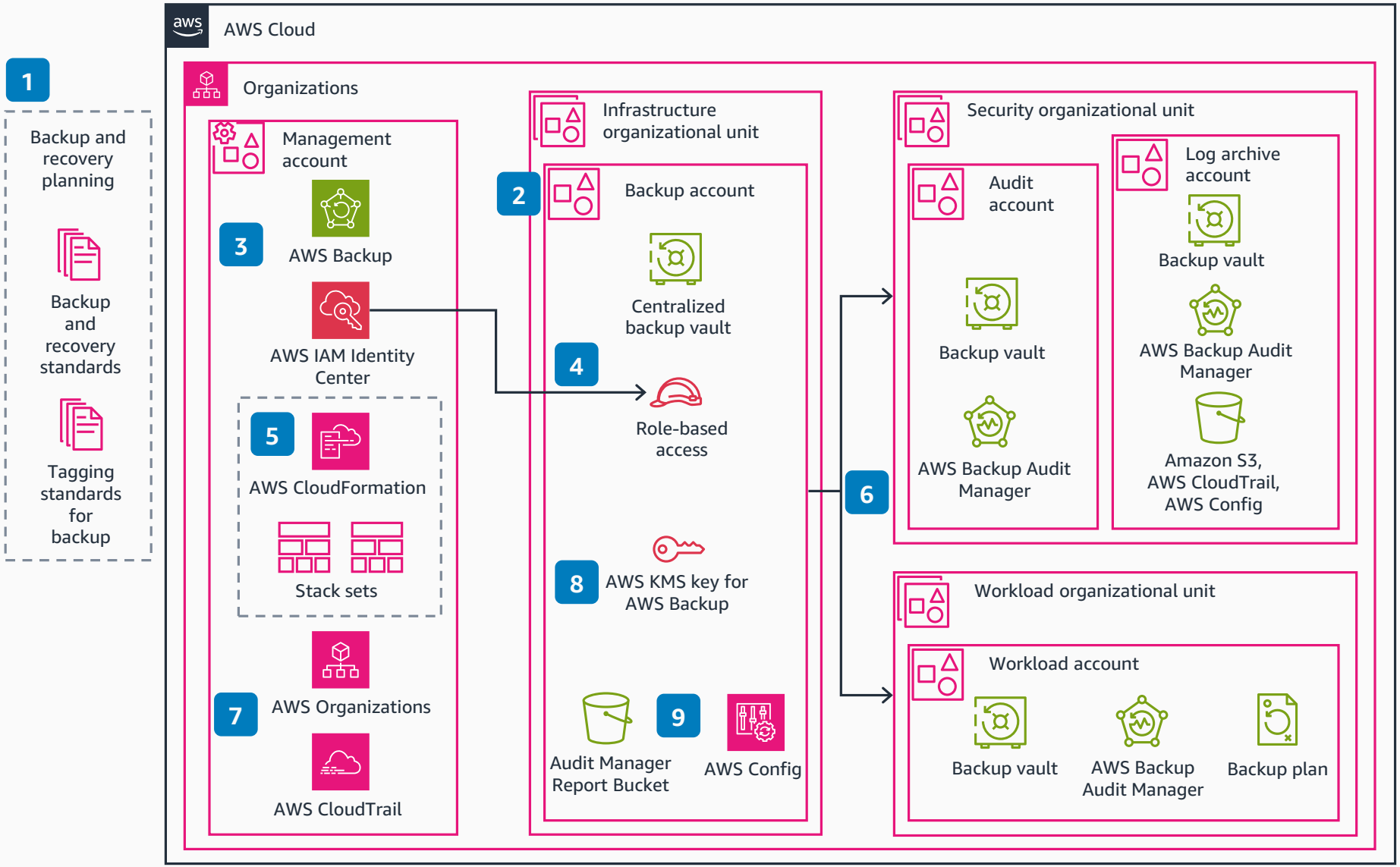
Guidance for Backup & Recovery on AWS

This architecture diagram shows a clear, scalable, and iterative way to set up backup and recovery within your cloud environment.



1. Create and publish backup, recovery, and tagging standards for backup operations.
2. Create a central backup AWS account to centralize all backups in **AWS Organizations**.
3. Activate **AWS Backup** in **Organizations** and delegate backup management to the central backup account.
4. Deploy role-based access for backup management through **AWS IAM Identity Center** (successor to AWS Single Sign-On).
5. Deploy **AWS Backup** supporting resources, such as backup vaults, through **AWS CloudFormation** service-managed stack sets.
6. Configure backup policies, create a default **AWS Backup** policy for **Organizations**, and attach **AWS Backup** policies to the organizational units in **Organizations**.
7. Implement preventative guardrails through service control policies to protect **AWS Backup** resources.
8. Encrypt backup data with a centralized **AWS Key Management Service** (AWS KMS) key.
9. Centralize monitoring and alerting through **AWS Config** and AWS Backup Audit Manager.

Reviewed for technical accuracy August 29, 2023

AWS Reference Architecture