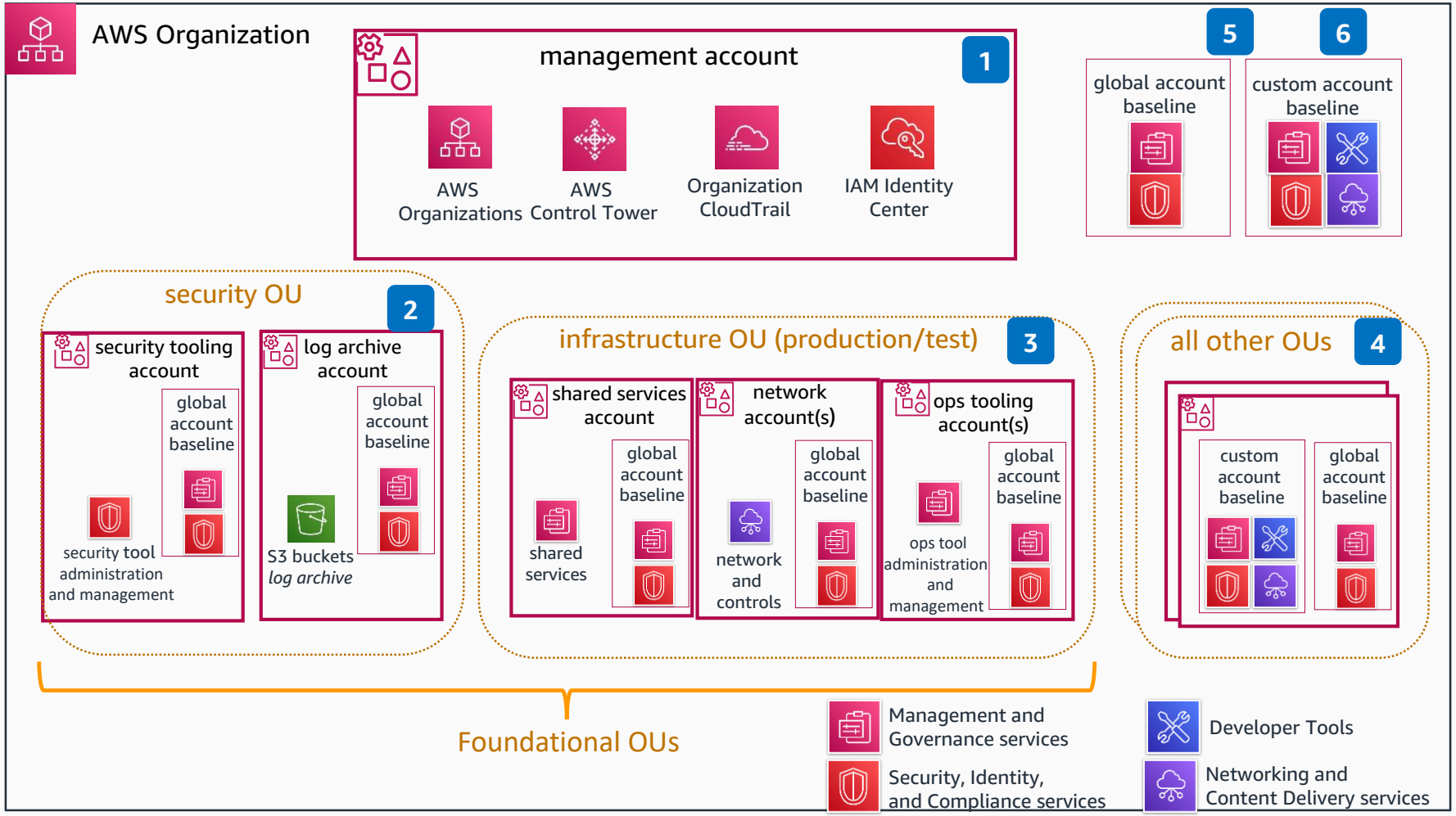
Guidance for Workload Isolation Boundary on AWS



1 **(CF7-S2)** The management account, also known as the payer account, is the AWS account where you enable **AWS Control Tower**. Control Tower enables **AWS Organizations**, an **Amazon CloudTrail** Organization Trail, and **AWS Identity and Access Management** (AWS IAM) Identity Center. (IAM Identity Center can be delegated to a Shared Services account.) The global account baseline should be applied to the management account. **Control Tower** is managed from this account, including the management of **Control Tower** detective and preventative guardrails.

2 **(CF7-S3)** The security organization unit (OU) is a foundational OU that should not contain any business applications. It is created by **Control Tower.** Your security organization should own and manage this OU, along with any child OUs and associated accounts. **Control Tower** creates a log archive and security tooling (sometimes called audit) account. The security tooling account should be used to manage the security services in the organization. This is achieved by delegating the management of supported security services to this account. The log archive account is the central aggregation point for organization audit, security, network, and application logs.

3 **(CF7-S2)** The Infrastructure OU is intended to contain shared infrastructure services. The accounts in this OU are also considered administrative, and your infrastructure and operations teams should own and manage this OU, any child OUs, and associated accounts. The infrastructure OU holds the following accounts: network account(s), operational account(s), and shared services account(s).

4 **(CF7-S1)** Organization units should be designed strategically by grouping accounts based on similar security, network, and access requirements.

5 **(CF7-S4)** Controls, services, and configuration that should be deployed and configured to *all* accounts in the organization are referred to as *global account baselines*. **Control Tower** provides an account baseline in all **Control Tower**-managed accounts and Regions, which includes **AWS CloudTrail**, **AWS Config**, deleting of default VPC components, and some preventative and detective guardrails. Additional controls, services, and configuration may also be required, and a mechanism to apply these to all newly created accounts should exist. There are some exceptions to this. For example: this baseline won't necessarily be deployed to accounts within the exceptions OU, and service control policies (SCPs) don't apply to the management account.

6 **(CF7-S5)** Controls, services, and configuration that may differ between Organization units are referred to as custom account baselines. For example, controls, network connectivity, and security and operational tool requirements may differ between production, nonproduction, or sandbox environments. To support scaling out of the organization, accounts should be organized logically within OUs so that these baselines can be configured for all accounts within an OU or multiple OUs, and not configured at the account level.

Reviewed for technical accuracy October 10, 2022

AWS Reference Architecture