KPMG

IAM Community Call - IHG Cloud Identity Security Engagement Spotlight

January 2024

Agenda

1. Introduction & Approach
2. Privileged Identity Framework & Access Types
3. Current State Assessment & Role Analysis
4. Guiding Principles for Target State
5. Target State Requirements & Architecture
6. Target State Roadmap

Engagement Overview

IHG Cloud Identity Security

IHG engaged KPMG to perform a risk analysis and assessment of identity controls across their multi-cloud environment.

The engagement team performed an assessment of IHG's AWS, GCP, and Azure environments through discovery workshops and a risk-ranked analysis of over 9,000 privileged roles and permissions.

Key findings from this assessment served as the foundation for the development of target state requirements and architecture for cloud identity controls across IHG's cloud ecosystem.

Cloud Permissions Discovery & Analysis

- Identify potential capability gaps across cloud identity control planes measured against leading practices
- In-depth discovery and analysis of privileged identities, roles, and entitlements across hyperscale cloud environments
- Define and apply a risk-based approach for analyzing privileged identities and permission types in the cloud
- Develop future state identity governance, access management, and privileged identity management requirements to reduce risk while maintaining user experience, velocity, and scalability

Target State & Remediation Roadmap

- Develop a holistic architecture to strengthen identity controls and capitalize on existing capabilities and technology investments
- Define a roadmap to rollout enhanced capabilities and address key improvements around people, processes, and cloud technologies
- Identify roles, responsibilities, and requirements needed to achieve the target state and maintain a heightened security posture across the organization

Our Approach to Cloud Identity Security

The engagement team approached IHG's challenge through the following phases of work:

Current State Assessment

Information gathering during discovery and current state assessment, including:

- Key identity-based observations and pain points
- Risk-ranked evaluation of privileged identities
- Identification of leading practices via KPMG engagement delivery and cloud security, IAM, and industry trends

Defined Target State

- Target state defined to close capability gaps and increase cloud maturity.
- Requirements and architecture created to guide the client to the target state by addressing defined security gaps and incorporating industry leading practices.

Implementation Roadmap

- Key activities defined to assist IHG in to transition towards target state.
- Project details, cost, and resourcing requirements established.

Cloud Identity Access Types

Access Type	Description
Individual Access	Access associated with a unique federated human identity that has been provisioned privileged access to a hyper scale cloud environment. Privilege for these accounts is governed outside of the cloud environment (directory services, IGA solution, etc.)
Shared Account Access	Account created and managed directly within cloud environment directories. These accounts maintains standing privilege and are interacted with by human users or group of users.
Non-Interactive Access	Accounts used for programmatic access between applications and/or cloud resources. This classification of account is created and managed directly in the cloud directory and persists for extended periods of time.
Workload Access	Workload access is defined as human interactive access to infrastructure created as part of a dynamic cloud workload (i.e., Virtual machines, databases, Kubernetes clusters, etc.)

KPMG Privileged Identity Management (PIM) Framework

The following privileged identity framework was leveraged to assess and classify key observations across security & IAM domains:

Governance

- Roles & Responsibilities
- Metrics & Reporting
- Policy & Procedure Management
- Cloud Strategy
- Resourcing & People Management
- Solution Architecture

Management

- Identity Lifecycle
- Access Request & Approval Workflows
- Access Recertification
- Access Modeling (Least Privilege)

Control

- Authentication & MFA
- Credential & Secrets Management
- Infrastructure Management
- Account Onboarding
- Access Modeling (Enforcement)
- Platform & Policy Management

Monitoring

- System & Account Reconciliation
- Session Recording & Monitoring
- SIEM Integration
- Behavioral Analytics
- Security & Compliance Reporting

Target State Requirements & Architecture

Sample Role Analysis Dashboard

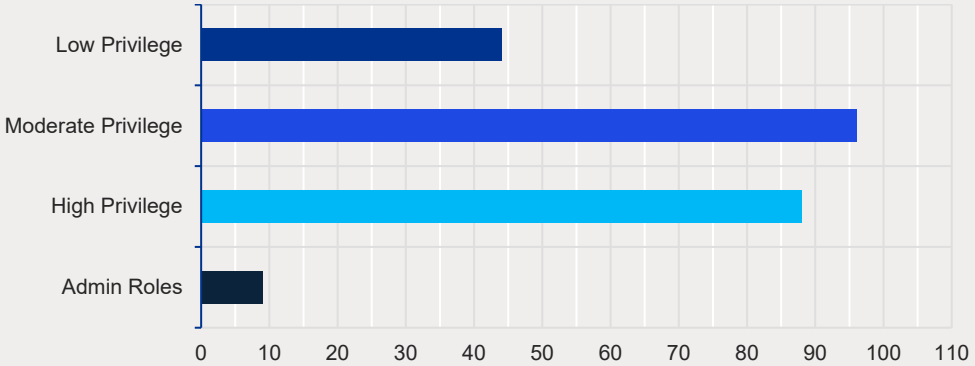
Overview

- 1,042 privileged users identified within IHG's GCP environment, managed by 237 roles across 4,315 role to user assignments.
- 149 users with administrator rights across the environment.

Risk Findings

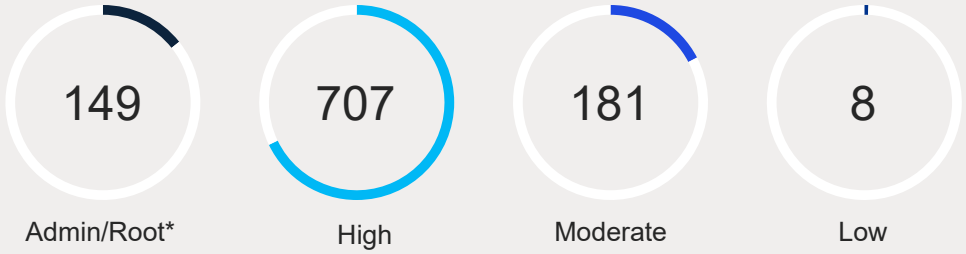
- 28 users assigned to organization-wide admin/root access.
- 16 service accounts with admin level privileges at project level.
- No lifecycle management for service accounts within GCP. nearly 4,000 identified by Wiz (CIEM).
- No separation of privilege, all users access the console with IHG primary credentials.

Role Breakdown by Privilege Type



	Admin Roles	High Privilege	Moderate Privilege	Low Privilege
Privilege Level	9	88	96	44

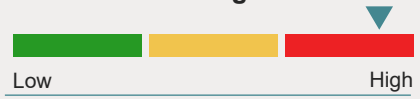
User Breakdown by Privilege Type



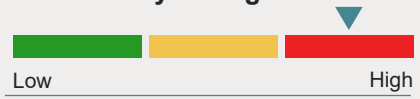
Privileged Risk Assessment

Number of Admins

Number of Privileged Users



Role / Policy Management



Observable Risks

Key Inputs & Driving Factors

The following challenges observed can prove difficult to navigate and restrict the ability to achieve a heightened maturity level.

Governance

- Policies & controls applied inconsistently across providers, leveraging disconnected or siloed solutions per environment.
- Lack of cloud identity-centric reporting metrics, KPIs, and KRIs, resulting in lack of visibility to key focus areas.
- Higher volume and dynamic nature of cloud-based accounts presents unique challenges as infrastructure scales and evolves.

Management

- Gaps in identity governance controls applied to privileged, non-privileged, and machine identities present inconsistencies in managing identity lifecycles.
- Manual provisioning and deprovisioning controls can increase amount of standing access and accumulation of excessive privilege.

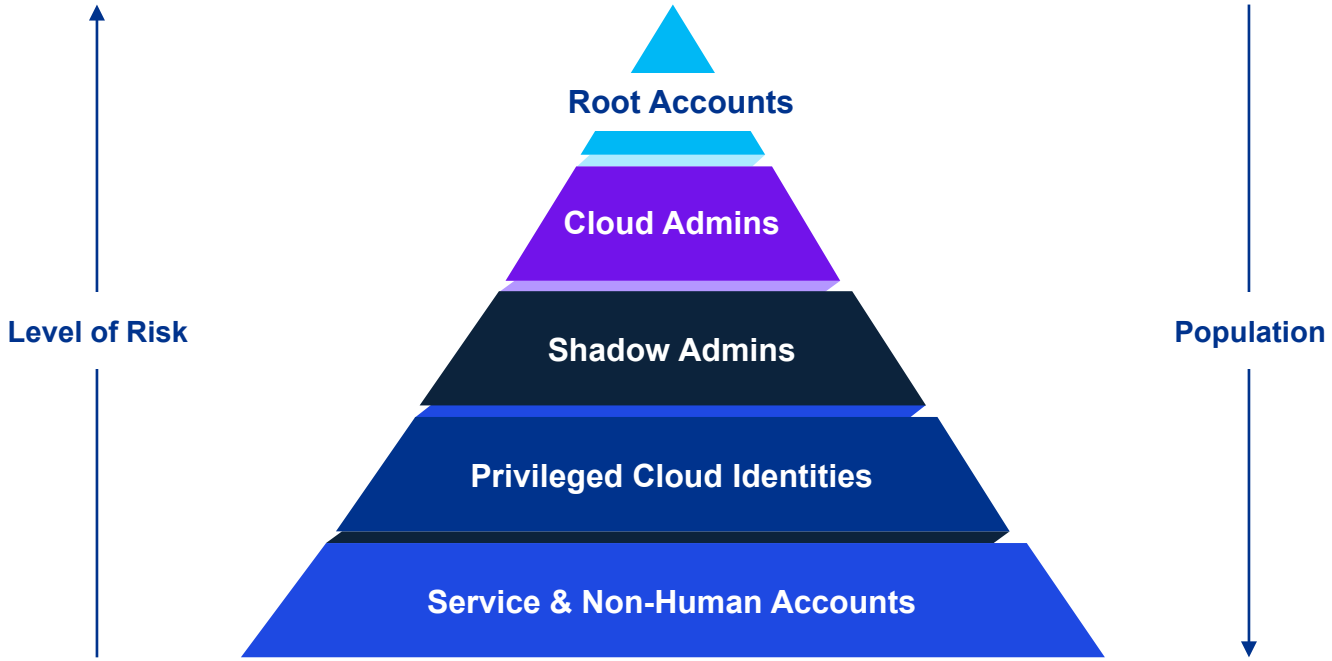
Control

- Credential rotation and session isolation for cloud directory-mastered accounts is often not applied due to lack of comprehensive discovery technique or connectors required.
- Discovery and management of service accounts, access/API keys, and machine identity credentials are often overlooked.

Monitoring

- Monitoring and alerting capabilities are often diminished by the volume of activity ingested across multi-cloud environments.
- Cloud consoles can be left open to users outside the organization and lack conditional or step-up authentication policies.

Identity-based Prioritization & Controls



Identity Type	Acces Mgmt.	PAM	Least Privilege	Secrets Mgmt.	Lifecycle Mgmt.	Compliance
Root Accounts (Shared)		✓			✓	✓
Cloud Admins (Individual)	✓	✓	✓		✓	✓
Shadow Admins (Individual)	✓	✓	✓		✓	✓
Privileged Cloud Identities (Individual, Workload)	✓	✓	✓		✓	✓
Service & Non-Human Accounts (Non-Int., Workload)			✓	✓	✓	✓

Guiding Principles for Target State Environment

As a result of the current state assessment, the client's strategic plan for risk reduction, and industry leading practices, the following principles were utilized in the development of target state requirements & architecture.

Minimize control gaps & inconsistencies	*Consolidate and enhance identity controls and processes*
Reduce attack surface & enforce accountability	*Limit use of shared accounts, transition towards federated access model*
Enhance account lifecycle management	*Expand IGA integration and introduce automation*
Secure highest-risk identities (Root & Cloud Admins)	*Privileged account vaulting, session monitoring, and credential rotation*
Reduce standing privilege in the cloud	*Integrate JIT access controls across cloud consoles & workloads*
Enhance monitoring, alerting, and reporting	*Tightly integrate SIEM & CIEM solutions with cloud environments*
Real-time misconfiguration identification & remediation	*Tailor and automate CIEM reporting, establish identification & response process*

Target State Requirements & Architecture

The primary objective of the target state was to define requirements and architecture needed to improve access controls, minimize creation of 'non-compliant' identities, and provide detailed flows for each account type / use case.

IGA

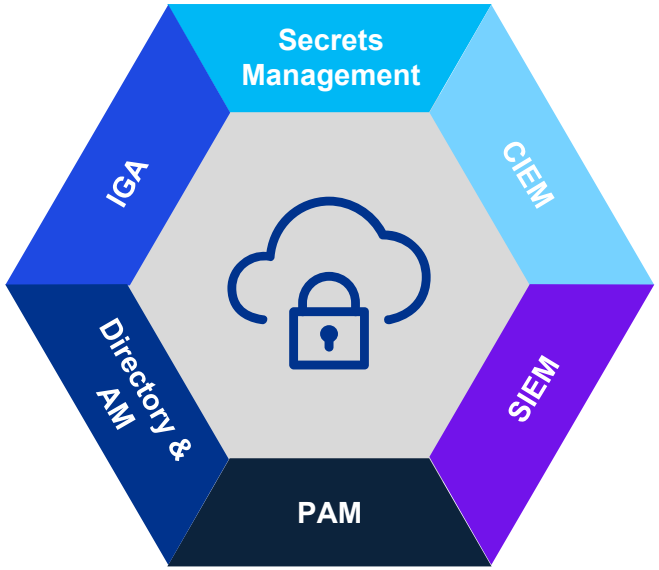
- Central solution for access request, certifications, and account provisioning / deprovisioning
- Leverage cloud connectors for integrated lifecycle management
- Increase visibility through inventory capabilities association of contextual account metadata

Directory Services

- Leverage virtual directory for 'flat' view of multiple active directory domains
- Virtual directory serves as single mechanism for integration with SSO / MFA solutions and PAM / JIT solutions for access policy management

Privileged Access Management

- Leverage connectors for credential rotation and session management of cloud-native accounts
- Introduce net-new solutions for just-in-time access to cloud consoles and workloads
- Integration with secrets management solution for securing cloud-native machine identities



Access Management

- Leverage cloud-hosted SSO / MFA solution for single point of entry across all cloud providers
- Enhance conditional access policies for access to downstream systems (i.e., just-in-time solutions)

CIEM

- Leverage tailored CIEM reporting capabilities for identification and remediation of misconfigured (over-provisioned) identities and roles
- Enhance visibility into cloud identity metrics via custom queries and dashboards

SIEM

- Deepen integration with hyperscale environments for stronger log aggregation and analysis
- Tailor alerts across cloud environments for faster recognition and response to potential threats

General Target State

Potential Risk

Lowest

Zero Standing Privileges

- Access rights no longer granted just-in-time.
- Least privileged access rights are created and deleted on the fly for each session.
- Greatly reduces risk of compromised access and the impact of the access.

Medium

Just-in-Time Access

- Access can only be elevated just-in-time, but at regular intervals.
- No restrictions on commands and permissions.
- JIT access reduces the risk of compromised access but does not reduce impact of the access.

Highest

Standing Access

- Standing access secured by PAM controls, vaulted, and isolated
- User accounts always exist in target systems (24/7 access).
- No restrictions on commands and permissions.
- Risk is mitigated but still present even with identity security and governance controls in place.

Guiding Principles for Managing Cloud Access

Identity Type		Use Case	Recommend Method	Environments
Extended IT IT Admins IT Ops Third-Party Vendors	**Developers** Engineering Teams DevSecOps Data Analysts	Secure access, controls, and experience for CSP services in the cloud	Native, zero standing privileged access	• AWS EC2, S3 • Azure SQL, VMs • Google Compute, Storage
		Secure access to workloads on cloud infrastructure (IaaS)	Dynamic, just-in-time access	• Linux & Windows VMs • Kubernetes Clusters • Docker • SQL Databases
		Secure access to datacenter & lift-and-shift workloads running in VMs	Vaulted, isolated access for standing accounts and system access	• Linux & Windows VMs • VPN Services • Oracle & SAP Services
		Secure access to third-party SaaS apps	Session protection and monitoring	• Salesforce • Confluence • Datadog

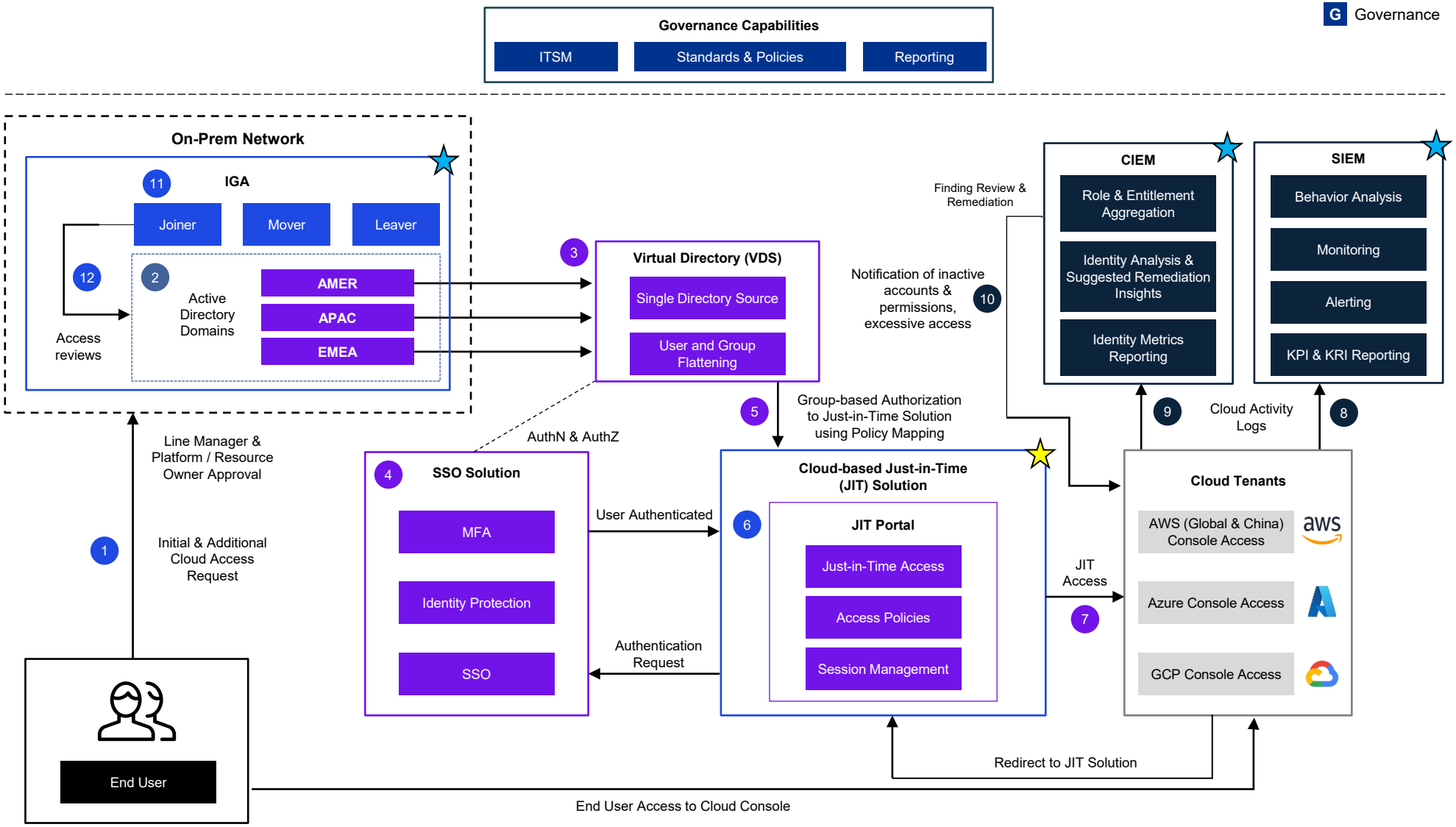
Target State Architecture – Individual

Legend

New Solution | Enhanced Capability | On-Prem Solution

Framework Layer

G Governance | M Management | C Control | M Monitoring



Processes & Functionality	
#	Description
1	Users request access to cloud resources through the IGA Solution. Each request should have two stages of approval (Line Manager, Platform / Resource Owner).
2	Users added to AD groups mapped to just-in-time policies that grant permission to assume roles on cloud hypervisors via the just-in-time solution.
3	Virtual Directory Service (VDS) provides a single directory view and normalizes data across Active Directory domains.
4	SSO and MFA challenge required to access just-in-time solution.
5	Directory group membership pulled into just-in-time solution and mapped to role policies.
6	Policies grant implied approval for users to elevate privilege just-in-time for daily operations. Approval workflow is available for ad-hoc elevation not permitted by group membership.
7	User access to cloud console is granted dynamically through sessions brokered by just-in-time solution.
8	Cloud logs are pulled into SIEM to alert and monitor on console activity.
9	Cloud logs are pushed to CIEM for identity data aggregation and entitlement review reported via queries and dashboards.
10	CIEM provides identity & role insights and suggested remediation activities to cloud administrators.
11	IGA solution used for automated review of security group membership
12	Access reviews are performed on a quarterly basis for users with membership to cloud directory groups.

KPMG

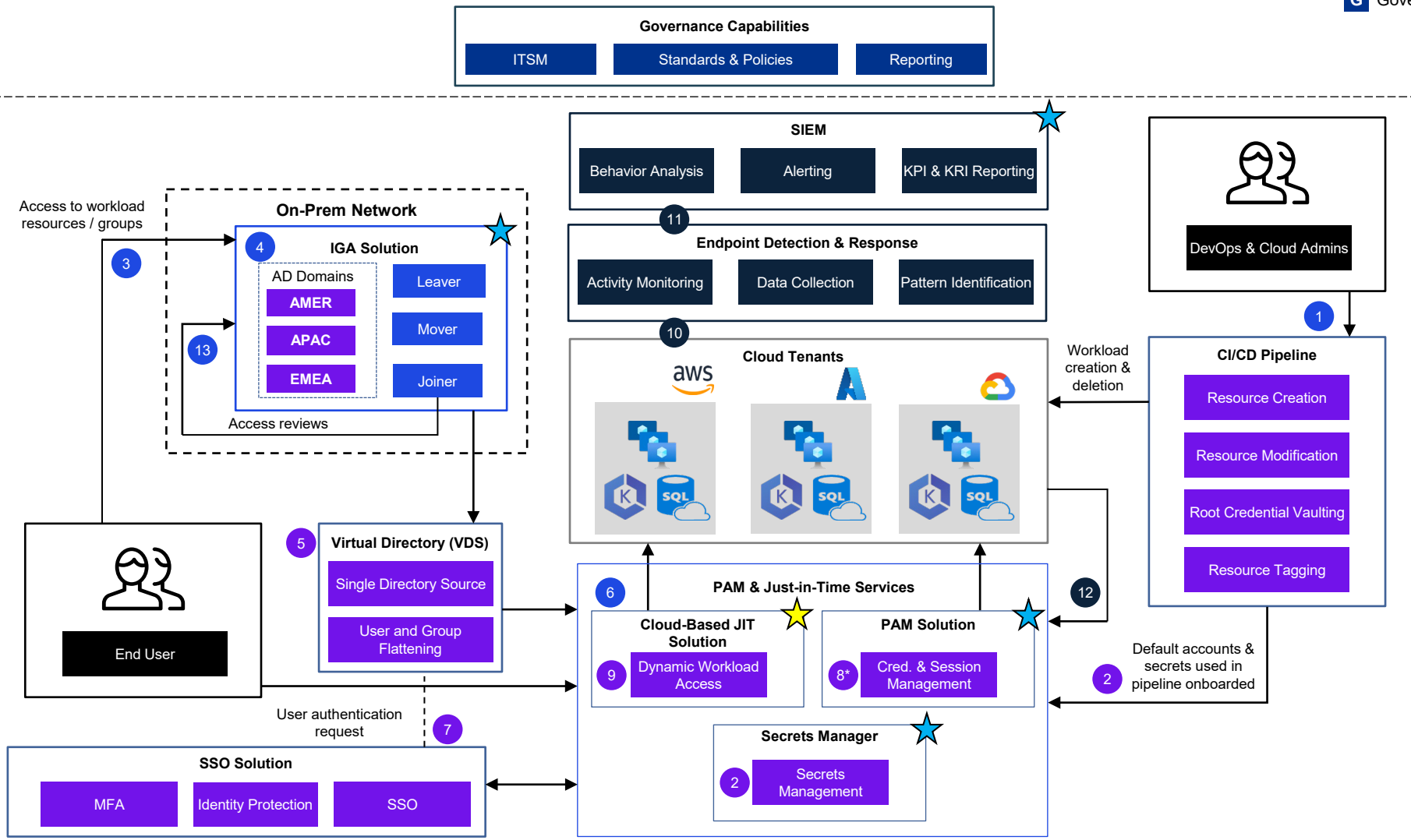
Target State Architecture – Workload

Legend

New Solution | Enhanced Capability | On-Prem Solution

Framework Layer

G Governance | M Management | C Control | M Monitoring



	Processes & Functionality
1	Workload creation in production cloud environments administered via CI/CD pipelines.
2	Default workload credentials created as part of resource instantiation secured in PAM. Credentials used in pipelines secured in Conjur.
3	Access to cloud resources requested through IGA solution to AD group membership. Each request should have two stages of approval (Line Manager, Platform / Resource Owner).
4	IGA Solution manages lifecycle of groups granting access to PAM and JIT solution.
5	VDS provides single directory view and normalizes data across IHG's Active Directory domains.
6	Directory groups are read into PAM & Just-in-Time Access Portals, which grant users access to PAM safes and eligible JIT privilege into cloud resources.
7	SSO and MFA challenge to access PAM solution and just-in-time access solution.
8	***Optional:** Default root and administrator account credentials checked out from PAM for break glass to access cloud resources.
9	Ephemeral accounts created on cloud resources, removing all standing privilege and credential management.
10	Endpoint Detection and Response (EDR) capabilities configured on cloud resources for activity monitoring and data collection.
11	EDR service forwards logs into SIEM tool for alerting and reporting.
12	Cloud integration with PAM used to reconcile root accounts as resources are modified and deleted.
13	Directory group membership to resource groups reviewed on a quarterly basis.

Principles for Roadmap Development

Cloud Security Programming

- Implementation efforts will consist of collaborative workstreams, each with an output empowering future projects and improving overall cloud security posture.

Tactical Prioritization

- The target state journey should begin with tactical remediation initiatives. The completion of these activities will rapidly improve the security posture of the cloud ecosystem.

Immediate Risk Reduction

- Operational, financial, reputational, and other risks will be mitigated throughout the target state implementation.

Phased Approach to Zero-Trust

- The activities included in this implementation will support the journey towards zero-trust by removing standing entitlements, enforcing least privilege, and implementing just-in-time access controls.

Measurable Success & Business Value

- Key performance and risk indicators delivered as part of these exercises will help quantify risk reduction & maturity improvements over time.

Illustrative Roadmap

Legend – Account Types

- Individual Interactive
- Root & Shared Interactive
- Standing Non-Interactive
- Workload Access
- All Account Types

Privileged Identity Framework Layer

	2024 Q1	2024 Q2	2024 Q3	2024 Q4	2025 Q1 & Q2
Governance	Intake Process, Planning, & Change Management				
	(1) Establish Definition of Privileged Cloud Access; Revise Cloud Identity Standards & Policies		(8) Define Cloud Identity KPIs/KRIs; Aggregate & Analyse Identity Data; Integrate Data with Reporting Solution; Automate Repeatable Reporting Process		
Management			(9) IGA Integration with Role-Mapped Security Groups; Define Access Request Process for Individual Interactive Accounts; Define Access Request Process for Shared Interactive Accounts; Access Review Process Defined & Deployed; Lifecycle Management and Access Review Processes Automated		(10) Data Discovery & Classification; Data Tagging; Privileged Data Access Controls Implemented
					(11) SaaS Application Discovery & Classification; Application & Data Risk Ranking; Implement SaaS Access Control & PAM Mechanisms
Control	(2) Analyse & Prioritize Accounts Based on Risk-Ranking; Removal of Inactive Individual Accounts; Prioritized Remediation of Privileged Identity Discovery Findings; Removal of Inactive Shared Accounts; Configuration of CyberArk Cloud Plugins; Onboard Cloud Root Accounts to CyberArk; Migrate Individual Accounts to Federated Model; Onboard Shared Cloud Accounts to CyberArk; Configuration & CyberArk Cloud Plugins; Removal of Inactive Service Accounts & Machine Identities; Onboard High-Risk Service Accounts to CyberArk; Remediate Overprovisioned Accounts				
	(3) Integrate SSO/MFA & Conditional Access Policies with Cloud Environments; Review & Create Catalogue of Cloud Roles; Remediate Over-Privileged Roles; Create AD Groups & Integrate Mapping to Cloud Roles; Remove Locally Assigned Privileges; Enforce Federal Access; Enforce Least Privilege; Automate Processes via IGA				
		(6) Define Requirements & Use Cases; Procure, Deploy, & Test JIT Solution; Analyse Pilot Outcomes	(7) Design JIT Solution (Console); Prioritize Rollout Approach; Build & Integrate with IAM, PAM, and Monitoring Controls; Deploy JIT Solution to AWS, Azure, & GCP Environments		
		Define Requirements & Use Cases; Procure, Deploy, & Test JIT Solution; Analyse Pilot Outcomes	Design JIT Solution (Workload Access); Prioritize Rollout Approach; Build & Integrate with IAM, PAM, and Monitoring Controls; Deploy JIT Solution to AWS, Azure, & GCP Environments		
Monitoring	(4) Design & Configure Cloud Identity Alerts and Reports; Review and Revise Detection and Response Procedures; Automate Log Analysis and Alerting Capabilities				
	(5) Define Key Metrics & Data Points for Analysis; Configure CIEM Reports & Alert Dashboards; Establish Reporting & Remediation Processes				

#	Project Name
1.	Enhance Cloud Identity Standards & Policies
2.	Account Onboarding, Remediation & Clean-Up
3.	Cloud Role Modelling, Authentication Enhancements, & Least Privilege Enforcement
4.	SIEM Solution Enhancements
5.	CIEM Solution Enhancements
6.	JIT Solution Validation & Pilot
7.	JIT Solution Rollout
8.	Cloud Identity Metrics & Reporting Dashboards
9.	IGA & ServiceNow Enhancements
10.	Privileged Data Discovery & Tagging
11.	Application Control Mapping

KPMG