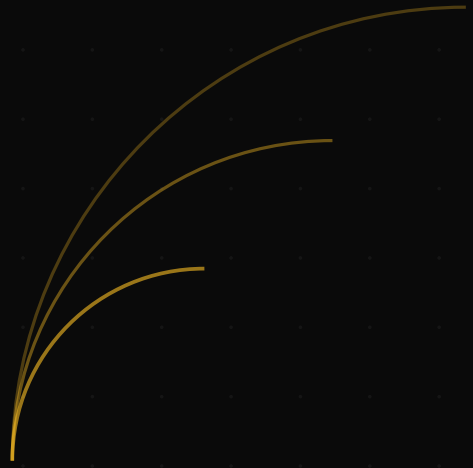
INFRASTRUCTURE, SECURITY, AND IT LEADERS

How to evaluate a cloud migration vendor



Cloud migration evaluation: network design, licence repatriation, egress costs, performance testing, and the security baseline that must come before workloads move.

Cloud migrations go wrong in the places proposals skim over: network architecture, licensing that doesn't transfer, and ongoing costs - egress and compute - that aren't in the implementation quote at all.

WHAT'S INSIDE

5 steps in this guide

01

Network design is frequently under-scoped

VPCs, subnets, transit gateways, firewall rules, and peering are routinely underscoped in migration proposals - and network design errors cause security incidents and performance failures at go-live. Require a network architecture deliverable, not an assumption.

02

Licence repatriation can add 20-40% to TCO

On-premises licences (Windows Server, SQL Server, Oracle DB) cannot always be used in the cloud. Licence repatriation analysis must be completed before the architecture is finalised - cloud licensing can add 20-40% to total cost of ownership if it's discovered late.

03

Egress and compute are ongoing costs the quote ignores

Cloud egress (data transferred out) and compute costs are significant, poorly understood, and excluded from implementation proposals. High-egress workloads can make cloud more expensive than on-premises. Model these against real workload patterns before committing.

04

Performance must be tested in the target environment

Application performance in the cloud depends on network latency, data-transfer costs, and resource sizing that can only be validated through load testing in the target environment. Most migration proposals exclude performance testing - put it back in scope.

05

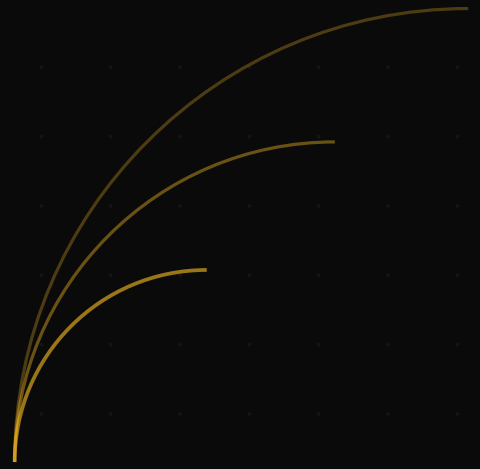
Establish the security baseline first

Identity and access management, secrets management, encryption, logging, and threat detection must be established before workloads migrate, not after. A migration onto an unhardened landing zone is a breach waiting to happen.

PUT THIS TO WORK

Walk into every evaluation with the vendor's own playbook.

- A vendor-proof scope, issued before any proposal
- Gap analysis scoring every proposal against your scope
- A risk-weighted interrogation kit for the vendor meeting
- Scope-drift detection across proposal versions



Start free at benchsideai.com

Your first project is free. No card required.