PATECCO
dynamic identity systems.

Who Has Access vs. Who Should - Key Differences Between Identity Management and Identity Governance

	Identity Management ➢ *Who gets access and how?*	Identity Governance ➢ *Should they have access?*
Primary Objective	Granting and managing access to systems, applications, and data	Governing who has access, why, and whether that access is appropriate
Core Functions	✓ User and role lifecycle ✓ Authorization handling ✓ Enforces access rules	✓ Access reviews and certifications ✓ Policy checks and risk analysis ✓ Role management ✓ Audit and reporting
Focus Area	Operational efficiency and security	Risk management, policy enforcement, and regulatory compliance
Scope of Access Control	Assigns access based on roles or attributes	Evaluates and validates access appropriateness continuously
Compliance and Audit Support	Basic logging	Detailed audit trails and compliance reporting
User Lifecycle Management	Automates provisioning, deprovisioning, and updates	Oversees access lifecycle from a compliance perspective
Visibility and Insight	Operates on real-time identity processes	Provides historical, contextual, and policy-based visibility into access
Risk Management	Limited - focuses on access provisioning	High - focuses on who should have access?
Business Value	Improves user productivity and operational control	Ensures access accountability and aligns IT with regulatory and business risk objectives

www.patecco.com

Tel.: +49 (0) 23 23 - 9 87 97 96

Ringstrasse 72 - 44627 Herne

E-Mail: info@patecco.com