Guidance for Change Management on AWS

AWS Organizations

management account

1 AWS Config

member account *n*

1 AWS Config

security organizational unit (OU)

log archive

1 AWS Config

4 S3 bucket *AWS Config*

infrastructure organizational unit (OU)

Operation tooling account

3 AWS Config *aggregator*

2 AWS Systems Manager

AWS CloudFormation

AWS Reference Architecture

---
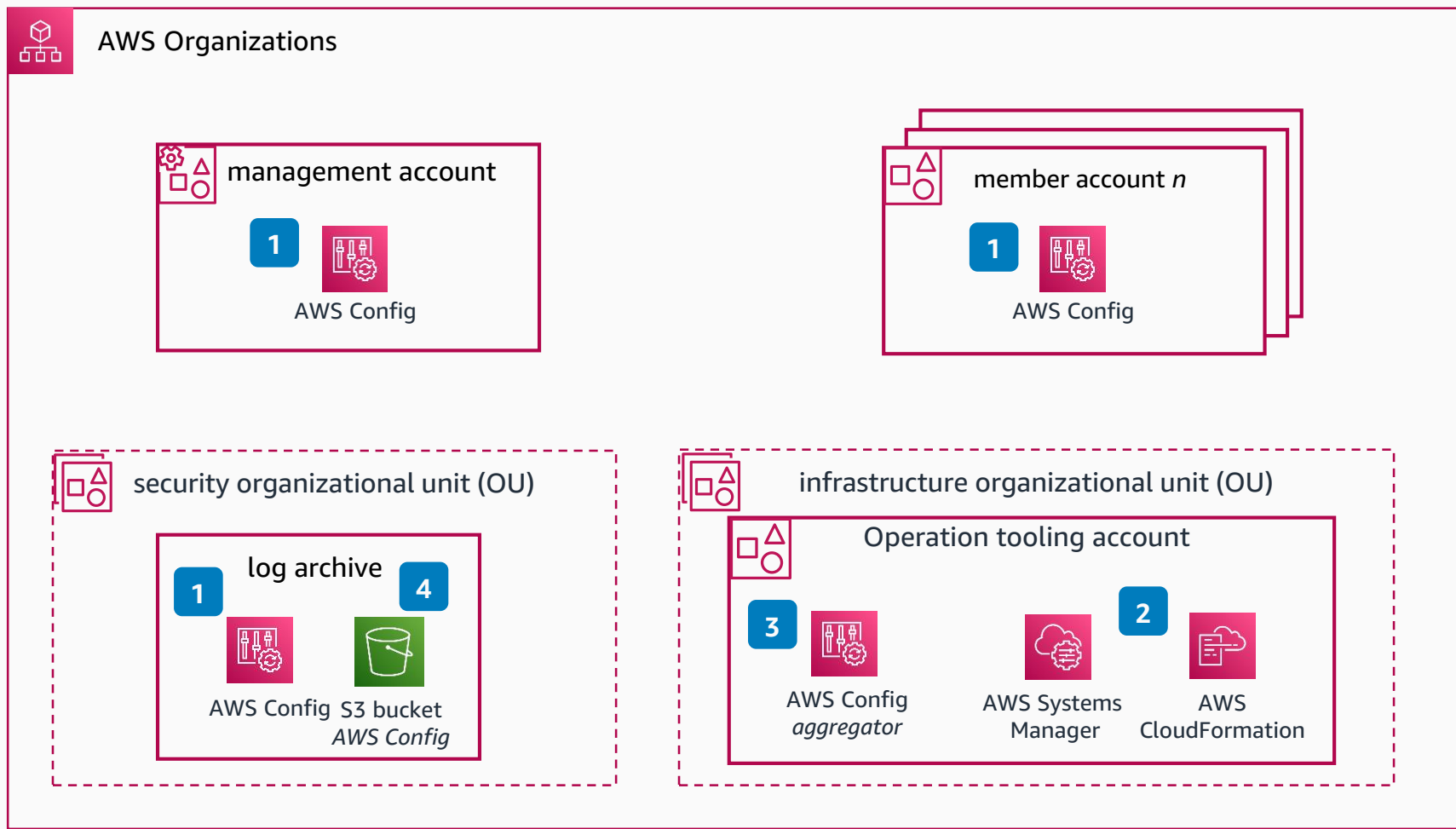
1 **(CF30 - S1)** Deploy an **AWS Config** recorder and delivery channel in the management account and all member accounts to track changes of all **AWS Config** supported resources. Note: **AWS Control Tower** will automatically deploy **AWS Config** and delivery channels in all **AWS Control Tower** managed member accounts and regions.

2 **(CF30 – S2)** Use **AWS Organizations** to delegate the administration of **AWS Systems Manager** and **AWS CloudFormation** to the operation tooling account. This will allow you to deploy changes by automation to accounts within your organization. For application-specific changes, we recommend using an application deployment account (not depicted here).

3 **(CF30 – S4)** Enable and configure an **AWS Config** aggregator in your operations tooling account to provide visibility to the resources, resource configurations, and changes in your organization.

4 **(CF30 – S4)** Configure all **AWS Config** delivery channels to send **AWS Config** snapshots and history to a centralized **Amazon Simple Storage Service** (Amazon S3) bucket in your log archive account to maintain a record of all historical changes. Note: If you are using **AWS Control Tower**, each **AWS Config** recorder has a delivery channel configured to send to the **AWS Control Tower S3** log bucket.