## **Job Description: IAM Principal Engineer (5‑8 yrs Experience)**

**Position Title:** IAM Principal Engineer – Multi‑Cloud Governance  
 **Career Level:** Principal / Lead Engineer  
 **Role Type:** Hybrid (onsite/office + remote), with regional presence

**About the Team:** You will help lead a greenfield enterprise IAM initiative across AWS, Azure/Entra, and GCP. You will work closely with executives, architecture teams, SailPoint governance, and cloud teams to drive modernization, automation, and secure identity posture.

**Impact:**

* Be the key technical driver of a scalable, code‑driven IAM program aligned to NIST, CSA STAR, and FFIEC.
* Help transition fragmented IAM control models into unified, automated identity governance (SailPoint, CyberArk, Veza integration).
* Lead policy-as-code enforcement, JIT access enablement, and cross-cloud federation modernization.

**Key Deliverables:**

* Design and implement RBAC/ABAC models across cloud platforms, federating via Okta and migrating AWS from Ping → Okta.
* Author Terraform modules for cloud IAM: roles, policies, service accounts; integrate gating via OPA, Checkov, or Sentinel.
* Automate secrets lifecycle: auto-rotation in AWS Secrets Manager, Key Vault, Secret Manager, and CyberArk via IaC.
* Configure JIT access: SailPoint-based workflows, Azure PIM, time-bound role elevation, and approval logic.
* Onboard Veza for identity posture visibility; build dashboards and feedback loops for continuous least-privilege enforcement.
* Oversee Splunk integration: ingest IdP, IAM, and secrets access logs; build IAM-specific dashboards and alerting.

**Skills & Qualifications:**

* 5–8 years IAM experience, with multi-cloud hands-on work (AWS, Azure/Entra, GCP).
* Strong knowledge of SailPoint IdentityIQ, Okta, Ping Identity, CyberArk.
* Deep federation experience: SAML 2.0, OIDC, OAuth; service-to-service federation (OIDC, Roles Anywhere, Workload Identity Federation).
* Proficiency in Terraform; expertise in PaC tools (OPA, Rego, Sentinel, Conftest).
* Scripting: Python, PowerShell, Bash.
* Familiarity with compliance frameworks: NIST 800‑53, FFIEC, CSA STAR, SOX, GDPR.
* Excellent communication and mentorship skills for working with architects and executives.

**Leadership Qualities:**

* Takes strategic ownership, mentors junior engineers.
* Advocates for security-first, automation-first culture.
* Communicates complex technical topics clearly to stakeholders and executives.

**Collaboration:**

* Works cross-functionally with Cloud Architects, Security Ops, DevOps, Comms, and Compliance teams.
* Partners with business units to enforce CMDB tagging, owner accountability, and audit preparation.

## **Job Description: IAM Senior Engineer (3‑5 yrs Experience)**

**Position Title:** Senior IAM Engineer – Cloud Governance  
 **Career Level:** Senior Engineer  
 **Role Type:** Hybrid (regional office / remote setup)

**About the Team:** You will join our expanding IAM Cloud team supporting identity infrastructure across AWS, Azure and GCP. The role is deeply technical, hands-on, and pivotal in enabling automation, compliance, and secure identity governance.

**Impact:**

* Implement critical parts of the multi-cloud IAM program—Terraform pipelines, federation flows, JIT access onboarding.
* Support pilot projects like Veza onboarding, Azure IaC kickoff, and secrets rotation automation.
* Help reduce privilege shadows by integrating telemetry-driven role reviews and access certification campaigns.

**Key Deliverables:**

* Implement Terraform-based IAM resources: roles/policies/service accounts for AWS, Azure, GCP.
* Script automation integrations (Python/PowerShell) for user/service provisioning, secrets syncing, and CMDB tagging.
* Assist in enabling JIT via SailPoint and Azure PIM; support pilot elevated access workflows.
* Support compliance automation: tag enforcement, least-privilege validation, drift detection triggers.
* Help onboard Veza and assist with dashboards that visualize identity metrics and excess privilege signals.

**Skills & Qualifications:**

* 3–5 years of IAM experience, including cloud environments (AWS, Azure, GCP).
* Experience with Okta or Ping Identity, SailPoint (or similar IGA), and CyberArk.
* Working knowledge of SAML, OAuth, OIDC, RBAC, ABAC.
* Practical Terraform experience; familiarity with IaC review pipelines.
* Ability to script in Python, Bash, or PowerShell.
* Understanding of identity compliance regimes: NIST, FFIEC, CSA.
* Strong problem-solving and written communication skills.

**Leadership & Collaboration:**

* Participates actively in solution delivery; supports technical decisions.
* Collaborates with Product, Security Operations, and DevOps.
* Engages in sprint planning, and contributes to technical ticket grooming and reviews.