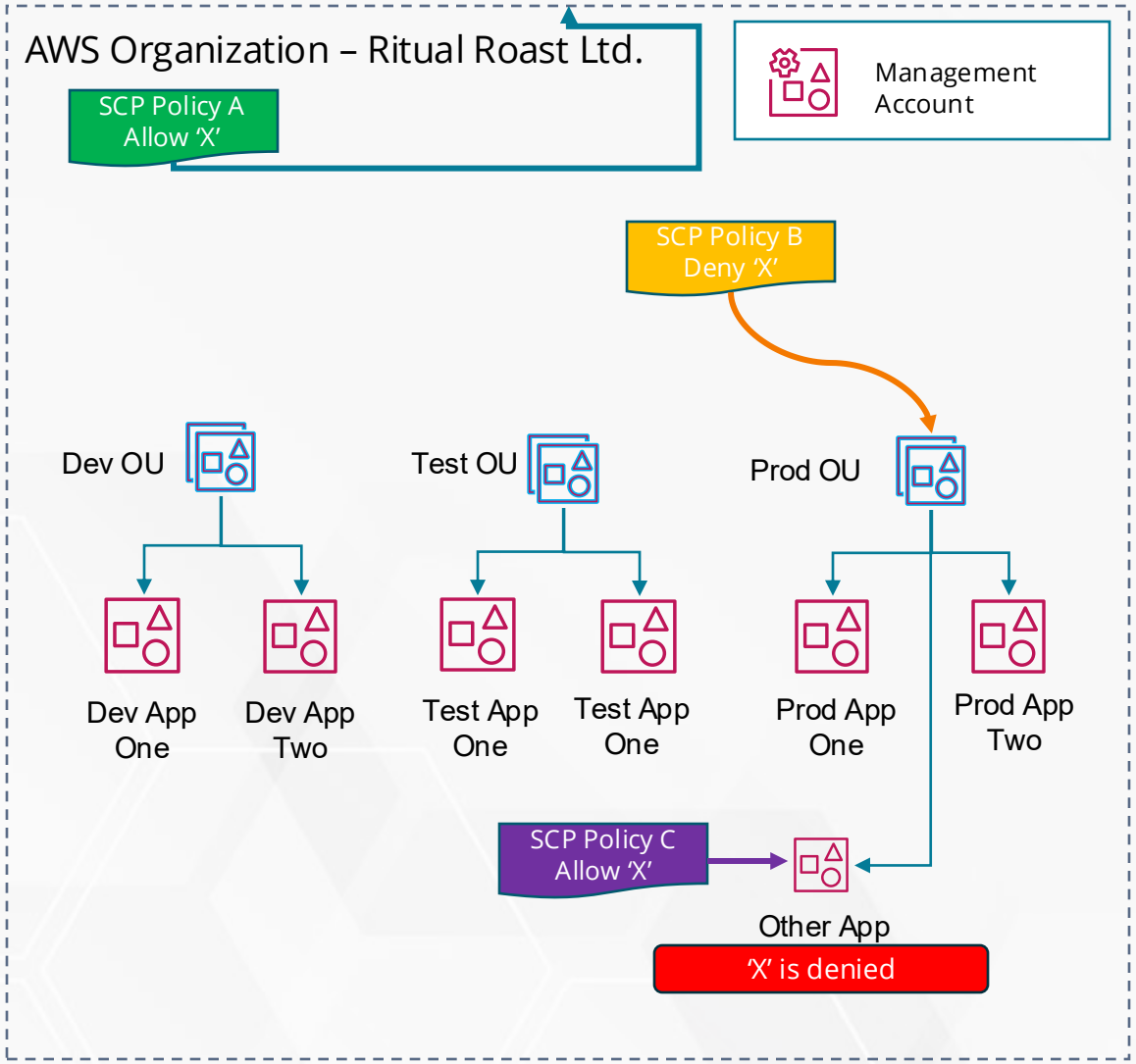
Introduction to Service Control Policies (SCPs)



Introduction to Service Control Policies (SCPs)



Introduction to Service Control Policies (SCPs)



- SCPs follow a **deny-by-default model**
- You can have multiple SCPs applied to the same OU
- To use SCPs, you must have configured your AWS Organizations with the all features enabled option.
- **SCPs are guardrails (account boundaries) – users still require identity-based or resource-based permissions to perform tasks in their AWS account**
- Effective permissions are the logical intersection between SCPs and IAM/resource-based policies
- SCPs do not affect users or roles in management accounts – only in **member accounts**.
- SCPs can restrict the actions of the root user of a member account *indirectly*
- An Allow statement in an SCP permits the Resource element to only have a **"*"** entry
- An Allow statement in an SCP can't have a Condition element

Allow list vs Deny list

- Deny List - actions are allowed by default, and you specify what services and actions are prohibited – ***This is the default setting***
- Allow List - actions are prohibited by default, and you specify what services and actions are allowed

FullAWSAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

+

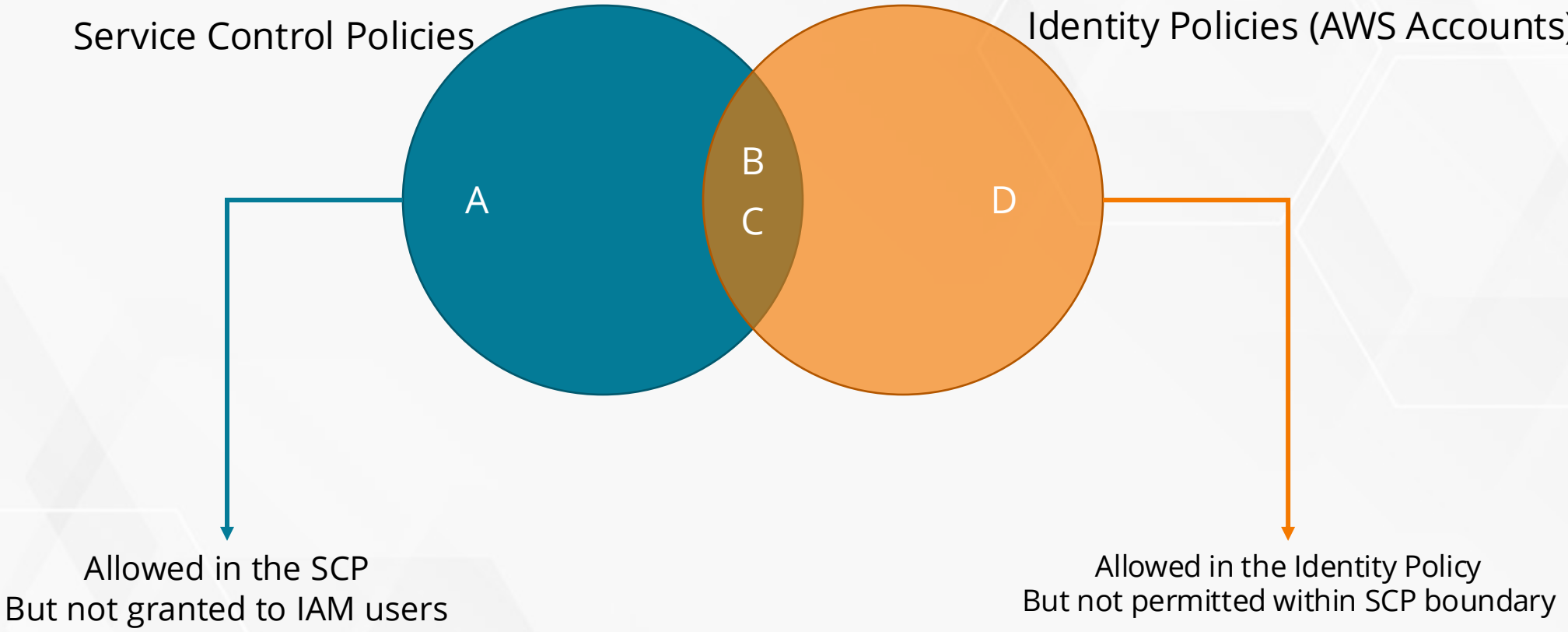
Deny DynamoDB

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "dynamodb:*",
            "Resource": "*"
        }
    ]
}
```

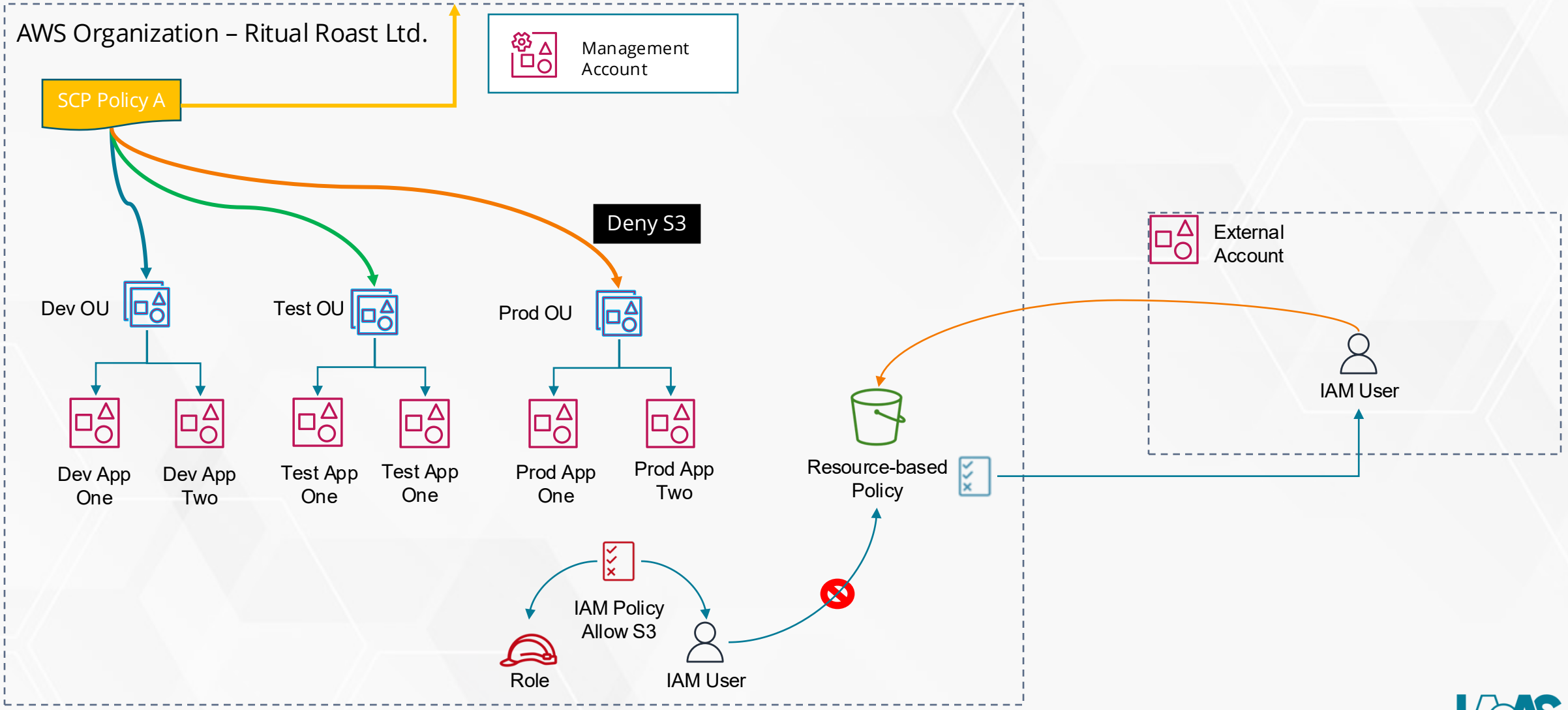
AllowS3EC2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Service Control Policies



SCPs don't affect users outside the Organization

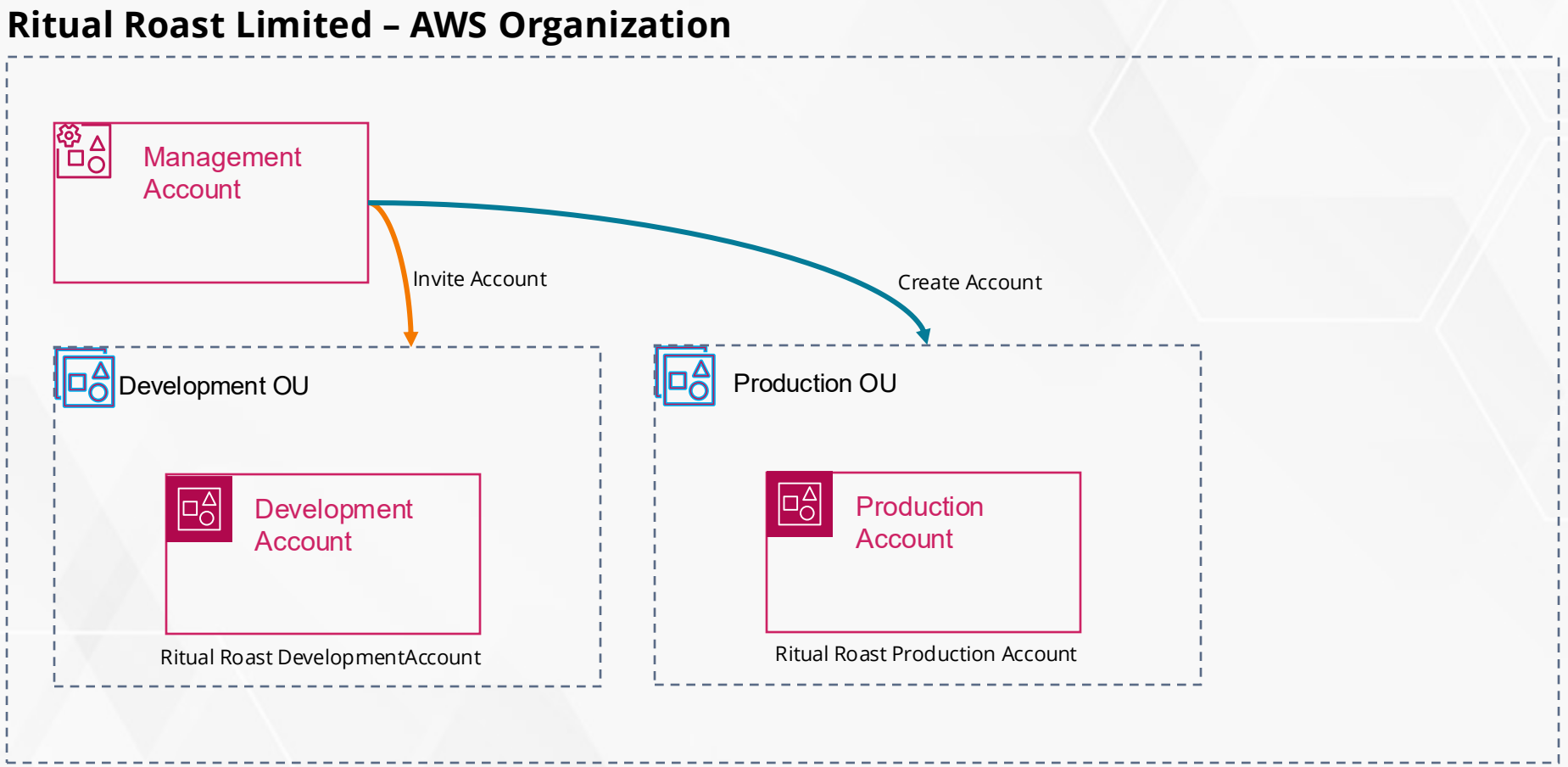


Create AWS Organizations, OUs and Accounts

Set up an AWS Organizations, OUs and AWS Member Accounts

AWS ACADEMY

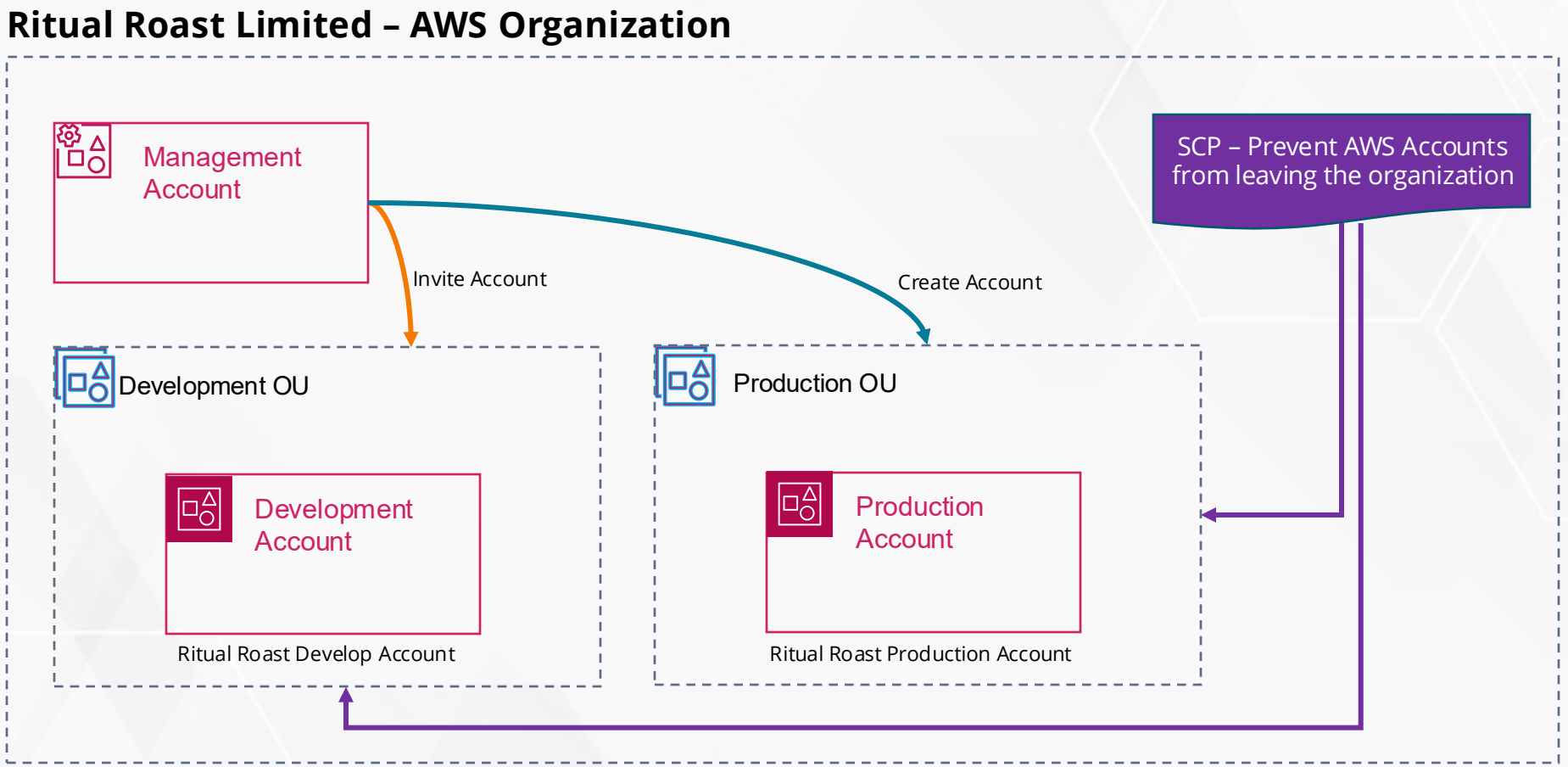
Lab – AWS Organizations, OUs and Accounts



Create AWS Organizations SCPs

Enable and configure Service Control Policies (SCPs) for AWS Organizations

Lab – Create AWS Organization and OUs

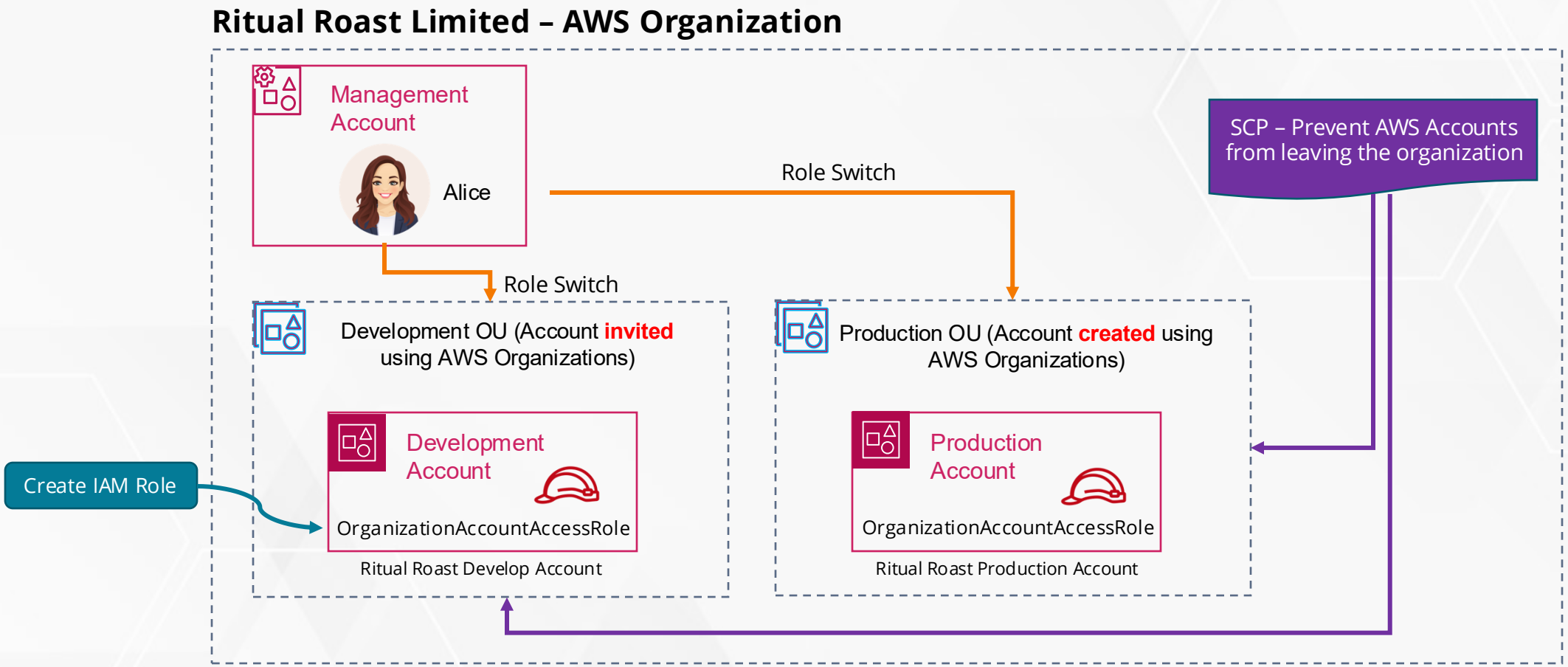


AWS Organizations and Cross-Account Access

Configure Cross-Account Access between AWS management account and member accounts

AWS ACADEMY

Lab – AWS Organizations & Cross Account Access



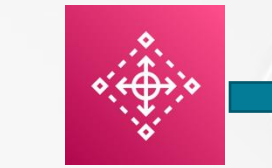
AWS Control Tower

Building Landing Zones on AWS

ACADEMY

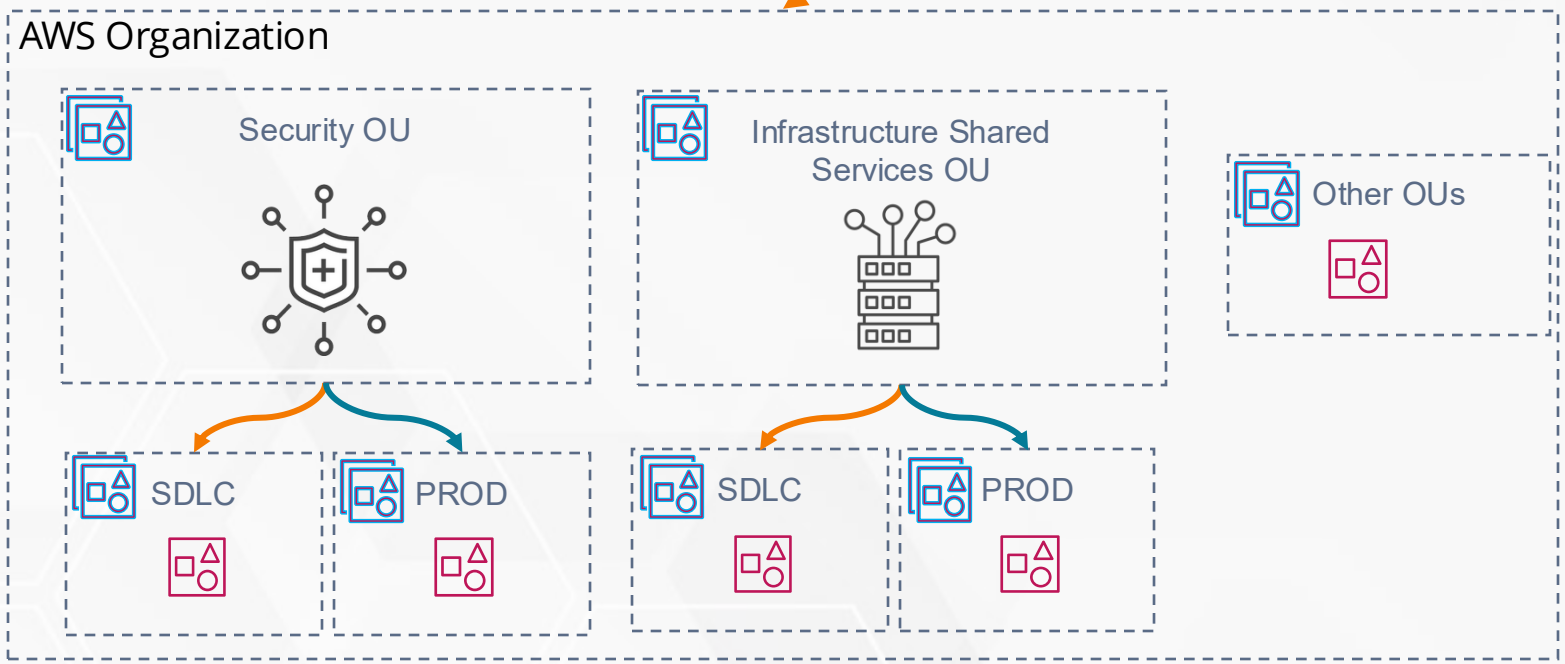
What is AWS Control Tower?

AWS Control Tower is an orchestration and governance service that can help you define your AWS Multi-Account strategy using tools like AWS Organizations, AWS Service Catalog and AWS IAM Identity Centre (previously known as AWS Single-Sign-On)



AWS Control Tower

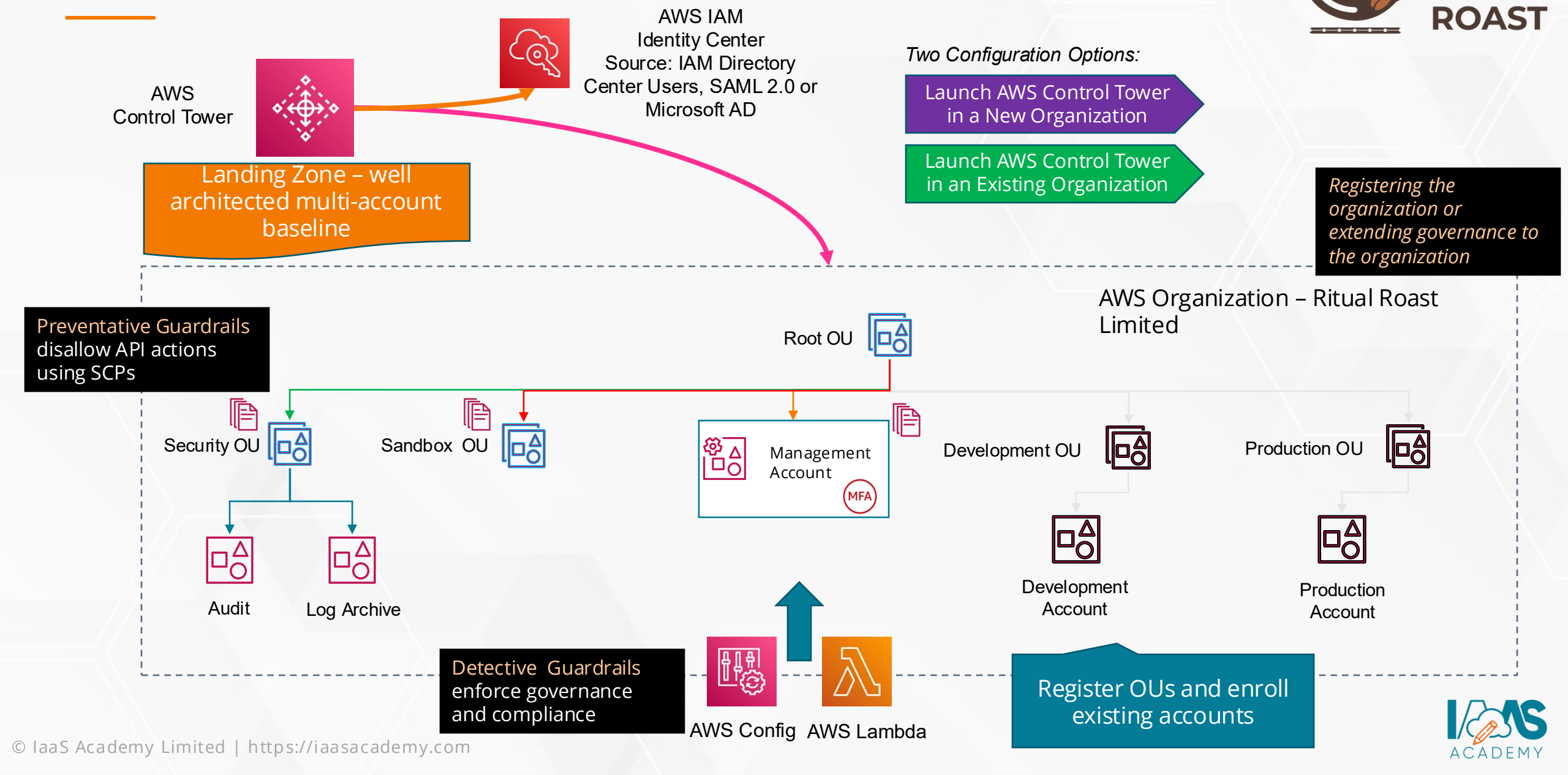
Landing Zone – *a well-architected, multi-account environment based on AWS recommended security and compliance best practices*



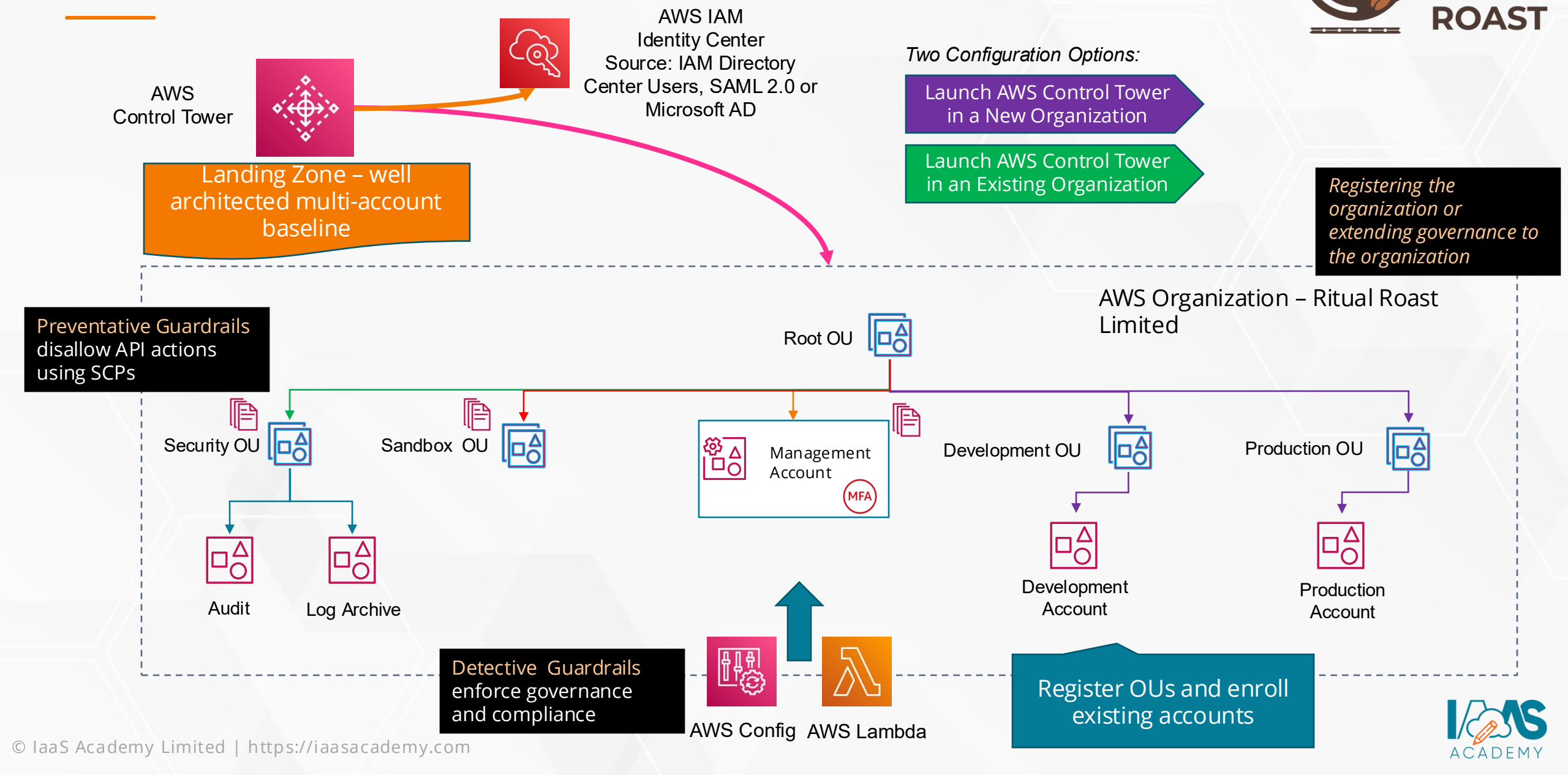
Key Features:

- **Landing Zone** – well-architected baseline multi-account environment.
- **Controls** – also known as guardrails (e.g., SCPs) - provide governance to your AWS environment and comprise *preventative*, *detective* and *proactive* controls.
- **Account Factory** – create new accounts using a configurable template. Control Tower can automate the account provisioning and enrollment for governance
- **Dashboard** – oversight into your landing zone and central administrative views

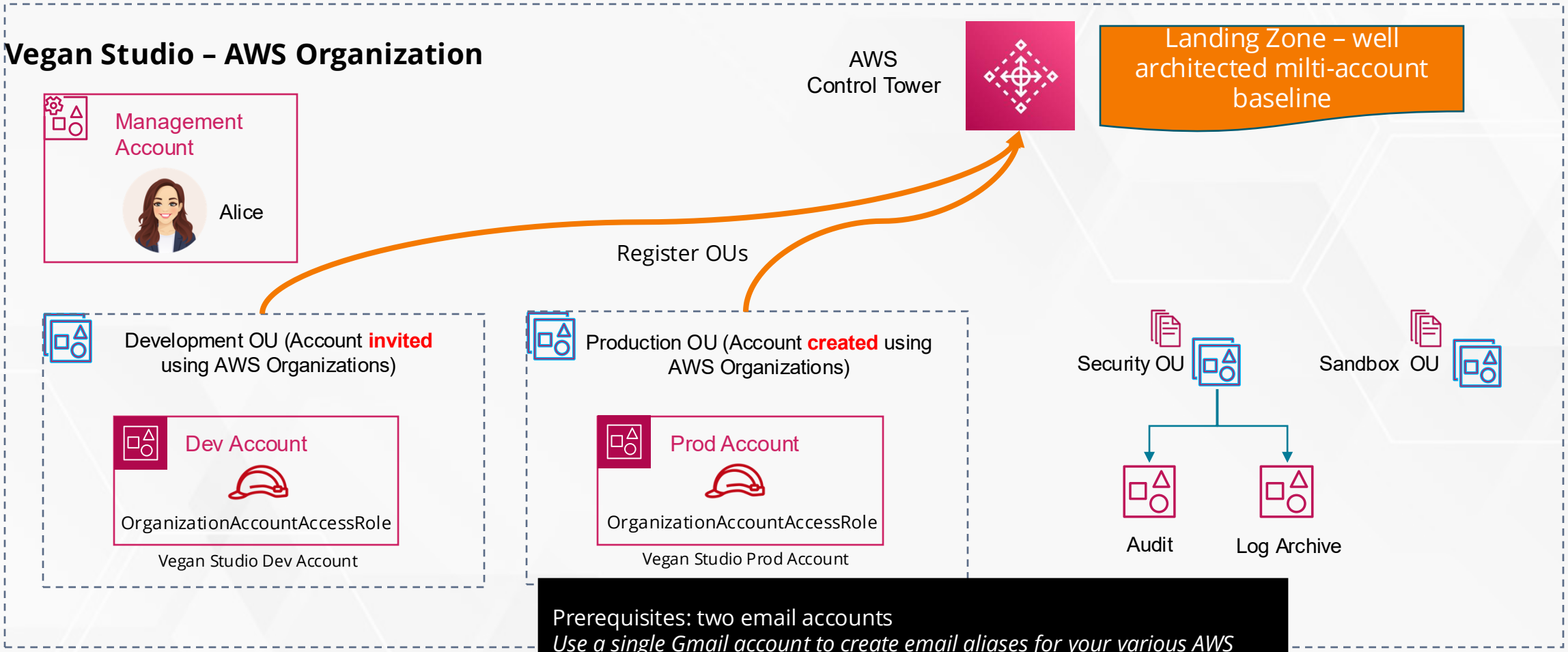
How it works?



How it works?



Setup Control Tower for an existing AWS Organization



Prerequisites: two email accounts

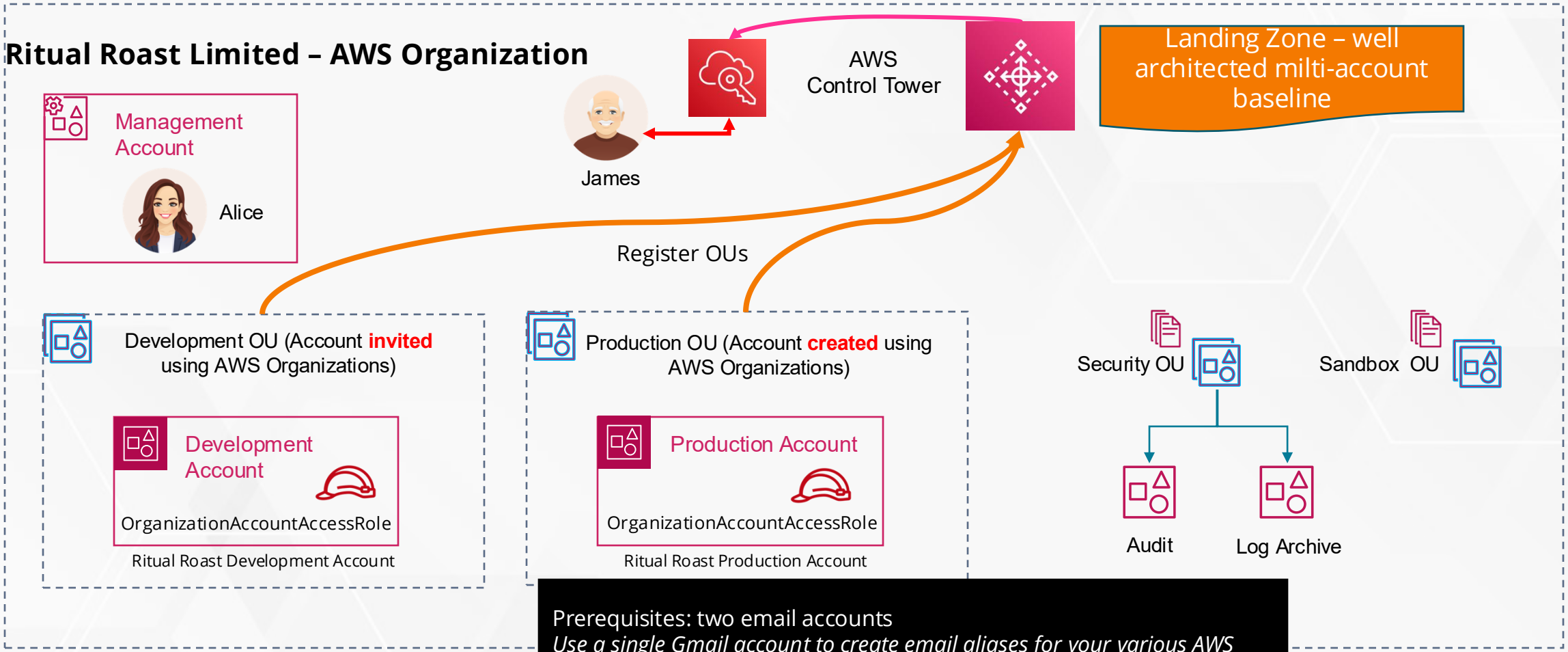
Use a single Gmail account to create email aliases for your various AWS accounts by simply adding the '+' sign followed by a combination of words at the end of your username but before the '@' sign. For this example, you can use mycompany+audit@gmail.com or mycompany+logarchive@gmail.com, where 'mycompany' is your Gmail username.

AWS Control Tower – LAB

Setup and Configure AWS Control Tower

ACADEMY

Control Tower for existing AWS Organization



Prerequisites: two email accounts

Use a single Gmail account to create email aliases for your various AWS accounts by simply adding the '+' sign followed by a combination of words at the end of your username but before the '@' sign. For this example, you can use mycompany+audit@gmail.com or mycompany+logarchive@gmail.com, where 'mycompany' is your Gmail username.

AWS Control Tower – LAB Part 2

Setup and Configure AWS Control Tower

ACADEMY