

— PLATFORM · TEMPLATE

AWS Control Tower vs. Terraform: The Landing-Zone Build-vs-Buy *Call*

KAANSYSTEMS.COM/LIBRARY/CONTROL-TOWER-VS-TERRAFORM-LANDING-ZONE · SEPTEMBER 16, 2026

— ABOUT THIS TEMPLATE

Control Tower is AWS's managed landing zone; Terraform is roll-your-own. For most regulated SMBs, Control Tower (or Control Tower + AFT) is the right call.

— THE TEMPLATE

Score each item honestly before you commit. If most of the left column is true, buy (Control Tower). If most of the right column is true, build (Terraform). If the guardrail rows point one way and the vending rows point the other, you are looking at AFT.

Team and ownership

- ☐ A named engineer owns platform (not "the whole team")
- ☐ Terraform already runs through CI with reviewed plans
- ☐ Someone can maintain a CodePipeline/CodeBuild footprint (AFT gate)
- ☐ The org would otherwise be vended by hand (points toward Account Factory or AFT)

Scope and constraints

- ☐ Estate is AWS-only for the foreseeable future (Control Tower is viable)
- ☐ There is a real non-AWS footprint (forces Terraform)
- ☐ Control Tower's OU opinions are acceptable, not a blocker
- ☐ Multi-cloud governance must live in one tool (forces Terraform)

Compliance and evidence

- ☐ SOC 2 or HIPAA scope is active or imminent

- ☐ A managed guardrail catalog would shorten audit prep (favors Control Tower)
- ☐ Git-based change history is your preferred evidence (favors Terraform)
- ☐ Centralized CloudTrail/Config to a locked log-archive account is required either way

Operations and cost

- ☐ You want AWS to own the baseline and its upgrades (favors Control Tower)
- ☐ You want the org to live under existing drift detection as code (favors Terraform)
- ☐ Landing-zone version upgrades as a managed event are acceptable
- ☐ You have priced the Config, CloudTrail, and S3 that any of these turns on

Exit

- ☐ You have considered what decommissioning Control Tower would take later
- ☐ You are comfortable with an AWS-native layer (Control Tower) vs. portable Terraform

Most SMBs find the left column mostly true and land on Control Tower, or find the guardrail rows true and the vending rows true and land on AFT. Teams with a platform owner and a Terraform habit tend to find the right column true and roll their own. All three are defensible; an unmade decision is not.

— WHAT IS AWS CONTROL TOWER, EXACTLY?

Control Tower is AWS's managed landing zone. You run a guided setup and it stands up AWS Organizations, a multi-account baseline, and the governance most regulated teams would otherwise assemble by hand. Specifically: preventive guardrails implemented as service control policies, detective guardrails implemented as AWS Config rules, centralized CloudTrail and Config logging shipped to a dedicated log-archive account, and Account Factory for vending new accounts against a standard blueprint.

The guardrails ship as a catalog with three postures: mandatory (always on), strongly recommended (AWS's opinion of a sane default), and elective (opt-in). That catalog is the real product. It encodes controls that map cleanly onto the "how is production isolated, how are logs protected" questions a SOC 2 or HIPAA assessor asks, and AWS maintains it as the service evolves.

The trade is opinionation. Control Tower has views on OU structure, its guardrails drift-check against their own model rather than against your infrastructure code, landing-zone version upgrades are a scheduled event you manage, and Account Factory provisions through Service Catalog, which is slow and awkward to drive from a pipeline. You customize within its rails, not around them.