



# Cloud Identity Playbook

**January 2022**

**Version 1.0**

**FINAL**

**Cloud Identity Working Group**

**Identity, Credential, and Access Management Subcommittee**

**and**

**Cloud and Infrastructure Community of Practice**

## Table of Contents

<b>Executive Summary</b>	<b>3</b>
Key Terms	4
Audience	5
Disclaimer	6
<b>Cloud Identity 101</b>	<b>7</b>
<b>Cloud Identity Journey Steps</b>	<b>10</b>
Step 1. Gain Support	11
Migration Scenarios	11
Hybrid Migration with No Identity Provider	11
Hybrid Migration with On-Premises Identity Provider	12
Full Migration	12
Generate and Share User Stories	12
Write a Business Case	13
Zero Trust Architecture Alignment	14
Step 2. Document Your Plan	16
Cloud Identity Strategy and Goals	16
Establish Quantifiable Metrics	19
Cloud Identity Policy	20
Step 3. Architecture Considerations	22
Identity Management	22
Credential Management	23
Access Management	24
Governance	25
Federation	26
Step 4. Test and Deploy Identity Automation	29
Emerging Topics	30
Cloud Infrastructure Entitlement Management (CIEM)	30
DevSecOps Identity	30
<b>Appendix A. Policies, Standards, and Guidance</b>	<b>33</b>
Policies	33
Standards	33
Guidance	33
<b>Appendix B. Acronyms</b>	<b>35</b>

## Executive Summary

This Cloud Identity Playbook is a practical guide to assist federal agencies as they start to or further expand the use of workforce Identity, Credential, and Access Management (ICAM) Services in a cloud operating model. Workforce identities are digital identities or accounts owned and managed by the agency, including employees and contractors. The most common Cloud Identity example is Identity as a Service (IDaaS). An IDaaS is typically an Identity Provider that offers Single Sign-On, Multi-Factor Authentication, and directory services in a single platform. It may provide additional features, but these are a core set.

This Playbook aims to answer two questions:

1. What are the defining characteristics that differentiate an on-premises Identity Provider from an Identity as a Service?
2. What are the government-wide best practices and lessons learned to use an Identity as a Service product?

This Playbook answers the questions with two distinct sections. The executive-style Cloud Identity 101 explains the main differences between an on-premises Identity Provider and an IDaaS. In this Playbook, on-premises is defined as an agency operating identity services on agency-owned and maintained infrastructure, typically a legacy approach. The advantage of IDaaS is that it centralizes and consolidates multiple identity capabilities and delivers them on a platform that offers the same cloud benefits like reliability, scalability, and security. Migrating to IDaaS allows an agency to provide identity services rather than operate and maintain the infrastructure.

The Cloud Identity journey answers the second question. It is written for ICAM program managers but can benefit anyone planning Cloud Identity projects or initiatives. There are four Cloud Identity journey steps:

1. [Gain leadership support](#) through collaborating on a migration path. Create user stories that encourage Cloud Identity services to improve user experience and business processes. Capture these in a business case. Align your business case with your agency's zero trust architecture initiative.
2. Identify your success factors and [document a plan](#) that addresses policy and strategy.

3. Understand unique Cloud Identity [architecture considerations](#) across identity management, credential management, access management, governance, and federation.
4. [Test and deploy](#) identity automation.

This Playbook offers recommendations and lessons learned from the Cloud Identity Working Group of the Federal Chief Information Security Officer Council's [Identity, Credential, and Access Management Subcommittee](#) in collaboration with the Federal Chief Information Officers Council [Cloud & Infrastructure Community of Practice](#).

## Key Terms

- **Assertion** - A digital statement from a verifier (usually an Identity Provider) to a Relying Party (usually an application) that contains subscriber (usually a username) information. It may also have additional attributes such as government employee, law enforcement agent, or authenticator type used in an access control decision.
- **Cloud Computing** - A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- **Cloud Service Model** - A Cloud Service Provider service model includes Software as a Service, Platform as a Service, and Infrastructure as a Service.
- **Credential Service Provider (CSP)** - Issues and manages credentials.
- **Digital Worker Identity** - A type of non-person entity specific to digital identity for software. Examples of digital worker identities include artificial intelligence, machine learning, bots, and potentially other software programs or services.
- **Federation** - The technology, policies, standards, and processes allow an agency to share digital identities, attributes, and credentials between trust domains or organizations. Usually through an assertion.
- **Identity as a Service (IDaaS)** - An ICAM service delivered in a Software as a Service cloud service model.
- **Identity Provider (IdP)** - Manage user authenticators and issue assertions used for federation. An Identity Provider could also operate as a Credential Service Provider if

they issue credentials.

- **Machine Identity** - A digital identity for physical hardware and a class of non-person entities in cyberspace. Examples of machine identities include servers, switches, printers, and other hardware devices.
- **Non-Person Entity (NPE)** - Any non-human with a digital identity in cyberspace.
- **Persona** - A digital identity unambiguously associated with a single person or non-person entity (NPE). A single person or NPE may have multiple personas, each managed by the same or different organization.
- **Workforce Identity** - A digital identity owned and managed by the agency, including employees and contractors.

## Audience

The primary audience for this Playbook is Agency Identity, Credential, and Access Management (ICAM) Program Managers. The table below lists secondary audience members and how to engage them with this Playbook.

Stakeholder	Stakeholder Type	Engagement Point
<i>ICAM Steering Committee</i>	Agency Governance Group	The enterprise should govern all agency identities to reduce cyber risk.
<i>Business Line Program Managers</i>	Interested Party	Create a unified user experience by leveraging existing enterprise ICAM services. Identify future ICAM capabilities.
<i>Cloud Management Office</i>	Office	Leverage enterprise ICAM services for centralized and secure authentication and authorization.
<i>Security Management Office</i>	Office	Generate a holistic view of security activities and events across platforms and environments through ICAM data.
<i>DevOps Office</i>	Office	Secure and automate DevOps identities.

Table 1. Stakeholder Table

## Disclaimer

The Cloud Identity Working Group of the Federal Chief Information Security Officer Council ICAM Subcommittee, in collaboration with the Federal Chief Information Officer Council Cloud & Infrastructure Community of Practice, developed this Playbook. U.S. Federal Executive Branch agencies can use this Playbook to plan Cloud Identity services related to the [FICAM Architecture Services Framework](#). This Playbook is not official policy, mandated action, or provides authoritative information technology terms. It includes best practices to supplement existing federal policies and builds upon [Executive Order 14028](#), [Office of Management and Budget Memorandum 19-17](#), and existing FICAM guidance and playbooks. Subject areas with intersecting scopes, such as cloud operating models, Federal Risk and Authorization Management Program (FedRAMP), and enterprise governance, are considered only to the extent that they relate to ICAM services delivered in a cloud service model. Privileged access management (e.g., superusers, domain administrators) is out of scope for this Playbook.

## Cloud Identity 101

Identity is foundational to security both on-premises and within cloud environments. It is the first touchpoint to access data and impacts user experience. In cloud environments, application access acts as a perimeter for protecting applications and workloads where traditionally these were network-based defenses. In this Playbook, on-premises is defined as an agency operating identity services on agency-owned and maintained infrastructure.

Transitioning to an ‘as-a-service’ model allows federal agencies to buy capabilities rather than invest in infrastructure. The most common Cloud Identity example is Identity as a Service (IDaaS). An IDaaS is typically an Identity Provider (IdP) that offers a Single Sign-On (SSO), Multi-Factor Authentication (MFA), and directory services in a single platform. The IdP also provides assertions that include identity and authentication information to an application to authorize access. For more information on Single Sign-On, see the [SSO Playbook](#).

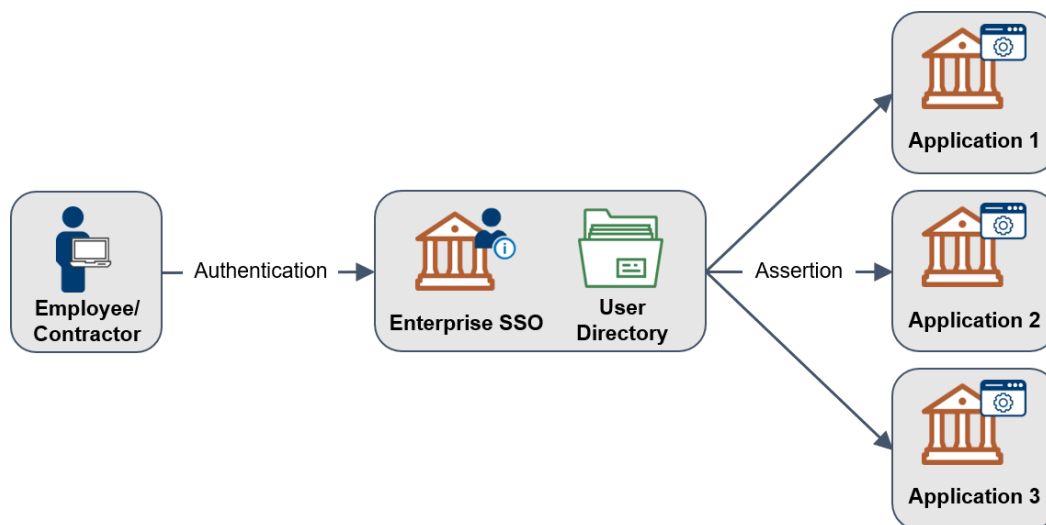


Figure 1. Enterprise SSO Overview





























The table below highlights the main differences between operating an on-premises or legacy IdP and leveraging an IDaaS based on the five essential cloud characteristics of the National Institute of Science and Technology (NIST).

Essential Characteristic	Legacy IdP	IDaaS
On-Demand Self Service	Complete control over all configuration settings.	Privileges are limited to those allowed by the service.
Rapid Elasticity	They are limited but potentially automated scaling to the number of dedicated servers.	Unlimited and automated scaling is transparent to the user and typically included in base IDaaS pricing.
Measured Service	Pricing is usually perpetual-based licensing or, by the number of instances.	Based on the total number of users, active users, or applications.
Resource Pooling	Hardware is dedicated commercial or government-furnished equipment maintained by a federal agency.	Hardware is shared, commercial hardware owned and maintained by a cloud service provider, logically segmented by customer.
Broad Network Access	Creating an internet-accessible service may require additional load balancers, network bandwidth, user device configuration, and geographic dispersion.	Globally available through geographic-based content delivery networks that offer up to or exceeding 99.99% (“four nines”) reliability.

Table 2. Differences between On-Premises Identity Provider and IDaaS

The adoption of cloud services adds challenges as well. Cloud services operate on a shared responsibility model. Some of the responsibility is with the cloud service provider and some with the agency customer. **Data classification and ICAM is always an agency customer responsibility in all cloud service models.** In no case should someone consider the cloud “secure” simply because the cloud provider is “responsible for security.” Principles such as least privilege, role-based access, multi-factor authentication (MFA), and the risk are always an agency customer responsibility, no matter the cloud service model.



Responsibility	On-Premises	IaaS	PaaS	SaaS
Data Classification and Security				
Client and Endpoint Protection				
<b>Identity, Credential, and Access Management</b>				
Application Security and Controls				
Network Security and Controls				
Host Infrastructure				
Physical Security				



 **Agency Customer**
 **Cloud Service Provider**

Figure 2. Shared Responsibility Model

See the [Data Center and Cloud Optimization Initiative Cloud Strategy Guide](#) for a holistic cloud strategy. Additionally, read the [OMB Cloud Smart Strategy](#) to understand the Federal Government's overarching strategic guidance on cloud adoption.

## Cloud Identity Journey Steps

Any journey has a map, but not all are the same. Use these four steps to plan your Cloud Identity journey. Your agency may already support and encourage cloud services while others need support.

1. [Gain leadership support](#) through collaborating on a migration path. Create user stories that encourage Cloud Identity services to improve user experience and business processes. Capture these in a business case. Align your business case with your agency's zero trust architecture initiative.
2. [Document your plan](#) in a strategy and policy.
3. Understand unique Cloud Identity [architecture considerations](#) across identity management, credential management, access management, governance, and federation.
4. [Test and deploy](#) identity automation.

## Step 1. Gain Support

Transitioning to an ‘as-a-service’ model will allow federal agencies to buy capabilities rather than invest in infrastructure. To gain support for an IDaaS migration effort within your agency, first think through the optional migration scenario, generate and share user stories and integrate them into a business case. Identity is a critical enabler to zero trust, so include how IDaaS supports your agency’s zero trust journey.

### Migration Scenarios

This section provides a basic overview of IDaaS starting points and migration paths. Agencies may have complex and coupled architectures that will require a more in-depth analysis. An agency may encounter unique challenges when deciding on an IDaaS migration path based on its starting point. There are three typical starting points usually based on an agency’s size.

Starting Point #1	Starting Point #2	Starting Point #3
Micro Agency	Small to Medium Agency	Small to Large Agency
<ul style="list-style-type: none"> <li>• Username and password for desktop authentication.</li> <li>• No Identity Provider capability.</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Windows Domain for PIV card desktop authentication</li> <li>• No Identity Provider capability</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Windows Domain for PIV card desktop authentication</li> <li>• Microsoft Active Directory Federation Services or other on-premises Identity Provider</li> </ul>

Table 3. IDaaS Migration Starting Point

There are two potential paths to an IDaaS migration; 1) hybrid migration or 2) full migration.

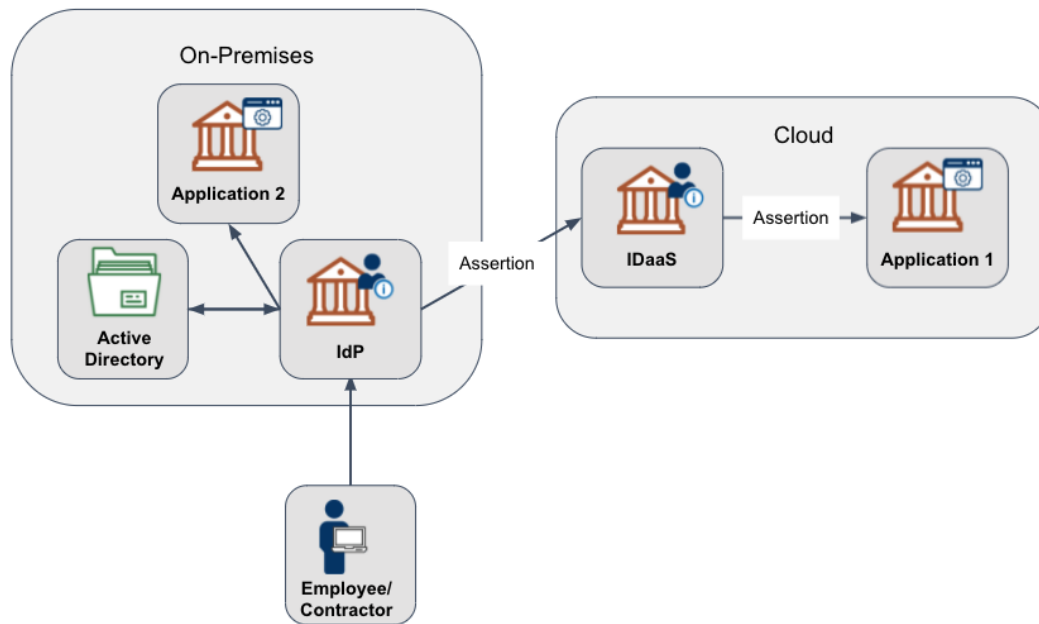


Figure 3. Hybrid Migration with On-Premises Identity Provider

### Hybrid Migration

This hybrid migration scenario retains specific components on-premises while adding additional IDaaS capabilities. This may include:

- 1) Keeping Active Directory and integrating with an IDaaS.
- 2) Federating the on-premises Identity Provider with an IDaaS.

An agency may choose this scenario if it has requirements for an on-premises Active Directory or Identity Provider capability. In this scenario, an agency may integrate cloud applications with an IDaaS while maintaining on-premises application access with the on-premises Identity Provider.



#### **Myth Busted - It's Cloud or Nothing**

Most agencies that utilize an IDaaS are operating in a hybrid configuration.

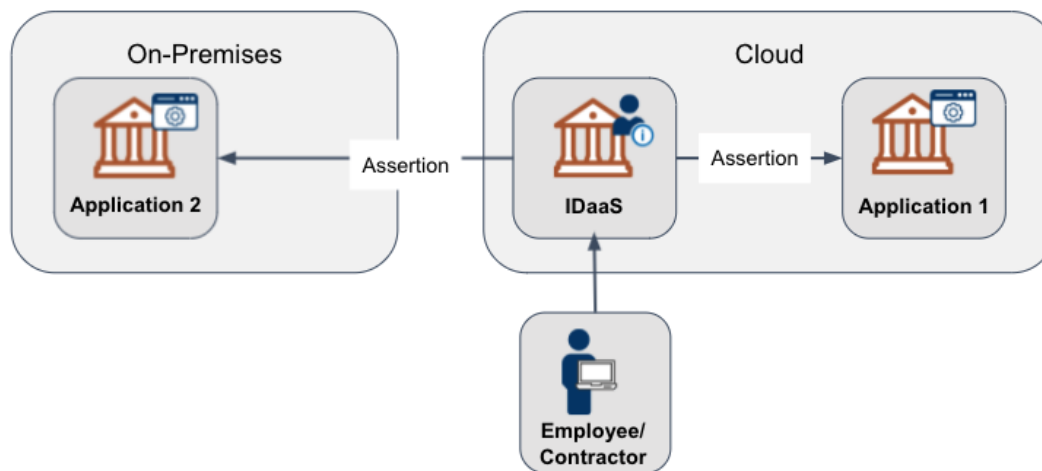


Figure 4. Full Migration to IDaaS

### Full Migration

The full migration scenario replaces all on-premises Identity Provider components with an IDaaS. This scenario includes replacing Active Directory and Active Directory Federation Services with an IDaaS. An agency may need an alternative solution for PIV desktop authentication, which Active Directory typically handles. An alternative solution may include using a comparable phishing-resistant authenticator as mentioned in the draft [OMB Federal Zero Trust Strategy](#).

#### Business Challenge - PIV Authentication in Full Migration Scenario



One common challenge faced by many agencies is IDaaS support for certificate-based authentication and desktop authentication. Many FedRAMP IDaaS support some form of certificate-based authentication. As of this writing, there is no current replacement for PIV desktop authentication that doesn't include operating an Active Directory domain.

The pros and cons of each approach are dependent on an agency's architecture, budget, and technical knowledge. The Federal CISO Council ICAM Subcommittee is a government-wide community for sharing best practices, demonstrations, and questions. Send an email to ICAM at GSA.gov to join.

## Generate and Share User Stories

[Writing Effective User Stories](#) is essential to understanding the user's purpose. Having descriptive summaries and detailed acceptance criteria will help your team know when a user story is considered complete or "done." See this modified example from the GSA Chief Technology Officer Office:

EPIC	USER STORY	ACCEPTANCE CRITERIA
As an <b>Acquisition Gateway User</b> , I need to access the Acquisition ordering platform behind a secure login <b>to</b> purchase products.	As an <b>Acquisition Gateway User</b> , I <b>want to use</b> a phishing-resistant authenticator <b>to</b> log in.	Ensure the Acquisition Gateway User can: <ul style="list-style-type: none"> <li>• Use an authenticator over the WebAuthN API.</li> <li>• Log in to the acquisition gateway.</li> </ul>
	As an <b>Acquisition Gateway User</b> , I <b>need</b> to review my previous bids in the Acquisition ordering platform <b>to</b> remove expired offers.	Ensure the Acquisition Gateway User can: <ul style="list-style-type: none"> <li>• Log in to Acquisition Gateway</li> <li>• Access the page to review items previously bid upon</li> <li>• Select one, or multiple, expired bids</li> <li>• Remove expired bids based on having the correct privilege</li> </ul>

Table 4. Example User Story

User stories describe a requirement that is independent of a specific tool. The example above mentions leveraging Web Authentication (WebAuthN), an Application Programming Interface (API) to leverage a device-generated phishing-resistant authenticator typically supported by an IDaaS and some on-premises Identity Provider tools. IT modernization to the cloud could shift the role of ICAM to enable business owners to maximize the effectiveness of their business and mission products.

[Single Sign-On](#), delivered by IDaaS, is a vital tool to improve security and user experience. SSO centralizes access and allows users to sign in once and directly access other agency applications and platforms.

## Write a Business Case

Next, the agency should draft a business case including funding considerations. In the

business case, as an example, an agency should articulate benefits and value such as how:

- How ICAM capabilities support zero trust.
- Migrating to an IDaaS enhances an agency's business processes.
- IDaaS can improve user experience, provide potential downstream cost savings, improve risk management and provide improved disaster recovery.

A vital element of a business case is a stakeholder analysis. Follow the analysis steps outlined in the [Data Center and Cloud Optimization Initiative Cloud Strategy Guide](#).

## Zero Trust Architecture Alignment

[Executive Order 14028: Improving the Nation's Cybersecurity](#) instructs agencies to accelerate their cloud migrations in a manner that adopts zero trust architecture. The following table outline how an IDaaS enables each zero trust pillar.

ZERO TRUST PILLAR	IDaaS ENABLER
Identity	IDaaS incorporates SSO, MFA, and directory services in a single platform that supports multiple phishing-resistant authenticator options. They may allow an Application Programming Interface to quickly query IDaaS identity stores information making it easier to answer security questions from a single location. A cloud service operates on modern platforms and can integrate new protocols and features faster than on-premises Identity Providers. Agencies can focus more on delivering identity services than maintaining identity infrastructure.
Device	An IDaaS may act as a policy enforcement point and leverage device identification and health attributes such as device type, operating system, operating system version, and location to aid access and authorization decisions.
Network	Software-defined network tools, cloud access security brokers, and other zero trust network solutions must integrate with an Identity Provider to provide identity attributes as part of an access and authorization decision. Cloud solutions often integrate more efficiently with other cloud solutions. An IDaaS may have the capability to act on risk indicators to detect a real-time session change (e.g., the user location changes from Virginia to California in a minute and triggers a re-authentication).
Application	An IDaaS may act as a centralized policy enforcement point. IDaaS may integrate more efficiently with threat protection data sources and leverage artificial intelligence and machine learning to apply continuous authorization decisions creating a dynamic enforcement point. Centralizing access also improves an agency's ability to <a href="#">gather log data to investigate and remediate cybersecurity incidents</a> .
Data	An IDaaS may support advanced access policies which use data tags as part of an access decision.

Table 5. ICAM Enablers for Zero Trust



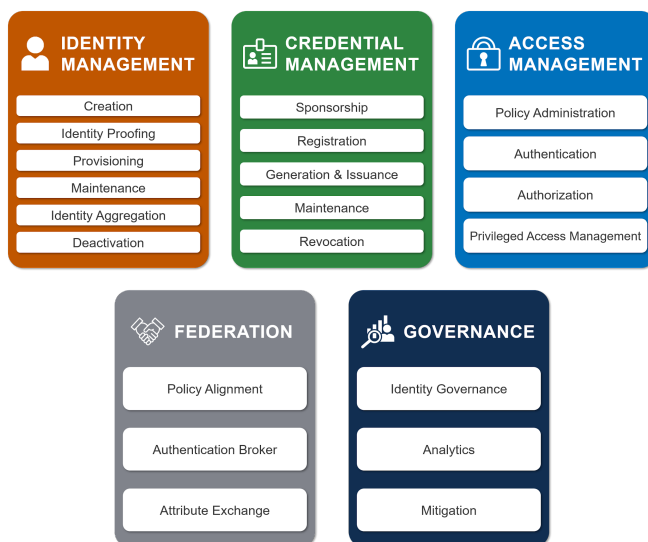
## Step 2. Document Your Plan

The first step in any journey is identifying the destination. Document your plan in three stages.

1. Draft a Cloud Identity Strategy, which outlines strategic goals and an approach.
2. Include quantifiable metrics to gauge success.
3. Write a policy to capture specific governance elements to help achieve the strategy.

### Cloud Identity Strategy and Goals

A Cloud Identity strategy helps an organization work in a concerted manner. An example of pairing a strategy to a goal is consolidating identity services (strategy) to prevent capability sprawl (goal). It is possible that the Cloud Identity strategy and policy are the same document for easy management or based on the agency's size. Large agencies may have different modernization, security, and identity-based strategies, while smaller agencies may



combine them into a single document. Use the [ICAM Practice Areas and Services Framework](#) to identify ICAM services and align your plan with the FICAM Architecture. There are five core services with many sub-services. The [ICAM Governance Framework](#) is also a great resource to identify ICAM capabilities, integration points, and enterprise governance examples and templates.

Figure 5. FICAM Services Framework

Core Service	Business Requirement	Cloud Option
Identity Management	Establish and manage identities for all users.	Most IDaaS tools come with directory services that sync with an on-premises directory. An IDaaS may also have a virtual directory capability. A virtual directory merges identity information for specific application needs (e.g., most applications may use email while others use a different combination or a User Principal Name). FedRAMP accredited remote identity proofing and supervised remote identity proofing services are also available.
Credential Management	Promote interoperability and efficiency across the federal government by buying and building ICAM solutions that use open, commercially-adopted standards.	Leverage an IDaaS that supports multiple types of phishing-resistant authenticators. An agency should target implementing passwordless options or completely removing passwords, even as part of an MFA.
Access Management	Adopt and use cloud-ready systems that provide an efficient and secure way to access resources.	A primary feature of IDaaS is SSO.
Governance	Monitor and respond to user behavior and events by using data as a strategic asset to make adaptive and risk-based decisions.	Ensure your IDaaS services can export logs to support user behavior analytics. A part of technical identity governance is performing access certifications and analytics for role mining, automated provisioning, / de-provisioning, and account discovery.
Federation	Leverage federated solutions to accept identity and authentication assertions made by other agency and mission partners when efficient.	Implement federated access through an SSO tool. As part of a federation, you may decide to operate an Open Authorization (OAuth) service for authorization tokens. A vital part of external federations is legal agreements to document the governance and technical requirements.

Table 6. Cloud Identity Strategy Business Requirements

Here are a few goals to consider as you define your Cloud Identity strategy:

1. **Prevent Capability Sprawl or Duplication.** With the ubiquity of identity and various IT mission applications, duplicative ICAM services within an agency could be pervasive. An agency strategy should first identify authoritative enterprise ICAM services. Preventing sprawl and duplication may start by analyzing ICAM capabilities within your agency's Chief Information Officer's Federal Information Technology Acquisition Reform Act authority. To reduce new acquisitions, communicate enterprise ICAM services through your agency's ICAM governance body.
2. **Centralize Services to Create an Enterprise Capability.** An agency may maintain multiple identity directories. A user may have numerous personas, but they should have one digital identity tied to a master user record within an agency. Manage digital identities at the enterprise level. An authoritative identity source within an agency is a repository of accurate information that feeds into your directory services. It may contain data sources that are not editable by a user. For example, users can update their phone numbers but not their clearance status.
3. **Person and Non-Person Entities.** Incorporate all identities within your strategy. NPEs may include Digital Workers, Machine Identities, or any other type of non-human who needs to access an agency service. Manage NPE identities in a slightly different manner that is potentially unique to the NPE type. For example, use the [Digital Worker Identity Playbook](#) to assess and mitigate the risk of using automated technologies while server machine identities may require a different method.
4. **Network Access.** One of the main differences between on-premises network authentication and IDaaS is the need to steer and monitor device traffic to an IDaaS to apply authentication and authorization decisions. Steering is dependent on device configuration to reach a website. Typically this is a Trusted Internet Connection approved cloud access methods such as a Cloud Access Security Broker, Secure Edge solution, or some type of direct connection through a forward or reverse proxy.
5. **Focus on Automation.** With the scale and size of an ever-increasing infrastructure, Agencies should implement automation where and when it is an advantage. See [Step 4](#) for recommendations on planning an automation workflow.



### Myth Busted - On-premises is More Secure than Cloud

Using cloud services is not more or less secure than on-premises. The single location aggregation of risk and internet-facing cloud presents new security challenges. The shared responsibility model enables more efficient and scaled defense (for example, patching is usually faster and easier for cloud services). Proper application of appropriate controls can yield a highly secure cloud deployment.

## Establish Quantifiable Metrics

An agency should then establish quantifiable metrics so that any member of the migration team can objectively identify success and failure. Agencies should tailor their metrics to address operational challenges. Some example metrics include:

- The length of time to provisioning or de-provision an account
- The number of orphaned accounts
- The number of integrated applications
- The number of MFA credentials supported (FISMA metric)
- The number of applications that only support phishing-resistant authenticators (FISMA metric)
- The number of manual processes automated.

Use your agency's operational value, or the rate of transactions in a given period, to identify where to set efficiency improvement goals. For example, if you have an operational metric of 24 hours to provision an account, an efficiency improvement would be to reduce that by 10%. Align the chosen metrics to federal policy, FISMA, or agency mission objectives to help translate improvement in metrics to progress in meeting overarching agency goals. For example:

1. **Policy Efficiency.** Identify metric improvements aligned with federal mandates, like the number of applications only accessible with a phishing-resistant authenticator.
2. **Operational Efficiency.** Identify metric improvements that show operational improvements, like decreasing the time to deprovision a user from two days to an hour.

### Budgeting IDaaS



Most IDaaS price products in three ways; the number of total users, the number of monthly active users, or the number of integrated applications. It's essential to understand the variable cost of each pricing method. Have this information ready when talking with an IDaaS vendor. Collect these data points as part of a Digital Identity Risk Assessment.

## Cloud Identity Policy

While the Cloud Identity strategy states the path to achieve an outcome, the Cloud Identity policy sets the boundaries to execute the strategy. Likely, your agency may already use some cloud-based identity services. Your Cloud Identity infrastructure should fit within your agency's vision for cloud services, modernization, and cybersecurity efforts. There should be specific call-outs of how ICAM supports those efforts, goals, or objectives in accomplishing your agency's mission. For example, streamline the user experience by consolidating access points. Recommend changes to highlight how ICAM supports your agency's mission and business processes if it does not.

The main strategies or policies to identify are cloud, modernization, and cybersecurity policy or vision (if it exists). For example, in the [Department of Defense \(DoD\) Modernization Strategy](#), the DoD has incorporated deploying an end-to-end ICAM infrastructure as an objective of its evolving cybersecurity goal. The DoD then wrote an [ICAM Reference Design](#) to support the objective. With this executive direction and support from Step 1, craft an agency policy to incorporate the following points.

1. **Agency ICAM Governance.** Enforce agency ICAM governance by implementing and maintaining an agency ICAM governance body and program management office. The governance body should include representatives from Information Technology, Human Resources, Finance, Acquisitions, General Counsel, Information and Physical Security, Privacy, and others as needed to deliver ICAM services. For ICAM governance examples, see the [ICAM Governance Framework](#) and [ICAM Program Management Playbook](#).
2. **User Management.** An IDaaS may implement role-based management through

groups to make user management easier. Additionally, IDaaS may support more risk-based access control models that incorporate location, time of day, device type, and other attributes as part of a policy enforcement point.

3. **Identify Authoritative Credentials.** Most agencies support PIV as a primary authenticator, but a smart card may not fit all use cases. Identify approved secondary authenticators and a process to approve new phishing-resistant authenticators. Testing may include accepting an external certification like Fast ID Online or another federal government agency. A secondary phishing-resistant authenticator can offer comparable security and improve user experience.
4. **Logging, Monitoring, and Audit.** An increase in web traffic may require additional security monitoring and log analysis in the Security Information and Event Monitoring system. Factor this additional workload on your cybersecurity defense and response teams and the potential to incorporate more automated processes. An IDaaS can support meeting the ICAM logging requirements in [OMB Memo 21-31](#). IDaaS acts as a centralized access point for logging account activity such as account creation, credential changes, attribute activity, credential usage, and account deletion or suspension.
5. **Centralize Access with Single Sign-On and Enable Federation.** It is expected that agencies will have PIV-enabled enterprise applications after the 2015 cyber sprint for internal and external users. Consider integrating all enterprise applications into an IDaaS to enable all applications with PIV or other comparable MFA options to create a consistent user experience. Centralizing access can improve credential management for all users, more easily support integrating various authenticators, and create a centralized federation point for external users.
6. **Require Digital Identity Risk Assessments.** A Digital Identity Risk Assessment (DIRA) identifies a user's transaction risk within a Federal Information Security Modernization Act boundary. Agencies are required to perform assessments as stated in [Office of Management and Budget Memo 19-17](#). If your agency doesn't have a Digital Identity Risk Assessment policy or process, consider writing one based on the [Digital Identity Risk Assessment Playbook](#).

## Step 3. Architecture Considerations

Many agencies face similar challenges when adopting IDaaS. This section includes architectural considerations aligned with the Federal ICAM (FICAM) Services Framework. One of the main benefits of using cloud-based tools is automation by leveraging programmatic interfaces and open standards for authorization, such as OAuth.

### Identity Management

Agencies can use IDaaS to create a global identity (also referred to as a master user record) within an agency and across cloud and on-premises environments. **Enterprise identity awareness is a zero trust capability.**

1. **Automate Identity.** One unique feature of IDaaS is the potential to automate manual processes. For example, automatically suspend a user's account after 14 or 30 days of inactivity. Leverage API integrations to automate lifecycle management processes with other IT Tools. For example, integrate IDaaS with an IT Service Management tool to track and audit permissions. Learn about [System for Cross-domain Identity Management](#), an open standard used by IDaaS and other cloud tools to automate user provisioning. **Automating identity processes is a mature zero trust capability.**
2. **Accurate Directory Information.** Before starting an IDaaS project, ensure correct source directory information. An IDaaS will replicate your on-premises directories to a cloud directory and may even support bi-directional information updates. At a minimum, most cloud directories support one-way sync to the cloud directory. It is better to clean your directory before rather than after replication.
3. **Virtual Directory.** Not all cloud application access is equal. Consider using a virtual directory to create unique personas for specific applications based on existing directory information. A virtual directory aggregates identity data from a variety of sources. For example, an application requires a particular attribute such as citizenship which is not in the directory record. An agency can use a virtual directory to create a unique application persona with data combined from various identity or data repositories. An IDaaS may support a virtual directory capability and act as a master user record.
4. **Entitlement Management.** Most cloud applications and platforms implement role-based entitlement management. Permissions are managed based on a user in a

group rather than individually. Groups may consist of unique roles such as government administrator, contractor administrator, contributor, or reader. All users in a group inherit the same permissions. Entitlement management is as easy as removing the user from that group.

5. **NPE Identity Management.** Each type of NPE, machine identity, or digital worker may require a different configuration or type of management. An initial step is to catalog the variety of NPE identities. Examples of NPE identities include service accounts, robotic process automation bots, scripts, and many others, depending on your use case and environment. Next, identify the highest risk devices and a method to secure their access.

## Credential Management

A smart card is not automatically a PIV in the same way that authenticators are not automatically phishing-resistant. Multiple components are required to bind and use an authenticator. IDaaS may support more types of phishing-resistant authenticators than on-premises tools. **Implementing phishing-resistant MFA for all workforce access is a zero trust capability.**

1. **Allow Multiple Phishing-Resistant Authenticators.** Federal employees and contractors are issued a PIV card for physical and digital access, but it may not fit every digital use case such as cloud, mobile, or command lines. Employees also need a comparable authenticator alternative if they lose or cannot use a PIV card. Use the [Digital Identity Risk Assessment process](#) to identify a minimum authenticator assurance level based on the user transaction risk. See this National Security Agency fact sheet on [potential secondary authenticator options](#) for workforce use cases.
2. **NPE Credentialing.** Agencies should conduct risk assessments on NPE access. Part of this is determining if, how, and when to enforce more stringent controls, auditing, and monitoring. An NPE credential is compromisable in the same way as a human user if the secret is discovered and may go undetected for a more extended period. An IDaaS may have the capability to act as an API access key centralized repository for easier management and auditing.
3. **Memorized Secrets.** A memorized secret is a password or a PIN. Only use passwords



as part of an MFA and as a last resort with additional controls. Until an agency can implement passwordless, phishing-resistant authenticators, follow [NIST Special Publication 800-63B](#) guidelines for passwords in IDaaS.

- Should allow passphrases.
- Shall check against breach corpora, dictionary words, repetitive characters, or context-specific and denied.
- Should offer a password strength meter.
- Shall limit the number of failed attempts before a lock-out or require a password reset.
- Should not require periodic password updates.
- Should be used as part of a multi-factor authenticator.
- Should allow a user to cut and paste a password.



#### **Risk Management Challenge - Unique Credentials**

Credentials should be assigned on an individual basis and not shared. If a credential must be shared, NIST recommends requiring individual authentication to access the shared credential.

## **Access Management**

A primary IDaaS capability is a centralized policy enforcement point that may integrate user and entity behavior analytics, risk-based access policies, and continuous validation. **Integrating risk-based access policies into an access decision is a zero trust capability.**

1. **Integrate Identity and Cloud Access.** Access in this context means creating network paths for users from an agency network (direct or through Virtual Private Network) and potentially for users not on an agency network. For example, the Email as a Service login page is accessible off-network but requires SSO, only accessible on the agency network. [Trusted Internet Connection 3.0](#) provides two cloud access options through either a Cloud Access Security Broker or a Security Gateway. Both may operate in a forward or reverse proxy mode to monitor traffic of the agency or bring your own device and apply access policies in real-time. This typically requires integration with an IdP.
2. **Protocol Monitoring.** Access comes in many protocols. Monitor access attempts over

all possible protocols such as HTTPS and secure shell — also factor in port translation technology that converts ports and protocols (e.g., Converts HTTPS into SSH).

3. **Enable Risk-Based Access Control.** Many cloud access tools can leverage telemetry decisions such as device type, browser type, location for Attribute-Based Access Control. Some IDaaS may provide native or, through an API, risk information to enforce risk-based access control, including behavior analytics and threat information feeds. Verify how and if an IDaaS can support this capability.

#### Access Policy by User Type



Application owners can determine ideal conditions for access, such as during working hours, from the United States, on a Government Furnished Equipment or approved device by reviewing access or activity logs. Centrally identify, implement, and track access policies and exceptions with an IDaaS.

## Governance

Identity governance includes both program oversight and technical controls. Agencies should investigate automating technical governance controls when and if cost effective and necessary based on a risk assessment.

1. **Certify Access.** Access certification or recertification is the process of an application owner or a manager attesting to someone's access and can be an automated or manual process. Access certifications should happen more frequently for higher impact applications, such as monthly or quarterly.
2. **Plan for Contingencies.** Verify IDaaS availability requirements and continuity procedures. Test disaster recovery scenarios regularly. Continuity planning may require collaborating with your IDaaS to identify strategies around geographic outages, denial of service attacks, or other potential outages.
3. **Configuration Monitoring.** Establish audit policies to monitor for configuration changes. Implement controls to prevent misconfiguration (e.g., default private or deny). When configurations change, inform or create a training event to ensure all administrators know about it.
4. **Policy-Based Governance.** A key success factor is an agency policy that defines

roles, identity lifecycle stages and procedures, and potentially a central repository of identity policies for infrastructure as code or multi-cloud management. Policy-based governance ensures consistent implementation of IDaaS policies.

5. **Monitor Activity.** Enable activity logging for all users. Log monitoring was a primary success factor in [detecting activity related to Solarwinds and Active Directory compromise](#).

### Workforce Training



Implement Cloud identity processes through open protocols and languages such as JavaScript Object Notation, System for Cross-domain Identity Management, OAuth, Security Assertion Markup Language, Open Policy Agent, and Open ID Connect. ICAM workforce training should incorporate these protocols and languages to include known weaknesses and how to overcome them.



### Workforce Challenge - Informing Users

Any changes to the user experience can degrade workforce efficiency. Make a plan to communicate changes and prepare your users.

## Federation

Federation is the technology, policies, standards, and processes that allow an agency to share digital identities, attributes, and credentials between trust domains or organizations. Usually through an assertion. Federation can be a technical mechanism to implement a Single Sign-On in an Agency (within the same trust domain). It is also a mechanism to federate between trust domains such as between agencies, mission partners, or other trust frameworks.

### Within the Same Trust Domain

1. **Assertion Profile.** The greatest challenge with federating in an agency is identifying if and how an application supports an assertion protocol. Additionally, applications may need specific attributes asserted from the IDaaS. Some IDaaS may have

pre-configured profiles to streamline application onboarding where this was previously a manual task. See the [Single Sign-On Playbook](#) section on planning application integration of more information.

### Across Different Trust Domains

1. **Trust Framework.** Federating across security or organizational boundaries requires a legal agreement and a technical exchange. An agreement between entities should identify each organization's required security and governance processes. Creating a template that includes the format and required attributes is a best practice. See [NISTIR 8149](#) for more information on trust frameworks.

#### Case Study - Trust Frameworks in Action

The integrity of a Trust Framework is vital when federating with external identities. The trust framework partners should have governance processes that may include a verified accreditation or audit process to ensure the identity proofing, authenticator, and federation assertion meets the intent of NIST Special Publication 800-63-3 requirements. Using a third-party audit service provides the additional assurance of secure and compliant operations. Some examples of trust frameworks include:

- The Federal Public Key Infrastructure (PKI) Policy Authority enforces a certificate policy, third-party auditing, and implements technical control through the Federal PKI certificate profiles and hierarchy. There are other [non-government PKI trust frameworks](#) that interoperate with the Federal PKI. The Federal PKI trust framework ensures federal employee and contractor credentials meet a NIST standard (FIPS 201) and are acceptable to all federal agencies.
- The Kantara Initiative is a non-government trust framework program. It operates conformity assessment, assurance, and grants trust marks to companies that show conformance to a Kantara standard based on NIST Special Publication 800-63-3. They accredit full identity service providers, component services, and Kantara accredited assessors. An agency may recognize a Kantara trust mark to federate with an external Identity Provider.
- The DirectTrust Health Information Service Provider is a PKI-based trust framework for healthcare community collaboration.

## Step 4. Test and Deploy Identity Automation

IDaaS products may vary in how they are configured and operated. This section provides technology and vendor agnostic steps to document an existing manual process for automation following a user experience format. Automating tasks may require a combination of native IDaaS capabilities and scripting, API requests, or tool integration.

1. **Document the Process.** The process may include all actions and outcomes from a user perspective. Documenting may follow a similar structure as the use case example provided in [Step 1](#). Example processes for automation include:
  - a. User account suspension due to inactivity.
  - b. Account provisioning or de-provisioning (onboarding).
  - c. Approve access requests for users in a specific group.
  - d. Report on suspicious activity.
  - e. Credential enrollment.
  - f. PKI Trust store management.
2. **Review Process Workflow.** The review may include a whiteboard session or watching a user perform the process. It also includes documenting pain points and dependencies to complete the task. The outcome of this step is a thorough understanding of the process.
3. **Generate an Automated Approach.** Review the workflow steps for complete or partial automation. Manual activities may include:
  - a. A series of approvals to provision an account, such as employee onboarding.
  - b. Data validation.
  - c. Generating reports.
  - d. Sending reminder emails.
  - e. Testing.
4. **Test and Implement Workflow.** After finding an optimal workflow, it is time to test and implement it. If possible, test in a non-production environment. If testing is only available in production, limit the impact to a small community of users or a non-mission critical task.

## Emerging Topics

The Cloud Identity Working Group discussed two emerging topics: 1) Cloud Infrastructure Entitlement Management and 2) DecSecOps Identity.

### Cloud Infrastructure Entitlement Management (CIEM)

Cloud Infrastructure Entitlement Management (CIEM) is a specific tool to manage identities in multi-cloud environments. A primary challenge in managing cloud entitlements is the pervasiveness of understanding entitlement risk. In this context, entitlement risk is the ability of an attacker to exploit how cloud services and resources are connected or extended. This attack technique is called a [Valid Cloud Account Privilege Escalation in MITRE ATT&CK](#). For example, a service account is an NPE account created to perform an automated action with specific privileges. A service account may have administrator privileges and, if compromised, is used by an adversary to conduct malicious activity. A CIEM can identify risk in people, service, and resource entitlements.

1. **People Entitlements** -Permissions for people to perform actions such as change information or access security settings.
2. **Service Entitlements** -Permissions for services to perform actions on a platform, such as starting or stopping services or performing automated tasks.
3. **Resource Entitlements** -Permissions to access specific resources such as a database, file storage, or workloads.

An IDaaS capability is usually limited to people processes and API key management. It may not be able to identify and manage entitlements in a multi-cloud environment. A CIEM may be part of a broader Cloud Security Posture Management tool or its own platform. See the [Cybersecurity and Infrastructure Security Agency \(CISA\) Cloud Security Technical Reference Architecture](#) on Cloud Security Posture Management for more information. A best practice in cloud entitlement management is to regularly review service accounts with administrator privileges and determine if they need a generic or fine-grained (custom) administrator role.

## DevSecOps Identity

DevOps is a term that emerged a few years ago to express how integrated teams of developers and system operators could work together to streamline the process of developing, testing, deploying, and operating at the speed of business. The ability to move through those cycles rapidly is also called the Continuous Integration/Continuous Delivery (CI/CD) pipeline. DevOps is a cross-functional effort, and the adoption of cloud services has accelerated this process.

Since the goal of the DevOps team is to get software operating in production quicker, security considerations are often more focused on the operational environment rather than the tools or the pipeline that is used to deploy the software. In high-velocity settings, the attack surface leveraged by an adversary may constantly change, putting the organization at extreme risk, as seen in the recent Solarwinds compromise. DevOps use credentials called Secrets which include username/passwords, API keys, SSH keys, and PKI certificates. Follow these recommended best practices to integrate ICAM best practices into DevSecOps.

1. **Manage DevOps Secrets.** The increased use of code to configure infrastructure places a greater demand on ensuring that the secrets used in these environments are well managed and not embedded in code. An agency may need an NPE Certificate Manager to automate the NPE certificate lifecycle. Separately, a Secrets Manager can serve as an API-based repository for automated secret check-in/out and rotation. Package the total code and configuration as a configuration item so that the entire content is known, tracked, and potentially verifiable through a software bill of material.
2. **Implement Custom Roles for Separation of Duties.** DevOps scripts may perform the same function across multiple development and production environments. Custom roles help segment access across security boundaries, but also to Secrets. A configurable separation can make sure a script that deploys the database does not have access to change the operational data in the database.
3. **Practice Production Security Practices.** It is common to share credentials across non-production environments or not apply common identity best practices (e.g., a

simple lab password or no MFA). Sharing credentials enables one compromised password to create a persistent access point. Practice production security practices in your test environments.

4. **Manage Programmatic Access.** Create and maintain a continuous device inventory for all environments, including the DEV, TEST, and STAGING environments. Inventory all of the tools with programmatic access and the component owner. A continuous inventory lessens the potential for introducing unknown devices or code.

See the [GSA Guide](#) on DevSecOps for more information.



# Appendix A. Policies, Standards, and Guidance

## Policies

1. [Executive Order 14028 -Improving the Nation's Cybersecurity](#)
2. [Federal Cloud Smart Strategy](#)
3. [Office of Management and Budget Memo 19-17](#)
4. [Draft Federal Zero Trust Strategy](#)

## Standards

1. [NIST Special Publication 800-63 -Digital Identity Guidelines](#)
2. [NIST Special Publication 800-145 -NIST Definition of Cloud Computing](#)
3. [NIST Special Publication 800-204B -Attribute-based Access Control for  
Microservices-based Applications using a Service Mesh](#)
4. [NIST Special Publication 800-207 -Zero Trust Architecture](#)
5. [NIST Special Publication 800-210 -General Access Control Guidance for Cloud  
Systems](#)

## Guidance

1. [CISA Cloud Security Technical Reference Architecture](#)
2. [CISA Zero Trust Maturity Model](#)
3. [Digital Identity Risk Assessment Playbook](#)
4. [Data Center and Cloud Optimization Initiative Cloud Strategy Guide](#)
5. [Enterprise Single Sign-On Playbook](#)
6. [FedRAMP Digital Identity Requirements \(Version 1.0\)](#)
7. [FICAM Architecture](#)
8. [ICAM Governance Framework](#)
9. [ICAM Program Management Playbook](#)
10. [General Services Administration -Cloud Information Center](#)
11. [NIST Interagency Report 8149 -Developing Trust Frameworks to Support Identity  
Federations](#)

12. [NIST Interagency Report 8335 -Identity as a Service for Public Safety](#)
13. [NIST Interagency Report 8360 -Machine Learning for Access Control Policy Verification](#)
14. [NIST Special Publication 1800-13 -Mobile Application Single Sign-On](#)
15. [National Security Agency Cybersecurity Information Sheet -Mitigating Cloud Vulnerabilities](#)
16. [Open Authorization \(OAuth\)](#)
17. [System for Cross-domain Identity Management \(SCIM\)](#)

## Appendix B. Acronyms

API	Application Programming Interface
CI/CD	Continuous Integration/Continuous Delivery
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
IDaaS	Identity as a Service
ICAM	Identity, Credential, and Access Management
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
OAuth	Open Authorization
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SSO	Single Sign-On