Plow

Cloud Migration Security

Pre-Migration Evaluation Checklist

Plow Networks

Prepared 2026

7101 Sharondale Court
Suite 200
Brentwood, TN 37027
plow.net

Most cloud migration security gaps are architectural decisions made before the move, not technical issues introduced after. This checklist walks the five evaluation dimensions an IT leader should resolve before workloads start moving: identity, data classification, network segmentation, compliance mapping, and operational visibility. Work through each section, mark what's resolved, and use the priority column to sequence the work that isn't.

How to use this: check each item that is fully resolved for your target environment. Any unchecked item is pre-migration work. Flag the high-risk gaps before the first workload moves.

Dimension 1 — Identity & Access

In the cloud, identity is the primary control plane. If the identity model is weak, every control downstream of it is weak too. Resolve these before migration:

☐ Authentication is consolidated to a single authoritative identity provider (no scattered directories)

☐ MFA is enforced for all administrative access, including service principals and break-glass accounts

☐ Privileged roles are assigned just-in-time, not standing

☐ Conditional access enforces device posture, location, and sign-in risk before granting resource access

☐ A joiner/mover/leaver lifecycle process exists and is automated where possible

☐ Service principals, managed identities, and API credentials are inventoried with a rotation policy

Dimension 2 — Data Classification

You cannot apply appropriate cloud controls to data you haven't classified. Define the scheme before any data moves:

☐ Classification tiers are defined (public, internal, confidential, regulated)

☐ A current inventory maps what data lives where today

☐ A decision exists for what migrates and what stays on-premises

☐ Each tier is mapped to specific controls: encryption, access restriction, retention, geographic constraints

☐ Regulated data has a documented destination built for its requirements

Dimension 3 — Network Segmentation

Cloud networks inherit no segmentation. What you don't deliberately design isn't there. Reason about blast radius before migration:

☐ VNet/VPC topology is designed with segmentation as a first-class concern (not a flat replica of on-prem)

☐ The most sensitive systems are isolated from the general network

☐ Traffic flow controls (ingress/egress) are defined between segments

☐ Private endpoints are used for sensitive services rather than public exposure

☐ For each workload: 'if this is compromised, what can the attacker reach laterally?' has an acceptable answer

Dimension 4 — Compliance Mapping

Regulatory requirements don't change in the cloud, but how you meet them does. Map controls before go-live, not before the next audit:

☐ Existing control framework is mapped against cloud-native equivalents

☐ Controls that translate cleanly are identified

☐ Controls that need new tooling (DLP, WAF, audit trails) are identified

☐ Controls that require process redesign are identified

☐ The cloud control map has been reviewed with your auditor

Dimension 5 — Operational Visibility

A migration that goes live without visibility turns the first incident into a forensic exercise. Decide these before cutover:

☐ Cloud log sources (control plane, identity, resource metrics) have a defined destination

☐ SIEM integration for cloud telemetry is planned and tested

☐ Detection rules are updated for the cloud threat profile

☐ Alerting thresholds and escalation paths are defined

☐ A pre-migration tabletop has been run for the most likely cloud incidents (credential compromise, public exposure, IAM misuse)

Post-Migration Threat Profile

Migration changes the threat surface. Plan detection and response against the post-migration profile, not the one you're leaving behind.

Risks That Shrink	Risks That Grow	Risks That Are New
Physical infrastructure threats	Identity-based attacks (phishing, token theft)	Control plane compromise
Hypervisor / host patch latency	Misconfiguration exposure	Cloud-native lateral movement
Edge DDoS (at infrastructure layer)	Service principal sprawl	Shadow cloud outside IT visibility
Basic infrastructure redundancy	Third-party SaaS trust boundary	Cost-based attacks (cryptomining, egress)

Migration Readiness Snapshot

Count the checked items in each dimension and record below. Any dimension under 70% complete is pre-migration work that should be scheduled before workloads move.

Evaluation Dimension	Items Resolved	Priority to Address
Identity & Access (of 6)	_____ / 6	☐ High ☐ Med ☐ Low
Data Classification (of 5)	_____ / 5	☐ High ☐ Med ☐ Low
Network Segmentation (of 5)	_____ / 5	☐ High ☐ Med ☐ Low
Compliance Mapping (of 5)	_____ / 5	☐ High ☐ Med ☐ Low
Operational Visibility (of 5)	_____ / 5	☐ High ☐ Med ☐ Low

Reading Your Result

All five dimensions above 70%: you're in a position to migrate with a defensible architecture. Sequence the remaining gaps into the migration plan.

One or more dimensions below 70%: these are the architectural decisions that become permanent the moment workloads run. Address them before the first workload moves, not after.

Planning a Cloud Migration?

Plow Networks helps IT leaders design defensible cloud environments from the start — identity, segmentation, compliance, and operational visibility built in before workloads move.

Talk to Our Cloud Security Team →