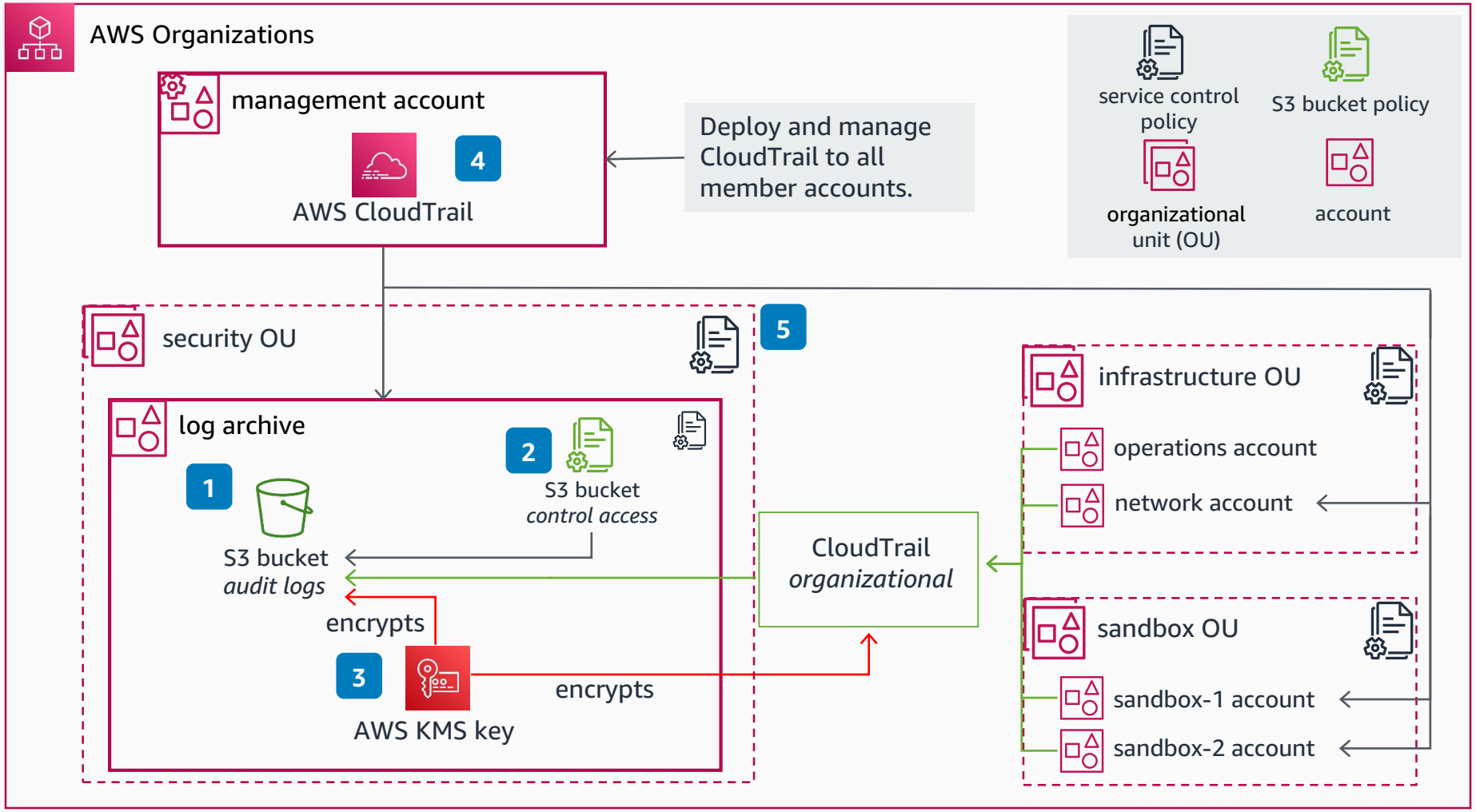
Guidance for Log Storage on AWS



1 **(CF1 - S1)** In your log archive account, create an **Amazon Simple Storage Service** (Amazon S3) logging bucket for your **AWS CloudTrail** instance.

2 **(CF1 - S2)** Configure the bucket policy to allow **CloudTrail** to write objects. Configure the ownership of the objects delivered to the bucket to be transferred to the log archive account.

3 **(CF1 - S1)** In the log archive account, in the same Region you created your bucket, create an **AWS Key Management Service** (AWS KMS) key. Use it to encrypt the bucket at rest.

4 **(CF1 - S2)** Sign back in to your management account, and deploy an organizational **AWS CloudTrail** instance to all your accounts in your organization. Use the **AWS KMS** key to encrypt the trail, and use the bucket in the log archive account as the recipient of the events recorded by the trail.

5 **(CF1 - S3)** Deploy service control policies across the organization and to the log archive account to protect the logs stored in the bucket and the trail in your organization, so it does not stop recording or get deleted.

Reviewed for technical accuracy November 8, 2022

AWS Reference Architecture