# 🛡️ IAM Cloud Program Growth Roadmap

## Overview

This document outlines a phased roadmap to guide the development and scaling of the IAM cloud engineering program within a multi-cloud enterprise context. The roadmap provides a strategy for a two-person IAM engineering team to support current priorities, guide future hiring, and establish an enterprise-class IAM function aligned to compliance (FFIEC CAT, NIST 800-53, CSA STAR).

It is intended for leadership visibility and to be documented in Confluence as a strategic guidepost.

## 🎯 Mission Statement

To design, standardize, and scale an enterprise-grade IAM function that secures identity and access across AWS, Azure/Entra, and GCP, supports DevSecOps, and enables business agility while maintaining regulatory compliance.

## 🚀 Phase 1: Stabilization & Foundation (Q3 2025 – End of 2025)

**Goal:** Establish standards, visibility, and core control enforcement for Azure/Entra and AWS.

### 🔹 Azure Landing Zone Support

* Document all IAM access flows and resource provisioning in Confluence
* Build IaC modules (Terraform) for roles, groups, service principals
* Refactor existing technical debt (hard-coded permissions, legacy groups)
* Map IAM resources to applications + owners (CMDB mapping)
* Implement Confluence-based IAM resource knowledge base
* Define process for cross-tenant access and M365 API access control
* Establish baseline certification process for Entra roles + app registrations

### 🔹 AWS Landing Zone Design Support

* Participate in LZ design and legacy gap analysis (IAM 1.0 → 2.0)
* Define standards for new AWS IAM roles, policies, service accounts
* Migrate IAM Terraform modules and assist with remote state management
* Map AWS IAM entities to owners + applications
* Begin building compliance visibility dashboards (Splunk, tagging, manual scripting)

### 🔹 Cross-Initiatives

* Document all authentication flows (Ping + Okta) in Confluence
* Begin code reviews + repository structuring for all IAM terraform repos
* Build ad hoc PowerShell + CLI scripts for IAM analysis
* Establish baseline tagging, ownership, and certification requirements

## 🏗️ Phase 2: Automation & Observability (2026 – Q2 2026)

**Goal:** Improve efficiency, transparency, and policy enforcement across clouds.

### 🔹 Central Inventory + Dashboard Development

* Build internal dashboards for IAM resource tracking and non-compliance
* Integrate data from:
  + Veza (once onboarded)
  + SailPoint (source of truth)
  + Wiz (via API)
  + CyberArk (manual mapping)
  + ServiceNow CMDB
  + Splunk (audit logs)
* Correlate roles, service accounts, permissions, and ownership

### 🔹 Compliance Automation + Certification

* Automate tagging audits and owner mapping validation
* Integrate SailPoint + ServiceNow for re-certification workflow
* Define rules for policy scope and risk scoring
* Develop drift detection tooling for IAM entities vs. Terraform

### 🔹 Okta Migration Finalization

* Support testing, federation integration, and cutover of AWS to Okta
* Document post-migration operational workflows
* Partner with federation team on secrets rotation and assertion validation

## 🌐 Phase 3: Scaling + Governance as Code (Q3 2026 and Beyond)

**Goal:** Harden IAM as a product. Scale with security, DevSecOps integration, and predictive compliance.

### 🔹 IAM as Code Maturity

* Formalize versioned IAM modules (per cloud)
* Enforce policy-as-code for tagging, ownership, role scope
* Introduce CI/CD checks for IAM Terraform PRs
* Implement self-service JIT model via SailPoint or Okta Workflows

### 🔹 Organizational Scaling

* Define hiring roadmap:
  + IAM Cloud Engineer (Terraform + tooling)
  + IAM Operations Engineer (certification + support)
  + IAM Architect (future-state design + tool ownership)
* Embed IAM engineers in cloud/platform working groups
* Create IAM steering council to govern policy exceptions, drift response, JIT eligibility

### 🔹 Long-Term Analytics & Insights

* Build behavioral models for privilege scoring (based on usage)
* Use AI/LLM agents to correlate IAM risks across cloud, CMDB, and SIEM
* Enable dashboard exports for audit readiness + executive reporting

## ✅ Success Metrics

* 100% of IAM resources mapped to app + owner
* 100% of Terraform modules reviewed + versioned
* All IAM access flows documented in Confluence
* <5% IAM resource drift across platforms
* SLA-driven access certification cadence in place

This roadmap will evolve quarterly and be version-controlled in Confluence. It acts as the foundation for IAM team scaling, hiring, tooling adoption, and engineering prioritization.