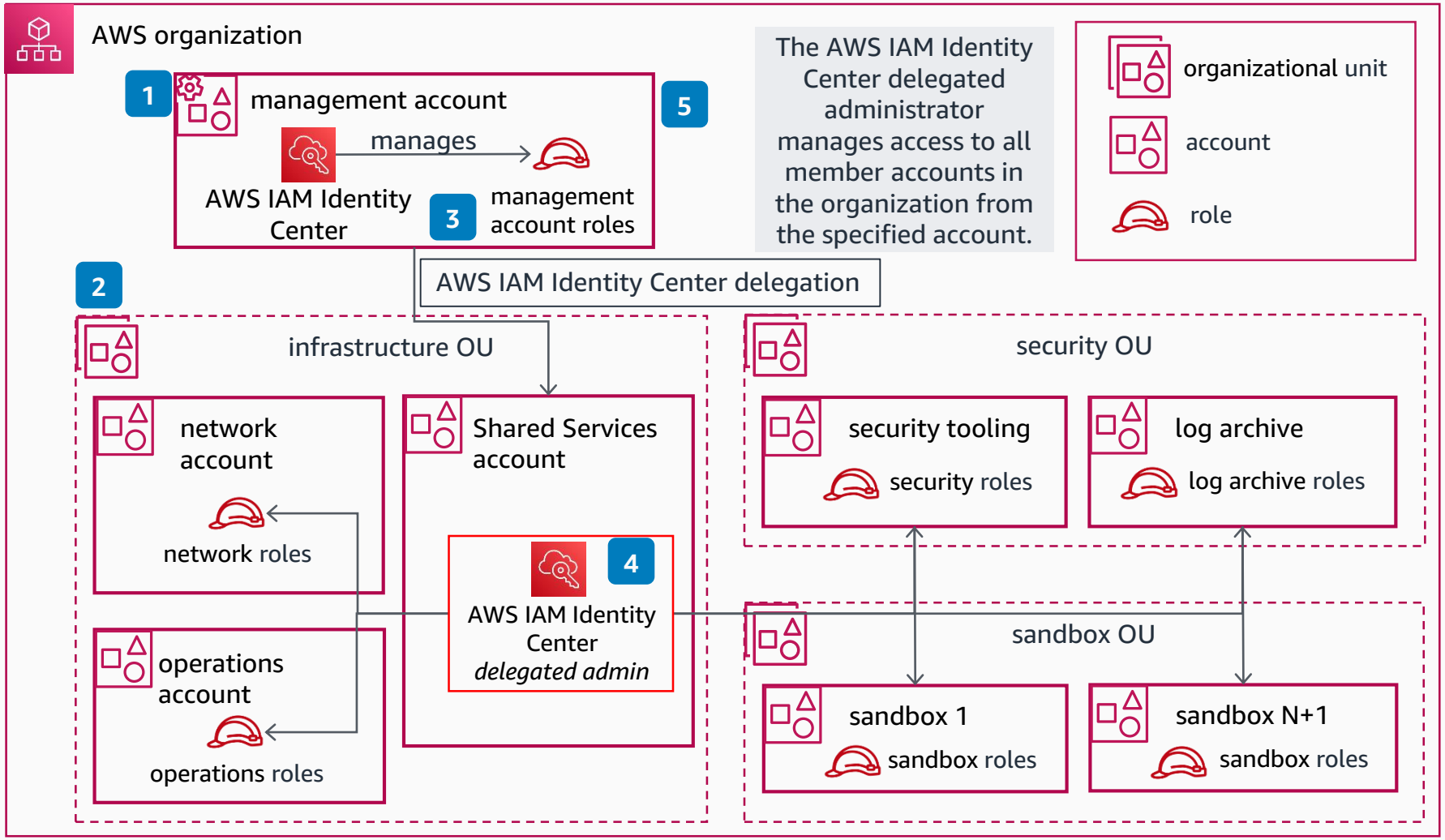
Guidance for Identity Management and Access Control on AWS



1 **(CF2 - S2)** On your management account, create an **AWS IAM Identity Center** instance and set up your organization.

2 **(CF2 – S1)** Create the initial set of recommended accounts to configure your foundation. Follow the recommendations included in the Production Starter Organization.

3 **(CF2 - S2)** Connect to your external IdP, or create the Users and Groups within **AWS IAM Identity Center** to organize access across your environment. Create permission sets for access to your management account and assign them to the management account users

4 **(CF2 – S6)** Delegate **AWS IAM Identity Center** to your Shared Services account, log in with the **AWS IAM Identity Center** role, create permission sets, and assign them to the groups and users for the member accounts in your AWS organization.

5 **(CF2 – S5)** Using your **AWS IAM Identity Center** role to administer the management account, create Preventive Controls using Service Control Policies in the management account, and delegate the security, network, and operation services to their corresponding AWS accounts in your environment.

Reviewed for technical accuracy September 27, 2022

AWS Reference Architecture