A GATHID LABS SERIES: A GLOSSARY

Get AI Ready with Gathid

A Glossary of AI and Identity and Access Terms

Term	Definition
Artificial Intelligence (AI)	A field of computer science that simulates human intelligence in machines. AI systems can analyze data, learn from interactions, and make decisions, enabling automation and predictive insights across various domains.
Identity Governance (IG)	Identity governance is the framework and set of processes that ensure that user access is maintained in compliance with organizational policies and regulatory requirements. It manages the lifecycle of identities through role assignments, access reviews, and certifications. Identity governance reduces the risk of unauthorized access, improves operational efficiency, and supports audit readiness, making it a critical component of an organization's overall security strategy.
Identity and Access Management (IAM)	A collection of technologies and processes within the Identity Governance framework, enabling and ensuring that the right individuals or entities have the appropriate access to the right resources. IAM reduces risks associated with unauthorized, and non-compliant access and improves access facilitation within an organizations Joiners, Movers and Leavers (JML) processes.
Knowledge Graph	A structured representation of related entities, their associated metadata, and their relationships to other data. In Identity Governance, knowledge graphs enable visibility through the virtual relationships between users, permissions, and resources, enabling relationship-based access insights.
Digital Twin	In the case of Identity Governance, digital twins present a virtual replica of the accounts and access levels within a physical or digital system. They are often used for user access policy simulation and monitoring. Enable cross-functional visibility while maintaining holistic access compliance.

Term	Definition
Non-Compliant Access	Access that violates organizational policies or regulatory requirements. This can include overly broad permissions, dormant accounts, or unauthorized system interactions, posing security and compliance risks.
Contextual Richness	The depth of information provided by a system, such as a knowledge graph, to understand attributes, relationships and interactions between entities. In Identity Governance, contextual richness ensures access decisions are informed by comprehensive related data, from one or many sources.
Dormant Accounts	An account that remains active but unused for an extended period. Dormant (aka stale) accounts are a common source of non-compliant access and pose security and financial risks if not properly managed.
Cross-Functional AI	AI systems that operate across multiple business domains or departments. While enabling collaboration and insights, cross-functional AI requires stringent access controls to prevent unauthorized data exposure.
Permissions	The specific rights, access levels, or privileges granted to an identity to access a system, resource, or data. Permissions must align with roles and responsibilities to maintain compliance and minimize risks.
Access Simulation	The use of tools like digital twins to replicate and analyze potential access scenarios. Simulations identify vulnerabilities and refine Identity Governance policies before deploying AI or other systems in live environments.
Dynamic Boundaries	Adaptive access controls that adjust based on context, roles, or changing conditions. Dynamic boundaries prevent unauthorized interactions between systems, especially in cross-functional AI deployments.
Operational Technology	Hardware and software that monitors or controls physical processes in industries such as manufacturing. OT access is critical in IAM to ensure that machines and systems are secure and compliant.

Term	Definition
Internet of Things (IoT)	A network of interconnected devices that collect and exchange data. In IAM and especially in the Industrial Internet of Things (IIoT), devices require secure identity governance to prevent unauthorized access to high-risk enterprise systems and assets.
Attribute Based Access Control (ABAC)	An access control method that dynamically analyzes permissions based on attributes about the identity and the access they fold. ABAC provides more granular control over identities and their appropriate level of access cross-functionally within the enterprize.
Role Based Access Control (RBAC)	An access control method that assigns permissions based on roles within an organization. RBAC ensures that identities have only the access necessary to perform their duties.
Supply Chain Optimization	The use of AI to analyze and improve supply chain processes. In IAM, secure access to inventory, logistics, and vendor data is essential for effective optimization.
Compliance Audit	A systematic review of policies, procedures, and systems to ensure adherence to regulatory and organizational standards. Identity Governance tools, including knowledge graphs and digital twins, help prepare for audits by maintaining clean, compliant access records.
AI-Driven Risk Mitigation	The use of AI to identify and address potential security and compliance risks. By integrating Identity and access (IAM and IG) insights, AI systems can prevent unauthorized access and streamline identity management.

Schedule a Demo | Learn More | Read Online