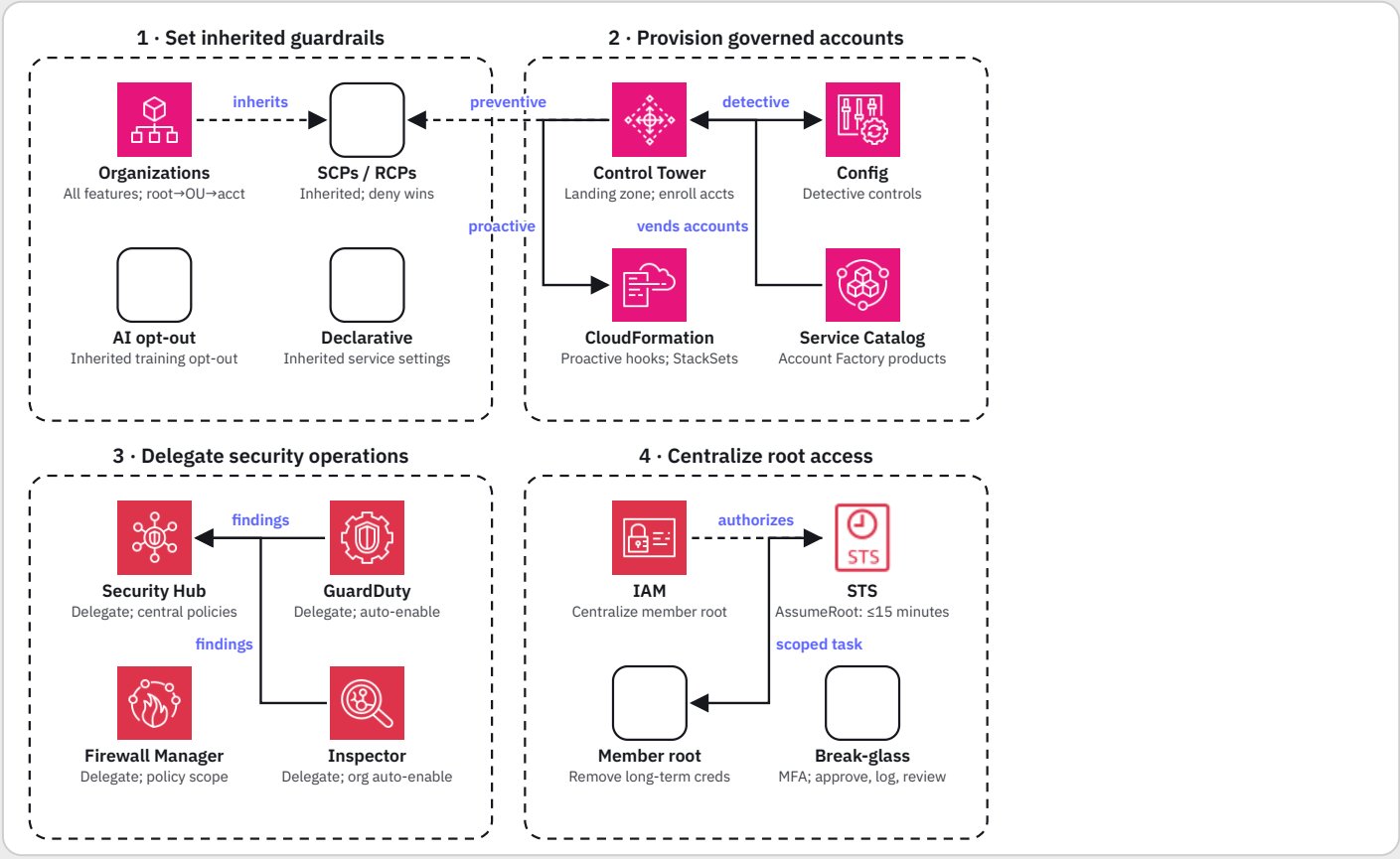
DOMAIN 6 · SECURITY FOUNDATIONS AND GOVERNANCE · 14% OF THE EXAM · TASK STATEMENT 6.1

Develop a strategy to centrally deploy and manage AWS accounts

Organize, govern, delegate, recover



1 Set inherited guardrails

Policy type determines inheritance: SCPs cap principals, RCPs cap resource access; neither grants permissions. AI opt-out controls AI training use; declarative policies enforce supported service settings.

2 Provision governed accounts

Control Tower applies mandatory controls automatically; optional controls require enablement. Enroll existing accounts; use Account Factory for new accounts and IaC with StackSets for custom baselines.

3 Delegate security operations

Separation of duties favors delegated security administrators outside the management account. Configure each service's trusted integration, Regions, and new-account coverage; delegation alone does not enable protection.

4 Centralize root access

Centralized root access supports member credential removal and task-scoped root sessions from the management or delegated administrator account. Restrict session permissions; protect management root separately with MFA.

Exam traps

- **Ceilings are not grants**: IAM/resource policies still need to allow access. SCPs exclude management-account principals and service-linked roles; RCPs exclude management-account resources.
- **Detective is not preventive**: Config reports noncompliance. Proactive CloudFormation hooks reject noncompliant supported resources before provisioning; they do not remediate existing resources.
- **AssumeRoot is not AssumeRole**: root sessions require an AWS managed task policy and last at most 15 minutes. Member credential removal does not remove or protect management-account root credentials.

Get practice exams and lessons for AWS Certified Security - Specialty

AWS Certified Security - Specialty Cheat Sheet

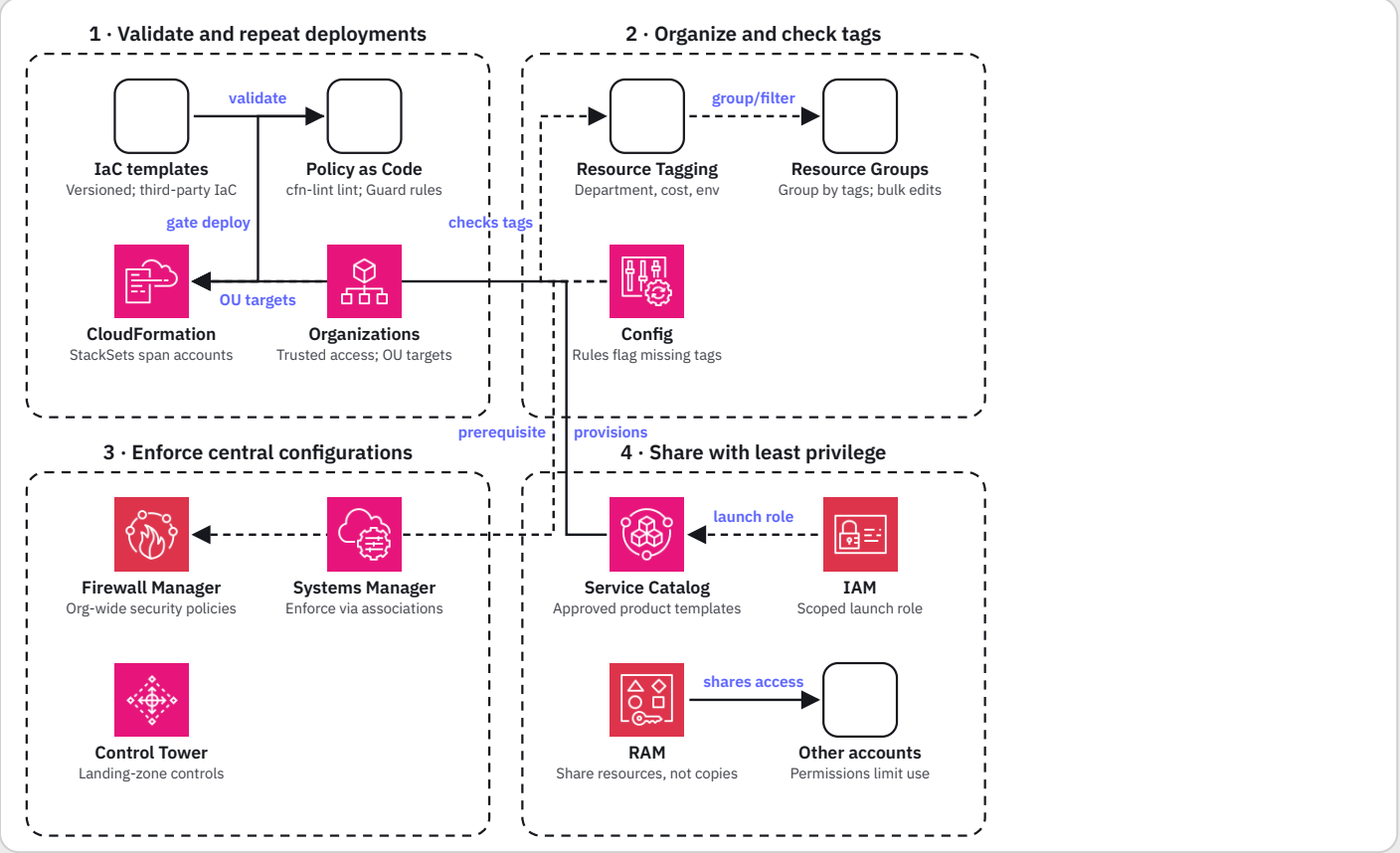
SCS-C03 · Domain 6 of 6

BlowStack

DOMAIN 6 · SECURITY FOUNDATIONS AND GOVERNANCE · TASK STATEMENT 6.2

Implement a secure and consistent deployment strategy for cloud resources

Validate, deploy, govern, share



1 Validate and repeat deployments

Static Analysis: cfn-lint checks template schemas; Guard evaluates Policy as Code rules. Gate deployment on failures; StackSets distributes templates across accounts and Regions, not automatic drift repair.

2 Organize and check tags

Use **tag policies** to standardize supported tag values; they do not require tags on untagged resources. Tag Editor bulk-edits; Config rules detect missing tags, with remediation configured separately.

3 Enforce central configurations

Use **AWS Firewall Manager** for organization-wide firewall policies, with Organizations and AWS Config prerequisites. Systems Manager associations maintain host configuration; Control Tower governs the landing zone.

4 Share with least privilege

AWS RAM shares supported existing resources, not copies. Service Catalog shares approved products; launch constraints supply a least-privilege IAM role for provisioning without broad end-user permissions.

Exam traps

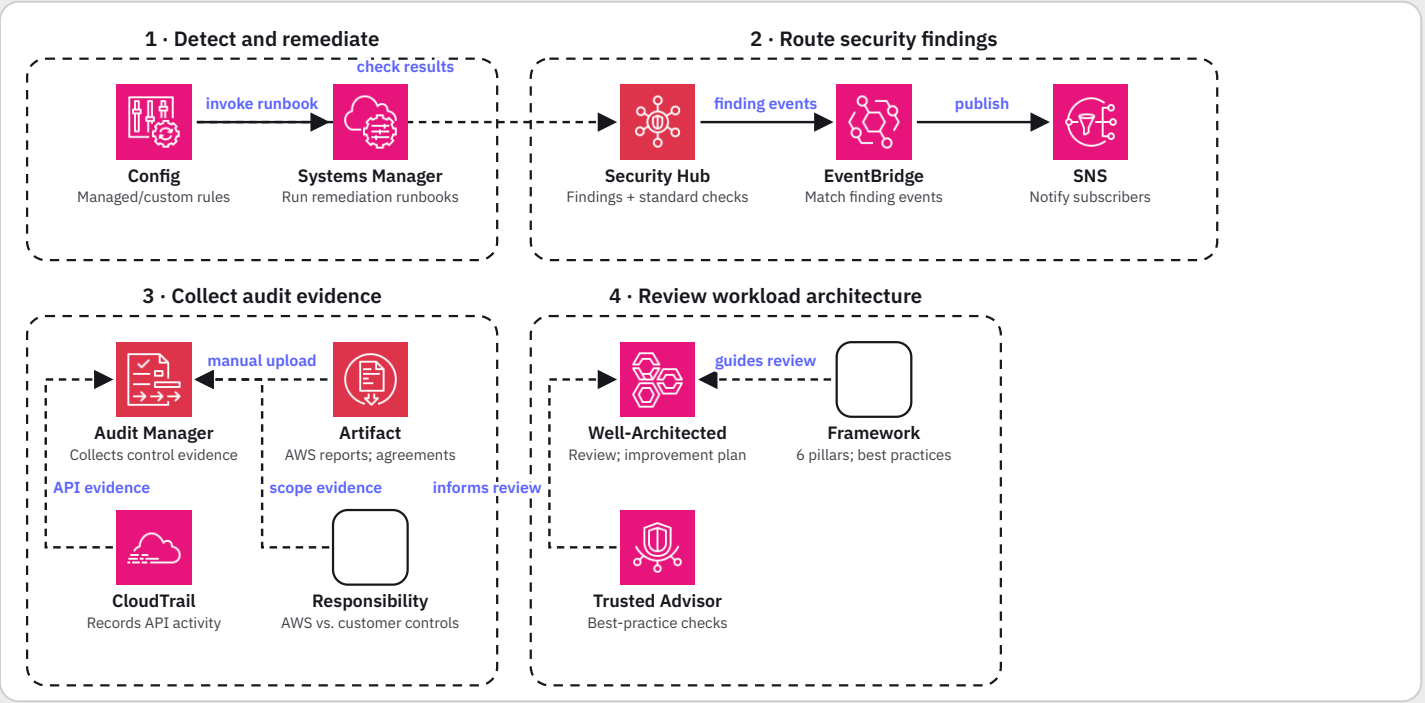
- **Service-managed StackSets** uses Organizations trusted access; self-managed permissions require administration and execution roles. OU targeting requires service-managed permissions.
- **Sharing a portfolio** does not deploy its products into recipient accounts. Service Catalog distributes approved deployment choices; AWS RAM shares access to supported existing resources.
- **Control Tower controls differ**: preventive controls restrict actions, detective controls report noncompliance, and proactive controls check supported resources before CloudFormation provisioning.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 6 · SECURITY FOUNDATIONS AND GOVERNANCE · TASK STATEMENT 6.3

Evaluate the compliance of AWS resources

Detect, remediate, gather, review



1 Detect and remediate

Choose **AWS Config rules** for resource compliance; enable recording and managed/custom rules. Configure automatic remediation through AWS Systems Manager Automation; evaluation alone does not repair resources.

2 Route security findings

Choose **AWS Security Hub** to centralize findings and run standards checks. Amazon EventBridge routes matching finding events to Amazon SNS; notification requires configured rules, targets, and subscriptions.

3 Collect audit evidence

AWS Audit Manager collects evidence for assessments, not certification. AWS Artifact supplies AWS reports and agreements; customers remain responsible for evidence of their own controls.

4 Review workload architecture

Use **AWS Well-Architected Tool** for workload reviews against six pillars and improvement plans. AWS Trusted Advisor supplies automated best-practice checks; neither provides regulatory certification.

Exam traps

- An AWS Config aggregator provides a **read-only view** across accounts and Regions; aggregation does not deploy rules or remediate resources.
- **AWS Artifact reports** document AWS controls, not customer workload compliance. AWS Audit Manager organizes assessment evidence; it does not certify compliance.
- **A finding is not a fix**: AWS Security Hub aggregates findings and evaluates controls; remediation requires separately configured automation or manual action.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 6 · SECURITY FOUNDATIONS AND GOVERNANCE · WHAT TO REMEMBER

Concepts and services of Security Foundations and Governance

Concepts to know

Policy Inheritance

Organization policies apply through the root, OU, and account hierarchy. SCPs and RCPs set **permission ceilings, not grants**; an applicable explicit deny cannot be overridden by an allow lower in the hierarchy.

Infrastructure as code (IaC)

Versioned templates make deployments repeatable and reviewable. Choose **StackSets for multi-account deployment**; use CloudFormation Guard for policy checks and cfn-lint for template validation before deployment.

Separation of Duties

Separate provisioning, security administration, and audit responsibilities. Choose **delegated administrator accounts** for supported security services to centralize operations without routine use of the organization management account.

Core services



AWS Organizations

Organizes accounts into OUs and applies organization policies. Choose **SCPs to cap principal permissions** or RCPs to cap permissions on supported resources; neither grants access.



AWS Control Tower

Establishes and governs a multi-account landing zone. Choose **preventive, detective, or proactive controls** to block actions, detect noncompliance, or validate resources before provisioning.



AWS Config

Records resource configurations and evaluates compliance rules. Choose **an aggregator for cross-account visibility**; configure remediation separately through AWS Systems Manager Automation.

Get practice exams and lessons for AWS Certified Security - Specialty