WHITE PAPER

# Why Legacy IGA Fails in the Modern Cloud Era

## About

This white paper outlines why a modern IGA solution is essential for security, compliance and operational efficiency. It also explains the importance of IGA automation to keep up with the pace of business and avoid the challenges of legacy IGA deployments.

## Introduction

Identity Governance and Administration (IGA) solutions have existed for over 20 years, and these solutions came about for a reason: ensuring job-appropriate user permissions and reviewing them for compliance is complex. This is due to factors such as the intricacies of role and group membership, proliferation of enterprise apps, and personnel change as employees join, leave, or move within the company.  However, the IGA space has failed to keep up with the evolving security requirements of a cloud-first world, the immense growth in SaaS and cloud infrastructure usage, and the increasing decentralization of application ownership. This has left the state of identity management in a similar crisis to the one that brought the need for IGA in the first place: chaotic, manual, expensive and rife with potential security gaps.

**What is needed is a new approach to IGA**. One which still takes into account the core business needs around processes for managing compliance (primarily through user access reviews), provisioning, and security, but that is purpose-built for the modern hybrid enterprise. This new and needed approach is known as Modern IGA, an automation-centric strategy that eliminates repetitive manual work and ensures that organizations aren't overwhelmed by access reviews, provisioning tickets, and identity exposures.

## How IGA Evolved

*Solving Identity and Compliance Complexity*

Identity Governance and Administration emerged as a category of solutions within the broader identity market. Initially, IGA was designed to address regulatory compliance needs within IT environments driven by the Sarbanes-Oxley Act (SOX). It became required for companies to  audit user access to IT infrastructure and applications.

Due to its focus on access, specifically monitoring and remediating permissions, the IGA market evolved from a heavily compliance-oriented tool to a space that also supported access administration for business enablement. As a result, many IGA vendors started offering provisioning capabilities. The complexity of enabling business users one permission at a time, led organizations to explore the concept of roles, as permission bundles. And while the idea of roles scoped to a single application worked, the IGA ecosystem struggled to deal with business roles for managing job-appropriate access across multiple applications. Defining these business roles was hard, and finding people who could own and maintain them was virtually impossible.

**IGA solutions became a common requirement for regulated companies at a time when on-premises and data-center-driven architectures were the norm.** During these early days of IGA, there were fewer enterprise applications, many of which were managed by IT directly. The first IGA solutions were designed with this structure in mind. These solutions were deployed on-premises and needed significant manual effort to deploy and maintain.

**The Cloud Changed the Identity Landscape.** As the on-premises centric enterprise adopted IGA, the IT environment changed - into a hybrid cloud enterprise with a sprawling and increasingly complex estate of infrastructure and apps, and a decentralized ownership and administration model. And identity became the new security perimeter.

**Legacy IGA tools didn't grow with the complexity, decentralization and security needs of the hybrid enterprise.**

## Businesses Feel the Pain of Legacy IGA

In recent years, the limitations of traditional, or legacy, IGA, have become very apparent, and have been painful for identity teams. Without an automated solution that fully integrates with the enterprise digital estate, identity teams are left dealing with an insurmountable burden of manual compliance, administration and security tasks.

The most significant IGA challenges that plague today's identity teams are:

- ✓ The lack of continuous integration across the enterprise IT infrastructure
- ✓ The difficulty of managing roles
- ✓ The need to address identity as the new security perimeter
- ✓ The complexity of deploying and maintaining legacy IGA

### *Legacy IGA Lacks Continuous Integration*

Modern enterprises often have a mix of apps, including cloud-based, on-prem, and homegrown applications, all of which are hard to integrate into legacy IGA systems. New applications are added every day by users across the organization, often managed outside of IT. The resulting impact of this app sprawl and decentralization is that the team that manages the IGA solution is left chasing application owners across the enterprise for information about permissions.

### *Legacy IGA Doesn't Solve for the Difficulty of Role Management*

While the concept of Role Based Access Control or RBAC, has long been a cornerstone of access management within organizations, it has proven to have significant limitations. Since the context to define and maintain roles scoped to a single, narrowly-purposed application often lies with an application owner, application-specific RBAC is often straightforward. However, defining and maintaining business roles with a broad scope across many cloud and on-prem applications is much more challenging – there is usually no person or team that has the context to own and maintain a business role.

Furthermore, as users move within the organization and new applications are introduced, the constant need to update business roles becomes overwhelming. Maintaining up-to-date lists of current members and permissions across multiple applications requires meticulous attention and frequent communication with application and data owners. In many cases, the staff who led the initial role deployment effort find themselves locked into a new task: full-time role maintainer and data/application owner chaser.

*Legacy IGA Doesn’t Focus on the Identity Security Perimeter*

In today’s “zero trust” world, identity has become the new security perimeter and is quickly becoming the single (primary) control point for IT security. In fact, research has shown that most cloud data breaches are rooted in access exposures, and that identity is now recognized as the most critical security vector. Legacy IGA solutions were not designed to support the security posture use cases that identity raises today. They don’t integrate out-of-the-box with many cloud infrastructure services and most SaaS applications, which limits their ability to monitor the enterprise identity posture and proactively detect and respond to identity threats.

*Legacy IGA is Hard to Deploy and Maintain*

Legacy IGA solutions have proven highly expensive, time-consuming, and difficult to maintain, often requiring episodic, one-off efforts and a significant amount of manual work (and highly trained professionals) even after a successful initial deployment.

## Identity Providers don’t meet the IGA bar

Identity Providers (IdPs) were conceived as modern directories for the cloud. IdPs excel at supporting use cases around directory, authentication and single-sign-on (SSO), and can even deliver identity lifecycle management to support SSO. But IdPs fall well short of meeting IGA requirements around compliance, provisioning and security, because they have a limited permissions model.

IdPs have a simple-minded view of permissions. They think of infrastructure and application permissions as accounts or groups that can simply be synced to IdP objects. IdP vendors claim to support modern IGA, but a majority of permissions in an enterprise are fine-grained permissions linked to accounts – they are not merely accounts and groups themselves. Enterprise use cases around audit, compliance, and least-privilege security demand a complete and accurate view of permissions, which IdP IGA can’t provide.

## Breakthrough Identity Governance Automation - A New, Modern Approach to IGA

What identity teams need, then, is a new approach to IGA. An approach that is purpose-built for the cloud and app era. In fact, this new approach for IGA - Modern IGA, is ideally anchored in automation that enables identity teams to manage key centralized business processes for compliance and access administration while also enabling the proactive security monitoring and remediation that is required to prevent data breaches.

Here are some core features that differentiate the approach of modern IGA from legacy IGA.

### App Integrations

Legacy IGA struggles with continuous app and infrastructure integration, often failing to keep up with the rapid adoption of cloud-based and home-grown applications. Modern IGA solves this by offering comprehensive coverage through no-code integrations based on APIs and robotic automation (the Zilla Universal Sync™ capability offered by Zilla Security is one such example). This allows organizations to onboard applications swiftly and efficiently, enabling ongoing integration across diverse app environments.

## AI-driven Role Management Profiles

Managing roles is a significant challenge in traditional IGA solutions. Modern IGA solutions use AI and Machine Learning to address this issue by automating the discovery and maintenance of business roles. AI-driven solutions (as demonstrated, for example, by Zilla AI Profiles™) continuously adjust user roles to ensure least privilege access, dramatically reducing the manual effort required to manage roles.

## Pre-approved Access

Modern IGA solutions ensure that role definition occurs in collaboration with application and data owners, so that the roles in deployment represent pre-approved access. This reduces the approval workload for joiners and movers by up to 75%, ensuring that access rights are granted more efficiently while maintaining least-privilege security.

## Identity Mapping

Managing both human and non-human identities with legacy IGA is very challenging. Modern IGA provides a comprehensive view of identities across the enterprise, mapping directories, roles, groups, granular permissions and the lineage of human and non-human accounts. This continuous monitoring enhances the organization’s ability to manage complex identity structures and identify excessive or rogue access (which are often overlooked by legacy systems).

## Reduce Risk

Traditional IGA solutions lack proactive measures to address identity risks, relying on periodic compliance initiatives to catch exposures. Modern IGA solutions support configurable policies  that fix misconfigurations before they lead to breaches. These policies can quickly identify and remediate misconfigurations, alert security staff or kick-off appropriate security workflows. The best-in-class tools offer both built-in policies that support the most common use cases while also enabling custom policy configuration. Zilla’s security module is an example of a robust, modern security policy engine as required for a modern IGA solution.

## Audit Evidence

Legacy IGA solutions often fail to support identity teams in their effort to meet audit requirements around accuracy and completeness. Modern IGA tools offer automated evidence gathering and packaging features that generate a detailed, auto-populated audit trail, capturing hard-to-track access details. This single system of record simplifies audits and eliminates the time-consuming manual processes associated with gathering evidence for auditors.

## Modern IGA Organizational Advantages

### *A New Approach for Access Reviews*

With Modern IGA, access reviews can be truly automated end-to-end, saving compliance teams valuable time and effort.

| Legacy IGA | Modern IGA |
|---|---|
| Manual data collection, correlation and campaign prep. | No-code integration, including robotic automation |
| Reviews burden and annoy business | Reduced burden with pre-approvals |
| Hard to make Auditors happy | Auditor-ready evidence |

### *A New Approach for Provisioning*

Modern IGA simplifies joiner-mover-leaver processes through AI-powered profiles, built-in integration with ITSM systems and automated change fulfillment. IT teams have become the de-facto owners of access provisioning and face ticket overload, and they also lack the context to make accurate access decisions across hundreds of applications and thousands of granular entitlements. The best modern IGA solutions help automate and manage that process via:

- **User lifecycle management with Joiner, Mover, and Leaver Policies:** Identity teams need configurable workflows to create JML (Joiner, Mover, Leaver) policies, ideally based on business profiles. They also need native ITSM integration so that there is a single system of record for ticketing and change auditing.
- **Self-Service Access Requests: Access Requests:** Even AI-profile based automation won't give users all of the access they need to do their jobs. Users need to be able to request application access with automated approval and fulfillment workflows.

| Legacy IGA | Modern IGA |
|---|---|
| Slow to grant access | Automated job-appropriate access |
| Hard to grant deep and broad access | Comprehensive granular provisioning |
| Can't track and validate changes | Single source of permission truth |

### *A New Approach for Security*

Modern IGA provides the visibility, monitoring, and remediation that security teams need to feel confident that their enterprise identity perimeter is secure.

| Legacy IGA | Modern IGA |
|---|---|
| ✓ Don’t know identity & access posture | ✓ Continuous entitlement monitoring |
| ✓ Lack visibility into high-risk changes | ✓ Continuous threat detection |
| ✓ Excessive & rogue permissions go unremediated | ✓ Single source of truth & change history |

## Conclusion

Identity Governance and Administration emerged as a much-needed solution for identity compliance and access administration, and it continues to be important for the modern enterprise. However, legacy IGA systems that were designed for the on-premise era are no longer equipped to handle the compliance, provisioning, and security requirements of the hybrid, decentralized, and sprawling IT landscape.

Modern IGA, on the other hand, addresses both the original access challenges that sparked the creation of IGA, but also solves for the limitations of legacy IGA. Businesses who want to remain compliant with regulatory needs, provision faster, and secure their identity perimeter can confidently do so with modern IGA.

If you’re interested in a Modern IGA solution, reach out to the Zilla Security team today. They offer a robust modern IGA solution that is equipped for today’s enterprise needs.