gathid
GATHERED IDENTITIES

WHITEPAPER

From Identity Management to Access Governance

The Fast Track to Visibility, Compliance, and Control

gathid.com info@gathid.com

gathid
GATHERED IDENTITIES

From Identity Management to Access Governance

The Fast Track to Visibility, Compliance, and Control

Executive Summary

Identity Management (IDM) and Access Governance have traditionally been treated as distinct disciplines. IDM has focused on provisioning and user efficiency, while Access Governance has addressed compliance, visibility, and control. However, in the face of growing regulatory pressure, cybersecurity threats, and the complexity of hybrid environments, these disciplines are now converging to ensure a unified, secure, and scalable identity strategy.

This whitepaper explores how organizations can evolve from traditional IDM practices to a modern, governance-first identity model. It examines the limitations of legacy IDM systems, defines the core principles of effective Access Governance, and presents a practical path to achieve meaningful outcomes—such as continuous visibility, policy compliance, and rapid time-to-value—across both connected and disconnected systems.

The Evolution and Limits of Identity Management

To understand why a shift from identity management to access governance is essential, it's crucial to first revisit the origins of identity management itself.

In the early days of enterprise IT, most systems and applications had their own proprietary, embedded identity stores. Each system managed its own user database, authentication, and permissions independently.

This created a sprawling, inconsistent access environment that was difficult to manage and secure. Centralized identity directories (like NIS and LDAP) eventually emerged to provide a single point of reference for user identities. However, these central directories were unable to directly provision users or manage entitlements across every proprietary system. This gap led to the rise of connector-based identity management platforms.

These identity management platforms relied on specialized connectors to translate provisioning actions from a central IDM system into the specific format and protocol required by each endpoint system. Connectors became the backbone of traditional IDM. The problem was: they were complex, brittle, and expensive to maintain. They also introduced security concerns because many required elevated privileges and direct access to production systems.

Today, many provisioning endpoints have evolved to expose more standardized interfaces, and cloud identity providers have become more common. This shift has made the traditional connector-based model increasingly obsolete. As a result, organizations are now seeking lighter, more agile governance approaches that avoid the fragility of connectors and instead focus on modeling access using available data—regardless of where it comes from.

While identity management systems have played a crucial role in streamlining operational workflows, they remain limited in their ability to deliver continuous visibility or enforce granular governance policies. As organizations grow and adopt more complex hybrid environments, the need for access governance becomes clear—not just as an extension of identity management, but as a distinct control layer.

The Emergence of Access Governance

Access governance emerged as a discipline to address the growing need for visibility, control, and accountability in increasingly complex IT environments. While identity management focused on provisioning and de-provisioning users, it lacked the ability to enforce policies, track access over time, or assess whether entitlements aligned with business risk. Access governance filled this gap by introducing a layer of oversight—enabling organizations to answer critical questions like who has access to what, why, and whether that access was appropriate.

Access governance focuses on defining, monitoring, and enforcing policies regarding user access rights across the entire organization.

Access governance plays a critical role in meeting compliance obligations. Regulations such as Sarbanes-Oxley (SOX), HIPAA, and GDPR require organizations to prove that access to sensitive data and systems is properly controlled and monitored. Access governance provides the structure needed to enforce these controls—ensuring access is granted based on clear policies, continuously monitored for potential violations, and promptly corrected when issues arise.

One of the key challenges of access governance is that it often involves systems (like physical or air-gapped systems and applications) that are disconnected or isolated from the centralized identity management system. This makes it difficult to achieve a holistic view of user access across the entire organization. Additionally, traditional identity management systems often struggle to handle the granular access controls required for compliance, such as conditional access based on factors like business role, third-party access or completion of mandatory training.

Why Integration Attempts Fall Short

While the appeal of a unified platform that seamlessly combines identity management and access governance is compelling, achieving this integration in practice has often been more challenging than expected. The business drivers behind identity management and access governance are often quite different, making it difficult to successfully integrate these two disciplines into a single platform.

Identity management is primarily focused on efficiency and user experience. Organizations implement IDM systems to streamline the process of user provisioning, reduce operational overhead, and ensure that users have appropriate access to systems and applications. The goal is to increase the speed and accuracy of user account management, often by automating repetitive tasks and reducing manual intervention.

In contrast, access governance is driven by security and compliance. The focus is on ensuring that users have the appropriate level of access based on their roles and responsibilities and that access is continuously monitored to detect potential security risks or compliance violations. Access governance requires a higher level of granularity and control, as well as the ability to enforce policies across disconnected systems and applications.

These differing business drivers have made it challenging to unify identity management and access governance into a single platform. Organizations often find that the complexity of integrating the two systems outweighs the potential benefits, particularly when legacy systems are involved or when access governance requirements are more granular than traditional IDM systems can handle.

Trust-Based Access and Governance: A Modern Approach

Given the limitations of traditional identity management systems and the challenges associated with integrating access governance, it is clear that a new approach is needed. Rather than relying solely on legacy IDM solutions, organizations can benefit from a more modern, trust-based approach that puts governance at the center of identity and access control.

Trust-based access governance represents a new approach to managing identity risk—one that eliminates traditional integration barriers and rethinks how organizations achieve visibility and control.

Instead of connecting to and controlling every system directly, this model starts by ingesting access data from wherever it resides—whether it's a cloud identity provider, an on-prem directory, an ITSM workflow, a physical access control system, or a user list in a legacy application. If the data can be exported, it can be modeled.

By creating a digital twin of real-world access, organizations gain a comprehensive, connected view of all users, systems, and entitlements. Access policies and controls are then validated against this model—allowing governance actions to be automated, monitored, and improved without requiring intrusive or high-risk integrations.

This decoupled architecture supports visibility across modern cloud environments, hybrid IT stacks, and historically disconnected domains like OT and PACS. It breaks the mold of traditional projects

that require months of design and connector development, and replaces it with an agile, "map first, ask later" methodology.

Organizations can begin asking (and answering) meaningful questions about their access landscape immediately—without rewriting their infrastructure or waiting to complete complex deployments.

Implementation Considerations

Organizations don't need to abandon their existing IDM infrastructure to adopt access governance. Instead, they can augment their existing systems with an independent governance layer that extracts identity and access data through non-intrusive methods to enhance visibility, control, and policy enforcement.

Governance platforms built on modern principles can ingest flat files, exports, or API responses from authoritative systems without requiring elevated privileges, agent deployments, or invasive integration projects. This makes it feasible to bring air-gapped, legacy, or operational technology environments into the access governance scope.

What makes this model particularly powerful is that it flips the traditional implementation methodology on its head. Rather than starting with weeks or months of discovery, requirements gathering, and detailed design documentation, trust-based access governance begins by ingesting and modeling existing data. If the access data can be exported, it can be analyzed—immediately.

This means teams can explore their access landscape immediately, asking live questions of the digital twin:

- Where are the highest concentrations of privilege?
- Where are policy violations likely to occur?
- Are there orphaned accounts, or excessive entitlements in sensitive systems?

This "model first, question later" approach delivers immediate visibility and uncovers governance opportunities that might otherwise go undetected for years.

Organizations should begin by establishing a baseline—an inventory of accounts, access rights, and role mappings across core systems. Once a digital twin of the current state is in place, they can introduce automation in phases: access review workflows, policy enforcement, segregation of duties analysis, and remediation alerts.

Critically, this rollout can be driven by business risk. Teams may focus first on privileged accounts, regulated systems, or departments with known compliance obligations. Over time, coverage can expand as the organization gains confidence in its access governance maturity.

This flexible, modular approach avoids the pitfalls of large-scale identity projects. It allows for early wins, lower risk, and alignment with audit cycles and security roadmaps.

Real-World Examples from the Field

Energy and Utilities Sector

In organizations that are responsible for operating critical infrastructure—such as utilities and energy providers—access governance is complicated by legacy control systems, regulatory mandates, and physical access control systems that are often air-gapped from IT environments. A modern, trust-based governance layer enabled one such organization to ingest access records from SCADA systems, Active Directory, and badge entry systems without requiring connector-based integrations. This visibility allowed the organization to uncover previously undocumented privileged access paths and non-compliant roles—achieving audit readiness in a matter of days.

Global Financial Institution

A multinational bank adopted a digital twin approach to accelerate its compliance with evolving SOX and GDPR requirements. By modeling access across their HR systems, cloud platforms, and local directories, the institution was able to enforce fine-grained entitlements and automate segregation-of-duties enforcement. The deployment required no changes to source systems and gave internal auditors daily identity and access maps to validate controls.

These real world examples demonstrate how a trust-based access governance model can deliver rapid, meaningful outcomes—even in complex, highly regulated environments. By decoupling governance from legacy IDM systems, organizations gained immediate visibility, uncovered hidden risks, and met compliance obligations without disrupting existing infrastructure.

Conclusion: Access Governance as a Strategic Enabler

Modern access governance flips the traditional identity management model on its head. Rather than starting with lengthy requirements and integration roadmaps, it begins by modeling what already exists. If access data can be exported, it can be analyzed—and questioned.

This "model-first" approach accelerates insight, enabling organizations to detect risk, validate compliance, and empower decision-makers quickly and confidently. It decouples governance from identity delivery and enables broad oversight across systems that were previously out of reach.
In a world where identity is the new perimeter, access governance is the control plane. Those who embrace this shift early will not only improve their security posture—they will redefine how identity risk is managed across the enterprise.

Call to Action

If you're rethinking your approach to identity, start with the one thing that changes everything: visibility. Trust-based access governance doesn't begin with integration—it begins with insight. By modeling your identity data as it exists today, you can identify risks, streamline compliance, and understand access across disconnected systems—all before committing to complex architectural changes. Request a baseline access snapshot. Interrogate your access data. Explore what's really happening in your environment—and decide your next move with clarity.

To get started, contact your identity governance advisor or reach out to Gathid for a no-integration assessment.