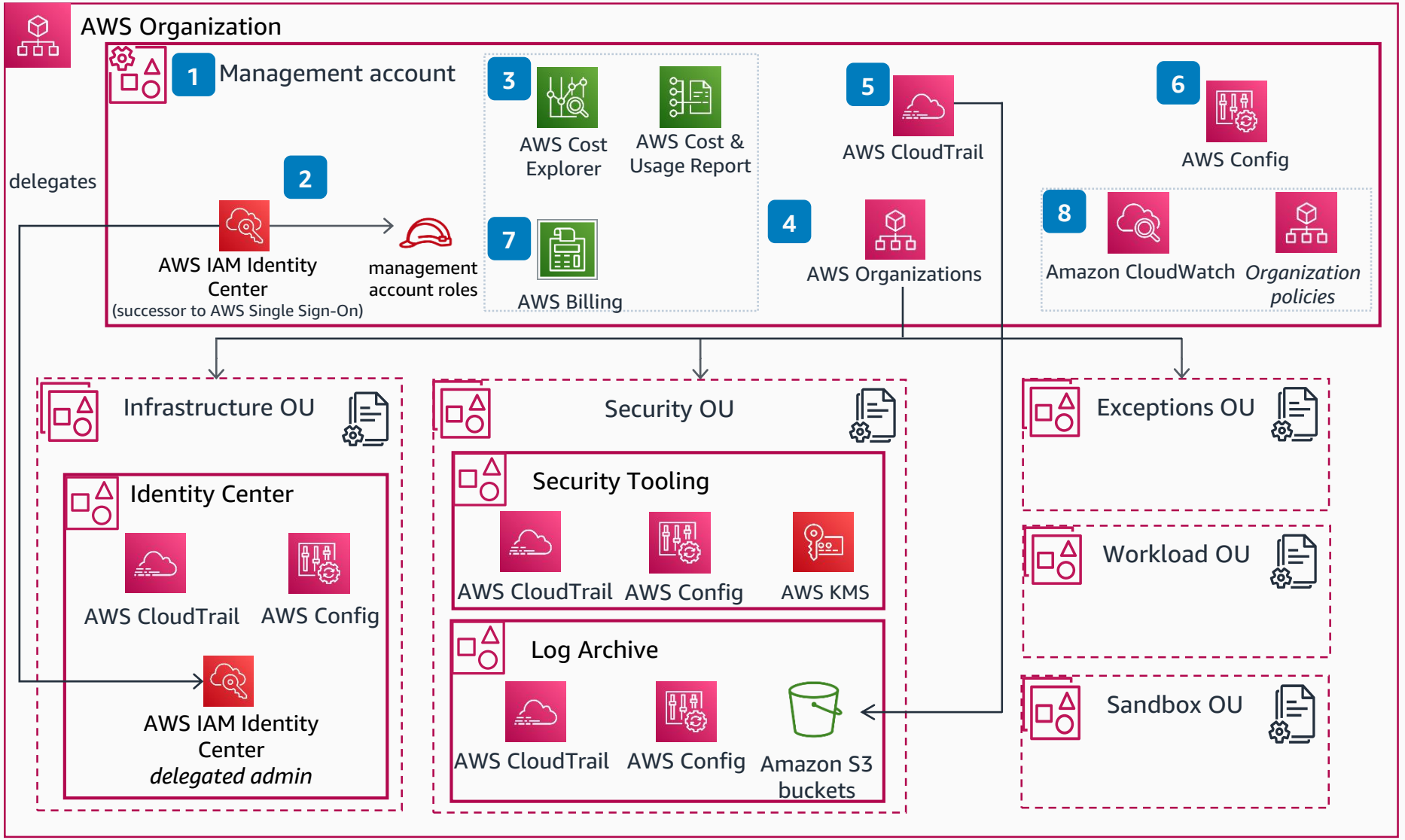
Guidance for Establishing an Initial Foundation using AWS Organizations



(CFLZ2-P1) Before you begin, identify a method to name your AWS accounts and determine the Regions you want to manage and operate in AWS.

1 **(CFLZ2-P2)** Create an AWS account with the AWS Management Console. Use a planned naming convention for root user email and account alias. Secure root user account and configure billing and tax information.

2 **(CFLZ2-P3)** Create and configure **AWS IAM Identity Center** and standard management account roles for administrative management. Apply security configurations to **IAM Identity Center** settings.

3 **(CFLZ2-P3)** Activate **AWS Cost Explorer** and create and configure **AWS Cost & Usage Reports**.

4 **(CFLZ2-P4)** Plan and deploy your foundational Organization Unit (OU) structure and accounts from **AWS Organizations**.

5 **(CFLZ2-P5)** Set up **AWS CloudTrail** to deploy **CloudTrail** to all AWS member accounts to deliver logs to a Log Archive **Amazon Simple Storage Service** (Amazon S3) bucket. Secure your log data using an **AWS Key Management Service** (AWS KMS) customer managed key.

6 **(CFLZ2-P6)** Deploy **AWS Config** to all accounts within the organization. Configure delivery of resource changes to a Log Archive S3 Bucket. Secure the log storage using an **AWS KMS** customer managed key.

7 **(CFLZ2-P8)** Create and publish a Tagging dictionary and enable Cost Allocation Tags.

8 **(CFLZ2-P9)** Deploy additional foundational security hardening configurations to your environment, using services such as **Amazon CloudWatch**.

Reviewed for technical accuracy April 17, 2023

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture