Identity, Credential, and Access Management Governance Framework

September 2021

Version 1.0

Identity, Credential, and Access Management (ICAM)
Governance Framework Working Group

Identity, Credential, and Access Management Subcommittee (ICAMSC)

Table of Contents

1. Introduction

Advances in technology have enabled more digital interactions and business transactions, offering the Federal Government an opportunity for faster, more reliable connections and operations in digital service delivery. These advances, however, also introduce particular challenges and risks. A few of these include:

- **Information security breaches:** Recent breaches, including the 2020 SolarWinds and 2021 Colonial Pipeline cyberattacks, demonstrate the ability of cybercriminals to steal data and even interrupt digital service delivery.
- **Increased attack surface areas:** Users can access much more information than they could in the past. Without proper access management controls, one compromised account can provide cybercriminals with a vast amount of data.
- **Data privacy breaches:** As digital transactions expand, the amount of personally identifiable information (PII) available on the Web also increases, leading to increased risk of unauthorized data access, monetary fraud, and identity theft.
- **Compliance violations:** New policies like the *Office of Management and Budget (OMB) Memorandum M-19-17*[1] introduce new directions which may take time to align with agency strategy and budget.

As emphasized in Executive Order (EO) 14028: *Improving the Nation's Cybersecurity*, "incremental change is insufficient to achieve the security needed to secure Federal Government networks. Significant investment and improvement are what the moment demands."[2] Securing Federal Government networks begins with knowing who is on the network, how individuals are accessing the network, and what resources are being accessed. Identity, Credential, and Access Management (ICAM) is the set of tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. A well-structured ICAM program supports agency business objectives, enhances an agency's cybersecurity, and enables agencies to serve their constituents in a secure manner. An authoritative ICAM governance structure, grounded in policy and focused on mission success, is the foundation to building and maintaining robust ICAM practices.

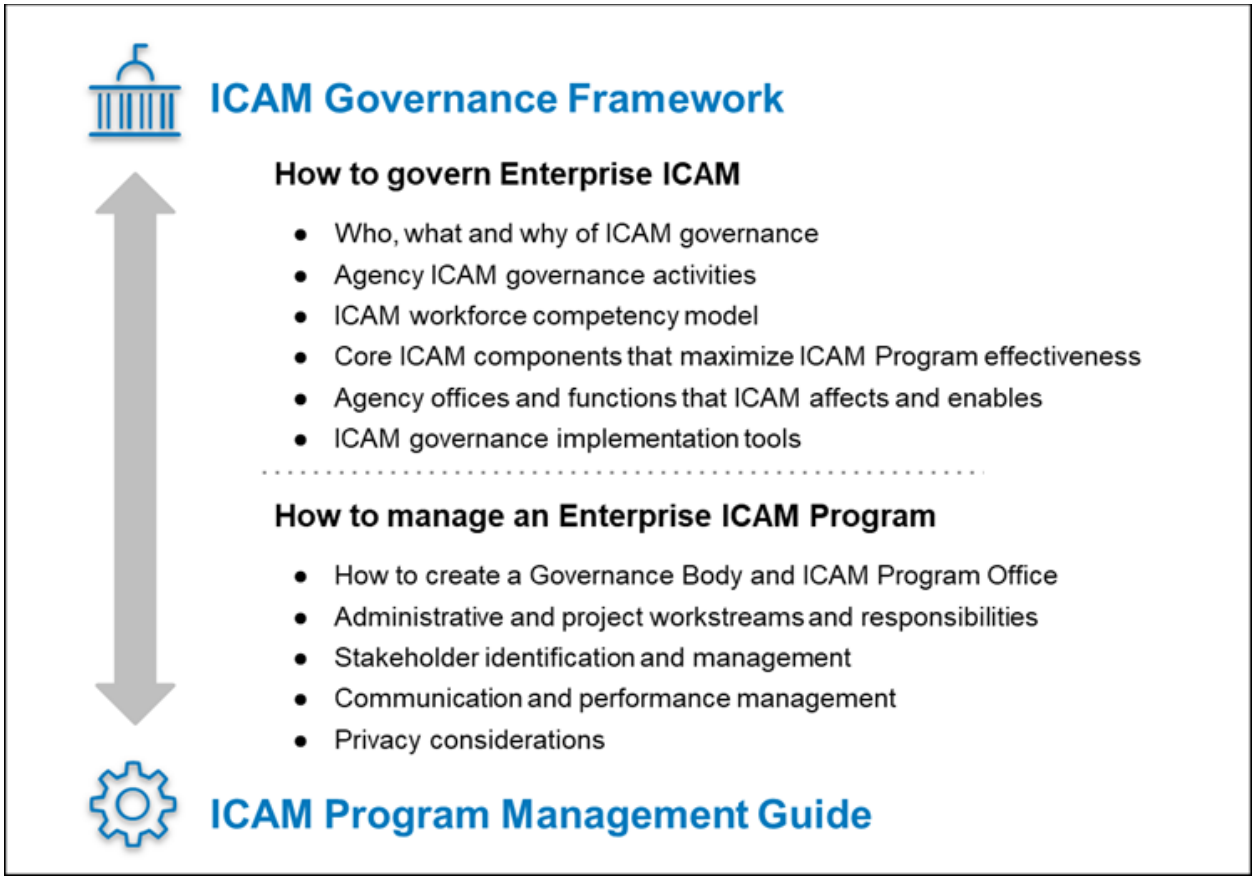
To support the development of robust agency ICAM governance, the Identity, Credential, and Access Management Subcommittee (ICAMSC) chartered the ICAM Governance Framework Working Group (IGFWG). The IGFWG, composed of ICAM practitioners from several federal agencies, developed this ICAM Governance Framework as a tool to help agencies build and improve ICAM governance structures, processes, and policies. The term "Framework" will refer to this document from this point forward.

This Framework will guide agencies on how to govern ICAM across the enterprise. For

[1] OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019
[2] Executive Order 14028, Executive Order for Improving the Nation's Cybersecurity, May 12, 2021

guidance on how to plan and implement an ICAM Program, see the ICAM Program Management Guide. Figure 1 identifies the relationship between this Framework, the FICAM Program Management Guide, and the topics addressed under each guidance.

Figure 1: ICAM Governance Framework versus ICAM Program Management Guide



1.1 Purpose

This Framework illustrates the value of enterprise ICAM governance to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives and to facilitate secure and effective agency mission delivery. For the purpose of this Framework, ICAM governance refers to the set of practices and systems that guides ICAM functions, activities, and outcomes.[3]

ICAM functions and activities are the foundation for many cybersecurity initiatives, and when all agency stakeholders are involved in discussions and decision-making, ICAM addresses many of the universal enterprise-level objectives facing agencies today. Many agencies have identified the following challenges for implementing ICAM governance:

- Lack of executive leadership support and understanding of how ICAM aligns to

[3] Federal Identity, Credential and Access Management (FICAM) Architecture, 2020

mission, Information Technology (IT), and cybersecurity goals
- The misconception that ICAM is only an IT concern and not a business enabler
- Lack of clear definitions of ICAM roles and responsibilities. ICAM is an essential business function that impacts and enables every office across an agency, but roles and duties for ICAM professionals and the key stakeholders supporting ICAM are ill-defined
- Lack of funding and other resources needed for system implementation, scaling, and integration hinders the ability of ICAM to support mission success

See Appendix B: Common ICAM Challenges for a list of the common ICAM governance challenges brought forth by the IGFWG.

Agencies can use this Framework to create or improve ICAM governance to:

- Obtain appropriate resources to support the deployment, maintenance, and adoption of enterprise ICAM capabilities
- Provide a consistent risk-based level of assurance for ICAM related decisions
- Improve federal enterprise and public identity experiences
- Support interoperability and federation of ICAM solutions
- Reduce duplication of effort, cost, and complexity resulting from disparate ICAM solutions and standards being used across agencies and mission areas
- Reduce risk and fraud
- Provide a consistent identity context across agencies

1.2 Scope

This document does not represent an official policy or mandated action. Instead, this Framework complements OMB guidance instructing federal civilian agencies to "designate an integrated agency-wide ICAM office, team, or other governance structure in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts."[4] It also aligns with the following policies and guidance documents:

- **Federal Information Technology Acquisition Reform Act (FITARA) Identity Data Collection requirements**[5] require agencies to provide a public version of enterprise data inventory
- **Federal ICAM (FICAM) Architecture**[6] provides a framework for agencies to use in ICAM program and solution roadmap planning. The FICAM Architecture focuses on enterprise identity processes, practices, policies, and information security disciplines

[4] OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019
[5] Federal Information Technology Acquisition Reform Act, Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L No. 113-291, December 19, 2014
[6] Federal Identity, Credential and Access Management (FICAM) Architecture, 2020

- **Executive Order (EO) 14028** ***Executive Order for Improving the Nation's Cybersecurity***[7] mandates agencies to improve cybersecurity posture, including adopting a Zero Trust Architecture (ZTA), which embeds security monitoring and authentication into every digital transaction
- **Trusted Workforce and Core Vetting Doctrine**[8] mandates agencies to move vetting processes towards an enhanced risk management approach

Where applicable, this Framework refers to two contexts of identity following OMB M-19-17.

1. **Federal enterprise identity**
    a. A federal enterprise identity, or, simply, enterprise identity, refers to the unique representation of an employee, a contractor, an enterprise user, such as a mission or business partner, a device, or a technology that ***a federal agency manages*** to achieve its mission and business objectives.
    b. In other words, if the agency manages the user's identity or device (e.g., can create, modify, suspend, revoke, or delete the identity record or device), it is a federal enterprise identity.
2. **Public identity**
    a. A public identity refers to the unique representation of a subject that a federal agency interacts with, but ***does not directly manage***, in order to achieve its mission and business objectives. Public identity may also refer to a mechanism of trust used to render services to the American public.
    b. In other words, if an agency does not manage the identity, it is a public identity.

1.3 Audience

The audience for this Framework includes federal agency executive leadership, and federal IT and ICAM practitioners who are responsible for, contribute to, implement, or are impacted by ICAM activities. The Framework serves this audience by helping agencies define a structure for how ICAM is governed across the enterprise. See Table 1 below for a list of stakeholders within each audience category.

Executive Leadership
Agency executives, such as Chief Information Officers (CIOs), Chief Financial Officers (CFOs), Senior Policy Officials, and Chiefs of Staff, may use this Framework to:

- More effectively communicate ICAM capabilities, impacts, policies, and procedures
- Make decisions, and set priorities to strengthen and strategically align their ICAM governance structure across their organization

IT and ICAM Practitioners

[7] Executive Order 14028, Executive Order for Improving the Nation's Cybersecurity, May 12, 2021
[8] Federal Personnel Vetting Core Doctrine, 86 Federal Register 2705, January 13, 2021

The Framework identifies the processes and patterns that ICAM program managers, IT partners, system and business owners, and various other federal ICAM partners can use to integrate enterprise ICAM to achieve their goals and objectives.

Table 1: ICAM Governance Framework Audience

ICAM Governance Framework Audiences	
Executive Leadership	IT and ICAM Practitioners
Chief Information Officers (CIO)	ICAM Program Managers
Chief Financial Officer (CFO)	System/Business Owners
Human Resources (HR)	System Architects and Engineers
General Counsel	Operations Teams
Chief Information Security Officer (CISO)	Cybersecurity Teams
Senior Agency Official for Privacy (SAOP)	Testing Teams
Chief Acquisition Officer (CAO)	Compliance and Audit Teams
Senior Official(s) responsible for Physical Security	Procurement Personnel
Chief Data Officers (CDO)	Personnel Security
Agency Chief-of-Staffs	Readiness Officers
Chief Technology Officer (CTO)	Emergency Managers
Chief Experience Officer (CxO)	

2. ICAM Governance Overview

Authoritative ICAM governance allows agencies to make ICAM resourcing, technology, and process decisions aligned to the agency's mission, including interactions with external service providers, external partners, and public and federal enterprise identities.

2.1 Benefits of ICAM Governance

A robust, authoritative governance structure with consistent practices, leadership support, and engaged participants enables an ICAM program that supports an agency's mission. Enterprise-level ICAM governance will lead to the alignment of ICAM to agency goals, consistent implementation across business lines, improved security, and cost reduction. ICAM governance also supports attribution, the tracking of access and activities by each user. ICAM is fundamental for the transformation to a modern data-centric architecture that is required to achieve a future-state, Zero Trust environment. Strong, effective ICAM governance enables the following outcomes and benefits.

Figure 2: Enterprise ICAM Governance Outcomes

1. Driving Missions

- Increases overall awareness of the importance and benefits of ICAM at the Executive Leadership level and throughout the organization
- Enhances knowledge of ICAM needed to make appropriate and timely decisions on ICAM-related activities
- Establishes well-defined roles and responsibilities within ICAM. Clearly defined roles and responsibilities help the agency streamline how ICAM offices work with other groups within the agency, avoiding stovepipes and increasing efficiency, which ultimately drives the ICAM mission and the agency mission at large

- Helps agencies understand ICAM governance and know who to contact for assistance and guidance

2. Enhancing Security

- Enables the consistent application of best practices to appropriately identify users, through robust governance
- Reduces delays in the issuance and removal of credentials, which speeds access to authorized systems and services while preventing inappropriate access of facilities or IT resources that may result in data tampering or theft
- Increases progress in implementing modern security and process improvements, such as multi-factor authentication (MFA) enforcement, improving the overall security posture of an agency
- Reduces risk for agency systems and services that would stem from inadequate auditing and monitoring, which may lead to unauthorized access to resources

3. Empowering Users

- Provides consistent, timely, and seamless identity creation, provisioning, and authorization to necessary systems
- Enhances end-user experience for employees, affiliates, and external constituents and mission partners using any integrated system. For example:
    - Streamlines processes and provides a better overall experience
    - Provides federal enterprise identities and public identities with the latest technologies to support ease of access to agency and organizational resources and information systems
    - Increases employee productivity through streamlining certain tasks allowing agencies to focus on mission-critical activities

4. Improving Cost and Business Efficiencies

- Promotes the ability to implement enterprise-wide capabilities via governance processes for application and system integrations, enabling agencies to shift away from component level or system level capabilities
- Reduces resource expenditures by enabling enterprise-wide capabilities, and the corresponding shift away from component level or system level capabilities, creating cost savings that can be shared among agencies
- Enables compliance and auditing by providing appropriate visibility and oversight and a clear path of expected milestones and reporting requirements. Streamlining auditing and business processes allows an agency to focus on mission-critical tasks

2.2 Enterprise ICAM Governance

Integrating ICAM into agency enterprise governance activities will allow ICAM to receive the

leadership attention needed for successful implementation and integration. Additionally, bringing ICAM to the forefront increases the likelihood that ICAM is included in mission-critical planning strategies. OMB M-19-17 requires the following stakeholders to be part of their agency's integrated agency-wide ICAM office, team, or other governance structure.

- Chief Information Officer
- Chief Financial Officer
- Human Resources
- General Counsel
- Chief Information Security Officer
- Senior Agency Official for Privacy
- Chief Acquisition Officer
- Senior Official(s) responsible for Physical Security
- Component organizations that manage ICAM programs and capabilities

Table 2 provides a high-level description of how ICAM governance supports each stakeholder, and the responsibilities each stakeholder has for supporting enterprise ICAM.

Table 2: ICAM Governance Stakeholders

Stakeholder	ICAM helps me meet my mission by..	I can help support enterprise ICAM by..
Chief Acquisition Officer	Verifying that acquisition sensitive information is only available to properly authorized individuals and that contractor personnel are associated with active contracts	Requiring the inclusion of standard language for ICAM-related requirements in Request for Proposals (RFPs) Examples include: • Specifying that ICAM systems must be compatible with enterprise solutions • Including support for enterprise ICAM solutions in evaluation criteria • Including a review in the acquisition process to verify that offices are not purchasing duplicative ICAM tools and solutions
Chief Data Officer	Making sensitive data available to only authorized individuals for the purpose appropriate to their needs	Requiring data owners to specify data access requirements Recognizing the purpose and limitations of data in a distributed environment Including links to appropriate digital policy rules in data tagging requirements Mapping owners of identity data and centralizing and maintaining that information

Chief Financial Officer	Verifying that financial information is only available to properly authorized individuals and that auditable separation of duties is enforced	Understanding that ICAM is a mission-essential program that needs appropriate resources Maintaining funding for ICAM programs and tools Identifying and quantifying cyber risk to promote enterprise risk management
Chief Information Officer	Enabling efficient onboarding and offboarding of agency personnel and timely adjustments to system access based upon changes in job roles and mission assignments Verifying that agency IT resources are only available to properly authorized individuals for the purpose appropriate to their needs	Collaborating on establishing ICAM policies and procedures to require adoption of enterprise ICAM capabilities Providing direct support and staffing to ICAM Program Office (if housed within the Office of the CIO (OCIO)) Establishing policies regarding who is allowed to access which data and resources
Chief Information Security Officer	Enabling visibility of all user and system accounts across the agency and aggregating information to analyze for patterns of risky behavior Providing the ability to view and audit privileged user sessions as required for critical or sensitive operations	Requiring implementation of identity risk management, personal identity verification (PIV) solutions, security tools, and access management tools Providing direct support and staffing to ICAM Program Office (if housed within the Office of the CISO (OCISO))
Chief Operating Officer(s)	Enabling enterprise-wide management-related competencies that prioritize ICAM services to enable improved program outcomes and performance of the agency	Forging connections between systems adopting enterprise ICAM solutions Supporting enablement and integration of enterprise ICAM solutions, preventing stovepiped solutions
General Counsel	Making sensitive legal findings and data available to only authorized individuals for the purpose appropriate to their need	Reviewing agreements with business partners to verify ICAM requirements are included Providing opinions on legal considerations relevant to agency ICAM policies and procedures

Human Resources	Enabling efficient hiring and termination of agency employees and timely adjustments to their assigned jobs providing accurate employment information to agency CIO, Chief Security Officer (CSO), CISO and others Integrating Learning Management Systems to track training, determine access based on employee's current certification levels, and support reporting requirements	Managing digital identities of federal enterprise entities Providing accurate and valid identity attributes to support authorization Collaborating with ICAM Program Office to create an efficient and effective employee onboarding and offboarding process
Personnel Security	Verifying that all employees and contractors operating within an agency have been properly vetted by the agency and have coordinated with the proper card management services to produce a PIV card Providing timely notification of downstream dependents, CIO, CSO, CISO and others on changes in personnel security status	Integrating enterprise ICAM into personnel security business processes and policies Determining classification levels for agency employee functions, so that ICAM can enforce the principle of least privilege by providing employees with the minimal amount of access needed to perform their job Supporting background investigations and continuous evaluation processes for federal enterprise entities Updating agencies' personnel security policies and guidance to reflect emerging ICAM requirements, whenever new guidance is published
Senior Agency Official for Privacy	Verifying that privacy information is available to only authorized individuals for the purpose appropriate to their need Working in concert with the CISO to verify that privacy information is properly secured and audited	Supporting privacy protections and reviewing Fair Information Practice Principles (FIPPs) to assist ICAM in achieving compliance[9] Developing policies concerning storage and use of PII Supporting privacy impact assessments (PIA) and system of records notices (SORN) for the appropriate use of identity information to support authorization

[9] Federal ICAM Program Management Guide

Senior Official(s) responsible for Physical Security	Verifying that all employees and contractors operating within an agency have access to the physical locations appropriate to their job and possess the proper PIV credentials for that access	Maintaining physical access systems to meet latest PIV card standards Coordinating with logical control ICAM systems to streamline onboarding and offboarding for physical and logical access Assessing facility security levels, categorizing security areas as Exclusion, Limited, or Controlled, and determining authentication factors needed for each area (3 for Exclusion, 2 for Limited, 1 for Controlled)[10]
Agency-wide ICAM Office	Enabling agency enterprise risk management capability to effectively govern and enforce ICAM efforts	Funding ICAM initiatives based on delivering business outcomes Deploying and maintaining common enterprise ICAM processes and capabilities
Component / Sub-Agency ICAM Office	Enabling component / sub-agency risk management capability to effectively govern and enforce component ICAM efforts	Deploying and maintaining common ICAM processes and capabilities that incorporate agency enterprise processes and capabilities and support component / sub-agency specific needs Aligning component / sub-agency ICAM solutions into information systems, preventing stovepiped and duplicative solutions
Emergency Response Official and Team	Informing emergency response teams for the ICAM stakeholders to engage in the event of unauthorized access to facilities and or resources resulting in a catastrophic data breach	Establishing federated approaches between public safety agencies to streamline and secure information exchanges and communications when responding to emergencies
System / Business Owners	Securing and regulating access to information systems managed by an owner	Supporting business processes that leverage identity data in their execution, and systems that manage access control Integrating enterprise and component / sub-agency ICAM solutions into information systems

[10] Physical Access Control System (PACS) Guide

		Providing ICAM capability requirements to component / sub-agency ICAM offices

2.3 Enabling ICAM Governance

For ICAM governance to be effective, it requires a framework, the support of stakeholders across an enterprise, and knowledgeable practitioners. Suggested ICAM governance framework core components and touchpoints are provided in Section 3: ICAM Governance Framework. This section provides examples of activities for governance stakeholders, stakeholders to engage, and examples of the common knowledge, skills, and tasks needed by ICAM practitioners.

2.3.1 Example Activities for ICAM Governance Stakeholders

- ✔ Establish and maintain advisory councils and working groups with liaisons from varying levels within the organization to facilitate two-way communication and feedback conveying capabilities, changes, and potential impacts of ICAM policies, procedures, and strategic planning to their respective business areas
- ✔ Evaluate current and outdated internal policies and make recommendations for changes
- ✔ Communicate the benefits of ICAM to stakeholders and executive leadership at an enterprise level
- ✔ Educate and inform agency staff on the importance of ICAM to the mission delivery
- ✔ Proactively communicate proposed changes to enterprise-wide ICAM solutions and services and their corresponding implementation benefits
- ✔ Establish agency ICAM best practices to facilitate efficiency and effectiveness to enhance security and the overall user experience
- ✔ Request resources to enable implementation of enterprise ICAM capabilities
- ✔ Engage with ICAM stakeholders and practitioners to share lessons learned and conduct knowledge sharing activities

2.3.2 Example ICAM and non-ICAM Stakeholders to Engage and Why

Table 3: Example Stakeholders to Engage and Why

Stakeholder	Why should I engage this stakeholder? Because they are…
IT Investment Board	Responsible for reviewing and approving enterprise IT funding activities

Appropriations Board	Responsible for reviewing and approving either appropriated or other specialized funds for overall mission/business driven activities
Agency Technology Authority	Responsible for reviewing technical solutions that may impact the enterprise (e.g., advising the IT review board on program investment decisions)
Identity Governance Review Board	Responsible for physical, personnel, and HR disciplines, in addition to Federal Information Security Modernization Act (FISMA) and acquisition decision-makers
Program Advisory Bodies	Responsible for providing recommendations on achieving ICAM goals and objectives from a business, academia and governmental perspective
Executive Sponsor	Responsible for providing overall program direction from both a strategic and operational perspective for ICAM. Serves as the chair for the program oversight group
Program Oversight Group	Responsible for providing the project management team and program manager with strategic direction for the program. Consists of ICAM subordinate staff or operating division representatives

2.3.3 Example ICAM Practitioner Competency Model

ICAM governance includes effectively hiring knowledgeable ICAM practitioners. The following example ICAM Competency Model may guide discussions with HR and enable effective hiring practices.

The foundation for developing the recommended competencies for ICAM is grounded in the FICAM Architecture[11] and the NIST Workforce Framework for Cybersecurity (NIST NICE Framework).[12] The FICAM Architecture is the Federal Government's enterprise approach to design, plan, and execute common ICAM processes. It defines three practice areas - identity management, credential management, and access management, as well as the supported areas of governance and federation.

Table 4 uses the NIST National Initiative for Cybersecurity Education (NICE) Framework to convert the FICAM Architecture practice area capabilities into knowledge, skills, and tasks. The NIST NICE Framework uses a simple formula to develop easy-to-read and understand statements for these areas.

- **Knowledge**: A retrievable set of concepts within memory. Multiple statements may

[11] Federal Identity, Credential and Access Management (FICAM) Architecture, 2020
[12] NIST Special Publication 800-181, Workforce Framework for Cybersecurity, November 16, 2020

be required to complete a task

- **Skill**: The capacity to perform an observable action. Multiple skill statements may be needed to complete a task and a single skill statement may be used to complete more than one task

- **Task**: An activity that is directed toward an achievement

An example of an ICAM Competency Model for identity management, credential management, and access management is shown in Table 4.

Table 4: ICAM Competency Model Example

	Identity Management	Credential Management	Access Management
Knowledge	1. Knowledge of identity lifecycle management 2. Knowledge of identity proofing methods, strengths, and weaknesses 3. Knowledge of identity directory technology and services 4. Knowledge of identity aggregation techniques 5. Knowledge of privacy laws and impact to identity data collection and maintenance 6. Knowledge of entitlements management and workflows	1. Knowledge of credential lifecycle management 2. Knowledge of authenticator types, strengths, and weaknesses 3. Knowledge of authenticator binding techniques 4. Knowledge of Federal Public Key Infrastructure (FPKI) policy and compliance requirements	1. Knowledge of authorization models 2. Knowledge of network and cloud authentication techniques 3. Knowledge of access policy lifecycle management 4. Knowledge of privilege access management 5. Knowledge of network routing
Skill	1. Skill in identifying an identity proofing process to an identity assurance level 2. Skill in configuring and maintaining an identity directory service 3. Skill diagnosing directory connection issues 4. Skill in performing identity lifecycle management 5. Skill in preparing and executing access review and recertifications 6. Skill in managing entitlements	1. Skill in identifying an authenticator to an authenticator assurance level 2. Skill in binding authenticators to directory records across various authenticators 3. Skill in performing credential lifecycle management	1. Skill in identifying an appropriate authorization model based on the use case 2. Skill in implementing authentication techniques across various environments 3. Skill in managing access requirements using a policy decision and enforcement point 4. Skill in implementing and managing privileged access management tools 5. Skill in troubleshooting access-related issues

Task	1. Perform identity proofing activities 2. Develop an identity directory maintenance plan 3. Review identity information for currency and accuracy 4. Install, update, and maintain identity directory services 5. Conduct role and group modeling 6. Create and automate workflows for provisioning, entitlements management, identity records management, and end-user activity notifications (e.g., expiring credentials)	1. Enroll users into a credentialing process 2. Bind an authenticator to an identity 3. Perform Credential lifecycle management actions such as activate, renew, reset, suspend, revoke, or terminate 4. Issue PKI and other types of credentials	1. Configure and manage single sign-on (SSO) services 2. Configure directory and agent integration with SSO 3. Identify methods and integrate applications with SSO 4. Operate and Manage policy decisions and enforcement points 5. Configure application access

Additional common ICAM Practitioner Competencies

- System Administration and Engineering
    - Build and integrate ICAM components
    - Operate ICAM systems
    - Manage network configuration
    - Manage public key infrastructure
- Business / Governance
    - Manage programs
    - Manage enterprise architecture
    - Define and monitor policies and standards
    - Facilitate compliance
    - ICAM service reporting such as operational (volume or capacity-based) and performance metrics (efficiency-based)
- Application Development
    - Integrate applications
    - Develop assertion protocols

While the NICE Framework does not include specific ICAM roles, the above ICAM competencies can be added to the below NICE roles.

- Operate and Maintain
    - System Administrator
    - Security Analyst
- Securely Provision

    - Software Developer
    - Enterprise architect
- Oversee and Govern
    - Cyber Executive
    - Privacy and Legal Compliance
    - Cyber Strategy Planner

3. ICAM Governance Framework

ICAM activities and the governance structure supporting them directly or indirectly affect multiple aspects of an agency's day-to-day functions. This document identifies four core ICAM components that an ICAM office needs to perform to maximize its effectiveness, along with ten ICAM touchpoints comprising the various offices and functions that ICAM affects and enables. The four core ICAM components are:

- Strategic Alignment
- ICAM Performance Management
- Federal Policy, Standard and Regulatory Compliance
- Enterprise Risk Management

The ICAM touchpoints are:

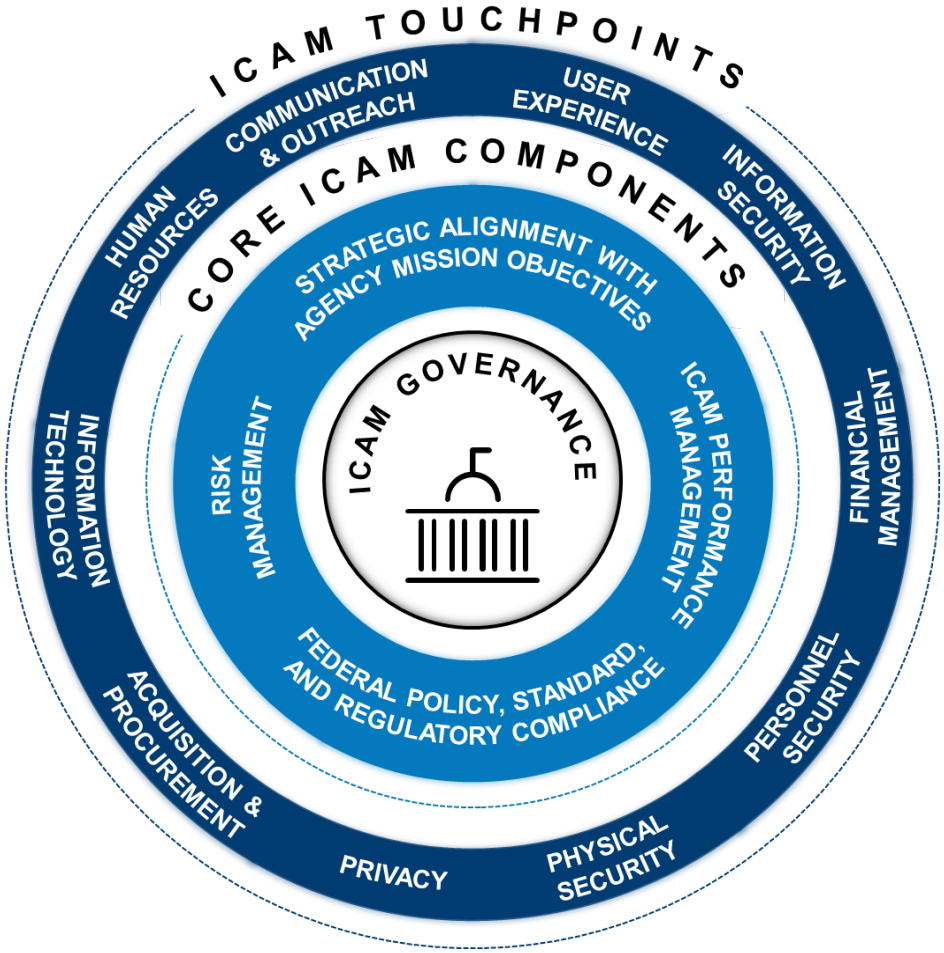
- User Experience
- Information Security
- Financial Management
- Personnel Security
- Physical Security
- Privacy
- Acquisition and Procurement
- Information Technology
- Human Resources
- Communication and Outreach

The following section provides several artifacts illustrating and describing ICAM components and touchpoints.

- Figure 3: Illustrates the ICAM components and touchpoints
- Figure 4: Illustrates the benefits of implementing each ICAM component
- Table 5: Describes the ICAM components, lists the benefits of each, and the challenges they address
- Table 6: Describes the ICAM touchpoints, lists the benefits of each, and the challenges they address
- Figure 5: Provides tools that can be leveraged to perform or support each component or touchpoint

See Appendix E: Agency Examples and Templates to download editable copies of Figures 3 and 4. Use and tailor these templates to align to your agency's mission and business objectives.

Figure 3: ICAM Governance Core Components and Touchpoints



3.1 Core ICAM Components

The IGFWG identified four core ICAM components that an ICAM governance structure needs to facilitate, perform or enforce to be successful. The benefits of implementing the core components are illustrated in Figure 4 below.

Figure 4: ICAM Governance Core Components and Benefits

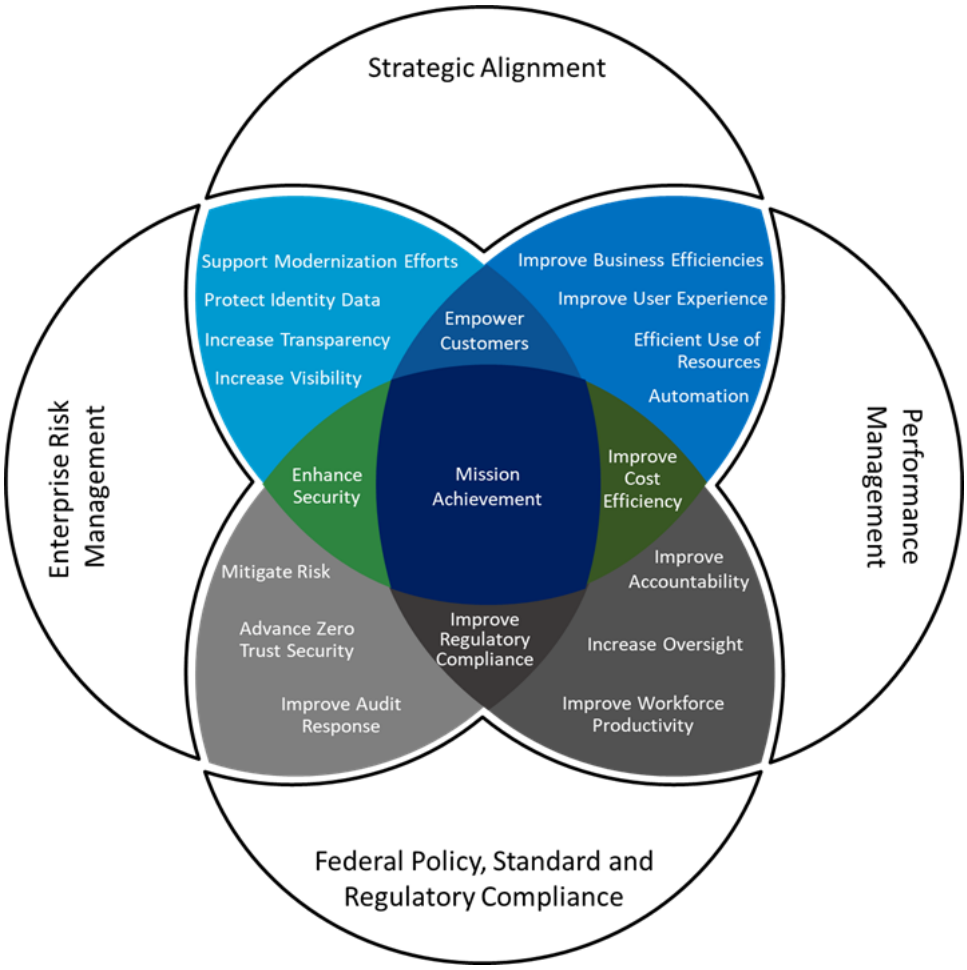


Table 5 describes the components and lists the benefits and challenges they address.

Table 5: ICAM Governance Core Component Descriptions

Description	Benefits	Challenges Addressed
Strategic Alignment		
Incorporates ICAM into agency strategic missions, and cybersecurity goals and objectives	Enhances security and reduces risk Enhances mission delivery	Lack of executive buy-in and leadership support

Integrates and unifies agency leadership to deliver ICAM solutions Harmonizes enterprise-wide approach to ICAM governance	Supports business objectives Provides transparency and visibility across Enterprise Improves user experience Provides reciprocity and faster onboarding Supports modernization efforts Enables trusted workforce and personnel security Enables physical and logical security Helps convey value added to all lines of business	ICAM is not viewed as a business enabler Lack of awareness of the interrelation between IT and cybersecurity goals Lack of overarching and consistent governance policies and processes across the agency Difficulty conveying the value of ICAM to all lines of business
ICAM Performance Management		
Tracks, manages, monitors, and reports on overall ICAM activity performance and metrics to measure resource contributions to specific missions, goals, and objectives Develops metrics that establish the link between agency mission, business objectives, and ICAM capabilities	Improves alignment of ICAM concepts and response to agency mission and objectives Improves user experience Improves personnel productivity Improves audit response Improves accountability for ICAM investment portfolio and outcomes	Lack of executive buy-in and leadership support ICAM is not viewed as a business enabler
Federal Policy, Standard and Regulatory Compliance		

Enforces agency-wide adoption of ICAM services through internal policies and practices with strong executive buy-in and support, alignment with the agency's business needs and mission, and compliance with applicable laws, regulations, and policies	Improves alignment to agency mission and objectives Supports agency compliance with federal laws, regulations, and policies Increases adoption of ICAM	Lack of executive buy-in and leadership support ICAM is not viewed as a business enabler Lack of overarching and consistent governance policies and processes across the agency New policies and standards may drive an 'adapt and tailor' approach to organizational business processes
Enterprise Risk Management		
Identifies, quantifies, and mitigates identity-based risks through successful operations, providing enterprise risk visibility	Enhances mission delivery Improves security, including both physical and personnel Reduces risk Enables dashboards, scorecards, and metrics	Lack of executive buy-in and leadership support ICAM is not viewed as a business enabler Lack of awareness of the interrelation between IT and cybersecurity goals

3.2 ICAM Touchpoints

ICAM touchpoints are various functions within an agency that ICAM affects or enables. Table 6 describes the ICAM touchpoints, lists the benefits of each, and the challenges they address.

Table 6: ICAM Touchpoint Descriptions

Description	Benefits	Challenges Addressed
User Experience		
User experience encompasses both public and federal enterprise identity experiences	**Federal Enterprise Identity:** Facilitates ease of conducting business Improves onboarding experience	Lack of executive buy-in and leadership support Resource constraints Failure rates negatively impact user experience

Facilitates secure and streamlined user experiences and provides users with the appropriate access while completing transactions (i.e., onboarding, authenticating) The impact of ICAM on a wide range of users underlines that ICAM is not an IT-isolated component	Lowers help desk costs through decreased failure rates, which often lead to help desk tickets Raises awareness that ICAM is not an IT-isolated component Improves customer service scores **Public Identity:** Increases consumer confidence in agency services Provides quick and frictionless access to applications Lowers help desk costs through decreased failure rates	
Acquisition and Procurement		
Removes silos between Acquisition and Procurement teams, reducing duplicative ICAM solutions and services across the enterprise Streamlines and incorporates ICAM priorities into acquisition and procurement processes Incorporates ICAM into procurement language and evaluation criteria, requiring new capabilities to support agency ICAM standards and capabilities Implements policies and procedures to maintain accurate identity data for contractors	Improves personnel productivity by providing unified and modern ICAM capabilities Improves personnel experience by removing confusion over which ICAM capability to leverage Improves public identity experience by removing confusion over which ICAM capability to leverage Improves the quality of contract data in ICAM systems	Lack of executive buy-in and leadership support ICAM is not viewed as a business enabler Resource and budget constraints
Human Resources		

Create employee identity data s during onboarding, which is integrated into ICAM throughout an employee's lifecycle Aligns ICAM with HR goals and current objectives	Improves employee onboarding experience Improves workforce productivity Improves offboarding processes Reduces overall expenditures by removing stovepipes between HR and ICAM	HR not understanding the role they play in ICAM Lack of executive buy-in and leadership support ICAM is not viewed as a business enabler Processes for onboarding and authenticating federal personnel not integrated between ICAM and HR functions
Information Security		
Enforces the principle of least privilege, verifying that users can only access the resources they need to perform their job functions, reducing the likelihood of unauthorized access, tampering, or extraction of data Maintains awareness of the ever-changing security risks and new mitigation methodologies	Improves security and reduces risk Enhances mission delivery	Lack of executive buy-in and leadership support Lack of awareness on the interrelation between IT and cybersecurity goals
Financial Management		
Prevents unauthorized access to financial data, often one of an organization's most highly prized assets Boosts the financial performance of an organization through the cost savings it brings via reduced help desk expenditures, data extraction and increased productivity due to lower user failure rates and onboarding periods	Enhances mission delivery Provides reciprocity and faster onboarding Improves employee productivity Reduces help desk expenditures	Lack of executive buy-in and leadership support Lack of communication regarding the value of ICAM to all lines of business ICAM is not viewed as a business enabler
Personnel Security		

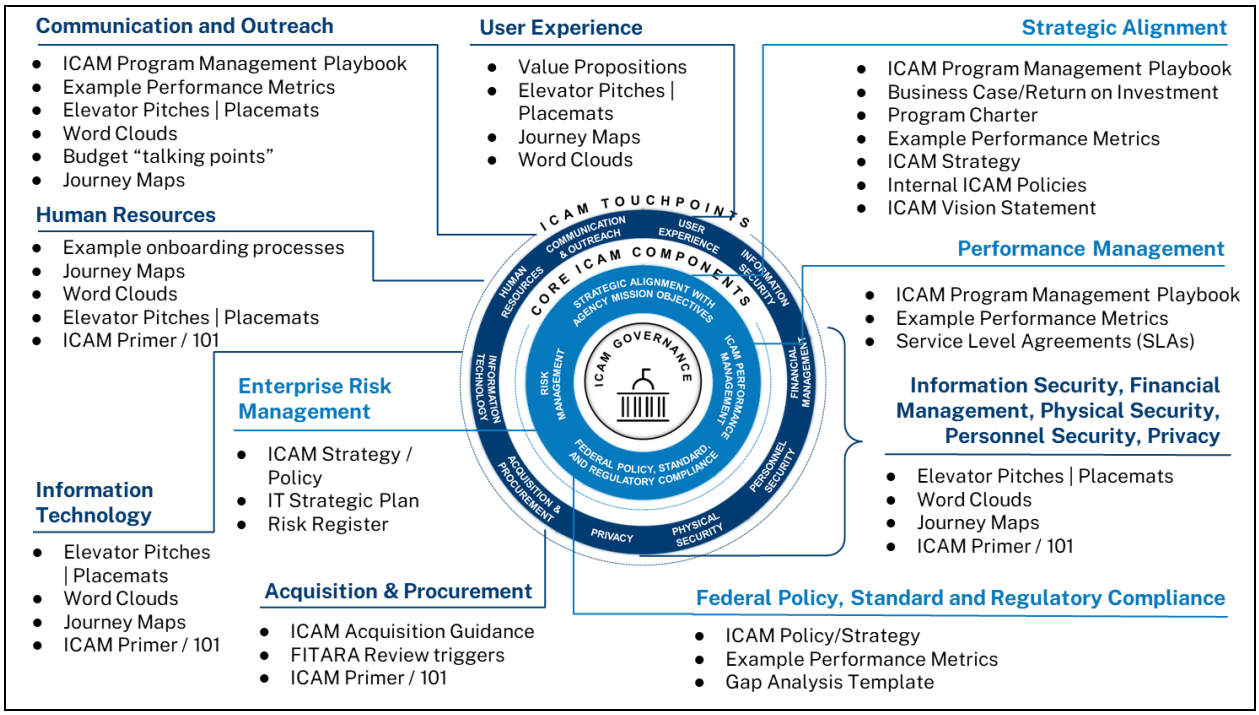
Enforces the principle of least privilege through logical access management, mitigating insider threat risks by verifying that employees only have access to the data they need to perform their job function Pairs background investigation information with identity data assists agencies in maintaining visibility of their higher-risk employees even when they switch departments/job functions Verifies that all employees and contractors operating within an agency have been properly vetted by the agency and have coordinated with the proper card management services to produce a PIV card or other authorized credential	Improves security and reduce risk Enhances mission delivery Provides transparency and visibility across the enterprise	Lack of executive buy-in and leadership support Lack of recognition of interconnection/interdependence of ICAM on other systems
Physical Security		
Prevents unauthorized individuals from accessing facilities through physical access management, reducing the likelihood of physical theft of agency assets or inappropriate access to on-premise resources	Improves security and reduce risk Enhances mission delivery Raises awareness that ICAM is not an IT-isolated component Provides a safer workplace	Lack of executive buy-in and leadership support Lack of recognition of interconnection/interdependence of ICAM on other systems
Privacy		
Enhances the privacy of public and federal enterprise identities by protecting PII from unauthorized access or tampering	Improves security and reduce risk Improves user experience Increases consumer confidence in agency services	Lack of executive buy-in and leadership support Lack of recognition of interconnection/interdependence of ICAM on other systems

		Lack of communication regarding the value of ICAM to all lines of business
Information Technology		
Verifies that the right individual accesses the right resource at the right time, for the right reason Reduces the burden on an IT help desk by reducing the number of calls for automatable ICAM-related processes, like password resets	Improves security and reduce risk Improves user experience Lowers help desk costs by preventing unauthorized access, which often needs IT remediation Improves customer service scores Improves personnel productivity Facilitates ease of conducting business Provides quick access to applications	Lack of executive buy-in and leadership support Failure rates negatively impact user experience
Communication and Outreach		
Increases agency awareness through consistent messaging concerning the benefits, importance, and wide-ranging applications of ICAM Helps prevent ICAM from falling into a stovepipe through persistent engagement with internal and external stakeholders	Reduces overall expenditures by removing stovepipes between the various agency offices and functions Raises awareness that ICAM is not an IT-isolated component Provides visibility and transparency across the enterprise	Lack of executive buy-in and leadership support Lack of communication regarding the value of ICAM to all lines of business Lack of recognition of interconnection/interdependence of ICAM on other systems ICAM is not viewed as a business enabler

3.3 Implementation Tools to Leverage

Figure 5 maps example implementation tools that can be leveraged to facilitate and enhance each ICAM component and touchpoint. Descriptions of the identified tools, why they are important, and agency examples and templates can be found in Appendix E: Agency Examples and Templates.

Figure 5: Example Implementation Tools



Appendix A: ICAM Primer

Identity, Credential, and Access Management is a fundamental cornerstone of an agency's digital service delivery. How agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services, as well as individuals' privacy.

What is ICAM?

ICAM is the set of tools, policies, and systems that allows an organization to enable **the right individual access** to the **right resource** at **the right time** for the **right reason** in support of federal business objectives.

Further detail on ICAM Practices Areas (Identity Management, Credential Management, and Access Management) and ICAM Supporting Elements (Federation and Governance) can be found in the FICAM Architecture.

Why is ICAM Important?

Organizations realize benefits from implementing well-structured ICAM governance. These benefits include:

1. Facilitates seamless access to agency systems (when an identity is established correctly), enhancing the end-user experience for federal enterprise and public identities
2. Increases productivity through streamlining certain tasks, allowing agencies to focus on mission-critical deliverables
3. Reduces security risks by speeding the revocation of access privileges, reducing the likelihood of unauthorized access to information systems

What Key ICAM Terms and Definitions should I know?

ICAM-related tools, systems, and policies can become very complicated and technical. The *Office of National Intelligence Information Sharing Environment (ISE) Introduction to ICAM Principles* describes key terms and definitions using plain language and everyday examples.

Appendix B: Common ICAM Challenges

The IGFWG identified the following ICAM governance challenges experienced at their agencies.

- Lack of executive leadership support and understanding of how ICAM aligns to Information Technology (IT) and cybersecurity goals
- The misconception that ICAM is only an IT concern and not a business concern as well
- Lack of clear definitions of ICAM roles and responsibilities. ICAM is an essential business function that impacts and enables every office across an agency, but roles and duties for ICAM professionals are ill-defined
- Confusion over who owns ICAM and where ICAM fits in an agency's organizational structure
- Lack of integration between ICAM governance and other agency governance boards
- Lack of coordination between Human Resources (HR) and ICAM concerning onboarding and offboarding processes
- Lack of overarching and consistent governance policies and processes across agencies
- Lack of funding hinders ICAM's ability to drive mission success.

Appendix C: ICAM and Zero Trust

Zero Trust is a security model for a network architecture that trusts no device and user by default, authenticating every transaction. NIST released Zero Trust Architecture guidance[13] in 2020, promoting the adoption of Zero Trust for more robust network security. On May 12, 2021, President Biden issued EO 14028, calling for the Federal Government to adopt security best practices and advance toward implementing Zero Trust Architecture.[14] ICAM is essential to this adoption, as robust identity processes form the foundation of any Zero Trust Architecture.

NIST defines Zero Trust as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised." One of the Zero Trust guiding principles is to "*treat every user, device, application/workload, and data flow as untrusted*. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies."

Key ICAM components for implementing a Zero Trust Architecture include:

- **Person and non-person entities (NPE):** Authenticate all users before providing access. Managing identities and providing secure MFA credentials is the first step in knowing who is requesting access.
- **Endpoints:** In addition to authenticating users, Zero Trust requires authenticating and approving endpoints, such as workstations, mobile devices, or internet of things (IoT) devices
- **Data, Assets, Applications, and Services (DAAS):** Definition and implementation of access policies is needed to implement the continuous evaluation aspect of Zero Trust

Importance of establishing a strong ICAM foundation before implementing Zero Trust:

- Zero Trust cannot be achieved without strong identity management and mature ICAM capabilities for NPEs
- A strong foundation of ICAM governance provides a comprehensive set of access control policies and guidelines, setting the foundation for agencies to implement Zero Trust principles

[13] NIST Special Publication 800-207, Zero Trust Architecture, August 11, 2020.
[14] Executive Order 14028, Executive Order for Improving the Nation's Cybersecurity, May 12, 2021

Appendix D: Common ICAM MythBusters

Myth	Buster
ICAM is an IT concern, not a business concern.	ICAM impacts all parts of an organization.
Acquiring and implementing the latest technology is the most crucial aspect of ICAM.	People (training, awareness, buy-in, etc.), processes (governance, roles, and responsibilities, etc.), and technology must all work in close harmony to achieve an agency's mission, meet business objectives, and prevent, manage, and mitigate enterprise risk.
Access Management is only about authentication.	Access management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services. When a user logs in to a service, they present their credentials, and the service confirms their credentials are valid (authentication) and grants or denies the user access based on the user's assigned permissions (authorization).[15]
Authentication and Authorization are the same things.	Both authentication and authorization confirm the identity of users and are often used interchangeably. In reality, they perform different functions. Authentication checks to see if a user is who they say they are. authorization grants a user access to certain things after they have been authenticated. One is not a substitute for the other.
Incorporating ICAM into the organization is the responsibility of the application owners.	ICAM is an enterprise-level responsibility.
PIV is ICAM.	Implementing HSPD-12 requirements is only the beginning of implementing ICAM. Digital identities, authorization, and authentication are all crucial parts of ICAM.
You can achieve Zero Trust without ICAM.	You can implement ICAM without Zero Trust, but you can't implement Zero Trust without ICAM. Having a strong ICAM foundation is the first step towards achieving Zero Trust.
Physical Access is a stand-alone or separate entity.	Physical access ties in closely with logical access for an effective ICAM program.

[15] Federal Identity, Credential and Access Management (FICAM) Architecture, 2020

Appendix E: Agency Examples and Templates

This section provides agency examples and templates that can be leveraged to perform or support ICAM governance core components and touchpoints. Agencies can use and tailor these tools per their specific requirements.

1. Business Case/Return on Investment

- **What:** Document that explains the need for funding, execution, and leadership buy-in to accomplish an ICAM office's vision. Should include a return on investment (ROI), which is a quantified estimate of the money and time an agency saves by implementing ICAM, based on a comparison of metrics before and after ICAM implementation
- **Why**: Decision-makers unfamiliar with ICAM are likely to be more supportive of an ICAM office if they understand the business benefits that ICAM brings to an agency
- **Example**: Veterans Affairs (VA) ICAM Business Case and Return on Investment:[16] https://community.max.gov/download/attachments/234815732/DRAFT%20VA%20ICAM%20Business%20Case.pdf?api=v2

2. ICAM Governance Charter

- **What**: A formal document that establishes ICAM program authority and assigns responsibilities in accordance with OMB M-19-17
- **Why**: A charter helps stakeholders understand their responsibilities for performing ICAM and what ICAM looks like at their agency
- **Example**: U.S. Department of Education ICAM Program Charter: https://www2.ed.gov/digitalstrategy/policyarchive/ed-icam-program-charter-1-4-2021-02-09-updated.pdf

3. Internal ICAM Policy

- **What**: An agency-specific policy requiring ICAM functions to be performed in a certain way to achieve compliance
- **Why**: Internal policies are mandated by federal government-wide guidance to implement the requirements of policies, like OMB M-19-17. Without well-structured internal policies, an agency's response could be unorganized and ineffective
- **Example:** United States Agency for International Development (USAID) ICAM Policy: https://www.usaid.gov/ads/policy/500/542

4. Performance Metrics:

- **What**: Measures to monitor agency and Federal regulatory compliance and progress

[16] MAX.gov login required

towards achieving agency mission and objectives, like Service Level Agreements (SLA)

- **Why**: Performance metrics allow an agency to determine if the agency's mission and objectives are being met. Aligning ICAM Performance Metrics to agency mission and strategic goals can help improve stakeholder support

5. Gap Analysis:

- **What**: Identifies gaps in an agency's ability to meet compliance requirements or policy mandates, and specific recommendations to address those gaps
- **Why**: A gap analysis helps agencies identify what actions are needed to come into compliance with a mandate, and prioritize steps to accomplish those actions
- **Example**: Gap Analysis Template

6. Risk Register

- **What**: A log of identified business risks, their potential impacts if left unaddressed, plans for mitigating each risk, and the status of those mitigation plans
- **Why**: Logging and tracking each risk helps prevent possible problems from 'falling through the cracks and going unaddressed until they begin to harm business functions
- **Example**: Risk Register Template

7. Strategy:

- **What**: Provides high-level goals and objectives for an ICAM program and identifies a centralized approach for achieving them
- **Why**: A Strategy guides the formulation of internal policies, architecture, technology, and more to guide all parts of an organization to work together towards common objectives
- **Examples**:
    - Department of Defense (DoD) ICAM Strategy: https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf (located under the *Identity, Credential, and Access Management* section)
    - Air Force ICAM Strategy: Air Force (AF) Identity, Credential, and Access Management (ICAM) Technical Roadmap

8. Budget Talking Points:

- **What**: Budget talking points when communicating about ICAM, often incorporated into a Business Case, that highlight how ICAM supports mission applications and can reduce costs
- **Why**: Adding examples and specific information around budget when communicating about ICAM can help to increase support for ICAM.

- **Examples**:
    - "By implementing password self-service, our agency has the potential to save xx over three years in help desk costs."
    - "By integrating and automating access requests with our IT service management (ITSM) and identity governance tool, our agency has saved xx over three years in help desk costs."
    - "Working Capital Funds boost ICAM performance"
    - "Annual financial Return on Investment will exceed $XX million"
    - "Implementing simple multi-factor authentication methods can help organizations prevent costly, time-consuming attacks"[17]
    - "According to IBM Security, the average cost of a data breach in 2020 was $3.92 million"[18]

9. Elevator Speech/Placemat

- **What**: A concise communication explaining the need for ICAM and its benefits, tailored for an audience with little background knowledge of ICAM
- **Why**: A prepared elevator speech equips personnel to try and convince executive leadership to support ICAM
- **Examples**:
    - DoD CIO ICAM Placemat: https://dodcio.defense.gov/Library/ (see the *Identity, Credential, and Access Management* section)
    - ICAM Placemat Template - Slide 1
    - Venn Diagram Template - Slide 2 : Depicts relationship between core ICAM components and benefits, emphasizing overlap between components needed to achieve benefits.
    - Core ICAM Components and Touchpoints Diagram Template - Slide 3 & 4 : Displays core ICAM components, surrounded by the various touchpoints that ICAM affects or enables. The template contains customizable text for agencies to tailor and use.
    - ICAM implementation tools (Slide 8) - Leveraged to facilitate and enhance each ICAM component and touchpoint.

10. ICAM 101/Primer

- **What**: A beginner-level introduction to ICAM including common terminology, definitions for ICAM, and real-world examples
- **Why**: Helps executive leadership and the various agency program offices understand ICAM and its importance in an easily understandable manner

[17] Department of Homeland Security ICAM Executive Primer, February 2019
[18] Cost of a Data Breach Report, July 2020

- **Example**:
  - Appendix A: ICAM Primer
  - Director of National Intelligence (DNI) Introduction to ICAM Principles: https://www.dni.gov/files/ISE/documents/DocumentLibrary/INTRO-TO-ICAM.pdf

11. Journey Map

- **What**: A visual that depicts an agency's current state of ICAM implementation, its desired future state, and activities along the way that will help achieve that future state
- **Why**: Provides an easily understandable snapshot of an ICAM vision
- **Example**: Journey Map (Slide 5 & 6)

12. Word Cloud

- **What**: A visual that demonstrates the benefits of ICAM governance for the various business functions and program offices of an enterprise
- **Why**: Agency-tailored word clouds will help start discussions on the importance of ICAM
- **Example**:
  - Word Cloud 1 Template (Slide 7): Provides examples of high-level benefits of ICAM governance
  - Word Cloud 2 Template (Slide 8): Provides specific examples of how ICAM governance benefits agencies

13. ICAM Reference Design

- **What:** A high-level, capability-focused description that outlines goals, processes, and procedures, and taxonomy for an ICAM program
- **Why:** Aligns technical capabilities with agency mission(s), bridging the gap between practical and strategic approaches
- **Example**: DoD Enterprise ICAM Reference Design: https://dodcio.defense.gov/Library/ (see the *Identity, Credential, and Access Management* section)

Appendix F: Policies, Standards, and Guidance [19]

[M-19-17]	OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019
[EO 14028]	Executive Order 14028, Executive Order on Improving the Nation's Cybersecurity, May 12, 2021
[NIST SP 800-63-3]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3; Digital Identity Guidelines, June 22, 2017
[A-130]	OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016
[NIST SP 800-53-5]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
[NIST SP 800-207]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture, August 11, 2020
[FISMA]	Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq., Public Law (P.L.) 113-283, December 8, 2014
[Federal Personnel Vetting Core Doctrine]	86 Federal Register (FR) 2705 pages 2705-2709, January 13, 2021
[FITARA]	Federal Information Technology Acquisition Reform Act, December 19, 2014
[FIPS 201-2]	Federal Information Processing Standard Publication 201-2, Personal Identity Verification of Federal Employees and Contractors, September 5, 2013
[CDM]	Continuous Diagnostics and Mitigation Program, 2012
[HSPD-12]	Homeland Security Presidential Directive-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
[NIST SP 800-116-1]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116 Revision 1, Guidelines for Use of PIV Credentials in Facility Access, June 29, 2018
[NIST SP 800-181-1]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181 Revision 1, Workforce Framework for Cybersecurity (NIST NICE Framework), November 16, 2020

[19] Any successive versions or updates to the policies, standards and guidance referenced above are considered in-scope for this Framework.

Appendix G: Acronyms

CAO	Chief Acquisition Officer
CDO	Chief Data Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
CTO	Chief Technology Officer
CxO	Chief Experience Officer
DAAS	Data, Assets, Applications and Services
DNI	Director of National Intelligence
DoD	Department of Defense
EO	Executive Order
FICAM	Federal Identity, Credential and Access Management
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FPKI	Federal Public Key Infrastructure
FR	Federal Register
HR	Human Resources
ICAM	Identity, Credential and Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
ISE	Information Sharing Environment
IT	Information Technology
MFA	Multi-Factor Authentication
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NIST NICE	NIST National Initiative for Cybersecurity Education
NPE	Non-Person Entity
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OMB	Office of Management and Budget
PACS	Physical Access Control System

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Public Law
RFP	Request for Proposals
ROI	Return on Investment
SAOP	Senior Agency Official for Privacy
SLA	Service Level Agreement
SORN	System of Records Notices
SP	Special Publication
SSO	Single Sign-On
USAID	United States Agency for International Development
VA	Department of Veterans Affairs
ZT	Zero Trust
ZTA	Zero Trust Architecture