KPMG

Navigating the Cloud for Identity Access Management

Solutions for the State of California

Identity and Access Management (IAM) has been a well-known and well-defined set of processes and tools intended to enable users' access to resources. The importance of well-designed and efficient IAM capabilities has a direct impact on business agility, efficiency, and critical data protection initiatives. Identity is a key enabler in allowing enterprises to collaborate and connect people to resources, but also a necessity in order to collaborate with business partners and customers.

In recent years, we have observed that the general trend towards adoption of cloud technologies is beginning to affect traditional IAM implementations and thinking as organizations continue to navigate the IAM landscape.

Extend Current IAM, Use Cloud IAM, or Both?

Typically, three key questions underpin the combining of cloud and IAM for many organizations:

- How do I extend my existing enterprise IAM capabilities to manage access to Cloud Service Providers (CSPs)?
- How should I leverage cloud-based IAM services to augment or replace legacy enterprise IAM investments?
- How do I bridge the gap as the IAM landscape evolves?

As enterprises struggle with these questions, vendor solutions in the cloud IAM space are nascent and continue to evolve. Some specific issues include:

- Many traditional IAM solutions do not naturally extend to CSPs.
- Native cloud-based IAM solutions are just now coming to market.
- Some vendors are positioning their solutions as native cloud-based IAM capabilities, but in reality are just on-premise solutions hosted in the cloud.
- Many point solutions exist in the market that claim to address more than they do.
- Underlying cloud identity standards are relatively immature, and vendor solutions are not helping to clarify their adoption.

Addressing Identity Data, Integration, and CSP Solution Risks

In our assessment of the key risks raised by IAM and the cloud, we believe that each fall into one of three broad categories. These risks represent key questions that organizations should consider in order to develop an effective approach for managing identity and access to the cloud:

- Risks related to **identity data** – "Identity data" includes stored data related to users' accounts, credentials, or attributes, all of which are fundamental to driving identity management processes.
- Risks related to **integration** – These risks relate to the processes and technologies that an enterprise employs to connect to or use cloud services.
- Risks related to **CSP solutions** – Some risks are inherent cloud provider solutions themselves. These risks focus on the IAM elements of CSPs.

Identity data

- Can existing enterprise identity data be used directly in CSP solutions, or should new external CSP accounts be provisioned rather than exposing enterprise identity data?
- How much identity data should be shared?
- How are CSPs protecting the data? Where is it stored? If it is synchronized into other geographies by the CSP, are there data privacy concerns?
- How is the identity data handled by the CSP? Who has the ability to modify the data? Is that ability shared with others?
- If data is synchronized rather than provisioning new accounts, how will ongoing changes to multiple copies of the data be dealt with? How will conflicts be handled/reconciled? Does this approach scale to multiple CSPs?

Integration

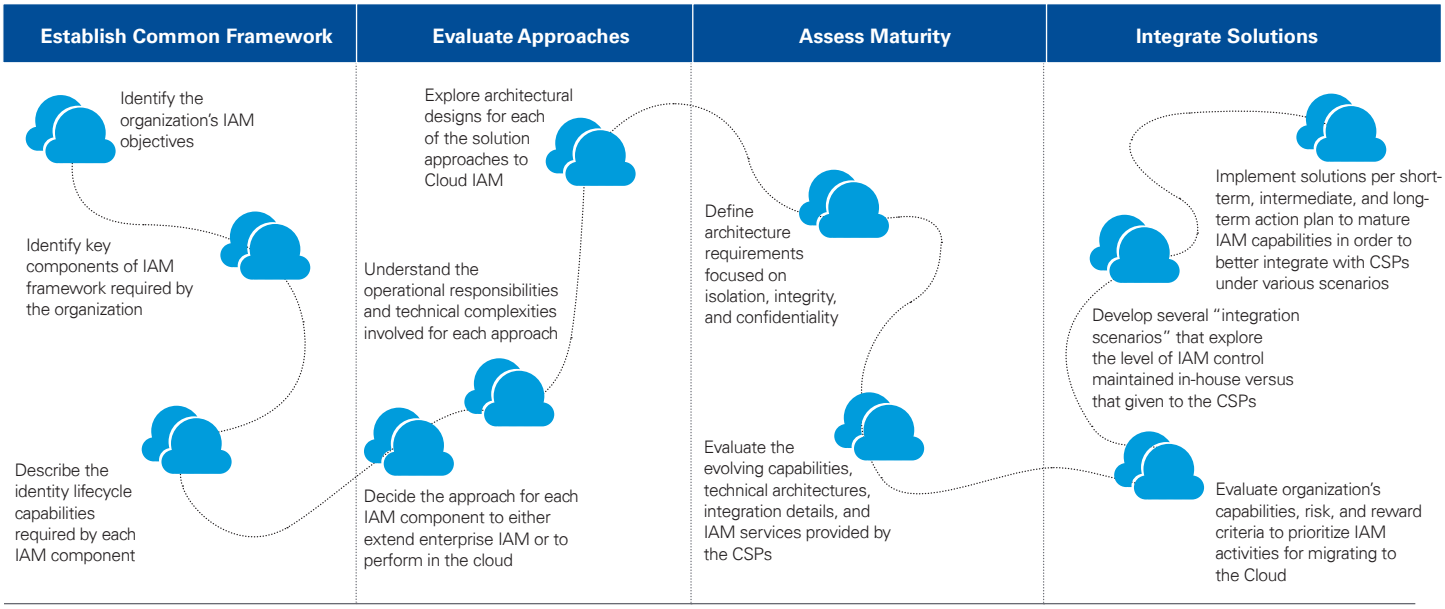
- Do all of the expected functions related to identity management (provisioning, SSO, self-service, reporting, etc.) work between CSP and the enterprise?
- Will duplicate and/or new processes specific to CSPs need to be created?
- Will new technical integration approaches (such as SAML, OAUTH, SPML) need to be implemented? Does the organization have the skills required?
- Do existing enterprise permissions map cleanly into the CSP's access model?
- Is the trust model implied by the standard contractual terms provided by many CSPs acceptable?
- Is the use of public identity providers acceptable? Is the enterprise willing to establish integration/trust relationships with them?

CSP Solutions

- Are CSP solutions—particularly those related to cloud-based IAM providers—mature?
- Are the underlying technical architecture and standards adopted by CSPs aligned with our enterprise?
- Have the availability concerns been addressed—when CSPs rely on enterprise identity data and when cloud-based IAM services are deployed?
- How will administrators (privileged users) for CSP solutions be managed? Should similar controls be put in place to manage them as would be for the enterprise, and is this possible?

KPMG Cyber's Cloud IAM Approach

In addressing these key cloud IAM questions, we have devised an approach that starts with establishing a common framework through integrating IAM solutions.



Starting With A Common "Identity" Framework

We recommend that organizations take a structured approach in evaluating options to move forward. Our approach to planning for solution implementation is based on our IAM framework. This framework is intended to provide a standard set of terminology describing IAM capabilities, which in turn provides a mechanism for thinking through in an orderly fashion ways that access can be provided.

The KPMG Cyber's IAM framework is equally relevant to cloud-based IAM models and traditional, enterprise IAM. We have helped many organizations define their IAM strategy—whether involving cloud components or not—using this or similar industry frameworks.

There are eight key components in KPMG Cyber's IAM framework that demonstrate the lifecycle of identity management.

Objective	Key components	Description
Access modeling	Role governance	Grouping of access rights into roles to align with business functions, typically organized by enterprise hierarchy. Ongoing management and oversight of these roles.
	Entitlement management	Repeatable processes related to the ongoing management of resource-level (such as application or operating system) access permissions. Translation of permissions to application roles. Analysis of permissions for completeness and conflicts.
Access creation	Identity management	User life-cycle processes (add, modify, remove) associated with establishment and maintenance of identities. Typically these processes involve data collection, approval of entitlements, and workflows.
	Provisioning	Fulfillment activities related to the creation of accounts and assignment of entitlements. Fulfillment can be automated or manual.
Access enforcement	Authentication	Real-time mechanisms to validate user credentials against an authentication store to confirm/deny the identity's access to resources.
	Authorization	Real-time decision and enforcement of policies to allow/disallow the access to resources.
Access review	Certification	Review and approval of assigned accounts and entitlements for a resource. Includes gap analysis between designed and actual access.
	Monitoring	Real-time monitoring as well as historic archival of authentication, authorization, and access events.

Extending Enterprise IAM vs. Performing IAM in the Cloud

Of primary importance to most organizations is establishing a coordinated IAM approach with CSPs now, as organizations find themselves in the cloud today, whether driven by measured planning or organic solutions from different parts of the business. The solutions to consider will depend on the implementation approach adopted for IAM whether extending the enterprise IAM versus performing IAM functions in the cloud.

- **Extending enterprise IAM to the cloud** – Core IAM functions are performed and controlled by the enterprise; however, the changes and impacts are manifested on the resources at the CSPs. In technical terms, the enterprise is the "IdP" (identity provider) and the CSP is the "SP"(service provider).
- **Performing IAM functions in the cloud** – Core IAM functions are performed and controlled by an "identity CSP," impacting the resources and services provided by the enterprise, other CSPs, or third parties (e.g., business partners) acting as a service provider.

In the table below, we have compiled a nonexhaustive list of planning approaches that most organizations are considering today, organized by the elements of KPMG Cyber's IAM framework.

Key components	Extending enterprise IAM	IAM in the cloud
Role governance	— Most organizations extend the local role governance model to the CSP roles assigned to user accounts in the cloud. CSPs (and cloud application entitlements) are expected to adhere to enterprise roles defined centrally. — This also involves the CSPs sharing access data for modeling, which will be performed within the organization's role management solutions. — One mechanism to allow sharing of enterprise authorization constructs with CSPs is through standards such as XACML for attribute or role-based access on CSPs.	— IAM in the cloud operates in a similar fashion to extending enterprise IAM, with the difference that the role management and governance processes are driven by a cloud-based role governance solution. — This involves making the CSP an authoritative source for enterprise roles, and modeling other service provider entitlements to fit into the available role constructs. — Mechanisms that enable this require the cloud-based role governance service to have full visibility into the application roles within all service providers (such as other CSPs/third parties).
Entitlement management	— Entitlement management processes to aggregate access information from all CSPs as well as to analyze the information per business rules (SODs, conflicting access, etc.) is performed by the enterprise. — Involves expecting all CSPs to share fine-grained entitlements for all user accounts with the enterprise analysis engine. — The mechanisms to apply the corrective action coming out of such analysis require the CSP to allow dynamically changing user account entitlements per enterprise needs.	— Differs slightly from extending enterprise IAM in that the entitlements analysis may be performed in the cloud. — Involves a significant amount of sharing of fine-grained CSP application entitlements from multiple service providers to the central cloud-based entitlements analysis service. — Most implementation mechanisms find it difficult to aggregate a full and thorough view of access from multiple CSPs in order to be able to provide a unified view of entitlements for analysis.
Identity management	— Most organizations own and operate the identity store, and drive the data collection and workflows/approvals within the enterprise. However, local lifecycle events (adds, modifications, and removal of users, for example) that change the identity data result in changes to the user accounts on the CSP services (e.g., applications). — Involves establishing a federation dialect to share identity data from local identity stores to CSP account information. — One example of a mechanism to achieve this is to perform "push-based" identity data updates/synchronization with the CSP using standards-based Web APIs.	— Operates similar to the extending enterprise IAM, with the difference being that a CSP acts as the Identity Provider (IdP) and hence the identity management engine resides in the cloud. — Approach requires the CSP to be able to receive enterprise lifecycle events directly and to update its IdP schema. These changes must be communicated to other Service Providers (SPs) within other CSPs or third parties like business partners. — One way to achieve this is by leveraging a near-complete identity management approach hosted in the cloud (i.e., an IdaaS) that implements management processes for cloud identities. The emerging solution from Identropy is one such approach. However, it is important to note that many IdaaS solutions are attempting to layer provisioning capabilities atop core identity management in the cloud (e.g., Symplified).

Key components	Extending enterprise IAM	IAM in the cloud
Provisioning	— Organizations trigger account creation/ modification/removal based on local business processes and policies. However, CSPs must be able to accept provisioning instructions from enterprise IAM solutions in the event that provisioning is automated. — Some mechanisms to achieve this include the use of SPML or SCIM from the enterprise IAM platform, or using Web APIs exposed by the CSPs to perform provisioning procedure calls.	— The difference between this model and extending enterprise IAM is that the cloud-based identity service now acts as the fulfillment engine to create accounts on service providers (e.g., other CSPs, third parties, etc.). This approach relies on existing integrations available between the IdaaS and other service providers. — Many mechanisms exist today in the form of cloud-hosted IdaaS solutions performing the fulfillment actions to create user accounts. Traditional IAM vendors have created cloud-hosted provisioning solutions (e.g., CA CloudMinder, Oracle On Demand Identity Provisioning, etc.), in addition to some specialized vendors (e.g., Symplified).
Authentication	— Most organizations are performing authentication against enterprise resources as opposed to individual authentication to CSPs. — Involves setting up a trust relationship with the CSP to allow sharing of tokenized authentication credentials from within the organization, as well as allowing validation of these tokens from the CSP against the organization. — SAML tokens are commonly used to convey authentication tokens to CSPs.	— This model operates similar to the extending enterprise IAM, with the difference being that the authentication infrastructure resides in the cloud. — This approach may limit the ability to apply different or more stringent authentication schemes for specific use cases. That is, cloud solutions may only provide a "one size fits all" approach to authentication. — Enabling this approach involves leveraging the CSPs' trust relationships with other service providers to share the tokenized authentication credentials, and to allow for validation against the authenticating CSP. — Some mechanisms to enable this include leveraging public authentication providers (e.g., Google, Facebook, etc.) or specialized cloud authentication providers (e.g. CA, PingOne, Oracle, etc.).
Authorization	— Dictates that the enterprise owns and drives the authorization policies as the policy administration point (PAP) in order to establish rules for policy decisions (PDP) for enterprise identities to access cloud services. — However, the real-time enforcement of the authorization policies is performed by the CSP when the local identities access cloud user accounts. — Involves sharing of local user authorization claims with the CSP to allow/disallow access to the cloud service. — One mechanism for this is to use standards like XACML to extend local authorizations to the CSP in real-time.	— Policy administration and decision making is externalized to a CSP, while access approval/ denial is enforced at the other service providers acting as PEPs to enforce the authorization rules. — The same mechanisms described in extending enterprise IAM could be used by the cloud-based PDP.

Key components	Extending enterprise IAM	IAM in the cloud
Certification	— Validation of accounts is triggered by review cycles within the enterprise, but facilitated by entitlement information from the CSP. — Involves correlating account and entitlements feeds from each CSP with identity information from the enterprise to identify valid/invalid access. — Mechanisms to achieve this may become complicated due to the diversity in how various CSPs structure their entitlements for user accounts in the cloud.	— Relies on a cloud-based certification engine for the aggregation, correlation, and attestation of user accounts/entitlements with identities. — Involves establishing entitlement feeds from other service providers (other CSPs/ third parties), as well as identity feeds from the identity provider (which could be the enterprise, other CSPs, or third parties). — Allows for the ability to customize access certification views for different audiences by isolating access information across different service providers. — One sample mechanism to achieve this is provided by SailPoint's Cloud Identity Bridge to unify entitlements from various cloud accounts for attestation purposes.
Monitoring	— Enterprises attempt to obtain a real-time view of granular access activities across multiple CSPs. — However, due to the nature of the cloud service model, correlating the actions from potentially many CSPs with a single enterprise identity context is quite challenging. — Due to this difficulty in getting a true unified view of cloud-based actions performed by an enterprise identity, it is highly recommended that organizations devise detailed and thoughtful approaches to extracting account usage information from CSPs and help ensure the ability to correlate this usage data to enterprise identities. This is especially important for privileged CSP accounts available to enterprise identities.	— Operates fairly similarly to extending enterprise IAM, with the difference being that a cloud-based monitoring engine attempts to correlate the activity from the services (other CSPs and third parties). — However, the challenges around creating a unified view of an identity's actions at other service providers is exacerbated in this model due to the additional complexity in obtaining usage and identity information from multiple sources, which could include the enterprise or other CSPs.

Bridging the gap as the IAM landscape evolves

How this industry will develop in the future in unclear, so organizations should also consider the following when establishing solutions today. At KPMG Cyber, we feel that cloud customers often downplay the strategic element to planning for IAM in the cloud. Supporting today's aggressive adoption of an admittedly developing cloud ecosystem requires an honest, realistic assessment of an organization's readiness to extend its on-premise IAM services and conduct cloud-based IAM, as well as understanding the capabilities of the organization's CSPs.

Organizations should spend time thinking through key strategic considerations for building enterprise-class identity solutions that leverage, extend to, and in some cases rely on cloud-based IAM. Below are examples of our perspective on these core areas for consideration:

— **Focus on user experience and IAM simplification during the deployment of cloud services.** Create a road map to leverage vast improvements provided by cloud IAM solutions in the user experience related to IAM (how users request access to resources) and infrastructure simplification (the need to spend less on the plumbing required to implement IAM)

— **Enhance extension of on-premise security policy and authorization through federation.** In the cloud computing environment, federated identity management plays a vital role in enabling organizations to authenticate their users of cloud services with the organization's chosen IdP. In that context, exchanging identity attributes between the SP and the IdP securely is also a requirement to make authorization decisions

— **Build a scalable architecture to extend IAM to new external user communities and partners.** With the exponential growth in collaboration, organizations that want to grow their global footprint and reach new markets need to rapidly extend their reach globally to large communities of users once thought to be "external" to the organization. Effective architecture planning around cloud-based identity services will allow rapid adoption and scale of new business models and initiatives

— **Consider technology and governance processes for the IAM target state.** Any technology transformation will alter or introduce new processes, and IAM deployments will include various process changes. Cloud customers should perform a careful evaluation of their target-state IAM model with consideration of their overall business processes.

Starting to Bridge the Gap

Overall, in terms of priority, there is no general answer as to which IAM function most organizations should focus on first in order to prepare for cloud integration. The answer is specific to the environment. Organizations should evaluate these criteria in order to help in prioritizing activity:

— *Capability* – Is the maturity of my existing enterprise IAM capability weak for a specific function, such as certification? If so, it is likely a good place to start in shoring up cloud readiness.

— *Risk* – Am I comfortable enough with the CSP's implementation of a specific IAM function to move the service to the cloud, or would doing so present too much risk?

— *Reward* – Is there a specific use case in my environment that provides an exceptional benefit in moving that IAM function to the cloud?

Client Reference Study

KPMG Cyber recently helped a global agricultural biotech client prepare its IAM infrastructure for use with CSPs, using precisely the techniques and analysis approach described above. This client's leadership showed increasing desire to migrate key IT and business functions to the cloud by leveraging CSP services (SaaS, PaaS, and IaaS).

In order to prepare for such cloud integrations, our work with the client had three primary objectives:

— Review the current enterprise IAM capabilities and perform a readiness assessment for their use with CSPs.

— Develop several integration scenarios that explore the level of IAM control maintained in-house versus that given to the CSPs as a means to assess risk.

— Recommend short-term, intermediate, and long-term approaches and an action plan for the client to mature its IAM capabilities in order to better combine with CSPs under various scenarios.

By performing a methodical review of our client's IAM capabilities with an eye toward the different requirements and risks posed by the cloud, KPMG Cyber helped the company identify particular areas of focus required to enhance its IAM infrastructure. For example, we noted that:

— The client's on-site IAM infrastructure, though evolving, was not optimized—or even prepared in some areas—to combine with CSPs.

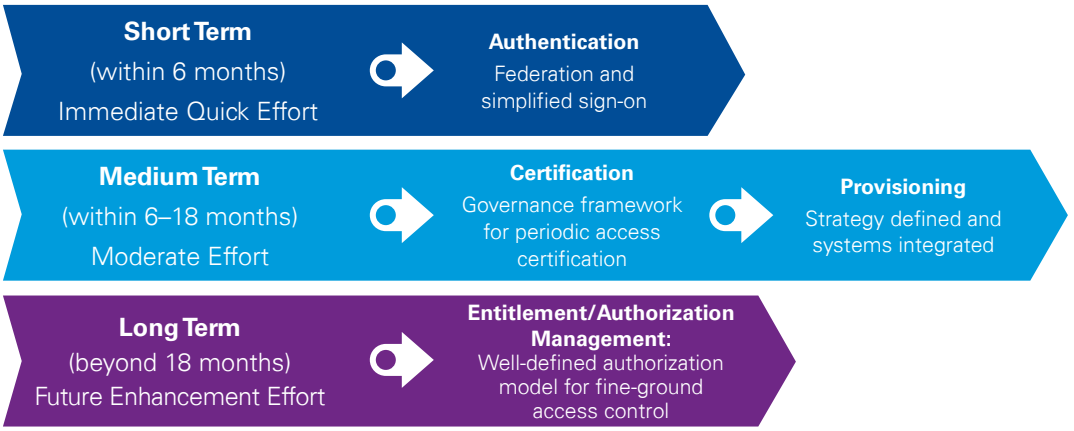
— Enhancing various IAM capabilities would involve efforts of varying complexity and priority. Most of these enhancements would need to be aimed at maturing the client's enterprise IAM capabilities. However, a successful execution of IAM processes would involve significant cooperation from the CSPs to allow IAM integrations.

— SaaS integration scenarios –

  – As an immediate effort, it is critical to focus on maturing **access modeling** capabilities such as role governance, as well as layering thorough **access review** capabilities such as access certification and monitoring of user activities.

  – This sets the foundation for the subsequent long-term effort to perform accurate and well-managed **access creation** with correct CSP entitlements, provisioned using federated provisioning techniques.

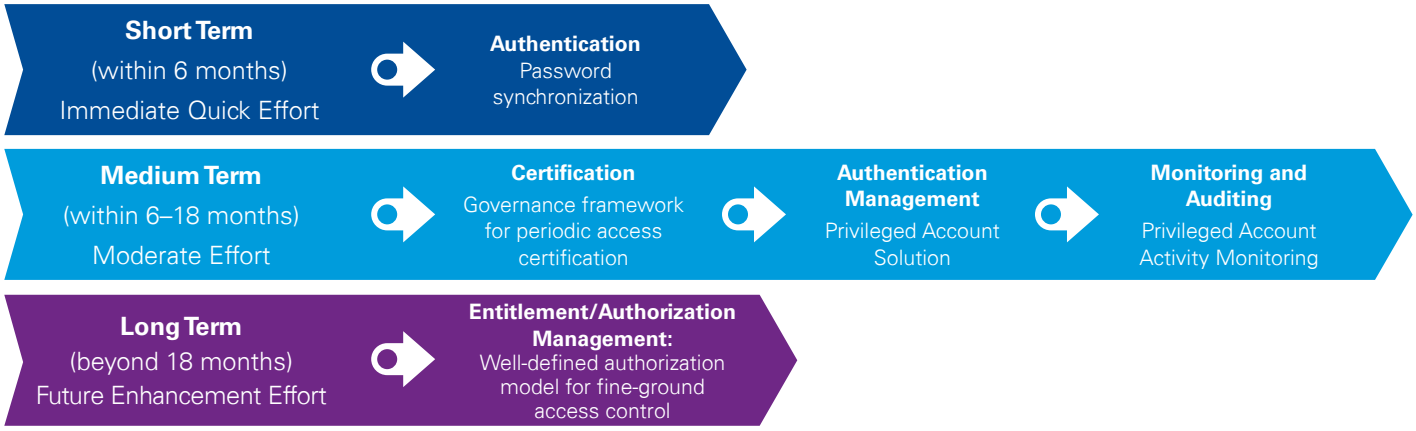
SaaS IAM Approach > High-Level IAM Action Plan



— PaaS and IaaS integration scenarios –

- As an immediate effort, it is critical to start with improving **access enforcement** components by synchronizing local administrative credentials with CSP administrative accounts for uniform passwords and authentication experience
- Similar to the SaaS scenarios, in the longer term, the improved benefits would come from better **access modeling** capabilities such as role governance for administrative roles, and **access review** capabilities such as access certification and monitoring of administrative activities on the CSPs.

Non-SaaS IAM Approach > High-Level IAM Action Plan



Contact us

Carlo Grifone
Principal, Advisory
T: 916-554-1678
E: cgrifone@kpmg.com

Dale Jablonsky
Director, Advisory
T: 916-798-4474
E: dale.jablonsky@kpmg.com

Tom Keane
Account Relationship Director
T: 916-554-1609
E: tkeane@kpmg.com

Vidhu Shekhar
Manager
T: 916-554-1127
E: vidhus@kpmg.com

kpmg.com/socialmedia