



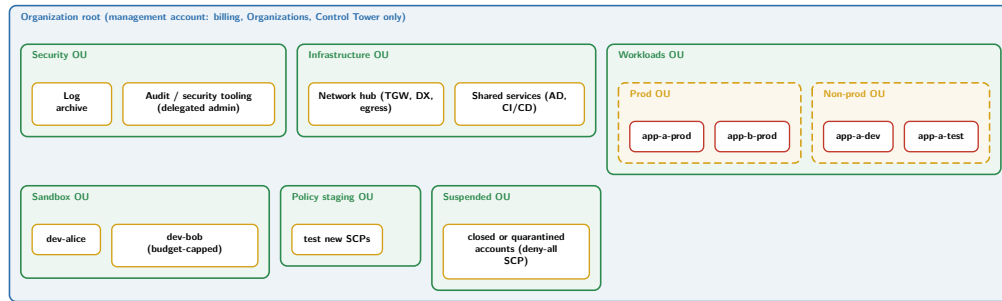
SAP-C02 Org Complexity 1: Multi-Account Governance

SAP-C02 Domain 1 Design Solutions for Organizational Complexity (26 %), tasks 1.3-1.5 | OU design, Control Tower and account vending, SCPs, RCPs, declarative and tag policies, Identity Center and ABAC, delegated administration, centralized logging and security, cost visibility

SAP-C02 Domain 1 Organizations Control Tower Identity Center

Why many accounts, and how to organise them

SAA recall: Organizations groups accounts, SCPs cap permissions, consolidated billing shares discounts. SAP asks you to **design** the structure: an account is the strongest isolation boundary (blast radius, quotas, billing, IAM). AWS guidance: group accounts by **function and policy**, not by company org chart, keep the management account empty, and put guardrails on OUs, not on accounts.



Recommended OU layout (AWS multi-account whitepaper). Policies attach to OUs; one account per workload per environment.

Control Tower piece	What it gives you
Landing zone	management, log archive and audit accounts, org CloudTrail, Config, Identity Center, region deny
Preventive controls	SCPs and RCPs (e.g. disallow changes to the log archive, deny regions)
Detective controls	AWS Config rules with results in the Control Tower dashboard
Proactive controls	CloudFormation Hooks that block non-compliant resources before creation
Account Factory / AFT	vend accounts from Service Catalog, or from Terraform in Git with customisations
Drift detection	reports manual changes to OUs, SCPs or shared accounts; repair from the console
Existing org	enrol existing OUs and accounts; Customizations for Control Tower (CfCT) for extra StackSets and SCPs

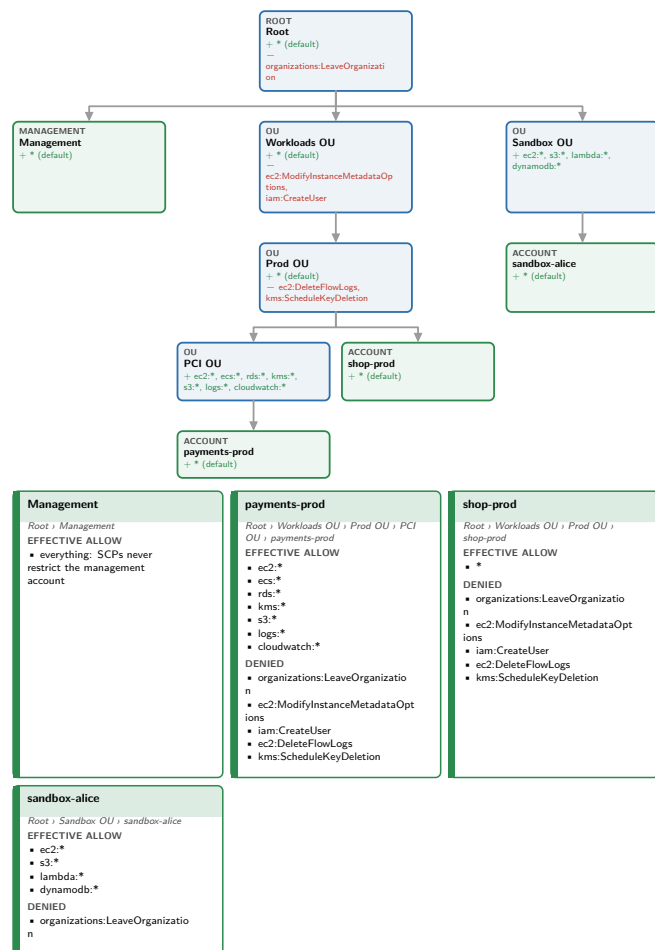
Organization policies

Policy type	Acts on	Example	Note
SCP	IAM principals in member accounts (max permissions)	deny regions outside the EU; deny leaving the org	never grants; not on management account; 5 per node
RCP	resources in member accounts	S3 and KMS only accessible by principals of my org (aws:PrincipalOrgID)	covers external callers that SCPs cannot touch
Declarative (EC2)	service configuration state	IMDSv2 required by default, block public AMI and snapshot sharing	enforced even if an API tries to change it
Tag policy	tag keys and values	CostCenter must be one of 5 values	enforce on chosen resource types
Backup policy	AWS Backup plans org-wide	daily backups of tagged resources to the vault	attached like SCPs, inherited
AI services opt-out	content use by AWS AI services	opt out of service improvement	org-wide

SCP: region guardrail with exemptions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "sts:*",
        "cloudfront:*",
        "route53:*",
        "support:*",
        "budgets:*",
        "waf:*",
        "globalaccelerator:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-west-1",
            "eu-west-3",
            "eu-central-1"
          ]
        },
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam:*:role/BreakGlass"
        }
      }
    }
  ]
}
```

INTERSECTION: an action is allowed only if EVERY level allows it; a deny anywhere above applies below



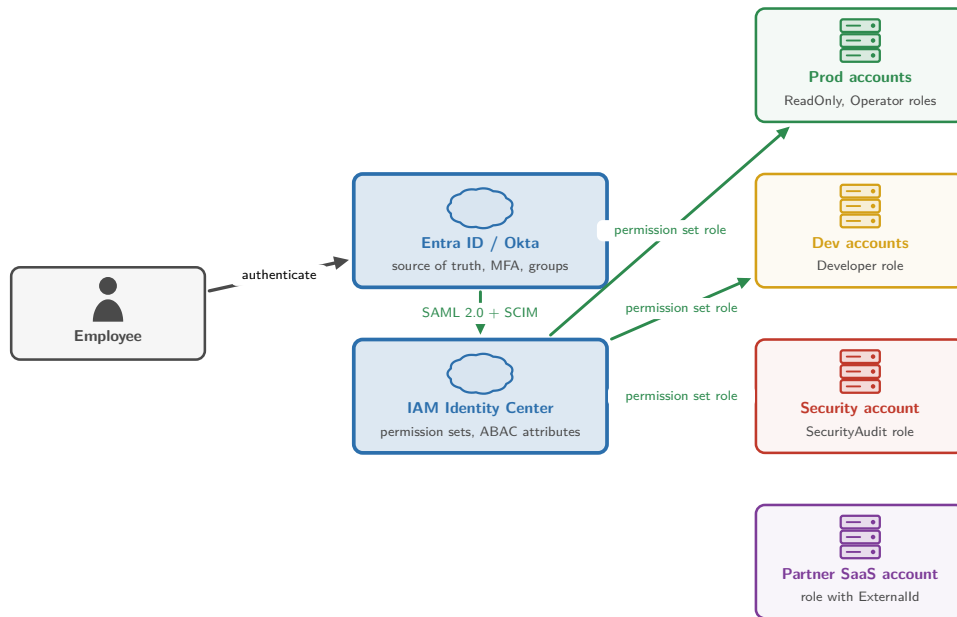
Guardrails only filter: the identity policies in each account must still grant the action.
No assignments listed = the default full-access guardrail (*) stays attached.

Deny-list strategy for most OUs (FullAWSAccess + targeted denies), allow-list for the tightly scoped PCI and Sandbox OUs.
Effective permissions of a leaf = intersection of allows on its path minus every deny above it.

REF	REQUIREMENT	CONTROL	OWNER	STATUS
Logging				100 % covered
R1	API logs immutable for 7 years	org CloudTrail → log archive bucket, Object Lock compliance	Security	Compliant
R2	Security findings in one place	Security Hub delegated admin + Security Lake	Security	Compliant
Data				75 % covered
R3	Workloads only in EU regions	SCP region deny (Control Tower)	Platform	Compliant
R4	No access to data from outside the org	RCP on S3/KMS with aws:PrincipalOrgID	Platform	Partial
Identity				100 % covered
R5	No root credentials in member accounts	centralized root access management	Security	Compliant
R6	Humans use SSO with MFA	Identity Center + external IdP	IAM team	Compliant
Config				50 % covered
R7	IMDSv2 on every instance	EC2 declarative policy	Platform	Partial
Cost				0 % covered
R8	Every resource tagged with CostCenter	tag policy + Config rule	FinOps	Not compliant
5 compliant · 2 partial · 1 not compliant				Overall coverage 75 %

Map each governance requirement to a preventive control first, a detective control second; partial and gap rows become the backlog.

Identity at organization scale



Users and groups are provisioned by SCIM from the corporate IdP; Identity Center turns group assignments into roles in each account. Third parties assume a dedicated role with an External ID, never Identity Center.

RBAC vs ABAC policy count

PROBLEM 20 project teams each need Developer, Operator and ReadOnly access to their own resources across 30 accounts. Count the permission sets to maintain with RBAC and with ABAC.

GIVEN

- P = 20 projects, F = 3 job functions
- IdP sends a 'project' attribute as a session tag (aws: PrincipalTag/project)

1 RBAC: one permission set per project and function

$P \times F = 20 \times 3 = 60$ permission sets

Why: each hard-codes its project's resource ARNs

2 ABAC: one per function

F = 3 permission sets

Why: condition `aws:ResourceTag/project = ${aws:PrincipalTag/project}`

3 Add project 21

RBAC +3 sets; ABAC +0 (tag the resources, set the user attribute)

Why: ABAC scales with tags, not policies

ANSWER 60 vs 3 permission sets; ABAC needs enforced tagging (tag policy, SCP denying untagged creation, deny tag changes).

CHECK ✓ Test: a Developer with project=blue gets AccessDenied on an instance tagged project=red.

Central operations and security

Capability	Org-wide design
Audit logs	organization trail (all accounts, all regions) to the log archive; CloudTrail Lake for SQL queries
Configuration	AWS Config in every account/region via StackSets or Control Tower; aggregator in the audit account; conformance packs
Threats and posture	GuardDuty, Security Hub CSPM, Inspector, Macie, Detective with a delegated admin; auto-enable for new accounts
Firewall policy	Firewall Manager: WAF, Shield Advanced, security groups, Network Firewall, DNS Firewall across accounts
Access review	IAM Access Analyzer: external access, unused access, policy checks in CI
Deploy baselines	CloudFormation StackSets with service-managed permissions, auto-deploy to new accounts in an OU
Share resources	AWS RAM: subnets (shared VPC), TGW, Resolver rules, IPAM pools, License Manager configs, Aurora DB clusters
Cost visibility	consolidated billing, Cost Categories by OU, cost allocation tags, Billing Conductor for pro-forma chargeback

MYTH

✗ An SCP can stop an external account from reading my bucket

✗ Put shared tooling in the management account to save an account

✗ Control Tower requires a brand-new organization

✗ One VPC per account is mandatory

FACT

✓ SCPs only restrict principals inside my org
Use resource policies and RCPs for external callers.

✓ Keep the management account empty
SCPs do not protect it, and its compromise owns the whole org.

✓ Existing organizations can be enrolled
Register OUs and enrol accounts; fix drift first.

✓ VPC sharing with RAM lets many accounts use central subnets
Network team owns the VPC, workload accounts own their resources.

Key takeaways

01 Accounts are the blast-radius boundary
one per workload per environment

02 Guardrails on OUs
SCP + RCP + declarative policies, tested in a staging OU

03 Identity Center + external IdP + ABAC
few permission sets, many accounts

04 Delegated admins in a security account
management account stays empty

05 Control Tower or AFT vends accounts
with baselines from StackSets

Q1 Third-party monitoring SaaS needs read access to 200 accounts. Secure pattern?

A A cross-account role in each account (deployed by StackSets) trusting the vendor's account with an External ID condition.

Q2 Prevent any principal outside the organization from accessing your S3 buckets, org-wide?

A Resource control policy (RCP) denying s3:* unless aws:PrincipalOrgID equals your org (with service exceptions).

Q3 Enforce IMDSv2 on all new instances even if a team calls the API with v1 settings?

A EC2 declarative policy (or an SCP denying RunInstances without ec2:MetadataHttpTokens = required).

Q4 New accounts must automatically get GuardDuty, Config and a baseline VPC. How?

A Delegated admins with auto-enable, plus StackSets (service-managed, auto-deploy) or Control Tower/AFT customisations.

Q5 Test a new SCP without risking production?

A Attach it to a policy-staging OU with test accounts first, then move it up.

Q6 Chargeback per business unit when accounts are grouped in OUs?

A Cost Categories based on accounts/OUs and tags; AWS Billing Conductor for pro-forma rates.

Q7 Workforce users in Okta must reach 300 accounts with MFA. Service?

A IAM Identity Center with Okta as external IdP (SAML + SCIM), group-based permission set assignments.

Q8 Developers in a sandbox OU must not exceed 500 USD per month. Control?

A AWS Budgets with a budget action applying a restrictive SCP/IAM policy (plus Sandbox SCPs).

Q9 Query all CloudTrail events of the org with SQL for an investigation?

A CloudTrail Lake event data store at the organization level (or Athena over the log archive).