Framework for Integrated Identity, Credential, and Access Management Governance

Version 2.1

March 2026

Identity, Credential, and Access Management Subcommittee (ICAMSC)

Table of Contents

1. Introduction

Advances in technology have enabled increased digital interactions and business transactions in the federal government, allowing for faster, more reliable connections and operations in digital service delivery. However, these advances also introduce identity management challenges and risks.

At the foundation of secure digital government service delivery are digital identities that rely on personally identifiable information such as names, attributes, or preferences. To protect these digital identities associated with identity management challenges and risks, agencies need an Identity, Credential, and Access Management (ICAM) strategy and practices that provide for reliable, secure, and private means for creating, storing, transferring, and using these digital identities. Strategy execution and practices can be achieved with an authoritative ICAM governance structure, grounded in policy and focused on mission success.

OMB Circular A-130 provides the overarching policy framework for managing Federal information technology as a strategic resource, requiring enterprise-wide governance for security, privacy, risk management, and technology integration to support mission needs. OMB Memorandum M-19-17 tailors A-130's principles for ICAM by directing agencies to integrate ICAM into existing governance structures. This embeds ICAM as a seamless component of broader enterprise frameworks, allowing agencies to automatically inherit A-130's security, privacy, and technology safeguards—positioning trusted identity practices as a foundational enabler for core missions while fostering innovation, transparency, and efficiency.

To support the development of robust agency ICAM governance, the Identity Management Cyber Security Division developed this ICAM Governance Framework as guidance to help agencies build and improve ICAM governance structures, processes, and policies. The term “Framework” (hereinafter referred to as the Framework) will refer to this document from this point forward.

1.1. Purpose

This Framework is intended to guide federal agencies in designing, implementing, and operating efficient, compliant, and mission-aligned ICAM governance within their enterprises and across the federal government. It defines ICAM governance as the overarching practices and structures that direct ICAM work. When properly set up with broad stakeholder involvement, it makes ICAM a powerful foundation for cybersecurity and directly tackles many enterprise-wide priorities agencies face (e.g., secure mission enablement, efficiency, risk reduction, and modern digital government).

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 user experience for the federal enterprise and its client base in industry and among the public
- Support interoperability and federation of ICAM solutions
- Reduce duplication of effort, cost, and complexity resulting from disparate ICAM solutions and standards used across agencies and mission areas
- Reduce risk and fraud
- Provide a consistent identity context across agencies

1.2. Scope

This document is limited to ICAM governance and is not intended to provide ICAM implementation guidance beyond the establishment of the ICAM governance function. It complements Office of Management and Budget (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."[1]

Governance differs from management and operations: it is the overarching system of practices, structures, and decision-making processes that ensures ICAM activities are aligned with agency mission outcomes, strategic priorities, and enterprise risk management goals.

This document does not constitute official federal policy or impose any mandated requirements. It provides practical guidance to assist agencies in developing or enhancing their own ICAM governance approaches.

1.3. Authority

At a minimum, governance in a federal department or agency must meet the requirements of applicable legislation, regulations, and directives while also incorporating good governance practices.[2] Although OMB M-19-17 is the focus of much of the government's attention concerning ICAM governance, guidance for ICAM governance implementation does not rest solely on OMB M-19-17. Instead, that guidance relies on various laws, regulations, directives, standards, and best practices that directly apply to ICAM functions and activities such as managing and controlling digital identities, accessing government services, IT planning, and managing risks. The items listed below are some of the drivers and best practices that support ICAM governance implementation:

[1] OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019

[2] NIST SP 800-100, Information Security Handbook: A Guide for Managers, March 7, 2007

- **Governance**—The following laws, directives, and specifications led to the establishment of the Chief Information Officers (CIO) Council and provide the basis for its ongoing oversight activities, as well as agency-specific ICAM governance activities.
    - **E-Government Act of 2002 (E-Government Act)**—Established the Federal CIO Council and the OMB Office of E-Government and Information Technology to promote interagency collaboration in providing e-government services.
    - **Federal Information Security Management Act of 2014 (FISMA 2014) Modernization** —Establishes the overarching framework for agency-wide security programs—FISMA 2014 (Public Law 113-283) requires each federal agency to develop, document, implement, and maintain an agency-wide information security program. This includes integrating security into agency operations, conducting risk assessments, implementing security controls, and ensuring continuous monitoring. Identity and access management (IAM) is explicitly called out as a critical area because unauthorized access is one of the primary risks to federal systems.
    - **National Institute of Standards and Technology [NIST] Special Publication [SP] 800-63-4, SP 800-53 Rev. 5, SP 800-39, SP 800-100, and NIST SP 800-207** which place ICAM's role in managing identities at the core of the federal government's Zero Trust strategy, further linking ICAM to security management. Current federal security guidance requires agencies to integrate security and risk management with agency strategic, operational, and budgetary planning processes.
    - **21st Century Integrated Digital Experience Act (21st Century IDEA)**—Requires secure connections (e.g., HTTPS) for public-facing digital services and accelerates digitization of forms/services with electronic signatures, indirectly supporting trusted identity verification and authentication (e.g., via shared tools like Login.gov for seamless, secure public access) to enable efficient, user-centered digital transactions aligned with ICAM goals for mission delivery and risk reduction.
    - **Federal Information Technology Acquisition Reform Act (FITARA)**—Evaluates agencies' performance in various IT categories, including ICAM acquisitions, and prohibits them from contracting for IT and requesting the reprogramming of IT funds without CIO review and approval.

- Cybersecurity Strategy (OMB M-22-09)—Establishes the federal Zero Trust Architecture (ZTA) strategy which requires federal agencies to implement strict phishing-resistant multi-factor authentication (MFA), centralize identity management, and incorporate device-level security signals in access decisions. [delete] secure, monitor, and segment networks to defend against advanced cybersecurity threats. .

- **Fiscal Responsibility and Internal Control**—The following laws drive federal programs' performance and financial responsibilities, which digital identity and ICAM governance are part of:
  - **Government Performance and Results Act of 1993 (GPRA)** – Requires agencies to prepare strategic plans and objectives and to annually report on performance. OMB M-19-17 specifically includes ICAM governance in this requirement.
  - **Clinger-Cohen Act of 1996 (Clinger-Cohen Act)** – Establishes the role of the agency CIO in federal IT and requires ICAM to be included in agencies' Capital Planning and Investment Control (CPIC) processes. OMB A-130[3] interprets implementation of the Clinger-Cohen Act for agencies.
  - **Federal Managers Financial Integrity Act of 1982 (FMFIA)** – Makes senior management responsible for establishing and maintaining internal controls to achieve the objectives of effective and efficient operations. OMB A-123 encourages agencies to integrate their internal control evaluation efforts, including those that apply to information technology and security, of which ICAM is a key component.

- **Best Practices**
  - **Control Objectives for Information Technologies 2019 Framework (COBIT® 2019)**—This tool from the Information Systems Audit and Control Association (ISACA) is a comprehensive framework developed to support understanding, designing, and implementing enterprise IT management and governance.[4]
  - **International Organization for Standardization (ISO)/International Electrotechnical Commission (ISO/IEC 38500:2024): Information Technology—Governance of IT for the Organization**—Provides guiding principles for members of governing bodies on the effective, efficient, and acceptable use of IT within their organizations.[5]

[3] https://www.cio.gov/policies-and-priorities/circular-a-130
[4] ISACA, Control Objectives for Information Technologies 2019 Framework, 2019
[5] ISO, ISO/IEC 38500:2024 — Information technology — Governance of IT for the Organization, February 2015

- **ISO/IEC TS 38501:2015—Information Technology—Governance of IT—Implementation Guide**—Provides guidance on how to implement arrangements for effective IT governance within an organization.[6]

1.4. 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.

1.4.1. Executive Leadership

Agency executives, such as Chief Information Officers (CIOs), Chief Financial Officers (CFOs), Senior Policy Officials, Chiefs of Staff, Chief Information Security Officers (CISOs), Senior Agency Official for Privacy (SAOPs), and others—may use this Framework to:

- Communicate ICAM capabilities, impacts, policies, and procedures more effectively.
- Make informed decisions, and set priorities to strengthen and strategically align ICAM governance across their organization.

1.4.2. IT and ICAM Practitioners

The Framework offers strategic guidance, governance patterns, and alignment principles that ICAM program managers, IT partners, system and business owners, cybersecurity teams, architects, engineers, compliance and audit staff, procurement personnel, and other federal ICAM contributors can use to:

- Establish and strengthen enterprise-wide ICAM governance structures,
- Integrate ICAM capabilities thoughtfully across agency systems, processes, and existing frameworks,
- Align ICAM governance and activities with agency missions, strategic objectives, and risk management priorities, and
- Support consistent, secure, and efficient identity, credential, and access management outcomes.

[6] ISO, ISO/IEC TS 38501:2015 – Information Technology – Governance of IT – Implementation Guide, April 2015

2. ICAM Governance Overview

2.1. Governance Overview

ICAM governance has specific components, including requirements, structure, focus, and actors roles. When considering governance implementation (in particular, agency decision-making processes), there is no "one size fits all" strategy for federal agencies. Design choices such as organization, placement (e.g., subordinate to security, risk, or IT governance), and centralized vs. decentralized structure options are all at the discretion of the Senior Agency Official. While some roles and responsibilities are defined by law, others are at the discretion of the agency. Regardless of each agency's decisions about governance design, overall FICAM governance is inherently multi-layered and functionally cross-cutting. As a result of the latter, the agency's ICAM program heavily depends on various other agency functions for its execution.

Table 1 lists the six governance components, a set of critical touchpoints, governance operating activities, and governance sustainment activities that map to the IT governance described in OMB Circular A-130. These items culminate in cross-agency governance coordination as shown in the Cross-Agency Governance Coordination Section, which provides a forum for information sharing and cross-organizational problem solving. These components are listed in the table below.

Table 1: Cross-Agency Governance

Core Governance Components	Critical Touchpoints
1. Strategy 2. Monitor (Performance and Risks) 3. Compliance 4. Resources 5. User Behavior 6. Acquisition	1. IT Governance 2. Security Governance (Information/Physical) 3. Budget and Acquisition 4. Risk Management 5. Performance and Accountability 6. Data Governance
Governance Operating Activities	**Governance Sustainment Activities**
1. Establish/Improve Governance 2. Understand Environment and Determine Agency ICAM Baseline 3. Evaluate Principles, Policies, Strategies, Plans, and Risks 4. Direct Resources 5. Monitor ICAM Performance and Risks	1. Implement 2. Audit 3. Improve
Cross-Agency Governance Coordination	
1. Communication 2. Collaboration 3. Credential Re-use	4. Risk Reduction 5. Coordination with External Organizations 6. Feedback to Government-wide Governance Bodies

Figure 1 below presents the cascading, multi-layered ICAM governance concept. Within the overall governance framework, goals and objectives cascade down, and performance and innovation roll up. Keep in mind that the Agency ICAM Governance layer may consist of sub-organizational governance layers, each contributing to the overall agency governance posture. Consistent with ISO/IEC 38500:2024, each governance layer will do the following:

- **Evaluate** the environment and current use of ICAM; this includes responsibilities, alignment of strategy, and ICAM development.
- **Direct** the preparation of the future state and strategy; this includes initiation of governance activities, roles/responsibilities, and acquisitions.
- **Monitor** the progress and success; this includes addressing risk and ensuring continuous improvement once the future state has been achieved.

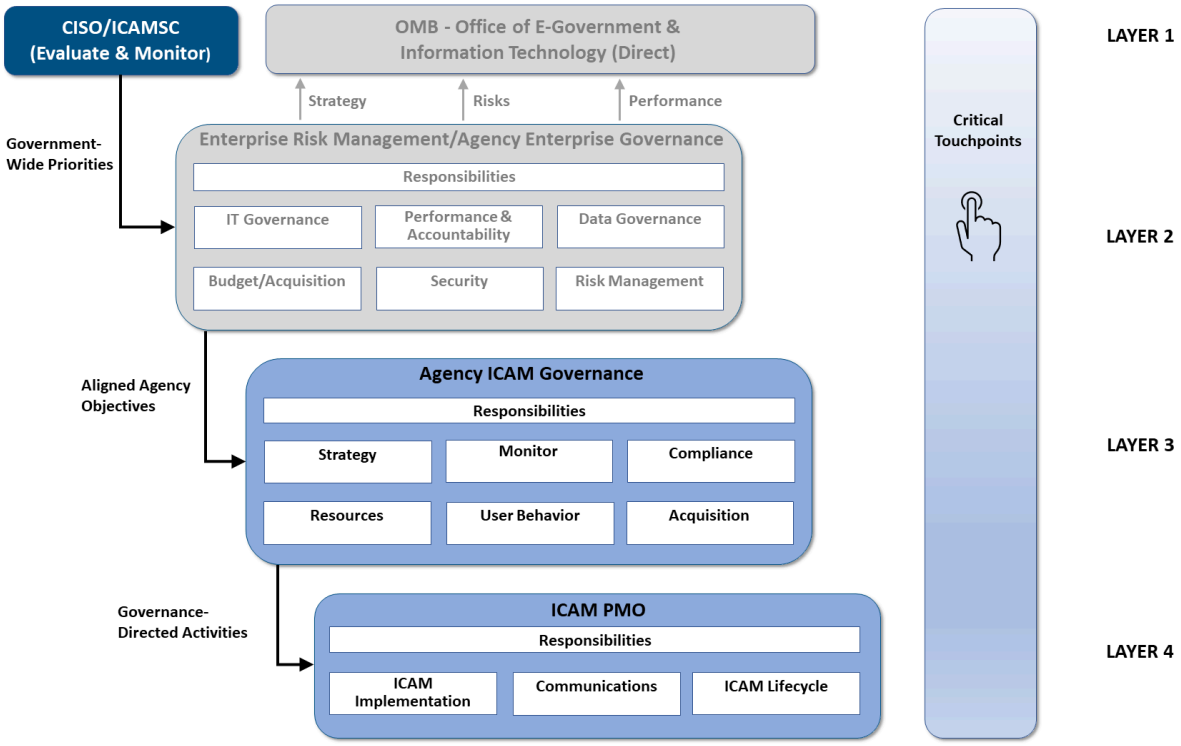


Figure 1: Multi-layered ICAM Governance Model

Government-wide Governance (Layer 1) is performed by OMB and the Federal CIO Council, which establish goals and objectives that flow down to Enterprise Risk Management/Agency Enterprise Governance (Layer 2). Agency Enterprise Governance, in turn, tasks the Agency ICAM

Governance layer (Layer 3), whose strategy is implemented by the ICAM PMO (Layer 4). This multi-layer governance concept is further discussed below.

Note: This document's focus is ICAM governance; therefore, it does not provide an in-depth discussion on the specific role of OMB or Enterprise Risk Management/Agency Enterprise Governance. For guidance on these areas, agencies should refer to OMB A-130, OMB A-11, OMB M-15-14, and OMB A-123.

Government-wide Governance (Layer 1)

According to an E-Government Act (see Appendix A: Laws, Policies, Standards, and Additional Resources) mandate, the OMB Office of E-Government and Information Technology is responsible for administering government-wide governance for implementing IT across the federal executive branch. Working with strategic partners such as the Federal CIO Council, Department of Homeland Security (DHS), Cybersecurity Infrastructure Security Agency (CISA), and NIST, the Office of E-Government and Information Technology publishes policy directives and sets priorities for implementing legislative mandates and executive orders pertaining to IT security and identity management. It sets metrics for agency reporting of progress toward the goals set by these policy directives and evaluates plans and requests for funds. It also monitors cross-agency risks and performance and updates goals and metrics appropriately. As a subcommittee of the Federal CIO Council's Federal Chief Information Security Officer (CISO) Council, the Identity, Credential, and Access Management Subcommittee (ICAMSC) "aligns the identity management activities of the Federal Government, and supports collaborative government-wide efforts to increase agency flexibility in addressing ICAM challenges; coordinate interagency efforts to meet agency mission needs; identify gaps in policies, procedures, standards, guidance, and services; and align ICAM policies and compliance with other cybersecurity initiatives."[7]

Enterprise Risk Management/Agency Enterprise Governance (Layer 2)

Many of the other agency management processes and governance bodies are critical touchpoints for ICAM governance. These include IT Governance, Security Governance, , Budget and Acquisition, Performance and Accountability, Risk Management, and Data Governance. ICAM governance activities must align to these processes; for example, ICAM-related plans and metrics must support the business objectives and performance metrics determined in the Performance and Accountability Report process. The degree of integration will vary for each agency, but these touchpoints are critical linkage points for institutionalizing ICAM governance.

Agency ICAM Governance (Layer 3)

Layer 3 is central to the concept of ICAM governance. In this layer, the agency establishes ICAM governance as required by OMB M-19-17. The agency-level ICAM governance strategy will lead

[7] Identity, Credential, and Access Management Subcommittee

to the alignment of ICAM to agency goals, consistent implementation across business lines, improved security, and cost reduction. The agency-level ICAM governance body should ensure that compliance with government-wide directives is monitored at all layers and that agency resources are deployed to ensure efficient and effective ICAM governance. This includes ensuring that the agency's acquisition programs align with federal priorities and user behavior is considered in the overall strategy and goal setting. Agency ICAM governance priorities must support government-wide priorities. Optionally, each major subunit of the agency may implement subordinate agency governance layers that adopt the strategy of and provide input to the overall Agency ICAM Governance layer.

Effective ICAM governance provides a vital tool for agencies to centrally manage risks associated with identities. The risk management feature of ICAM governance is present in the strategy component, as plans are tuned to the agency's risk tolerance, but is also present in the monitoring component and ensures treatment of risks (controls) such as least privilege or separation of duties.

The following sections discuss the governance roles and operating activities that individual agencies should consider as they establish and maintain their ICAM governance programs.

ICAM PMO (Layer 4)

The ICAM Program Management Office (PMO) is not strictly part of ICAM governance. However, it encompasses the execution or build layer for agency ICAM and is responsible for implementing solutions in conjunction with stakeholder organizations such as the IT department, system owners, business process owners, physical security, and human resources. In addition to implementing ICAM within the agency, the ICAM PMO is responsible for communicating with agency stakeholders and users to ensure that everyone understands the ICAM goals and priorities and the value they bring to the agency. The ICAM PMO also manages ICAM lifecycle activities for the agency. Users and the technical team supporting the ICAM PMO often conceive innovations that are considered by the Agency ICAM Governance layer.

Governance Roles

The following tables are organized in four categories (Federal Governance Bodies, Internal Standards Body, External Service Customers, and Agency-Level Stakeholders) to list the ICAM governance stakeholders and their roles.

An important first step in establishing an effective governance program is to identify the stakeholders and roles associated with that governance. According to COBIT® 2019 (see Appendix A: Laws, Policies, Standards, and Additional Resources), one common reason governance fails is lack of executive-level support. In agreement with this supposition, NIST SP 800-53 Rev 5. recommends that organizations consider establishing champions for information security and privacy and, as part of including the necessary knowledge base, assign specialized

expertise and resources as needed. OMB M-19-17 takes it one step further and designates a staff member from the Office of the Chief Operating Officer (COOs), or the agency equivalent role, as the "Executive Champion" to ensure that regular coordination occurs among agency leaders, as well as business process and systems owners.

The following tables are organized in four categories (Federal Governance Bodies, Internal Standards Body, External Service Customers, and Agency-Level Stakeholders) to list the ICAM governance stakeholders and their roles.

2.5.1 Federal Governance Bodies

Table 2: ICAM Governance Stakeholders

Stakeholder Name	Stakeholder Role
Office of Management and Budget (OMB)	Assists the President in overseeing the preparation of the federal budget and supervises its administration in Executive Branch agencies. Provides policy, direction, and oversight for the implementation of ICAM initiatives. Serves as the lead agency for e-government implementation.
Federal Chief Information Officers (CIO) Council	Improves practices in the design, modernization, use, sharing, and performance of federal government agency information resources. Charters the work of the Federal Public Key Infrastructure (FPKI) Policy Authority as well as the ICAMSC.
Federal Chief Information Security Officer (CISO) Council	Oversees interagency CISO collaboration and communication. Identifies and recommends strategic high-priority IT security initiatives to advise the Federal CIO Council and OMB. Focuses on the following strategic areas: Identity management, comprehensive risk assessment and framework, vulnerability response, shared services, and performance metrics.
Identity, Credential, and Access Management Subcommittee (ICAMSC)	Subcommittee of the CIO/CISO Council. Oversees all aspects of identity management: secure access, authentication, authorization, credentials, privileges, and access lifecycle management Provides opportunities for agencies to raise issues and challenges associated with the planning, implementation, and operation of ICAM programs and solutions. Develops specific guidance and tools to assist agencies' abilities to meet ICAM policy objectives and overcome identified ICAM implementation challenges. Fosters cross-government collaboration on information sharing, lessons learned, and best practices related to ICAM.

Stakeholder Name	Stakeholder Role
Federal Privacy Council	Improves agency practices for the protection of privacy. Serves as an interagency coordination group for Senior Agency Officials for Privacy and for Chief Privacy Officers in the federal government, promoting adherence to the letter and spirit of laws and best practices advancing digital privacy.

2.5.2 Internal Standards Body

Table 3: ICAM Internal Standards Body Stakeholders

Stakeholder Name	Stakeholder Role
National Institute of Standards and Technology (NIST)	Promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. Specific to ICAM, NIST develops and evolves identity and access management standards, guidance, best practices, profiles, and frameworks for federal agencies.

2.5.3 External Service Customers

Table 4: External Service Customer Stakeholders

Stakeholder Name	Stakeholder Role
American Public and Businesses	Individuals and businesses that require access to government systems and resources. The government-wide approach to ICAM must address the varying needs of these communities, focusing mainly on the characteristics of the two user segments: Government-to-Citizen (G2C) and Government-to-Business (G2B).
State, Local, Foreign, and Tribal Governments	Governments that transact business on behalf of their constituencies or higher levels of government. Partner with the federal government on identity management initiatives.

2.5.4 Agency-Level Stakeholders

Table 5: Agency-Level Stakeholders

Stakeholder Name	Stakeholder Role

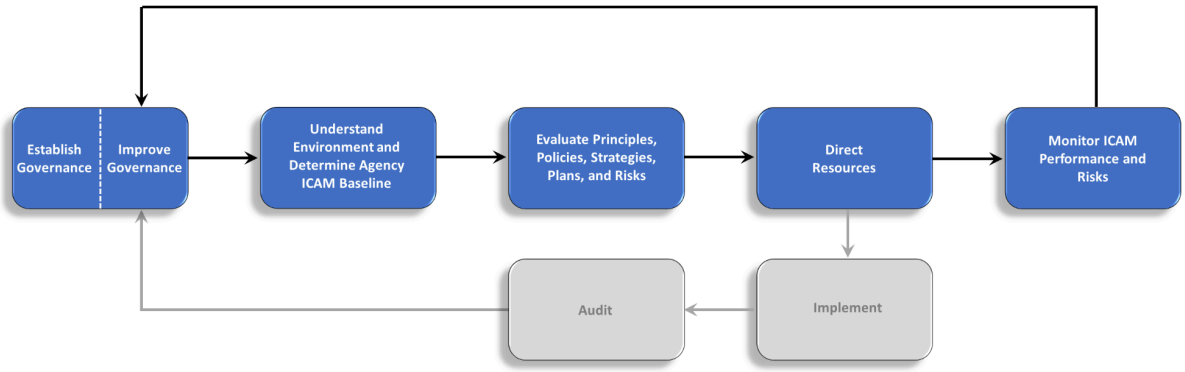
Head of Agency	Establishes ICAM Governance within the agency and designates the Executive Champion.
Agency Partners and Affiliates	Contractors working on behalf of the federal government and affiliates that do business with or consume the services provided by federal agencies. Portions of this population use Personal Identity Verification (PIV) credentials to access agency facilities and information systems while others use non-PIV credentials and require only occasional access to agency assets.
Business Process/System Owners	Individuals within an agency responsible for managing a set of activities, programs, and systems that are critical to operations and use ICAM services.
General Counsel	Provides legal oversight over an agency's ICAM program, administering security clearance review programs and ensuring that ICAM programs abide by all applicable laws and regulations.
Human Resources (HR)	Creates a digital identity for each employee within the agency's HR applications. Collects information on federal employees to assist ICAM efforts with automated and monitored onboarding, offboarding, and privilege management.
Office of the Chief Financial Officer (OCFO)	Processes and submits budget requests for ICAM investments. Ensures that each agency investment leverages ICAM requirements and tools.
Office of the Chief Information Officer (OCIO)	Coordinates with the agency's Chief Financial Officer (CFO) to ensure that the IT programs and activities are cost-effective. Ensures that appropriate security controls are applied, determines how the ICAM solution will impact the security of existing applications, and incorporates ICAM into the agency's Enterprise Architecture (EA).
Office of the Chief Information Security Officer (OCISO)	Develops, employs, and publishes security policies, programs, and standards to guard the agency's personnel, property, facilities, and information. Has leadership and authority over security policy and programs within the agency and can coordinate with the Personnel Security and Physical Security divisions.
Personnel Security	Coordinates with managers' HR departments to determine position sensitivity levels for each position occupied within the agency.

	In coordination with the Office of Personnel Management (OPM), performs its validation and clearance role for enterprise-level ICAM by ensuring that all agency employees and contractors receive an appropriate background investigation and periodic reinvestigation to access federal facilities and systems.
Physical Security	As an integral part of ICAM, protects federal employees as assets by managing the security of agency buildings, such as resolving conflicts concerning entry to facilities and verifying that those seeking to gain access to federal buildings are authorized to do so.
Privacy Office	Administers data privacy management by establishing policy to govern the use, collection, storage, and dissemination of personally identifiable information (PII) for all agency employees, contractors, and affiliates. Maintains an agency's System of Records Notices (SORNs) and supports Privacy Impact Assessments (PIAs) for all IT investments, including ICAM.
ICAM PMO/Technical Team	Team responsible for performing actual ICAM work such as creating policies, architecture, and plans.

Implementing Agency-Level Governance

Agencies should tailor their ICAM governance practices to their own organization's mission, operations, and IT security needs.[8] This section provides guidance to those within the agency responsible for establishing ICAM governance, as well as overall management control. This guidance is divided into five (5) categories of ICAM governance operation:

1. Establish/Improve Governance
2. Understand Environment and Determine Agency ICAM Baseline
3. Evaluate Principles, Policies, Strategies, Plans and Risks
4. Direct Resources
5. Monitor ICAM Performance and Risks



Establish/Improve ICAM Governance

The Agency Head establishes ICAM governance, with agency-wide authority to direct resources toward ICAM strategies and plans, that aligns with federal and agency priorities and assures associated threats and vulnerabilities are mitigated and/or remediated.

The Agency Head initiates these operations by establishing ICAM Governance, providing the top-down authority to direct resources toward strategies that align with federal priorities and mitigate security threats. Establishing ICAM governance fulfills OMB M-19-17 mandates and anchors the FISMA 2014 requirement for a unified, agency-wide security program. ICAM governance bodies serve as the critical conduit, cascading policies and strategic impacts down through established communication channels into every business area.

Key Activities:

[8] NIST SP 800-100, Information Security Handbook: A Guide for Managers, Page 3, March 7, 2007

- Initiate an ICAM governance function and designate an Executive Champion from the Office of the Chief Operating Officer or equivalent (OMB M 19-17, NIST SP 800-53 Rev. 5)
- Assign key roles and responsibilities (OMB M 19-17, Clinger-Cohen Act, E-Government Act, FITARA, FISMA 2014)
- Assess the skills and capabilities of the ICAM team and provide opportunities for development (NIST SP 800-53 Rev 5., Control PM-13)
- Establish integration with other agency governance structures (e.g., IT Review Board, Senior Management Council)
- Improve governance processes based on previous year's performance in accomplishing agency goals, the impact of ICAM on agency programs, and documented audit results (FISMA 2014)[9]

Understand Environment and Determine Agency ICAM Baseline

ICAM governance will help governance stakeholders maintain understanding of the environment (e.g., policies, laws, innovations, user behavior) as well as the baseline and revisions of the overall ICAM environment (e.g., strategy, architecture, and plans).

According to the best practice concepts from COBIT® 2019 and ISO/IEC TS 38501:2015 (see Appendix A: Laws, Policies, Standards, and Additional Resources), organizations must determine context for both the internal and external environments. In the federal environment, the internal context is found in Cross-Agency Priorities (CAPs), the President's Management Agenda, Agency Strategic Plans, OMB A-123 risk assessment reports, and agency performance reports. Additionally, agencies should establish the ICAM baseline, including documenting existing user behavior, identity stores, policies, architecture, and processes (NIST SP 800-53 Rev. 5, Control PM-11).

The government-wide governance bodies (Layer 1) monitor the technology, user trends, and activities of other agencies and non-federal entities, such as state governments and industry, to determine external context.

Based on the context and baseline, the agency should develop its overall strategy of the future state and then, by analyzing the gaps between the future and current state, prepare its plan of action (e.g., consolidation of identity stores, moving to cloud identity, etc.).

Key Activities:

- Understand user behavior
- Understand internal and external environments

[9] Federal Information Security Modernization Act of 2014, Public Law 113-283, December 18, 2014, Title 44 U.S.C., Section 3554, Federal agency responsibilities, Page 3080: "(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;"

- Document ICAM baseline/Inventory (current state)
- Conduct risk assessment (as recommended in NIST SP 800-63-4 and the Digital Identity Risk Assessment [DIRA][10] Playbook) as necessary
- Document agency-wide ICAM strategy and architecture (future state)
- Conduct gap analysis
- Prepare action plans

Other Consideration: In determining the agency context, agency ICAM governance should consider the agency's organization-wide risk management strategy to understand the security and privacy risk tolerance for the organization (NIST SP 800-53 Rev. 5, Control PM-9).

Evaluate Principles, Strategies, Policies, Plans, and Risks

ICAM governance evaluates strategies, plans, and policies against federal and agency priorities and objectives.

The agency-wide approach to ICAM governance must be harmonized with other governance activities' statutory requirements and best practices. In addition, ICAM governance must incorporate agency strategic missions and cybersecurity goals and objectives into its plan. In this way, agency leadership is unified in the delivery of ICAM solutions, with the overall effect of enhancing security and reducing risk.

Key Activities:

- Evaluate agency-wide ICAM Program Strategy and Architecture against agency objectives and CAPs
- Evaluate ICAM plan and program for acceptable risk and alignment to priorities
- Determine metrics that establish the link between agency mission, business objectives, and ICAM capabilities

Direct Resources

ICAM governance directs resources toward achievement of agency and federal objectives using ICAM technologies and approaches. This governance activity directs the creation of strategies and plans, policies, use of funds, and acquisitions.

OMB M-19-17 requires an ICAM-specific policy, process, and technology solution roadmap that addresses ICAM for the entire enterprise and aligns with the government-wide ICAM architecture and Continuous Diagnostics and Mitigation (CDM) program requirements to direct and control the deployment of identity solutions within the agency. These internal policies and procedures must include access control (NIST SP 800-53 Rev. 5) and privacy considerations.

[10] GSA, Digital Identity Risk Assessment Playbook, June 15, 2025

Both FISMA 2014 and FITARA reinforce this concept of direct and control—requiring that the CIO approve IT acquisitions and ensure that security compliance and ICAM considerations are included. As goals and objectives are passed down and innovation flows up, ICAM governance ensures that resources are directed toward plans that best meet agency objectives.

Key Activities:

- Direct resources to develop plans, policies, and strategies as well as business cases for ICAM; this should be considered part of CPIC
- Direct the ICAM PMO to develop the Agency-Wide Solution Roadmap, as required by OMB M-19-17.
- Direct resources to enable implementation of enterprise ICAM capabilities
- Direct testing of identity controls as part of the security control testing and/or integrated control program
- Direct and approve the acquisition of solutions to achieve agency objectives (FITARA)
- Communicate the ICAM benefits and changes to stakeholders and executive leadership at an enterprise level

Other consideration: The ICAM PMO should consider the agency Security Program Plan when developing the Agency-Wide Solution Roadmap and other ICAM plans.

Monitor ICAM Performance and Risks

ICAM governance should establish a monitoring system to track and report on overall ICAM activity performance and metrics; measure resource contributions to specific missions, goals, and objectives; and answer the question "Did we reach the future state?"

Performance monitoring and reporting in the federal government can be subject to overlapping requirements. Three (3) key performance measurements are recommended for establishing effective ICAM monitoring: 1) cybersecurity and risk management metrics aligned with the ICAM lifecycle, for measuring changes in the agency ICAM posture, including changes in user access privileges; 2) metrics related to CDM dashboards and FISMA 2014 reporting; and 3) e-government and business objectives metrics associated with processes affecting access for citizens, access for businesses, and internal federal government operations. These metrics will align to CAP goals and agency goals.

Key Activities:

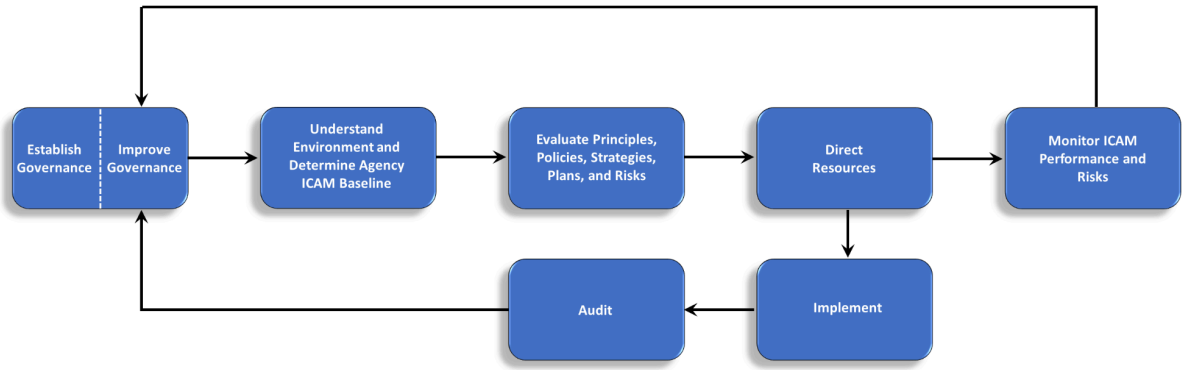
- Monitor agency outcomes supported by ICAM
- Monitor ICAM metrics – identity and role repository, orphaned accounts, privileged accounts
- Monitor ICAM-specific risks as part of the agency's integrated internal control assessment, Identity assurance risk, and the risk management framework

- Support annual report submissions – Agency Performance Report, Security Report (Identity specific), Security Incident Reporting (Identity), and E-Government Reporting

Sustain and Improve Governance

In addition to the ICAM agency-level governance implementation activities discussed previously, there are three (3) additional supporting functions necessary to the success of ICAM governance:

1. Implement
2. Audit
3. Improve



Implement

In addition to an ICAM governance body, an ICAM PMO can support the execution and operation of projects and workstreams. An ICAM PMO complements and supports the program governance body.

Achieving changes in ICAM implementation across the agency is challenging because that effort is part of practically every system, from physical security and human resources to citizen services and fraud detection. A dedicated ICAM PMO responsible for implementing, communicating, and managing the lifecycle of the ICAM solution provides a solution for this challenge. It ensures that individual components of the ICAM program operate efficiently and achieve the expected results within the defined budget and schedule.

Some agencies may not require both an ICAM governance body and an ICAM PMO; however, the implementation and continuing lifecycle activities must then be addressed by the ICAM governance body. In such cases, an ICAM Technical Team taking direction directly from the ICAM governance body may be sufficient to meet the ICAM implementation needs.

Key Activities:

- Educate and inform agency staff about the importance of ICAM to the mission delivery
- Proactively communicate proposed changes to enterprise-wide ICAM solutions and services and their corresponding implementation benefits
- Engage with the Executive Champion to share lessons learned and conduct knowledge-sharing activities
- Manage project and administrative workstreams
- Build or acquire solutions

Audit

Although the term "audit" often has a negative connotation, in the context of ICAM governance it is a necessary function to obtain feedback on compliance and effectiveness. ICAM governance should seek opportunities for internal audit and reviews in conjunction with the Office of the Inspector General (OIG) or other assessment groups.

Audit is both required and necessary for optimizing ICAM governance. The audit process should include regular, independent reviews of ICAM governance performance, delivery of outcomes, and adherence to law. The OIG within an agency has statutory responsibilities to assess security in addition to providing insight into management practices. Audit results may suggest changes to the governance model or context to drive successful ICAM performance.

Key Activities:

- Test policies and effectiveness of controls
- Assess the maturity of the ICAM program and its attainment of the intended outcomes
- Provide audit results to the Executive Champion; as necessary and appropriate, also provide audit results to government-wide governance bodies
- Take action to remediate deficiencies

Improve

To sustain and continuously improve ICAM governance, the Executive Champion should consider audit results, staff feedback, and the achievement of outcomes.

ICAM governance must continuously improve. This culminating activity considers input from the other components, including context, plans, policies, metrics, and audit, and seeks opportunities to improve process performance and outcome achievement. A mature ICAM program offers the agency a repeatable, measurable approach that is capable of providing more reliable results and providing process clarity for the project team. Mature ICAM governance will regularly review and update its processes.

Key Activities:

- Consider performance and timeliness—Did the agency achieve its objective?
- Consider feedback—user surveys, audit reports, etc.

- Consider compliance with laws—FITARA, Privacy Act, FISMA 2014, E-Government Act, and agency-specific law or regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Update governance processes for the next performance cycle

Cross-Agency Governance Coordination

Finally, as described previously in Layer 1, agency ICAM governance must be linked to and occur in coordination with the OMB and the ICAMSC to maximize cross-organizational communication, collaboration, credential re-use, risk reduction, fraud detection improvement, and contribute to cross-boundary governance.

The Federal CIO Council has an increased role to play as the inter-departmental coordination activity for IT programs. In support of this role, the E-Government Act requires the Council to consult with federal, state, local, and tribal government leaders, as well as leaders in the private and non-profit sectors concerning IT programs and solutions. As a subcommittee of the Federal CIO Council and the CISO Council, it falls to the ICAMSC to take on this inter-departmental coordination role for ICAM, which includes updating governance guidance, synthesizing data from agency ICAM governance, and coordinating the federal government's interactions with external organizations. As with the agency ICAM governance function, the Federal CIO Council and OMB will direct, evaluate, and monitor this government-wide ICAM governance function.

Key Activities:

- Review the Agency-Wide Solution Roadmap for alignment with government-wide goals—CAP goals, credential re-use, cybersecurity, and e-government metrics
- Review agency ICAM audit results and monitor remedial actions when deficiency could affect other agencies
- Working with the Performance Improvement Council, review ICAM performance metrics
- Seek feedback from NIST, the General Services Administration (GSA), and OMB on the possible need for additional guidance, technical standards, testing, or interoperability frameworks

Outcomes/Performance Metrics

Outcomes and metrics are particular to an agency's objectives and thus are at the discretion of agency leadership. Table 6 provides examples of possible outcomes and performance metrics.

Table 6: Outcomes and Performance Metrics Examples

Outcome	Description	Example Evidence
Drive Mission	Agency mission and business objectives are achieved by using ICAM. Establishes ICAM governance with 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. CAPs are achieved through government-wide governance activities.	Percentage of agency objectives supported by ICAM (Quantitative) ICAM governance is established and operating across the department (Qualitative) Percentage of CAP objectives achieved by using ICAM (Quantitative)
Enhance Security	Increases progress in implementing modern security and process improvements, such as Zero Trust and multi-factor authentication (MFA) enforcement, improving an agency's overall security posture. Reduces delays in issuing and removing credentials, which speeds access to authorized systems and services while preventing inappropriate facility or IT resource access that could lead to data tampering or theft.	Security improvement is delivered on time and at or below budget (Quantitative) Percentage of employees who are no longer with the agency but retain their system access (Quantitative)
Empower Users	Provides consistent, timely, and seamless identity creation, provisioning, and authorized access to necessary systems. Enhances end-user digital experience for employees, affiliates, and external constituents and mission partners.	Time in days or hours to provision (Quantitative) Percentage of credentials used that are also useable for comparable services in other organizations (Quantitative)

Outcome	Description	Example Evidence
Improve Cost and Business Efficiencies	Implement enterprise-wide capabilities through governance, 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.	Number of component-level systems or reliance on single-context external-facing systems (Quantitative) Cost savings of moving to enterprise-wide systems (Quantitative)

Appendix A: Laws, Policies, Standards, and Additional Resources

Laws

[21st Century IDEA]	21st Century Integrated Digital Experience Act, Public Law No: 115-336, December 20, 2018
[Clinger-Cohen Act]	Clinger-Cohen Act of 1996, Public Law 104-106, February 10, 1996
[E-Government Act]	E-Government Act of 2002, Public Law 107–347, December 17, 2002
[FISMA 2014]	Federal Information Security Modernization Act of 2014, Public Law 113-283, December 8, 2014
[FITARA]	Federal Information Technology Acquisition Reform Act, Public Law 113-291, December 19, 2014
[FMFIA]	Federal Managers Financial Integrity Act of 1982, Public Law 97-255, September 8, 1982
[GPRA]	Government Performance and Results Act of 1993, Public Law No: 103-62, August 3, 1993
[HIPAA]	Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, August 21, 1996
[Privacy Act]	Privacy Act of 1974, as Amended, Public Law 93-579, as codified at 5 U.S.C. 552a, October 18, 1988

Policies

[OMB A-11] OMB Circular A-11, Preparation, Submission, and Execution of the Budget, August 29, 2025

[OMB A-123] OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 15, 2016

OMB A-130 OMB Circular A-130, Managing Federal Information as a Strategic Resource, July 28, 2016

[OMB M-15-14] OMB M-15-14, Management and Oversight of Federal Information Technology, June 10, 2015

[OMB M-19-17] OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019

[OMB M-22-09] OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022

Standards

[ISO/IEC 38500:2024] ISO, ISO/IEC 38500:2024 — Information technology — Governance of IT for the Organization, February 2024

[ISO/IEC TS 38501:2015] ISO, ISO/IEC TS 38501:2015 – Information Technology – Governance of IT – Implementation Guide, April 2015

[NIST SP 800-39] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011

[NIST SP 800-53] NIST SP 800-53, Rev 5, Security and Privacy Controls for Information Systems and Organizations, December 2020

[NIST SP 800-63] NIST SP 800-63-4, Digital Identity Guidelines, August 26, 2025

[NIST SP 800-100] NIST SP 800-100, Information Security Handbook: A Guide for Managers, March 7, 2007

Additional Resources

[CDM] Continuous Diagnostics and Mitigation Program, December 3, 2024

[COBIT® 2019] ISACA, Control Objectives for Information Technologies 2019 Framework, 2019

[DIRA] GSA, Digital Identity Risk Assessment Playbook, June 15, 2025

[ICAMSC] Identity, Credential, and Access Management Subcommittee

Appendix B: Acronyms

Acronym	Definition
CAP	Cross-Agency Priority
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISA	Cybersecurity Infrastructure Security Agency
CISO	Chief Information Security Officer
COBIT®	Control Objectives for Information Technologies
COO	Chief Operating Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
DIRA	Digital Identity Risk Assessment
EA	Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
FMFIA	Federal Managers Financial Integrity Act
FPKI	Federal Public Key Infrastructure
G2B	Government-to-Business
G2C	Government-to-Citizen
GPRA	Government Performance and Results Act
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
ICAM	Identity, Credential, and Access Management

Acronym	Definition
ICAMSC	Identity, Credential, and Access Management Subcommittee
IDEA	Integrated Digital Experience Act
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMO	Program Management Office
SORN	System of Records Notice
SP	Special Publication
ZTA	Zero Trust Architecture