MajorKey CYBERARK

The Next Evolution of Identity Governance

A practical guide for IAM leaders moving from manual complexity to scalable, automated, audit-ready identity governance.

INTRODUCTION

When Identity Becomes Infrastructure

Managing identity is no longer just about granting access. It is about protecting the connective tissue of the business. However, every new hire, contractor, SaaS application, entitlement, and non-human identity adds complexity and risk. What was once manageable through manual processes has become a sprawling ecosystem of users, systems, policies, and compliance obligations.

The challenge is not simply controlling access. It is gaining the ability to define, enforce, and **verify who** has access to **what**, and **why**, with confidence and consistency. Modern identity governance provides that clarity by **embedding visibility, automation, and accountability into security and operations** in a way that strengthens security, supports compliance, and scales with the business.

This guide outlines a practical path for evolving identity governance from manual and reactive to **automated, AI-powered, scalable, and audit-ready**. It is designed for IAM leaders responsible for identity processes, compliance outcomes, and business alignment.

Table of Contents

PART ONE

Today's Toughest Identity Governance Challenges

Even experienced IAM teams face friction as identity environments grow. The main issue is rarely lack of expertise. It is scale.

Shadow IT and Application Sprawl

Business teams adopt SaaS tools faster than IT can track them. Application inventories quickly fall out of date, and visibility gaps weaken governance and risk management.

You cannot govern what you cannot see.

Bottlenecked and Inconsistent Onboarding

When applications compete for limited integration resources, onboarding slows. Legacy systems require custom work. Requests pile up, productivity stalls, and manual effort increases.

Delayed access is more than an inconvenience. It is a governance and productivity risk.

Manual Process Overload

As applications and identities multiply, access reviews and entitlement mappings become repetitive and error prone. Manual fatigue leads to inconsistent decisions and elevated risk.

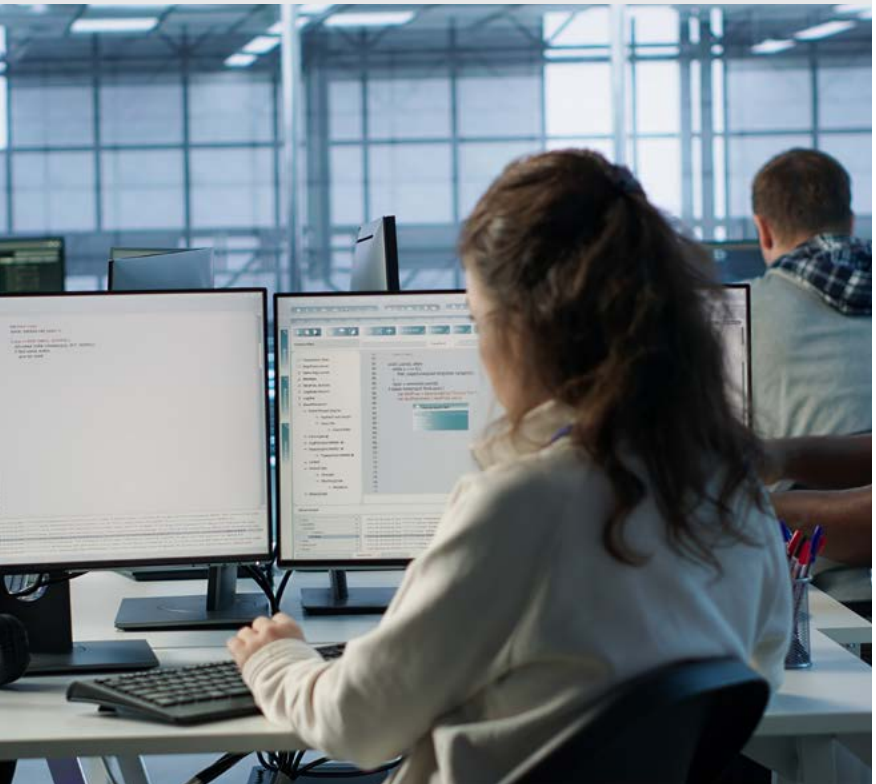
Manual effort does not scale, and inconsistency is where risk hides.

These challenges are systemic and widespread. They are the direct result of growth without automation. **Manual governance cannot keep up with this scale.**

PART TWO

Why Automation and AI Matter Now

Manual identity management does not scale to modern environments. **Automation and AI provide the speed, consistency, and visibility** required to meet audit and compliance requirements without adding headcount.



Automated Application Discovery and Onboarding

Outdated spreadsheets and static app lists are no longer effective. Integration is the answer, but it can be challenging. CyberArk ZUS (formerly Zilla Universal Sync) quickly onboards applications without standard user-management APIs, ensuring continuous visibility.

ZUS automatically discovers and standardizes entitlement data across cloud, custom, and on-prem apps, enabling IAM teams to create a **dynamic, organization-wide system of record for governance**. This inventory supports **value-based onboarding**, so teams can prioritize based on business impact and risk.

With accurate entitlement data, CyberArk IGA supports policy-based access decisions, automated workflows, and clear reviews. Identity teams and app owners can manage onboarding, reduce delays, and improve governance.

The result: **Broader, faster application coverage, better alignment with business goals, and identity programs that provide clear value rather than just incremental compliance.**

Smarter Role Management with AI

AI-driven insights eliminate guesswork and can be applied in the following ways:

- Role mining reveals real access patterns
- Dynamic roles evolve with organizational change
- Intelligent approval routing ensures the right decisions reach the right owners.

The result: **Cleaner entitlements and more meaningful access reviews.**

PART THREE

Compliance, Under Control

When identity governance is heavily manual, compliance becomes a recurring disruption. Teams scramble to gather evidence, track down application owners, reconcile spreadsheets, and justify inconsistent access decisions under tight audit timelines.

A**utomation changes this dynamic**. When governance controls are embedded into everyday identity processes, compliance is no longer a periodic event. It becomes a **continuous outcome of how access is requested, reviewed, approved, and adjusted** across the environment.

This approach enables:

- **Risk-focused access reviews** that prioritize meaningful exceptions instead of volume
- **Consistent and repeatable review decisions** driven by policy rather than interpretation
- **Audit-ready evidence** captured automatically through normal workflows
- **Reduced reliance on spreadsheets** and manual attestations

With automation in place, access certifications are easier to execute and produce more defensible results. Reviewers are able to focus on what matters. IAM teams spend less time assembling proof and more time addressing real risk. Audits become more predictable, less disruptive, and easier to support with confidence.

When compliance is embedded into daily identity workflows, the conversation shifts from simply passing audits to more strategic issues such as how identity governance is owned, operated, and scaled.

PART FOUR

Identity Governance as an Operating Model

The next evolution of identity governance is not simply about improving compliance outcomes. It is about **establishing a sustainable operating model** that aligns identity, risk, and business velocity at scale.

As environments decentralize, IAM leaders need to move past managing individual controls and **focus on governance as a continuous discipline**. Automation and AI embed governance into access requests, approvals, and reviews across the organization.

In a mature model, identity governance shifts to an integrated control layer supporting daily operations and clear accountability.

- **Shift focus from processes to outcomes** and redirect the effort toward meaningful exceptions and risk reduction, rather than repetitive, low-value approval cycles
- **Establish consistent accountability** across application owners, reviewers, and identity teams by engaging them with features like application onboarding nominations
- **Demonstrate governance value** in terms the business understands, including reduced exposure, improved efficiency, and faster access enablement by rapidly onboarding apps and using AI-based role mining

With governance embedded into normal identity workflows, IAM teams can scale without adding complexity, making identity decisions more intentional, defensible, and aligned with changing business needs. As a result, identity governance shifts from a reactive function to a strategic control capability that supports growth while maintaining trust, consistency, and control across the enterprise.

CONCLUSION

Next Steps for Modern Identity Governance

Modern identity governance means consistent access control, clear risk visibility, and scalable processes. By embedding automation and AI, IAM leaders move beyond manual oversight toward continuous compliance and intentional decisions.

Governance becomes a resilient, strategic operating model that replaces periodic reviews with ongoing control that supports security, compliance, and business growth. Now is the time to transform from manual functions to scalable, outcome-focused governance aligned with evolving needs.

Take the Next Step

If your organization is ready to modernize identity governance, **MajorKey can help**.

Working alongside CyberArk, we partner with IAM leaders to **assess current maturity, modernize governance processes, and implement automation-driven identity programs** that scale with the business and stand up to audits.

Scan the QR code or click here to contact us and learn more.

Visit our resource hub for additional governance resources with CyberArk