Cloud Migration Security Checklist

Use this quick-reference list to secure every phase of your cloud migration.

1. Inventory all data and classify by sensitivity
2. Map each workload to compliance controls (NIST, ISO, HIPAA, etc.)
3. Establish zero■trust principles (identity verification, micro■segmentation, continuous auth)
4. Enforce MFA and least■privilege IAM roles
5. Encrypt data in transit and at rest (plus key■rotation schedule)
6. Build Infrastructure■as■Code templates with policy■as■code guardrails
7. Stream logs to a centralized SIEM/SOAR
8. Automate vulnerability scans for VMs, containers, and serverless functions
9. Maintain immutable, offsite backups (3■2■1 rule)
10. Test incident■response runbooks quarterly
11. Schedule compliance audits vs. CIS/NIST benchmarks
12. Monitor for drift with CSPM/CNAPP tools
13. Review emerging tech: confidential computing, post■quantum crypto
14. Train staff in secure cloud coding and operations
15. Report progress to the board with clear KPIs (MTTD, patch cadence, etc.)