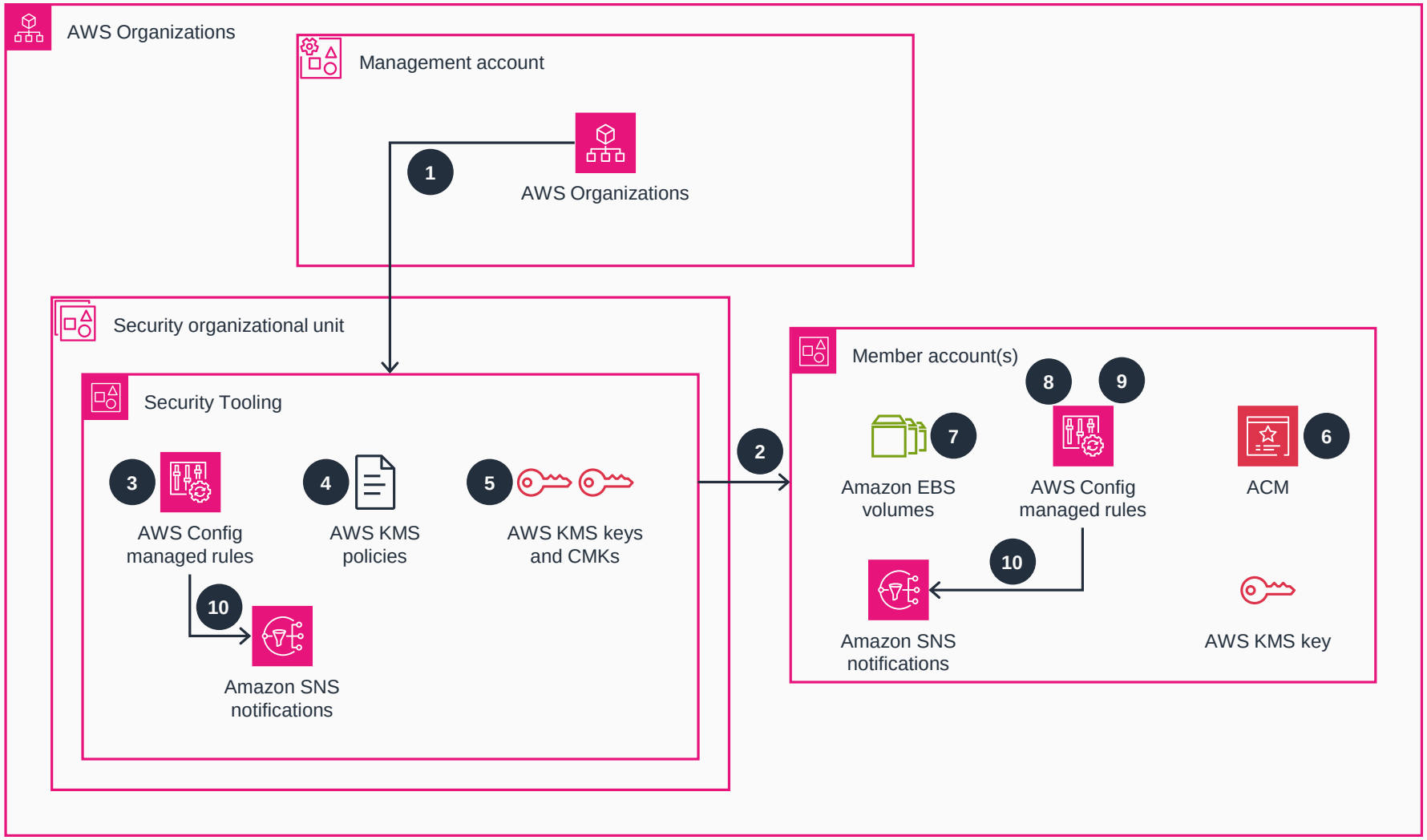
Guidance for Encryption & Key Management on AWS

This architecture diagram shows how to implement a customized encryption and key management strategy on AWS, enabling you to encrypt data at rest and in transit, provide least privilege access to keys, report on anomalies, and rotate keys.



1. Deploy and configure an AWS Security Tooling account for central key storage operations and sharing with **AWS Organizations**.
2. Enable **AWS Key Management Service (AWS KMS)** automatic key rotation for **AWS KMS** key lifecycle management.
3. Deploy an **AWS Config** managed rule to monitor **AWS KMS** lifecycle management in the Security Tooling account.
4. Configure **AWS KMS** key policies to allow secure access across **Organizations**.
5. Use AWS-managed **AWS KMS** keys and customer managed keys (CMKs) as required by your governance requirements.
6. Use **AWS Certificate Manager (ACM)** to automate the generation and management of SSL certificates.
7. Enforce **Amazon Elastic Block Store (Amazon EBS)** volume default behavior to be encrypted on generation. Monitor the encryption using **AWS Config** managed rules on all **Organizations** member accounts.
8. Deploy **AWS Config** managed rules to monitor the encryption of AWS services with network connections.
9. Deploy **AWS Config** managed rules to monitor the encryption of AWS services with persistent data.
10. Receive notifications for compliance using **Amazon Simple Notification Service (Amazon SNS)**.

Reviewed for technical accuracy February 20, 2024

AWS Reference Architecture