ELEVATE
SOLUTIONS

GUIDE · IT STRATEGY & OPERATIONS

Cloud Migration Done Right

On budget, no downtime

Step-by-step guide to moving to cloud infrastructure securely — phases, risk mitigation, cost controls, and security baselines for Azure, AWS, and Microsoft 365.

01 — KNOW WHAT YOU HAVE FIRST

Pre-Migration Assessment

Most migration overruns are discovered, not caused. The server nobody documented, the line-of-business app that hard-codes an internal IP, the license that does not transfer. Two to four weeks of assessment is cheaper than finding these mid-cutover.

Inventory four things

INVENTORY	WHAT TO RECORD
Applications	Name, owner, vendor, version, server(s) it runs on, who uses it, business criticality, vendor support status for cloud hosting. Flag anything end-of-life — an unsupported OS should not be migrated as-is.
Data	Volume per system (GB/TB), growth rate, sensitivity classification (PHI, client files, financial records), retention obligations, current backup location and method.
Dependencies	What talks to what: app-to-database links, scheduled jobs, file shares mapped in login scripts, scanners that drop files to a server, integrations with practice-management or EHR systems. Azure Migrate and AWS Application Discovery Service can map these automatically; verify the map with the people who run the apps.
Licenses	Per-server vs. per-user terms, whether the license permits cloud hosting (some vendors require a hosting addendum), Windows Server and SQL Server license mobility, what your Microsoft 365 plan already includes so you do not buy it twice.

Classify every workload: the 5R model

Every application gets exactly one label. The label drives effort, cost, and sequence.

PATTERN	WHAT IT MEANS	WHEN IT FITS
Rehost “lift and shift”	Move the server as-is to an Azure or AWS virtual machine. Fastest, least disruptive, least optimized.	Stable apps you cannot change; deadline-driven moves (lease ending, hardware failing).
Replatform	Small changes for a managed service — SQL Server to Azure SQL Managed Instance, file server to SharePoint Online or Azure Files.	When a managed equivalent removes patching and backup burden at similar cost.
Refactor	Rebuild for cloud-native services. Highest effort and risk, highest long-term payoff.	Custom apps with active developers and a business case. Rarely first-wave.
Retire	Shut it down. Typical environments carry servers nobody has logged into in a year.	Anything with no users, no data obligation, no dependency. Cheapest migration is none.

Retain	Leave it on-premises, deliberately, with a documented reason and a revisit date.	Latency-sensitive equipment (phone systems, scanners, lab devices), apps with hosting restrictions, regulatory holds.

Bandwidth and latency reality check

Do the arithmetic before you schedule anything. Moving 2 TB over a 100 Mbps circuit takes roughly 48 hours at full line rate — and you will not get full line rate during business hours. Seed large datasets ahead of cutover with incremental sync (Azure Migrate replication, AWS DataSync, or the migration tooling built into Microsoft 365 for mail and files), so the final cutover only moves the delta. Then check the other direction: if a desktop app makes hundreds of small database calls per screen, 30–60 ms of added round-trip latency can turn a 1-second screen into a 30-second one. Test the worst app from the office before committing it to rehost.

Compliance constraints to settle in writing

- [ ] **Data residency** 1
  Pin region selection (e.g., Azure West US 3, AWS us-west-2) before building anything. Confirm whether any client contract or regulation restricts where data may sit, including backup and failover copies.
- [ ] **Business Associate Agreement (healthcare)** 2
  If PHI touches the platform, execute the BAA first. Microsoft includes BAA terms in its online services agreement for covered services; AWS executes a BAA through AWS Artifact. Confirm every service you plan to use is on the vendor's HIPAA-eligible list.
- [ ] **Client and ethical obligations (legal)** 3
  Some engagement letters and outside-counsel guidelines restrict where client files may be stored or require notice before moving them. Review before, not after.
- [ ] **Retention and legal holds** 4
  Migration must not break an active litigation hold or shorten a retention clock. Map existing holds to Microsoft Purview retention policies or your archive platform before mail and files move.

TCO worksheet

Compare three-year totals, not month one. Cloud spend is operational and ongoing; the savings show up in what you stop buying. These are the rows we use in planning conversations — fill in your own numbers.

LINE ITEM	CURRENT (ANNUAL)	CLOUD (ANNUAL)
Server hardware refresh (annualized over 5 years)		
Server OS, database, and virtualization licensing		
Compute and storage (VM/instance run rate, managed services)		
Microsoft 365 / SaaS subscriptions		
Backup and disaster recovery (software, storage, second site)		

Internet circuits (upgraded bandwidth, redundancy)
Data egress and inter-region transfer (often forgotten)
Server room costs: power, cooling, UPS, physical security
Support labor or managed services for the environment
One-time migration cost (tooling, labor, parallel running)

02 — SEQUENCE BEATS SPEED

Phased Migration Plan

Identity moves first, because everything after it authenticates through it. Then the workloads users feel least, building toward the ones they feel most. Each phase runs the same loop: pilot, validate, cut over, and keep a rollback path open until validation closes.

> **THE NO-BIG-BANG RULE**
>
> Never cut over identity, email, files, and servers in one window. A single-weekend "everything moves" plan has no rollback path — if one workload fails, you are debugging four at once with users locked out. Phases isolate failure: any one phase can roll back without touching the others.

The four phases, in order

PHASE	SCOPE	WHY THIS POSITION	ROLLBACK PLAN
1	Identity — Microsoft Entra ID	Deploy Microsoft Entra Connect (or cloud sync) from Active Directory, register MFA for all users, stand up Conditional Access in report-only mode. Nothing user-facing moves yet.	On-premises AD remains authoritative throughout. Disable sync; users keep signing in exactly as before. Lowest-risk rollback of any phase — which is why it goes first.
2	Email — Exchange Online	Hybrid or cutover migration of mailboxes in batches. Users notice mail before almost anything else, but mailbox moves are mature, reversible, and batch-sized.	In hybrid mode, move a failed batch back to on-premises Exchange. Hold the MX record change until the pilot batch is validated; MX is the point of no easy return.
3	Files — SharePoint Online / OneDrive / Azure Files	Migrate shares with Microsoft 365 migration tooling. Restructure during the move — permission sprawl copied as-is becomes permission sprawl in the cloud.	Keep source shares read-only, not deleted, until validation closes. Rollback = re-share the originals and resync the delta.
4	Workloads — Azure / AWS servers and apps	Rehost or replatform per the 5R labels, lowest-criticality first. The last mover is your most critical line-of-business system, after the process is proven on three or four easier ones.	Replication-based tools (Azure Migrate, AWS MGN) leave the source server intact and current. Rollback = power the original back on and repoint DNS. Keep sources powered off but preserved for 30 days post-cutover.

Run every phase through the same loop

- [ ] **Pilot** 1
  5–10 users or one low-criticality server. Include at least one power user and one person from the loudest department — they find what IT misses.
- [ ] **Validate** 2
  Written test list with named owners: sign-in works, mail flows in both directions, files open with correct permissions, the app performs at office latency, backup of the new environment runs. A phase is validated when the list is signed, not when nobody has complained yet.
- [ ] **Cut over** 3
  Move the remaining batches during the announced window. One person owns the go/no-go call, and the no-go criteria are written down before the window opens.
- [ ] **Hold the rollback open** 4
  Source systems stay intact and restorable until validation closes — typically 2–4 weeks after cutover. Decommissioning during the validation window converts a bad day into a bad month.

Cutover windows and communications

Cut over evenings or weekends, never the night before payroll, a filing deadline, or a billing run — check the business calendar, not just the IT calendar. Freeze all other IT changes for 48 hours around each window. Communicate three times: one week out (what is moving, what changes for users, exact date), the day before (a reminder plus any action users must take, such as re-adding an account on a phone), and the morning after (what changed, how to get help, with a screenshot if sign-in looks different). Publish a help channel that does not depend on the system being moved — if email is cutting over, give a phone number.

03 — SECURE ON DAY ONE, NOT DAY NINETY

Security & Governance Baseline

A new tenant or cloud account is not secure by default — it is functional by default. Build the landing zone before the first production workload arrives. Retrofitting controls onto a live environment is slower, riskier, and politically harder.

CONTROL	BASELINE STANDARD	WHERE (AZURE / M365 · AWS)
MFA + Conditional Access	MFA for every account, no exceptions for executives or service desks. Block legacy authentication. Require phishing-resistant MFA for admin roles.	Microsoft Entra Conditional Access · AWS IAM Identity Center + MFA enforcement
RBAC, least privilege	No standing global admins beyond two break-glass accounts. Admin rights granted per role, time-limited where the license allows (Microsoft Entra Privileged Identity Management). Separate accounts for admin work.	Azure RBAC, Entra roles · AWS IAM roles and permission boundaries
Network segmentation	Workloads in segmented virtual networks; databases never exposed to the internet; admin access via VPN or bastion, not open RDP/SSH. Default-deny inbound.	Azure VNets, NSGs, Azure Bastion · AWS VPCs, security groups, Systems Manager Session Manager
Encryption defaults	Encryption at rest is on by default in Azure Storage and Amazon S3 — verify rather than assume for VMs and databases. Enforce TLS for data in transit. Decide early whether any data class requires customer-managed keys.	Azure Key Vault, storage encryption · AWS KMS, S3 default encryption
Logging on day one	Audit and sign-in logs flowing to retained storage before production data arrives. You cannot investigate week-one incidents with logging enabled in week six. Set retention to match your compliance obligation, not the default.	Microsoft Purview audit, Entra sign-in logs, Azure Monitor · AWS CloudTrail, CloudWatch
Threat monitoring	Enable the platform's native detection layer at launch and route alerts to a mailbox or channel someone actually reads.	Microsoft Defender for Cloud · Amazon GuardDuty
Cost guardrails	Budgets with alert thresholds at 50/80/100% of forecast, in place before the first VM. Tag every resource with owner and purpose at creation; untagged resources are unaccountable resources.	Microsoft Cost Management budgets, Azure Policy tag enforcement · AWS Budgets, tag policies

BACKUP IS NOT AUTOMATIC — SHARED RESPONSIBILITY

Microsoft and AWS are responsible for the platform staying up. You are responsible for your data in it. Microsoft 365 retention and the Recycle Bin are not backup: they will not save you from a ransomware-encrypted sync, a malicious insider, or a deletion discovered after the retention window. Deploy third-party backup for Microsoft 365 (Exchange Online, SharePoint Online, OneDrive) and platform backup for servers (Azure Backup, AWS Backup) with at least one copy that is immutable or otherwise isolated from your admin credentials. This matters because ransomware was present in 44% of breaches, up 37% year over year Verizon DBIR 2025 — and cloud-synced data encrypts just as quickly as on-premises data.

One more day-one rule: the identity controls above are the controls that matter most, because most attacks go through people, not infrastructure — the human element was involved in 60% of breaches. Verizon DBIR 2025 A migrated environment with MFA enforced and legacy authentication blocked is meaningfully harder to compromise than the on-premises environment it replaced. One without them is the same environment with a bigger attack surface.

04 — THE MIGRATION ENDS WHEN THE OLD GEAR IS GONE

Post-Migration Optimization

First-pass cloud sizing is a guess made under deadline. The savings come from the review cycle afterward — and from actually turning off what you left behind. Teams that skip this section pay for two environments indefinitely.

Right-size on a 30/60/90 cadence

DAY	REVIEW
30	First full utilization picture in Azure Advisor or AWS Compute Optimizer. Downsize anything sustained below ~20% CPU and memory. Delete orphaned disks, unattached IPs, and stopped-but-allocated VMs left over from the cutover. Compare actual spend to the TCO worksheet and explain every variance.
60	Second pass with a fuller business cycle (month-end, billing runs) in the data. Add auto-shutdown schedules for dev/test and any server only used in business hours — a 12×5 schedule cuts that VM's compute cost roughly in half. Review storage tiers: move cold data to cool/archive tiers (Azure Storage tiers, S3 Glacier classes).
90	Commitment decision (below), final validation sign-off, decommission checklist executed, runbooks updated. The project formally closes here, not at cutover.

The reserved-capacity decision

Azure Reservations, Azure savings plans, and AWS Reserved Instances or Savings Plans trade flexibility for a discount that commonly lands in the 30–60% range depending on term and service — but only on workloads that actually run steadily. Decide at day 90, never at day 1. Commit when a workload has run 60–90 days at stable size, will exist for the full term, and is already right-sized — committing to an oversized VM locks in the waste. Start with one-year terms; reserve your steady core and leave variable workloads on pay-as-you-go. Revisit annually.

Decommission checklist — 12 items

- [ ] **Confirm validation is signed for every phase** 1
  Nothing on this list starts until the last rollback window has closed in writing.
- [ ] **Archive a final image of each retired server** 2
  One last backup to retained storage before wiping, held per your retention schedule. Cheap insurance against "we needed one file off that box."
- [ ] **Wipe and dispose of hardware with documentation** 3
  Certified data destruction with certificates retained — drives that held PHI or client files do not go in a dumpster or on eBay.

- [ ] **Cancel or true-down licenses** 4
  On-premises Exchange, server CALs, virtualization, backup agents, antivirus seats for retired servers. Calendar the renewal dates so auto-renew does not outlive the hardware.
- [ ] **Cancel circuits and colocation contracts** 5
  MPLS links, point-to-point circuits, colo space serving only the old environment. Watch notice periods — some require 60–90 days.
- [ ] **Remove DNS records and firewall rules for retired systems** 6
  Stale records and open ports pointing at nothing are reconnaissance gifts and future troubleshooting noise.
- [ ] **Disable and then delete retired service accounts** 7
  Disable for 30 days first to catch anything still authenticating with them, then remove.
- [ ] **Remove retired systems from monitoring and backup jobs** 8
  Dead hosts generate alert noise that trains people to ignore alerts; orphaned backup jobs consume storage and fail nightly.
- [ ] **Update the asset register and network diagrams** 9
  Documentation that still shows the 2024 server room fails its first audit question.
- [ ] **Rewrite runbooks for the new environment** 10
  Restore procedure, new-user onboarding, incident response steps, after-hours access. A runbook that says “log into the Hyper-V host” is now fiction.
- [ ] **Run a full restore test in the new environment** 11
  Restore a mailbox, a SharePoint document, and a complete VM from the new backup platform, and time it. Backup you have not restored from is a hypothesis. Record the result as your new recovery baseline.
- [ ] **Notify your insurer and update compliance records** 12
  Cyber-insurance applications and compliance documentation describe your environment; a migration changes the answers. Update them before renewal, not at claim time.

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

ELEVATE
SOLUTIONS

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io