

Cloud Identity Playbook

**September 2021**

**Version 1.0**

**DRAFT / PRE-DECISIONAL**

**Cloud Identity Working Group**

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

**and**

**Cloud and Infrastructure Community of Practice**

**Table of Contents**

[**Executive Summary**](#_9k29wgjpzanm) **2**

[**Cloud Identity 101**](#_bnmlxi13ao6y) **5**

[**Cloud Identity Journey Steps**](#_514y719xyyin) **7**

[Step 1. Gain Support](#_i3igxeja6brx) 8

[Step 2. Identify a Plan and Success Factors](#_i768dyam9n5y) 10

[Step 3. Architecture Considerations](#_iyraerdpiulf) 17

[Step 4. Test and Deploy](#_v3kzv58ys4tg) 23

[**Appendix A. Policies, Standards, and Guidance**](#_e3ergpz6whif) **26**

[**Appendix B. Acronyms**](#_lwiwemg874ca) **27**

# Executive Summary

This Cloud Identity Playbook is a practical guide to assist federal agencies as they either start to or expand the use of Identity, Credential, and Access Management (ICAM) Services in a cloud operating model. This playbook is designed to explain Cloud Identity as well as offer lessons learned and guidance to federal agencies starting or expanding their use of ICAM in the cloud. Cloud Identity, in the context of this playbook and sometimes referred to as Identity-as-a-Service (IDaaS), is the application of ICAM processes, patterns, and technology to cloud-based services such as software, platform, or infrastructure as a service.

This playbooks aims to answer two questions:

1. How is ICAM in the cloud different from ICAM on-premise?
2. What are the government-wide best practices and lessons learned to extend ICAM to the cloud?

The first question is answered in the executive-style Cloud Identity 101 section. The advantage of ICAM in the cloud is that it offers the same benefits as cloud infrastructure. It features a highly scalable infrastructure that is reliable, global, secure, and sized to fit your agency rather than expected volume. The second question is answered through steps in a Cloud Identity journey. It is written for ICAM program managers but can benefit anyone involved in planning Cloud Identity projects or initiatives. There are four Cloud Identity journey steps.

1. [Gain leadership support](#_i3igxeja6brx) through user stories that encourage cloud ICAM services that improve user experience and business processes. Capture these in a business case.
2. [Document your plan](#_i768dyam9n5y) in a strategy and policy.
3. Understand unique Cloud Identity [architecture considerations](#_iyraerdpiulf) across identity management, credential management, access management, and governance.
4. [Test and deploy](#_v3kzv58ys4tg) cloud-enabled services and capabilities incrementally.

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](https://community.max.gov/pages/viewpage.action?pageId=234815732) in collaboration with the Federal Chief Information Officers Council [Cloud & Infrastructure Community of Practice](https://community.max.gov/display/Egov/CIO%2BCouncil%2BCloud%2Band%2BInfrastructure%2BCommunity%2Bof%2BPractice).

## Key Terms

* **Cloud Identity** - The application of ICAM processes, patterns, and technology, typically delivered in a Software as a Service model, to cloud-based services such as software, platform, or infrastructure as a service. This term is used interchangeably with Identity as a Service, or IDaaS.
* **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 that includes Software as a Service, Platform as a Service, and Infrastructure as a Service.
* **Federation** - The technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.
* **Identity as a Service (IDaaS)** - Industry term for Software as a Service providers of ICAM services.
* **Identity Provider** **(IdP)** - Sometimes referred to as a Credential Service Provider, an IdP manages user authenticators and bound credentials. It also issues assertions to other Identity Providers for authentication and authorization patterns.
* **Machine Identity** - Otherwise known as a Non-Person Entity (NPE). Broad term for a digital identity of any NPE in cyberspace. This may include organizations, hardware devices, software applications, and information artifacts.

## Audience

This playbook is written for Agency ICAM Program Managers as the primary audience. The below table lists secondary audience members and how to engage them with this playbook.

|  |  |  |
| --- | --- | --- |
| **Stakeholder** | **Stakeholder Type** | **Engagement Point** |
| *ICAM Steering Committee* | Agency Governance Group | The enterprise should govern all agency identities to reduce cyber risk. |
| *Business Line Program Managers* | Interested Party | Create a unified user experience by leveraging existing enterprise ICAM services. Identify future ICAM capabilities. |
| *Cloud Management Office* | Office | Integrate your identity processes with existing enterprise ICAM services. |
| *Security Management Office* | Office | Generate a holistic view of security activities and events across platforms and environments. |
| *DevOps Office* | Office | Secure and automate DevOps identities. |

Table 1: Stakeholder Table

## Disclaimer

This playbook was developed by 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. This playbook is intended to help U.S. Federal Executive Branch agencies understand and plan use of cloud infrastructure as it relates to the [FICAM Architecture Services Framework](https://playbooks.idmanagement.gov/arch/services/). This playbook is not official policy or mandated action and does not provide authoritative information technology terms. This playbook includes best practices to supplement existing federal policies and builds upon [Executive Order 14028](https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity) and [Office of Management and Budget Memorandum 19-17](https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf), as well as existing federal identity guidance and playbook. Subject areas with intersecting scope, 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 either operating FICAM services or performing FICAM processes in a cloud service model.

# Cloud Identity 101

Identity is foundational to security on-premise and within cloud environments. It is the first touchpoint to access data and impacts the entire user experience in a cloud service. In the context of this playbook, **Cloud Identity or Identity as a Service (IDaaS), typically delivered in a Software as a Service model, is the application of ICAM processes, patterns, and technology to cloud-based services such as software, platform, or infrastructure as a service.** In cloud environments, identities act as a perimeter for protecting applications and workloads where traditionally these were network-based defenses. The below table highlights the main differences based on the National Institute of Science and Technology (NIST) five essential cloud characteristics.

|  |  |  |
| --- | --- | --- |
| **Essential Characteristic** | **On-Premise Identity** | **Cloud Identity** |
| On-Demand Self Service | Full control over all configuration settings. | Controls limited to those allowed by the IDaaS. |
| Rapid Elasticity | Limited, potentially automated scaling to the number of dedicated servers. | Unlimited, automated scaling which is transparent to the user and typically included in base IDaaS pricing. |
| Measured Service | Pricing is usually perpetual-based licensing or by number of instances. | Cloud pricing is typically based on volume such as number of uses, applications, or authentications per month. |
| Resource Pooling | Typically dedicated government-furnished equipment owned and maintained by a federal agency. | Shared, commercial hardware owned and maintained by an IDaaS provider which is segmented by customer. |
| Broad Network Access | Access is restricted to an agency network. Creating an internet-accessible service may require additional load balancers, network bandwidth, and geographic dispersion. | Globally available through geographic-based content delivery networks that offer between 99.99 to 99.9999 reliability. |

Table 2. Differences between On-Premise Identity and Cloud Identity

Overall, IDaaS has many benefits over on-premise identity services. The most common pattern for IDaaS is Single Sign-On (SSO) or Identity Provider. SSO and Identity Provider terms may be used interchangeably, but essentially perform the same function of managing user authenticators and access to applications. It is also the primary pattern to federate or share digital identities, attributes, and credentials managed by other agencies.

The adoption of cloud services adds challenges as well, one of which relates to security. Cloud services operate on a shared responsibility model where some of the responsibility is with the cloud provider and some with the cloud consumer. In no case should one consider the cloud to be “secure” simply because the cloud provider is “responsible for security”. Principles such as least privilege, role-based access, multi-factor authentication (MFA) will always be an agency responsibility no matter the cloud service model. The below graphic identifies the unique security considerations of an IDaaS.

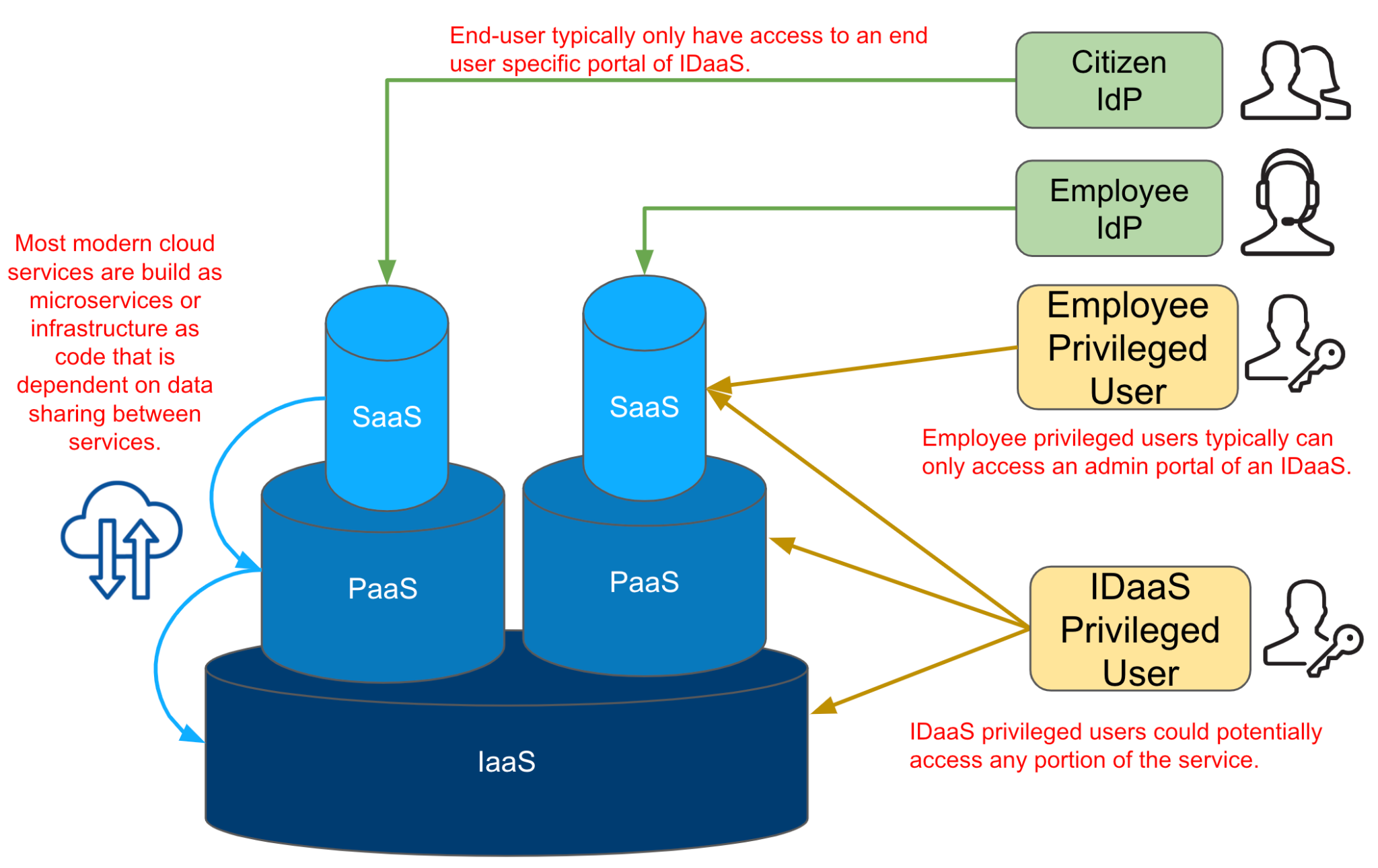


Figure 01. Unique Security Considerations of an IDaaS

For more information on developing a holistic cloud strategy for your agency, see the [Data Center and Cloud Optimization Initiative Cloud Strategy Guide](https://community.max.gov/display/Egov/Agency%2BIT%2BModernization%3A%2BEducational%2BResources%2BBuilding%2BBlocks). It is also recommended to understand the Federal Government's overarching strategic guidance on cloud adoption: the [Cloud Smart Strategy](https://cloud.cio.gov/strategy/).

# Cloud Identity Journey Steps

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

1. [Gain leadership support](#_i3igxeja6brx) through user stories that encourage cloud ICAM services that 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](#_i768dyam9n5y) in a strategy and policy.
3. Understand unique Cloud Identity [architecture considerations](#_iyraerdpiulf) across identity management, credential management, access management, and governance.
4. [Test and deploy](#_v3kzv58ys4tg) cloud-enabled services and capabilities incrementally.

## Step 1. Gain Support

In order to gain support for a cloud migration effort within an agency, consider the following sub-steps.

### Generate and Share User Stories

[Writing Effective User Stories](https://tech.gsa.gov/guides/effective_user_stories/) is important to understand the user’s purpose. Have descriptive summaries and detailed acceptance criteria to help your Team know when a user story is considered complete or “done.” See this example from the [GSA Chief Technology Officer Office](https://tech.gsa.gov/guides/user_story_example/).

|  |  |  |
| --- | --- | --- |
| **EPIC** | **USER STORY** | **ACCEPTANCE CRITERIA** |
| As an **Acquisition Gateway User, I need** to access the Acquisition ordering platform behind a secure login **so that** I can purchase products. | As an **Acquisition Gateway User, I need** to input authenticator information **so that** I can login. | Ensure the Acquisition Gateway User is able to:   * Select authenticator options * Input authenticator information * Log in to the acquisition gateway |
| As an **Acquisition Gateway User, I need** to review my previous bids in the Acquisition ordering platform **so that** I can remove expired bids. | Ensure the Acquisition Gateway User is able to:   * Log in to Acquisition Gateway * Access the page to review items previously bid upon * Select one, or multiple, expired bids * Remove expired bids based on having the correct privilege |

Table 3. Example User Story

User stories should emphasize that cloud presents a completely different engagement model to an organization, including its ICAM processes. A cloud migration fundamentally shifts the role of ICAM: now, it seeks to enable business owners to maximize the effectiveness of their business and mission products. [Single Sign-On](https://playbooks.idmanagement.gov/docs/playbook-sso.pdf) is an important pattern that enables user experience for business owners.. SSO aggregates how users access cloud services, but also why they access cloud services, information that helps business owners adjust their products to better serve users.

### Write a Business Case

Next, the agency should draft a business case including funding considerations. In the business case, an agency should articulate how:

* ICAM capabilities support Zero Trust, and
* Migrating such capabilities to the cloud enhances an ICAM program, thereby enhancing a Zero Trust Architecture.

A key 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](https://community.max.gov/display/Egov/Agency%2BIT%2BModernization%3A%2BEducational%2BResources%2BBuilding%2BBlocks).

### Zero Trust Architecture Alignment

[Executive Order 14028: *Improving the Nation's Cybersecurity*](https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity) instructs agencies to accelerate their cloud migrations in a manner that adopts Zero Trust Architecture. ICAM is a critical enabler to the five pillars of zero trust.

|  |  |
| --- | --- |
| **ZERO TRUST PILLAR** | **ICAM ENABLER** |
| Identity | ICAM is the identity pillar and ecompasses all digital identities, people and machines, either managed by an agency or external users attempting to access agency resources. |
| Device | Device identification and health attributes such as device type, operating system, operating system version, and location can aid authorization decisions at a policy enforcement point. |
| Network | Agencies can deploy forward or reverse proxy to act as policy enforcement points and apply access policies in real-time to both government furnished and bring your own devices. |
| Application | Application access is integrated with an SSO tool to centralize access, policy enforcement, and monitoring. |
| Data | A data tagging strategy can help segment and implement fine-grained access (e.g. all private data can only be read by human resources group users). This outcome is more achievable with modern cloud security and data loss prevention tools. |

Table 4. ICAM Enablers for Zero Trust

## Step 2. Identify a Plan and Success Factors

The first step in any journey is identifying the destination. Your agency can take one of two approaches.

1. **Incremental** - Identify single services to test and deploy based on identified goals, metrics, and outcomes. When that service is successful, repeat with another service. The advantages of this approach is waiting for cloud capabilities or tools that are mature enough to meet your agency’s needs.
2. **Full Migration** - Identify comparable cloud identity services and incrementally or migrate services from on-premise to the cloud providers.

The [ICAM Practice Areas and Services Framework](https://playbooks.idmanagement.gov/arch/services/) is a great starting point to map business requirements to technical solutions. The ICAM Governance Framework is also a great resource to identify ICAM capabilities, integration points, and enterprise governance examples and templates.

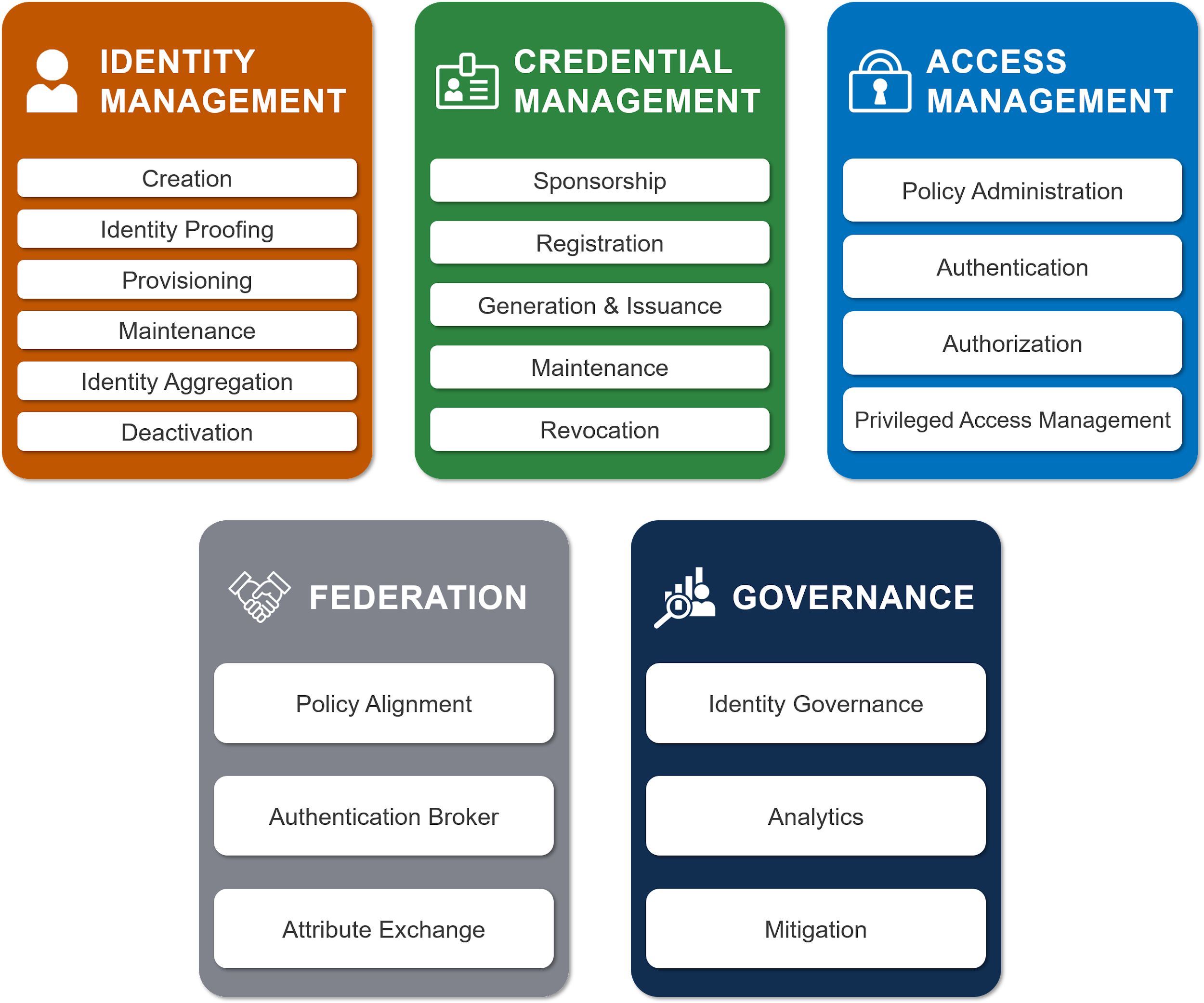


Figure 02. FICAM Services Framework

|  |  |
| --- | --- |
|  | **Myth Busted - It's Cloud or Nothing**  The majority of agencies are operating ICAM in a hybrid cloud environment. |

### Cloud ICAM Strategy and Goals

A Cloud ICAM strategy and goals help an organization work in a concerted manner. An example pairing of a strategy to a goal is to identify how to consolidate identity services (strategy) in order to prevent capability sprawl (goal). It is possible that the ICAM Policy and Strategy are the same document for ease of management or based on the size of the agency. Large agencies may have separate strategies for modernization, security, and ICAM while smaller agencies may decide to combine them into a single document. Use the ICAM Services Framework to identify ICAM services. There are five core services with a number of sub-services. The FICAM Architecture also provides a component example for typical services and how they align with the FICAM Architecture.

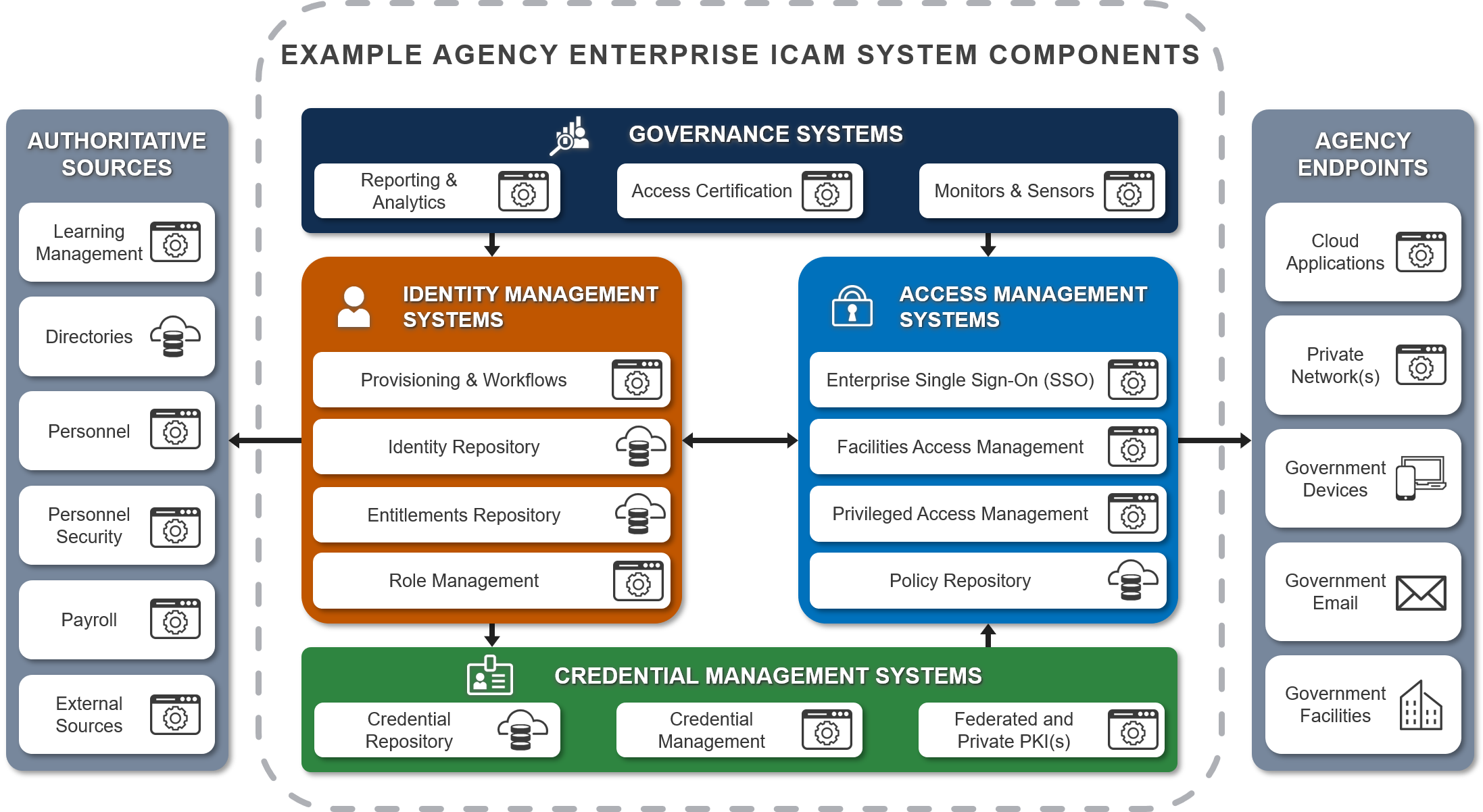


Figure 03. FICAM System Components

|  |  |  |
| --- | --- | --- |
| **Core Service** | **Business Requirement** | **Cloud Option** |
| Identity Management | Establish and manage identities for all users. | A majority of Cloud Identity tools come with directory services or can leverage an on-premise directory. Virtual Directories are another option to merge 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 cloud services or application frameworks that use modern authenticators that meet NIST Special Publication 800-63-3 Authenticator Assurance level 2 or higher. This may include one-time pin authenticator mobile applications, Web Authentication or WebAuthN, or other secondary authenticators mentioned in your policy. |
| Access Management | Adopt and use cloud-ready systems that provide an efficient and secure way to access resources. | The majority of cloud identity services are access management tools for either enterprise, citizen, or privileged access management. |
| 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 cloud ICAM services can export logs to support user behavior analytics. A part of technical identity governance is performing access certifications and agnostic ICAM analytics for role mining, provisioning and de-provisioning automation, and account discovery. |
| Federation | Leverage federated solutions to accept identity and authentication assertions made by other agency and mission partners when efficient. | Federated access is usually implemented through a SSO tool. As part of federation, you may decide to operate an oAuth service for authorization tokens. A key part of some federations are legal agreements for identity pattern reciprocity. |

Table 5. Cloud Identity Strategic Goals

### Cloud Identity Starting Point

The most common first use of cloud identity is access management or a SSO tool for enterprise use cases and federation.

Here are a couple points to consider as you define your Cloud Identity strategy.

1. Most cloud applications implement role-based access. Plan to understand and implement consistent role-based access through your access management tools.
2. Your agency may already use Cloud Identity services. It may only be a matter of identifying a primary service and then reducing duplicate services already in place.
3. A key aspect of leveraging cloud identity services is application compatibility. Not all applications are written equally and may implement identity patterns differently (e.g. some applications may allow provisioning in an assertion while others may not). Use the [Single Sign-On Playbook](https://playbooks.idmanagement.gov/docs/playbook-sso.pdf) as a cloud access planning guide.
4. With the increase in internet traffic, account for additional monitoring and log analysis in your Security Information and Event Monitoring.
5. One of the main differences between on-premise ICAM and cloud ICAM is the need to steer and monitor device traffic to apply authentication and authorization decisions. **Device management and ability to deploy device agents is a key Cloud Identity pattern to monitor and assess traffic agnostic of the network or connection.** [Executive Order 14028](https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity) identifies comprehensive security monitoring as a key component of Zero Trust Architecture. Steering is dependent on how a device is configured to reach a website through a Trusted Internet Connection approved method such as a Virtual Private Network, Virtual Desktop Interface, a Cloud Access Security Broker or Secure Edge solution, or some type of direct connection through a forward or reverse proxy.
6. Consider federating all types of human access. It is very common to have Personal Identity Verification-enabled enterprise applications after the 2015 cyber sprint. The more modern approach is to federate access with your SSO to allow a greater variety of modern authenticators and centralizing access management.

|  |  |
| --- | --- |
|  | **Myth Busted - On-premise is More Secure than Cloud**  On-premise resources and services are just as vulnerable as cloud services. While the ubiquity of access required for cloud services may create more security challenges, cloud services can be more secure because they usually leverage faster update and patching cycles than on-premise applications. |

### 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 unique operational challenges. Some example metrics include:

* The length of time to deprovision an account
* The number of orphaned accounts
* The number of applications integrated
* The number of identity processes, and
* The number of manual processes automated.

Use your agency’s operational value, or the rate of transactions in a given time period, to identify where you want to set operations 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 chosen metrics to federal policy and agency mission objectives, to help translate improvement in metrics to progress in meeting overarching agency goals. For example, identify before migration which metrics would, if improved, show evidence of compliance with federal mandates, like Cloud Smart, and which others would show evidence of operational improvements, like faster review cycles. Include your metrics within your strategy.

|  |  |
| --- | --- |
|  | **Budgeting IDaaS**  Most Cloud Identity products are priced by number of users, number of authentications, number of integrated applications, or per application connector. Have this information ready when talking with an IDaaS vendor. These data points are also collected as part of a Digital Identity Risk Assessment. |

### Cloud ICAM Policy

While the Cloud ICAM Strategy states the path to achieve an outcome, the cloud ICAM Policy sets the boundaries to achieve the strategy. It is very likely your agency may already use some Cloud Identity services. Your cloud identity infrastructure should fit within your agency vision for cloud services, modernization, and cybersecurity efforts. Within those broader agency policies, there should be specific call-outs of how identity supports those efforts and potentially goals or objectives in accomplishing your agency’s mission. If it does not, recommend changes to highlight how ICAM supports your agency mission and business processes.. The four main strategies or policies to identify are cybersecurity, modernization, cloud, and a Chief Information or Information Security Officer’s policy or vision (if it exists). For example, In the [Department of Defense Modernization Strategy](https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF) they’ve incorporated deploying an end-to-end ICAM infrastructure as an objective of their evolving cybersecurity goal. The Defense Department then wrote an [ICAM Reference Design](https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf) to support the objective. With this executive direction and support from Step 1, craft an agency policy to emphasize or reduce the following points.

1. **Prevent Capability Sprawl or Duplication** - With the ubiquity of identity and variety of IT mission applications, duplicative ICAM services with an agency could be pervasive. An agency policy should identify authoritative enterprise ICAM services. Part of this exercise could include identifying mission application ICAM services to promote as an enterprise service or identifying duplicate services among your general support systems as well as mission applications within your Chief Information Officer’s Federal Information Technology Acquisition Reform Act authority. Identifying and communicating enterprise ICAM services will help reduce new ICAM acquisitions for existing services.
2. **Centralize ICAM Services to Create an Enterprise ICAM Capability -** Identify Authoritative ICAM Services that align with the FICAM Services Framework. An authoritative identity source within an agency is a repository of accurate information that feeds into your directory services. It may contain data sources which can or can not be edited by a user. For example, a user can update their phone number but not their clearance status. Along with authoritative identity sources, identify authoritative authenticators and access tools for workforce and external user SSO. A Personal Identity Verification (PIV) smart card is the required primary means of authentication, a secondary authenticator may be issued and bound to the same directory record and offer comparable security.
3. **Identify Core Services to Maintain On-Premise** - Continuity of operations may require a back-up method for continued on-premise operation of ICAM services. Some core services such as directories or specific types of access tools should remain on-premise. Agencies have found that even though they operate services on-premise, they most often have to replicate data to a cloud service anyway. Keep this in mind.
4. **People and Non-Person Entities** - Incorporate ICAM for people and NPEs, otherwise known as Machine Identities, within your strategy or policy. NPEs are the multitude of devices (or any non-human identity) on your network or the internet that need an identity or credential to perform their function. Their identities and credentials should be managed in a similar yet slightly different pattern based on the type of device or NPE. For example, use the [Digital Worker Identity Playbook](https://playbooks.idmanagement.gov/docs/playbook-digital-worker.pdf) to assess and mitigate the risk of using automated technologies.
5. **Require Digital Identity Risk Assessments** - A Digital Identity Risk Assessment identifies the risk of user transactions 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](https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf). If your agency doesn’t have a Digital Identity Risk Assessment policy or process, consider using the [Digital Identity Risk Assessment Playbook](https://playbooks.idmanagement.gov/docs/playbook-dira.pdf).

## Step 3. Architecture Considerations

Many agencies face similar challenges when extending ICAM services to the cloud. This section includes architectural considerations aligned with the Federal ICAM (FICAM) Services Framework. Cloud Identity architecture should include all aspects of ICAM for a comprehensive enterprise capability. One of the main benefits of using Cloud Identity tools is the ability to automate more processes by leveraging programmatic interfaces and open standards for authorization such as OAuth.

### Identity Management

1. **Role Management** - Most cloud applications and platforms implement role-based access. Manage permissions by group rather than individual. Base groups on roles such as government admin, contractor admin, contributor, or reader. All users in a group inherit the same permissions. Entitlement management is as easy as removing the user from that group or role.
2. **Accurate Directory Information** - Before starting a cloud identity project, make sure your directory information is accurate. You will replicate your on-premise directories to a cloud directory and it is better to do this action before, rather than after replication.
3. **Automating Identity** - One unique feature of IDaaS is the potential to automate a lot of manual or scripted processes. LIfecycle management, often referred to as the joiner-mover-leaver process, should be leveraged to its fullest. For example, just because a user is removed from a directory or access tool, that account may still exist in an application. Leverage automated lifecycle management processes that enable lifecycle management actions simultaneously or a manual workflow integrated with an IT Service Management to track and audit processes. [System for Cross-domain Identity Management](http://www.simplecloud.info/) is an open standard and common pattern in IDaaS to automate user provisioning.
4. **Virtual Directory** - Not all cloud application access is equal. Consider using a virtual directory that can create unique personas based on existing directory information for specific applications. For example, if an application requires a specific attribute such as citizenship and that attribute is not contained in the existing record, you can use a virtual directory to combine two identity sources to create the attribute configuration you need for an access decision.
5. **Machine Identity Management** - Similar to not all application access is equal, neither are machine identities. Each type of device or digital worker may require a different configuration or type of management. A good initial step is to get an idea of the variety of devices and methods of identity. This can include service accounts, Application Programming Interface tokens, secure shell keys, DevOp secrets, and device Public Key Infrastructure certificates. Then you can move on to identify the highest risk devices and a method to secure their identity.

|  |  |
| --- | --- |
|  | **Governance Challenge - Enforcing Least Privilege**  Least privilege is granting only the privileges necessary to perform a task. For example, if someone is assigned responsibility to manage user passwords they should not be assigned a role that also manages resources. This may require some testing to determine the appropriate mix of privileges to complete a task. Gather 30 days of user activity to analyze what permissions are necessary and then create a role or group- based on that group. Some platforms may support privilege check-out for short instances when a higher privilege is needed. |

### Credential Management

1. **Use the best authenticator for the use case** - One of the advantages of using modern software is using modern authenticators. Every federal employee and contractor is required to have a PIV card, but it may not fit every use case. Secondary authenticators may be issued and bound to the same directory record and offer comparable security. 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](https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/CSI_MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF).
2. **Machine Credentialing** - Agencies should make a risk decision about managing non-person credentials including if, how, and when to enforce more stringent controls. Machine credentials should be managed in a similar yet slightly different pattern based on the type of device or NPE. For example, DevOps use secrets (typically authentication credentials such as username/passwords, API tokens, etc.) which should be available when validly requested and approved, and this may include programmatic requests for a secret upon access request to a target system. The secrets must be rotated regularly to reduce the period an attacker who has acquired a secret can operate. Some secrets are ephemeral in nature and expire automatically. All secrets should be revocable so that they can ensure they can’t be used after an attack on the secret is discovered.
3. **Passwords Are Inevitable** - Password (otherwise known as memorized secrets) use is inevitable. Follow [NIST Special Publication 800-63B](https://pages.nist.gov/800-63-3/sp800-63b.html) guidelines for passwords such as:
4. Should be an alphanumeric between 8 to 64 characters
5. Shall be checked against breach corpuses, dictionary words, repetitive characters, or context-specific and denied
6. Should offer a password strength meter
7. Shall limit the number of failed attempts before a lock-out or require a password reset.
8. Should not require periodic password updates.
9. Should be used as part of a multi-factor authenticator
10. Should support the use of a password manager through allowing a cut- and-paste function

|  |  |
| --- | --- |
|  | **Rotate Access Keys, Not Passwords:** NIST recommends agencies not require password rotation. Instead, programmatic access keys should be rotated and not embedded in unencrypted code. Where keys and secrets are used, consider using a secrets management tool. |

|  |  |
| --- | --- |
|  | **Risk Management Challenge - Unique Credentials**  Credentials should be assigned on an individual basis and not shared. User audit logs can also help track the use of shared credentials. If a credential must be shared, NIST recommends requiring individual authentication to access the shared credential. |

### Access Management

1. **User Access to XaaS** - Users must be able to connect to the cloud service. This means creating network paths for users coming from an agency network (direct or through Virtual Private Network) but also potentially for users not on an agency network. For example, Email as a Service login page is accessible off-network but requires SSO which is only accessible on network”.
2. **Protocol Monitoring** - Access comes in many protocols. Monitor access attempts over all possible protocols such as https and secure shell. Also, factor in the use of port translation technology.
3. **Leverage Modern Cloud Access** - Many cloud access tools can leverage telemetry for access decisions such as device type, browser type, location. Check with your access management vendor how and if they support this capability.
4. **Proxy It** - [Trusted Internet Connection 3.0](https://www.cisa.gov/publication/tic-30-core-guidance-documents) provides two cloud access options through either a Cloud Access Security Broker or a Security Gateway. Both may operate in a forward to reserve proxy mode to monitor traffic and apply access policies in real-time.

|  |  |
| --- | --- |
|  | **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 analyzing ideal access conditions, access policies and exceptions are identified and implemented or tracked through access tools and audit logs. |

### Governance

1. **Certify Access** - Access certification or recertification is the process of an application owner or a manager to attest to someone's access. This could be an automated or manual process. For higher impact applications, this should happen more frequently, such as monthly or quarterly, than low impact applications.
2. **Plan for Contingencies** - Cloud admin portals may be secured differently for continuity of operations. Follow vendor best practices for “break glass” admin accounts such as ensuring they are not linked to an individual and use an MFA that is different from other methods. Test disaster recovery scenarios on a regular basis. This may require collaborating with your cloud service provider to identify scenarios 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 Everything** - Cloud services embed access based on policies that are machine-readable and executable. 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. This ensures a consistent implementation of agency cloud identity policies.
5. **Monitor Activity** - Enable activity logging for privileged users and all users, if possible.

|  |  |
| --- | --- |
|  | **Workforce Planning**  A majority of cloud ICAM patterns are based-on open protocols such as JavaScript Object Notation, SCIM, oAuth, Security Assertion Markup Language, Open Policy Agent and Open ID Connect. A good workforce training tip is to become familiar with these protocols. |

|  |  |
| --- | --- |
|  | **Workforce Challenge - This is Different**  Any changes to the user experience can degrade workforce efficiency. Plan to communicate changes to prepare your users for a changing experience. |

### **Federation**

Use federation where it improves user experience and security. This Playbook uses the [FICAM Architecture](https://playbooks.idmanagement.gov/arch/)’s definition of Federation, which views it as “the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.”

1. **Trust Relationship** - Federation is equal parts technology as it is policy. An agreement between entities should identify the required security and governance processes of each organization. A template that includes the format and required attributes is also a best practice. See [NISTIR 8149](https://csrc.nist.gov/publications/detail/nistir/8149/final) for more information on trust frameworks. The Federal PKI and the PIV card certificates issued from it are one example of an inter-agency trust framework.
2. **Exchanging Attributes** - One advantage to using either a cloud-based or on-premise SSOn tool is that most support moden assertion protocols to act as an authentication broker. This also means the ability to share identity attributes using an assertion protocol like Security Assertion Markup Language or Open ID Connect.

|  |
| --- |
| **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 which 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 compliance operations . In the context of FedRAMP, this is a third party assessment organization or an annual compliance audit for the Federal Public Key Infrastructure Shared Service Providers. External examples used by federal agencies include the Kantara Initiative or the Health Information Service Provider for DirectTrust. The Trust Framework requirements set the standard for which external digital identities and what NPEs are authorized to agency resources. |

## Step 4. Test and Deploy

Before deploying new services or enhancements, test them in a sandbox or production-like environment. Cloud services embed access based on policies that are machine-readable and executable. Everything a user does in the cloud is policy-based with the majority of access policies written in JavaScript Object Notation. Open source tools are available to test policy changes before they are implemented in a production environment.

### Test and Deploy Cloud Identities

Testing ICAM changes follow a similar pattern between on-premise components and cloud components except with a focus on leveraging automation.

1. **Document existing process** - Document the existing process to include the actions and outcomes from a user perspective. This may follow a similar structure as the use case example provided in [step 1](#_i3igxeja6brx).
2. **Review process workflow** - This includes identifying the unique steps to achieve the outcome.
3. **Identify challenge(s)/pain point(s)** - Every process has some obstacle or barrier to achieving the outcome. In the user story example, the intermediate steps to login include selecting an authenticator and inputting authenticator information. Those can be seen as necessary obstacles to achieving the outcome.
4. **Update workflow with desired outcome** - The desired outcome is accomplishing the goal with as little obstacles as possible. In our previous example of logging in, is there a way to maintain security while improving the user experience? Potential options may include passwordless authentication with a push notification or a WebAuthN request.
5. **Implement workflow** - After an optimal workflow is found, it is time to test and implement it. When testing, choose a small population that does not include all administrators so you are not locked out of your environment.

### Integrate ICAM into DevSecOps

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 pipeline. This is necessarily 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 environments the things that can be attacked by an adversary (aka the attack surface) may change constantly and this can put the organization at extreme risk as seen in the latest Solarwinds hack. Follow these recommended best practices to integrate ICAM into DevSecOps.

1. **Manage DevOps Keys and Secrets** - The increased use of code to configure infrastructure places a greater demand on ensuring that the secrets that are used in these environments are well managed. Access tools can provide several mechanisms to help in this regard but there may be then need for other tools, specifically Certificate Management tools and Application Programming Interface management tools that will be necessary as configuration of cloud environments becomes more highly automated. The total code and configuration needs to be packaged as a configuration item so that the entire content of a delivery can be known and tracked in operation.
2. **Implement Custom Admin Roles for Separation of Duties** - Deployment engineers will likely have access to systems at administrator level and these entitlements need to ensure that separation of duties is employed. The ICAM system can be configured such that separations enforce that an individual that deploys the database does not have access to change the operational data IN the database but can only manage the database itself.
3. **Create Unique Credentials** - To ease the burden of manually managing credentials, they are often reused across projects and across team functions (e.g. This is our lab password). This enables one stolen credential to be able to be used over and over for other purposes. Practice production security practices in your test environments.
4. **Manage Programmatic Access** - Extend inventory of devices to those in the pipeline, including DEV, TEST, and STAGING environments and inventory all the tools that have programmatic access to the pipeline as well as who owns these components.

See the [GSA Guide](https://tech.gsa.gov/guides/dev_sec_ops_guide/) on DevSecOps for more information.

## 

# 

# 

# Appendix A. Policies, Standards, and Guidance

## Policies

1. [Executive Order 14028 - Improving the Nation’s Cybersecurity](https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity)
2. [Federal Cloud Smart Strategy](https://cloud.cio.gov/)
3. [Office of Management and Budget Memo 19-17](https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf)

## Standards

1. [NIST Special Publication 800-63 - Digital Identity Guidelines](https://csrc.nist.gov/publication/detail/sp/800-63/final)
2. [NIST Special Publication 800-145 - NIST Definition of Cloud Computing](https://csrc.nist.gov/publications/detail/sp/800-145/final)
3. [NIST Special Publication 800-204B - Attribute-based Access Control for Microservices-based Applications using a Service Mesh](https://csrc.nist.gov/publications/detail/sp/800-204b/final)
4. [NIST Special Publication 800-207 - Zero Trust Architecture](https://csrc.nist.gov/publications/detail/sp/800-207/final)
5. [NIST Special Publication 800-210 - General Access Control Guidance for Cloud Systems](https://csrc.nist.gov/publications/detail/sp/800-210/final)

## Guidance

1. [Digital Identity Risk Assessment Playbook](https://playbooks.idmanagement.gov/docs/playbook-dira.pdf)
2. [Data Center and Cloud Optimization Initiative Cloud Strategy Guide](https://community.max.gov/display/Egov/Agency%2BIT%2BModernization%3A%2BEducational%2BResources%2BBuilding%2BBlocks)
3. [Enterprise Single Sign-On Playbook](https://playbooks.idmanagement.gov/docs/playbook-sso.pdf)
4. [FedRAMP Digital Identity Requirements (Version 1.0)](https://s3.amazonaws.com/sitesusa/wp-content/uploads/var/www/html/sites/www/app/wordpress/wp-content/blogs.dir/482/files/2016/06/FedRAMP_Digital_Identity_Requirements_v1.0.pdf)
5. [FICAM Architecture](https://playbooks.idmanagement.gov/arch/)
6. [ICAM Program Management Playbook](https://playbooks.idmanagement.gov/pm/)
7. [General Services Administration - Cloud Information Center](https://cic.gsa.gov/)
8. [NIST Interagency Report 8149 - Developing Trust Frameworks to Support Identity Federations](https://csrc.nist.gov/publications/detail/nistir/8149/final)
9. [NIST Interagency Report 8335 - Identity as a Service for Public Safety](https://csrc.nist.gov/publications/detail/nistir/8335/draft)
10. [NIST Interagency Report 8360 - Machine Learning for Access Control Policy Verification](https://csrc.nist.gov/publications/detail/nistir/8360/final)
11. [NIST Special Publication 1800-13 - Mobile Application Single Sign-On](https://csrc.nist.gov/publications/detail/sp/1800-13/final)
12. [National Security Agency Cybersecurity Information Sheet - Mitigating Cloud Vulnerabilities](https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF)

# Appendix B. Acronyms

|  |  |
| --- | --- |
| 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 |
| PIV | Personal Identity Verification |
| SSO | Single Sign-On |