MORAN

IAM Governance

BEST PRACTICES

morantechnology.com
888-699-4440

Contents

BACKGROUND

Identity and Access Management (IAM) is often first seen as a technical service—usernames, passwords, and login issues. In practice, IAM is much broader: it is the mechanism through which institutional decisions about people, data, and services are translated into day-to-day operations.

This guide is intended for university leaders and governance participants whose decisions shape how identity, access, security and risk, and user experience are managed across the institution. It explains why IAM governance is distinct from—and complementary to—other governance efforts, and why it works best when sustained over time. Institutions engage with IAM governance to advance security, efficiency, and user experience—often all three.

Governance for IAM should support informed, collaborative decision-making while respecting the varied traditions, institutional cultures, and operating models found across your institution.

HOW IAM GOVERNANCE IS UNIQUE

Institutions often find that Identity and Access Management does not fit neatly into existing governance categories. While IAM is enabled by technology, its impact reaches well beyond IT systems.

Identity and access questions tend to surface where data stewardship, security expectations, operational needs, and user experience intersect. Decisions about who should have access, when access should begin or end, and how exceptions are justified often span multiple governance domains.

Without a shared space that reflects broad institutional needs and perspectives, these decisions can wind up deferred, escalated informally, or addressed inconsistently. They may also be made implicitly within technical teams based on immediate needs rather than institutional priorities. IAM governance provides an intentional forum for decisions that would otherwise fall between existing governance structures.

WHY IAM GOVERNANCE NEEDS TO BE AN ONGOING EFFORT

IAM programs grow and evolve over time along with the institution. Governance that keeps pace with that growth stays grounded in real business needs and delivers continuous value. What the process looks like and produces will change over time. Balancing immediate needs with long-term sustainability takes deliberate effort.

Before and during an IAM implementation, governance often focuses on defining priorities, ensuring institutional requirements are represented, and supporting major project decisions. This may include clarifying core populations and lifecycles, identifying data integration needs, aligning with related initiatives, and guiding testing and readiness activities.

Many of these needs are finite and project-oriented, making them great candidates for focused working groups or subcommittees, while a smaller core team maintains a broader, institution-wide view of priorities, resources, and alignment.

As IAM technologies and capabilities mature and automation increases, the emphasis of governance naturally shifts. Access decisions become more visibly tied to authoritative data sources, with clear efficiencies and delays that affect service delivery and user experience.

At this stage, new questions begin to surface. Where is friction appropriate to shape behavior, and where does it create unnecessary work? Which access decisions should be standardized, and which require flexibility or extra review? As needs change, how should risk tolerance be applied? Which priorities deliver the greatest value for the investment?

These are healthy questions that reflect a maturing program. Sustained IAM governance provides a vehicle for adaptation, helping to revisit priorities, respond to new needs, and maintain alignment as technology, expectations, and institutional goals evolve.

DESIRED OUTCOMES OF IAM GOVERNANCE

IAM governance is most effective when oriented around clear institutional outcomes instead of specific tools, processes, or implementation approaches. While governance models vary by institution, effective efforts are guided by a shared understanding of priorities, tradeoffs, and success.

A well-functioning IAM governance process helps institutions:

- Maintain alignment between institutional strategy, policy, and IAM-related decisions
- Support informed prioritization of IAM-related initiatives, investments, and sequencing—providing clarity where security, privacy, operational needs, and user experience intersect
- Increase transparency and consistency around decision rationale, risk tolerance, and exception handling
- Promote an institutional view of identity and access that balances local needs with shared priorities—ensuring that variation and customization are intentional, justified, and visible
- Provide an objective forum for evaluating tradeoffs and setting direction across organizational boundaries

Together, these outcomes provide a practical way to assess whether IAM governance is contributing strategic value over time.

HOW IAM GOVERNANCE COMPLEMENTS EXISTING GOVERNANCE

IAM governance is not an additional layer of bureaucracy. It is an intentional way to engage the institution around decisions that cut across identity, data, risk, and user experience—areas that are often addressed separately elsewhere. Because identity is foundational to how people interact with systems, data, and services, IAM considerations naturally surface across programs, departments, and initiatives throughout the organization.

It's important to acknowledge that the word "governance" can be an obstacle, reinforcing perceptions of bureaucracy. Some institutions choose to frame this work as a Steering Committee, Stewardship, or Council, recognizing that the goal is shared understanding, prioritization, and sustained alignment. In practice, IAM governance must work alongside existing structures, with many of the same leaders participating in multiple committees.

When data governance defines authoritative sources, IAM governance helps determine how and when those sources drive access. When security governance establishes risk tolerance, IAM governance supports consistent interpretation across systems and populations. When IT governance prioritizes initiatives, IAM governance helps identify identity-related dependencies that may enable—

or constrain—successful outcomes. In each case, IAM governance builds on existing foundations rather than replacing them, grounding shared decisions in institutional goals and day-to-day realities.

THE ROLE OF LEADERSHIP IN IAM GOVERNANCE

IAM governance does not require leaders to become technical experts. It benefits most from the perspectives of leaders whose primary focus is the day-to-day work of the institution—teaching, research, student life, administration, and service delivery.

Leadership engagement is most impactful when it clarifies institutional priorities, reinforces consistency across programs and teams, and helps balance competing demands related to privacy, risk, efficiency, and experience. IAM governance also helps prevent decisions about access, risk, and prioritization from being made by technical teams in a vacuum, ensuring those decisions remain grounded in institutional priorities rather than technical convenience.

Because identity and access decisions surface real constraints related to data quality, process design, risk tolerance, and user experience, governance discussions often help participants develop a clearer understanding of how different parts of the institution operate and where their challenges intersect.

Over time, this shared context can support more collaborative decision-making, reduce siloed approaches to common problems, and encourage a more institutional view of IAM's impact.

IAM governance is not intended to manage day-to-day IAM operations or prescribe technical implementation details. Instead, it defines direction, priorities, and outcomes—while relying on IAM practitioners to design and execute solutions that meet those goals. Clear separation between governance and operations allows leaders to focus on institutional judgment while enabling technical teams to apply their expertise effectively.

In this way, leadership participation resembles stewardship more than oversight—helping the institution make coherent, values-aligned choices while allowing technology to fade into the background for the people it serves.

COMMITTEE STRUCTURE AND PARTICIPATION: PRACTICAL EXAMPLES

To be effective and sustainable, IAM governance benefits from clear structure and representative participation.

While no single model fits every campus, experience across institutions suggests IAM governance works best with a small, stable core group and the ability to engage additional perspectives as needed.

CORE STEERING GROUP

Begin with a core steering group that meets regularly and provides continuity, prioritization, and decision support. This group should be small enough to function efficiently, while broad enough to reflect the institutional impact of identity and access decisions.

Commonly represented roles include senior IAM leadership, information security and risk functions, physical safety, and designated domain stewards responsible for institutional data and policy decisions (such as Human Resources or participant/student administration). It is also important to

include legal, privacy, and risk/compliance perspectives, along with leaders from key programs or operational areas who can represent service delivery and user experience needs.

In practice, many organizations designate a chair or co-chairs—often the IAM Architect, IAM Lead, or a senior sponsor—to facilitate discussion and maintain momentum. A co-chair may be a data steward or other senior leader to help balance technical and business perspectives. While the group typically works toward shared understanding and alignment, clear facilitation helps avoid stalled decisions and provides a path for escalation when consensus cannot be reached.

The most important factor is whether members are empowered to represent their area and communicate decisions back to their peers. Prioritize decision makers over subject matter experts for the core group. Subject matter experts make invaluable contributions, but their participation is often better suited to focused subcommittees, where their expertise shapes recommendations rather than extending deliberation at the decision-making level.

FOCUSED SUBCOMMITTEES

Subcommittees are typically short-lived, project-based efforts that do the investigative work before a topic reaches the steering group. Drawing on subject-matter expertise and real operational experience, they help ensure that decisions are based on actual institutional needs rather than vendor presentations or high-level summaries that may not reflect day-to-day realities. When a recommendation arrives at the decision-making level, tradeoffs are already clarified and options narrowed. This prevents the common pattern where steering groups repeatedly defer decisions while seeking more information, sometimes for months at a time.

Examples of subcommittee work include policy analysis, access model design, technical evaluation, and stakeholder feedback.

Subcommittees typically persist only as long as their work remains active, reporting progress and recommendations back to the steering group. This core-and-subcommittee structure helps maintain a stable, well-informed decision-making body while allowing the IAM governance process to adapt as priorities, staffing, and technologies evolve.

COMMON PATTERNS TO BE MINDFUL OF

Over time, IAM governance efforts can lose effectiveness when scope expands too broadly, when decision-making bodies become unwieldy, or when discussions focus primarily on tools and controls rather than institutional priorities. Recognizing these patterns early makes it easier to recalibrate before they compound.

The Governance Maturity: Signals and Implications table in the appendix describes common institutional moments where governance needs shift, what those shifts tend to look like in practice, and questions worth raising in response.

CLOSING SUMMARY

IAM governance is most effective when understood as an institutional capability rather than a technical obligation. It benefits from sustained engagement, thoughtful alignment with existing governance efforts, and a clear separation between governance and operational responsibilities.

When approached this way, IAM governance helps institutions move forward with greater confidence—allowing security, compliance, efficiency, and user experience to reinforce one another rather than compete.

APPENDIX:

Note:

IAM, and especially IAM governance, is not a science; it's an art — highly subjective and relative to institutional needs, maturity, and culture. Maturity models and rubrics are most useful when treated as tools for conversation—helping institutions understand their current posture, identify where governance adds the most value, and set realistic expectations for evolution over time.

IAM GOVERNANCE MATURITY: SIGNALS AND IMPLICATIONS

IAM governance maturity does not progress in a straight line and it's unlikely to look the same across institutions. It can help to look at maturity as a set of signals that indicate when governance needs are changing. These signals can indicate how IAM is interacting with institutional operations—and what that suggests for governance engagement.

The following chart is intended to help governance groups recognize patterns and decide when deeper engagement or focused exploration may be appropriate. Recognizing these signals can help institutions tailor IAM governance to current needs, allowing engagement models, participation, and focus areas to evolve alongside the IAM program itself.

Institutional moment	What it may look like	Governance questions or engagement to consider
Recognition of misalignment or risk (e.g., security incident, audit finding, compliance concern)	Access does not reflect policy. People are surprised by who can or cannot access certain systems. Risk discussions become more urgent and concrete.	Is this an isolated issue or a sign of broader misalignment? Are institutional priorities and risk tolerance clearly understood and consistently applied?
Major IAM capability change (implementation, replacement, or re-evaluation)	Different groups describe the same people differently. Access rules vary by system or department. New or edge-case populations do not fit existing processes, leading to repeated exceptions or delays. The same access questions resurface across projects.	Do we have shared understanding of who our key audiences are and how they should be treated? Are affiliations and access expectations consistent across the institution? Should governance help clarify direction before solution decisions harden?
Budget cycle, funding change, or resource constraint	Current IAM capabilities or staffing are questioned in light of cost. Platforms or services are being evaluated for consolidation or replacement. A grant, initiative, or dedicated funding source has ended or is ending, leaving ongoing commitments without a clear owner.	Which current IAM investments are delivering clear value, and which should be reconsidered? Where are resource gaps creating risk or service gaps? How should priorities be sequenced given available capacity?
Major authoritative source or downstream system change (e.g., ERP replacement, LMS	Project planning raises recurring questions about access timing, roles, and data dependencies.	Are identity and access assumptions clearly understood and aligned across projects? Do current

or research platform implementation)	Multiple teams seek clarity on how identities, populations, and approvals should be handled. IAM considerations begin to influence project scope, sequencing, or readiness criteria.	definitions of audiences, affiliations, and lifecycles support upcoming needs? Where would shared direction or early clarification help avoid rework, exceptions, or misalignment as implementation progresses?
Expansion or change in institutional populations (e.g., affiliates, contractors, visiting scholars, partners)	New groups do not fit existing onboarding or access processes. Manual work increases. Different units handle the same population differently.	How should these populations be defined and supported institutionally? Are current approaches creating unnecessary variation or risk?
Shift in research posture or regulatory environment	New restrictions affect who can access data or systems. Approval processes change. Confusion emerges about what is allowed or required. Necessary reporting or data may not be easily accessed.	How should IAM practices adapt to new requirements while preserving appropriate flexibility? Are tradeoffs clearly understood by affected stakeholders?
Merger, acquisition, divestiture, or major organizational restructuring	People are unsure which systems they should access. Expected boundaries change. Ownership of data and decisions becomes unclear.	Are current identity sources, targets, and access principles still valid? Is there shared understanding across affected units during the transition?
Significant staffing or leadership change (IAM, security, data stewardship, IT, or executive leadership)	Decisions slow down. Past rationale is lost. Different answers emerge depending on who is asked.	Are decision rights and priorities still clear? Should governance re-establish shared context and expectations following the transition?
Growing visibility of IAM impact on daily work and experience	Access improvements are noticed and referenced. Requests emerge to extend IAM capabilities to additional systems, roles, or populations. Differences in experience become more visible.	Where is IAM delivering clear value today, and where are expectations beginning to grow? Which new use cases or populations should be prioritized next? How should the institution balance expansion, consistency, and risk as IAM capabilities mature?
Re-engagement after prior IAM governance activity paused	Past decisions feel outdated. New pressures or opportunities have emerged. There is uncertainty about where to restart.	What has changed since the last engagement? Which assumptions should be revisited based on lived experience? How can governance re-engage in a way that reflects current needs?

IAM GOVERNANCE MATURITY: MATURITY RUBRIC

The following may be helpful as a perspective to facilitate conversation, reflection, and a self-assessment of IAM Governance maturity at your organization.

	Initial	Developing	Defined	Managed	Optimized
Governance process	IAM governance is ad-hoc and reactive.	Basic or informal IAM governance structure in place.	Formal IAM governance structure with defined roles & responsibilities.	IAM governance is integrated with institutional strategic goals.	IAM governance is proactive and adaptive.
Stakeholder engagement	Limited stakeholder involvement.	Initial or informal stakeholder engagement.	Regular stakeholder engagement & communication.	High level of stakeholder engagement & collaboration.	Full integration with institutional processes and culture.
Policies / artifacts	No formal governance structure or documented policies.	Some documented policies and procedures.	Comprehensive set of documented policies and procedures.	Regular review and update of IAM policy, resources, & process.	Continuous optimization & adaptation to emerging trends & challenges.

IAM GOVERNANCE MATURITY: RACI CHART

This sample RACI (Responsible, Accountable, Consulted, Informed) chart provides a starting point for clarifying roles and expectations across common IAM governance activities. Organizations should adapt it to reflect their own structures, culture, and decision-making norms.

While executive leadership and governance bodies retain accountability for strategy, policy, and risk decisions, IAM practitioners—often led by the IAM Architect or IAM Lead—play a central role in facilitating discussion, providing technical and architectural context, and translating organizational priorities into implementable solutions.

Governance Activity	CIO / Senior IT Leadership	IAM Team / Architect (Facilitator & SME)	Domain Authority / Domain Steward	Information Security / Risk	Business / Data Owners
Define IAM Strategy & Vision	A	R	C	C	I
Develop / Approve IAM Policies (e.g., MFA, SSO, RBAC)	A	R	C	C	C
Define Identity Lifecycle Stages & Triggers	I	R	A	C	C
Maintain Authoritative Sources of Identity Data	I	C	A	C	R
Approve Role Definitions & Access Models (RBAC/ABAC)	C	R	C	C	A
System Onboarding Standards & Integration Criteria	A	R	C	C	C
Platform Configuration & Implementation	A	R	I	C	I
Policy Enforcement & Exception Management	A	R	C	A	C

IAM Risk Assessment & Compliance Mapping (FERPA, HIPAA, CMMC, etc.)	A	R	C	A	C
Monitor and Manage Privileged Access (PAM)	I	R	I	A	I
Identity Verification & Account Claim	I	R	A	C	I
Public Safety / Physical Security	I	C	I	C	I
Review of New App Procurements for IAM Alignment	A	R	C	C	C
Audit Logging, Reporting, and Incident Response	C	R	I	A	I

Legend:

- R = Responsible: owns and executes the work
- A = Accountable: ultimately answerable; approves final output
- C = Consulted: has subject-matter knowledge to contribute; two-way communication
- I = Informed: needs to be kept up to date; one-way communication

Notes:

Institutions may distribute these responsibilities differently; the intent of this RACI is to distinguish between senior domain-level decision authority and operational business ownership.

- The IAM Team / Architect is typically responsible for execution and facilitation, but not the authority for defining business rules. IAM practitioners provide technical, architectural, and operational context to support informed governance decisions.
- CIO or senior IT leadership retains accountability for strategic alignment and policy ratification.
- Domain Authorities / Domain Stewards (e.g., Registrar, CHRO, or equivalent senior leaders) hold decision-making authority for domain-level data, including acceptable use, privacy and regulatory risk, and institutional impact within their area of responsibility.
- Security and risk functions often share accountability for enforcement, compliance, and privileged access controls.
- Business / Data Owners are responsible for the operational ownership of data within defined domains, including data quality, lifecycle processes, integrations, and day-to-day management. These roles are typically held by leaders responsible for the care, feeding, and maintenance of authoritative systems and processes.