

— PLATFORM · TEMPLATE

Do You *Actually* Need an AWS Landing Zone?

KAANSYSTEMS.COM/LIBRARY/WHEN-DO-YOU-NEED-AWS-LANDING-ZONE · SEPTEMBER 16, 2026

— ABOUT THIS TEMPLATE

You don't need an AWS landing zone on day one. A single account is fine until real data, a compliance requirement, or a second environment turns it into a liability.

— THE TEMPLATE

Run this top to bottom. Any single checked box in the "tipping points" section means you have outgrown the single account. The rest tells you which target to build and what "done" looks like.

Tipping points (check any that are true today)

- ☐ Real customer data, PHI, or PII lives in production
- ☐ There is a SOC 2 or HIPAA requirement, signed or imminent
- ☐ A customer or investor security review is on the calendar
- ☐ The team is larger than 2-3 engineers with AWS access
- ☐ There is more than one environment (prod / staging / dev)
- ☐ You need clean per-team or per-customer cost or access isolation

If zero boxes are checked (stay single-account, do the basics)

- ☐ MFA enforced on every human with console access
- ☐ Root user locked away, not used, alarmed on login
- ☐ CloudTrail enabled and logging
- ☐ A budget alarm exists so a runaway resource is not a surprise invoice

If any box is checked, no compliance yet (minimum viable landing zone)

- ☐ Management/org account created; nothing runs in it

- ☐ Log-archive account receiving org-wide CloudTrail with S3 Object Lock
- ☐ Security/audit account for delegated security tooling
- ☐ Separate prod and non-prod workload accounts (not separate VPCs)
- ☐ IAM Identity Center for human access; zero per-account IAM users
- ☐ A non-overlapping CIDR plan covering accounts you have not created yet

If a box is checked and compliance is real (full landing zone)

- ☐ The five-OU topology from the build guide is in place
- ☐ Service control policies attached and exercised, not just written
- ☐ Delegated security tooling (GuardDuty, Security Hub, Access Analyzer)
- ☐ Tooling decision made deliberately (Control Tower vs. Terraform)
- ☐ Org definition under version control and drift detection

Most teams find themselves with one or two tipping-point boxes checked and none of the structural work started. That is a normal, fixable place to be. The path from there is to build toward the target the checked boxes point to, and no further.

— WHAT DOES A SINGLE AWS ACCOUNT ACTUALLY COST YOU?

Nothing, until you have production data, more than a couple of engineers, or a compliance obligation. Then it costs you on five fronts at once, and the bill arrives all at the same time.

- **Blast radius.** The account is the only hard security wall AWS gives you. One leaked CI token, one over-permissive role, one phished laptop, and the attacker has the whole company, because there is no inside wall to stop at.
- **IAM sprawl.** Roles and policies accumulate faster than anyone prunes them. By the time you look, there are dozens, at least one carries a `Resource: "*" nobody remembers granting, and "who can touch production" has become a policy-analysis research project instead of a list of names.`
- **No hard environment isolation.** Prod and dev share an IAM universe, the same account-scoped service quotas, and the same KMS keys. The load test that exhausts Lambda concurrency takes production down with it. Separation is a naming convention, which is to say it is not separation.
- **Muddy billing.** One account means one bill. Attributing spend to a team, a customer, or an environment depends entirely on tags that were enforced for about six weeks in 2023, so the allocation report is fiction with a currency column. Better tagging helps ([cost-aware tagging](#) is the fix), but a tag is a weaker boundary than an account.
- **A weak audit boundary.** When a SOC 2 or HIPAA assessor asks how production is isolated from development, "a tag" is an expensive answer. Assessors expect isolation to be structural, not procedural,

and for a HIPAA workload the gap between those two words is a remediation project.

None of this is a problem for a two-person prototype with no real users. All of it is a problem the week you sign your first customer.