DOMAIN 6: MANAGEMENT AND SECURITY GOVERNANCE

Core Competency
- Design and implement security governance controls
- Enforce organizational security policies
- Manage multi-account architectures
- Ensure audit and compliance readiness using native AWS tools

6.1 Design and Implement Governance Controls
AWS Organizations Features
- Use Organization Units (OUs) to group accounts by function/security needs
- Service Control Policies (SCPs) set max permission boundaries across OUs
- Consolidated Billing for centralized management of multiple accounts
- Trusted Access allows services like SSO, Config, GuardDuty to manage accounts centrally

Service Control Policies (SCPs)
- SCPs restrict permissions but do not grant them
- Types of SCPs:
- Deny List: Deny all actions on restricted services
- Allow List: Explicitly allow certain actions only
- Tag Conditions: Enforce resource creation only with required tags
- Attach SCPs to OUs, not to users or roles
- Always keep one admin account with full access to avoid lockout

Tag Policies
- Enforce consistent tagging by controlling allowed tag keys and values
- Applied to accounts under AWS Organizations
- Use cases: cost allocation, compliance, automation triggers

6.2 Manage AWS Accounts and Organizational Units
Best Practices for Multi-Account Security
- Account Vending: AWS Control Tower
- Least Privilege IAM: SCPs combined with role assumption
- Security Tooling Account: Centralized GuardDuty, Macie, Config, Security Hub
- Log Archive Account: Long-term, immutable logging
- Billing/Account Management: Centralized via management account
- Use Organizations with IAM Identity Center (SSO) for unified access management

6.3 Design and Implement a Delegated Administration Model
Cross-Account Access Strategies
- IAM Roles + STS for cross-account role assumption
- AWS RAM to share subnets, transit gateways across accounts
- Delegated Admin account to manage services like Config, Macie
- Use STS AssumeRole with conditions (IP, tags, MFA) for secure delegation

Delegated Administrator Best Practices
- Limit delegation to specific services only
- Use resource-based policies where applicable (e.g., S3, SNS)
- Use permissions boundaries for created roles
- Monitor delegated actions with CloudTrail and AWS Config

6.4 Design and Implement Security Compliance Controls
AWS Config
- Tracks configuration history and monitors AWS resource state
- Managed Rules evaluate compliance (e.g., S3 bucket not public)
- Remediation triggers automatic fixes via Lambda or SSM
- Conformance Packs group compliance rules into deployable sets (e.g., CIS, NIST, PCI)
- Use Config Aggregator to consolidate multi-account compliance into management account

AWS Security Hub
- Centralized security posture dashboard monitoring GuardDuty, Macie, Inspector
- Integrates with third-party tools and custom findings
- Supports CIS AWS Foundations Benchmark and AWS Foundational Security Best Practices
- Custom insights allow filtered views (e.g., high-severity findings only)

AWS Audit and Compliance Tools
- AWS Artifact: download compliance reports (SOC, PCI, ISO)
- AWS CloudTrail: logs all management events across regions
- Access Analyzer: detects unintended access from IAM/resource policies
- Amazon Detective: investigates suspicious activity from CloudTrail and VPC logs
- Use Object Lock (WORM) in S3 for regulatory compliance (e.g., SEC 17a-4, HIPAA)

Common SCS-C02 Scenarios (Domain 6)
- Restrict all EC2 actions except DescribeInstances in dev accounts: Use SCP deny list targeting dev OU
- Centralize S3 access logs across accounts: Create log archive account, use organization trail, and bucket policies with cross-account access
- Enforce encryption for all new S3 buckets in the org: Use AWS Config rule s3-bucket-server-side-encryption-enabled
- Visibility into compliance with CIS benchmark: Enable Security Hub plus conformance packs across accounts
- Manage compliance documentation for ISO 27001: Download reports from AWS Artifact

Summary Cheat Sheet
- Central account control: AWS Organizations
- Permission boundaries: SCPs
- Multi-account security: GuardDuty/Macie delegation
- Compliance evaluation: AWS Config, Security Hub
- Resource sharing: AWS RAM
- Secure access across accounts: STS, IAM roles
- Compliance docs: AWS Artifact
- Log centralization: CloudTrail + S3 archive account
- Automated remediation: AWS Config + Lambda

Recommended AWS Resources
- AWS Organizations Guide
- SCPs Best Practices
- AWS Config Rules Reference
- Security Hub User Guide
- AWS Artifact
- AWS Compliance Programs

Presented with xmind AI