

IAM / IGA Glossary

Identity Governance & Administration (IGA)

The discipline and platforms covering identity lifecycle, access certification, SoD, and audit reporting for enterprise access.

Joiner-Mover-Leaver (JML)

The three identity lifecycle events an IGA program automates: onboarding, role/department changes, and offboarding.

Birthright Access

Access automatically granted based on a defined role or job attribute, without an individual request.

Role-Based Access Control (RBAC)

Assigning access through roles mapped to job functions, rather than granting entitlements one at a time.

Attribute-Based Access Control (ABAC)

Access decisions driven by attributes (department, clearance, project) evaluated at request time, complementing RBAC.

Segregation of Duties (SoD)

A control preventing one identity from holding two entitlements that together create a fraud or error risk.

Access Certification / Access Review

A periodic process where a reviewer confirms that existing access is still appropriate.

Entitlement

A specific, grantable unit of access within a target system or application.

Entitlement Catalog

A centralized, business-readable inventory of entitlements across applications, used for

governance and certification.

Identity Warehouse

The aggregated, current record of every identity and its access, built from authoritative sources and reconciliation.

Provisioning / Deprovisioning

Granting or removing access in a target system, typically automated by an IGA platform.

Reconciliation

Comparing what an IGA platform believes a user has against the target system's actual access state.

Connector

The integration component that lets an IGA platform provision, deprovision, and read access in a target system.

Disconnected Application

A system with no automatable connector, requiring manual, SLA-tracked access fulfillment.

Authoritative Source

The trusted system of record (typically HR) that drives identity lifecycle events.

Non-Human Identity / Service Account

An identity representing a system, application, or automated process rather than a person, requiring its own governance model.

Least Privilege

Granting only the access required to perform a role, and no more.

Privileged Access Management (PAM)

Controls -- vaulting, session isolation, just-in-time access -- for administrative and other high-risk credentials.

Zero Trust

A security model that evaluates every access request on identity and context, rather than trusting network location.

SCIM (System for Cross-domain Identity Management)

A standard protocol and schema for provisioning identities between systems.

OAuth 2.0

An authorization framework allowing an application to access resources on a user's behalf via tokens.

OpenID Connect (OIDC)

An identity layer on top of OAuth 2.0 that adds authentication (who the user is) to OAuth's authorization model.

Single Sign-On (SSO)

Authenticating once to access multiple applications, typically via a federated identity provider.

Federation

Trusting an external identity provider's authentication rather than maintaining separate credentials per application.

Policy Decision Point / Policy Enforcement Point

The component that evaluates an access policy (PDP) and the component that enforces its decision (PEP) at the resource.