

IDENTITY & ACCESS MANAGEMENT.



Every account, role, and permission an organization grants is a potential path in — **and the accounts nobody remembers to review are the ones attackers find first**. IAM turns identity from a one-time provisioning task into a continuously governed control.

- LEAST PRIVILEGE
- PRIVILEGED ACCESS
- ACCESS REVIEWS
- LIFECYCLE AUTOMATION

01 THE MECHANISM

Identity Lifecycle
Provisioning, modifying, and de-provisioning accounts in step with a person's actual role — **onboarding, transfers, and offboarding.**

Privilege Management
Granting **elevated access only for the task and duration required**, then revoking it automatically.

Access Certification
Periodically requiring **managers or data owners to re-affirm** that existing access still matches business need.

02 THE FLOW

The Provisioning Cycle PER IDENTITY

1

A new hire, contractor, or role change triggers an **access request tied to a defined role template.**

2

The request routes to an approver — **typically the manager or resource owner** — before access is granted.

3

Access is **provisioned automatically to match the approved role**, not manually replicated from a peer's account.

The Governance Cycle ONGOING

1

Entitlements are **reviewed on a recurring cycle** against current job function and business need.

2

Dormant accounts, orphaned access, and privilege creep are flagged for removal.

3

Offboarding triggers **immediate revocation across every connected system**, not just the primary directory.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Identity Lifecycle Management	Automates provisioning, role changes, and de-provisioning tied to HR events.
Privileged Access Management	Time-bounds and monitors elevated access to sensitive systems and data.
Access Certification & Review	Requires periodic manager or owner sign-off that access still matches need.
Authentication & MFA	Verifies identity strongly before any access decision is made.

04 ACCESS GOVERNANCE APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Manual Spreadsheet Tracking	No	Falls out of date the moment a role change isn't manually logged.
Copy Access From a Peer	No	Silently replicates years of accumulated, unreviewed privilege creep.
One-Time Provisioning, No Review	No	Access outlives the business need that originally justified it.
Standing Admin Privileges	No	Elevated access sits active and exploitable long after the task is done.
Combined IAM Program (Lifecycle + PAM + Certification + MFA)	Yes	Keeps every account's access matched to a current, approved business need.

IDENTITY & ACCESS.

PROVISION · ELEVATE · CERTIFY

05 PROGRAM OPERATIONS

Orphaned accounts are a leading source of breach. Access that outlives its owner's role is exactly what attackers look for.

Standing privilege is a bigger risk than the access itself. Time-bound, just-in-time elevation limits the exploitable window.

Reviews only work if owners understand what they're certifying. Vague entitlement names get rubber-stamped.

Offboarding speed matters as much as onboarding rigor. A termination that doesn't cut access same-day leaves a live door open.

06 CONTROL MAPPING

NIST SP 800-63

Digital identity guidelines covering authentication and identity assurance levels.

NIST SP 800-53 (AC FAMILY)

Access control safeguards for federal and enterprise systems.

CIS CONTROLS V8.1

Account and access control management safeguards.

ISO/IEC 27001 ANNEX A

Access control policy requirements for certified ISMS.

07 WHAT THIS DOES NOT SOLVE

Compromised credentials with valid access

A stolen but correctly-provisioned credential **still passes every IAM check.**

Excessive trust in a single approver

A rubber-stamp manager approval **defeats the review's purpose.**

Shadow IT outside the identity system

Tools provisioned outside IAM's visibility have **no lifecycle governance at all.**

Business pressure to bypass process

Urgent access requests routinely **skip the queue "just this once."**

08 MYTHS VS. REALITY

MYTH	REALITY
"MFA alone solves identity risk."	MFA verifies who's logging in; it says nothing about what that account is allowed to do.
MYTH	REALITY
"Access reviews are a compliance checkbox."	A rigorous review catches privilege creep that automated provisioning misses.
MYTH	REALITY
"Admins need standing access to do their job."	Just-in-time elevation covers nearly every admin task without leaving access open.
MYTH	REALITY
"Offboarding is IT's job alone."	HR, managers, and IT all own pieces of the timely de-provisioning chain.
MYTH	REALITY
"More roles means more precise access."	Role sprawl without cleanup creates its own kind of unmanaged complexity.

09 SPEAK THE PROGRAM — KEY TERMS

IAM

The systems and processes that **provision, govern, and revoke** user access across an organization.

PRIVILEGED ACCESS (PAM)

Controls that **secure, monitor, and time-bound** elevated administrative access.

LEAST PRIVILEGE

Granting only the **minimum access required** to perform a specific task.

PRIVILEGE CREEP

The gradual accumulation of **unnecessary access** as a person changes roles over time.

ACCESS CERTIFICATION

A periodic review requiring an owner to **confirm existing access is still needed.**

JUST-IN-TIME ACCESS

Temporary, **time-bound privilege elevation** granted only for the duration of a specific task.