IAM Cloud Program - Executive Summary

Objective:

Establish a scalable, secure, and compliant IAM function across AWS, Azure/Entra, and GCP to support application modernization, cloud landing zones, and enterprise security objectives. This roadmap outlines a realistic phased strategy for a two-person IAM engineering team with clear deliverables, hiring signals, and success metrics.

Program Pillars

- Compliance: Aligned to NIST 800-53, FFIEC CAT, CSA STAR
- Governance: SailPoint + ServiceNow for access reviews and policy adherence
- Infrastructure as Code: Terraform across AWS, Azure, and GCP
- Tooling Integration: CyberArk, Splunk, Veza, Wiz, Okta (Ping decommission)

Roadmap Phases

Phase 1: Stabilization & Foundation (Q3 2025 - End 2025)
- Build out IAM standards for Azure Landing Zone + AWS 2.0
- Refactor technical debt and migrate Terraform modules
- Document access flows, roles, and application mappings in Confluence
- Stand up IAM resource certification process and knowledge base

Phase 2: Automation & Observability (2026 - Q2 2026)
- Launch central IAM inventory and compliance dashboards
- Integrate Veza, SailPoint, Wiz, CyberArk, and ServiceNow
- Automate tagging, owner validation, and access review workflows
- Finalize AWS -> Okta migration and document operational runbooks

Phase 3: Scaling & Governance as Code (Q3 2026+)
- Introduce policy-as-code and CI/CD enforcement for IAM resources
- Implement JIT access via SailPoint or Okta Workflows
- Build IAM hiring roadmap (Engineer, Ops, Architect)
- Develop analytics around privilege scoring and AI-driven IAM observability

IAM Cloud Program - Executive Summary

Key Success Metrics

- 100% IAM resource-to-owner mapping
- 100% Terraform module coverage for IAM
- Documented IAM access flows across all clouds
- <5% resource drift across platforms
- SLA-backed recertification cycles in place

This roadmap is version-controlled in Confluence and updated quarterly. It enables executive alignment, hiring prioritization, and funding justification for IAM platform evolution.