INDEPENDENT HANDS-ON PROJECT

AWS Multi-Account Landing Zone Blueprint

Organizations, preventive guardrails and centralized audit logging

Portfolio track	Independent Hands-on Engineering
Evidence level	Terraform fmt, init and validate passed
Author	Saurabh Dindokar

Evidence boundary: This is a public-safe personal implementation lab. It is not client production work, and no live deployment is claimed.

Overview

A safety-first Terraform blueprint for organizational units, an example regional Service Control Policy, centralized organization CloudTrail, KMS-encrypted versioned log storage and lifecycle retention around a Control Tower-managed landing zone.

Engineering Problem

A multi-account foundation needs isolation, preventive controls and centralized evidence before application teams scale. The blueprint models Terraform-managed components adjacent to Control Tower without falsely claiming to reproduce Control Tower itself.

Architecture

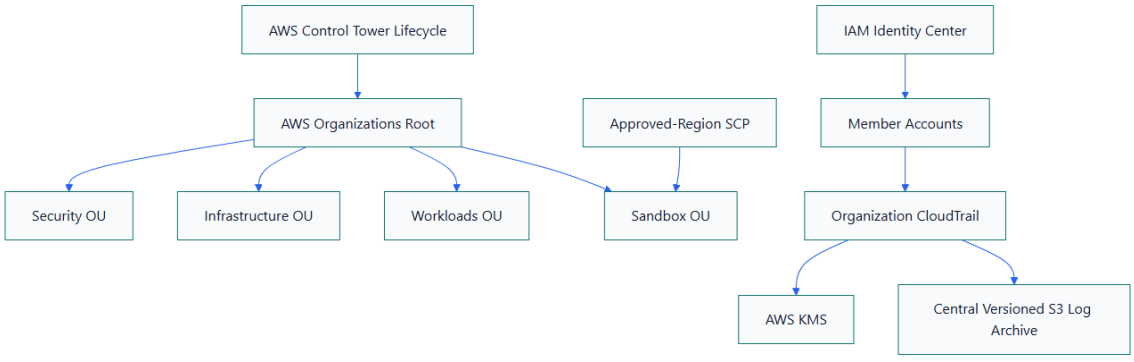

Figure 1. AWS Multi-Account Landing Zone Blueprint architecture

What I Implemented

- Made AWS Organizations creation opt-in and protected it from accidental destroy.
- Defined Security, Infrastructure, Workloads and Sandbox organizational units.
- Created an approved-region SCP example and attached it only to the Sandbox OU.

- Built a versioned, public-blocked, KMS-encrypted S3 log archive with Glacier transition and retention controls.
- Configured a multi-region organization CloudTrail with global events and log-file validation.

Important Technical Decisions

- Control Tower setup and lifecycle remain in the supported Control Tower workflow.
- The Terraform code models adjacent foundations and an adoption path instead of claiming Control Tower installation.
- SCPs are tested in an isolated OU before broader attachment.
- Organization creation is disabled by default to prevent unsafe experimentation.

Security Controls

- Organization CloudTrail centralizes audit evidence.
- Log files use KMS encryption, S3 versioning, public-access blocking and validation.
- The regional SCP is a preventive guardrail, not a substitute for IAM permissions.

Reliability and Operations

- Dedicated Security, Infrastructure, Workloads and Sandbox boundaries support account isolation.
- Lifecycle and versioning protect log evidence while controlling long-term storage.
- Real adoption should include dedicated Audit and Log Archive accounts plus delegated security administration.

Cost and Cleanup Guardrails

- Log ingestion, KMS requests and S3 retention are design inputs.
- Logs transition to Glacier Instant Retrieval after 90 days and expire according to a variable retention period.
- The blueprint avoids any automatic organization apply and warns against using an employer management account.

Validation Evidence

The following local checks passed on 2026-08-13:

```
terraform fmt -check -recursive
terraform init -backend=false
terraform validate
```

Scope boundary: Format, initialization and validation passed on 2026-08-13. No sandbox plan, Organizations change, SCP test, Control Tower initialization or organization-trail deployment is claimed.

Delivery and Verification Runbook

- 1. Establish management-account safeguards
- 2. Initialize Control Tower through supported lifecycle
- 3. Create or adopt organizational units
- 4. Test SCP in Sandbox OU

- 5. Configure central KMS and log archive
- 6. Enable organization trail
- 7. Review controls and delegated administration

Technology Stack

Terraform | AWS Organizations | AWS Control Tower | Service Control Policies | AWS CloudTrail | Amazon S3 | AWS KMS | IAM Identity Center

Key Learnings

- Infrastructure evidence must distinguish code validation, plan review and live deployment.
- Security, reliability, cost and cleanup decisions should be documented before apply.
- A useful platform lab includes verification and rollback thinking, not only resource declarations.