CYBERARK®
THE IDENTITY SECURITY COMPANY

MajorKey

eBook

Signs Your IGA Program Needs a Reboot

Table of Contents

Why You Need a Modern IGA Program

Identity Governance and Administration (IGA) is 100% focused on minimizing the problems and complications of identity and access management in the enterprise. Modern IGA is ideal for solving several key business problems:

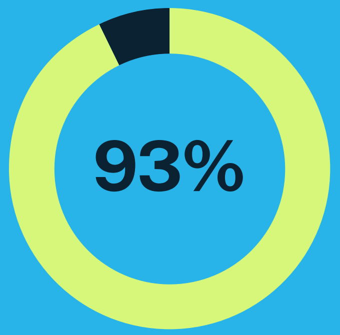
- Performing effective **user access reviews** for both compliance and security purposes.
- Efficiently executing **user access changes** for employees and contractors who are joining the organization, leaving the organization, or changing roles within it.
- Gaining **visibility** into all entitlements and identities across the enterprise, including machine identities.
- Maintaining **identity security** within the organization by discovering and reducing identity vulnerabilities.

User access reviews are a critical element of most compliance initiatives as well as being important for cybersecurity. An IGA program centralizes existing permissions, organizes the review process reviews, revokes permissions that shouldn't have been granted, and documents the process for internal and external auditors. Compliance requirements are broad, including standards such as SOX, PCI-DSS, GDPR, HIPAA, DORA, and others.

User access changes are ongoing activities, and mistakes or delays can impact employee productivity. An IGA program helps accelerate user access changes while reducing errors and ensuring least-privilege access across the user lifecycle.

Identity security is critical because identity-related vulnerabilities are the leading vector for cybersecurity attacks. These vulnerabilities include excess privileges, orphan accounts, service accounts that are improperly managed, inappropriate use of group accounts, and many more. An IGA program provides visibility and governance of the identity environment to minimize the risk of attack.

Despite the value of an effective IGA program, many organizations struggle to successfully implement one. For example, in a recent survey, just 6% of respondents said they had their IGA processes fully automated (Source: 2025 State of IGA Survey Report). However, the benefits of a modern IGA program are numerous: you'll get thorough and robust automation via extensive built-in integrations, AI-based accelerators for provisioning and users reviews, and automated data collection to demonstrate security and regulatory compliance. Are you ready?



93% of companies have suffered two or more identity breaches in the last year.[1]

[1] CyberArk, Identity Security Threat Landscape Report 2024, 2024

The Key Signs That You Need to Push the Reboot Button on Your IGA

1 You don't have visibility into who has access to what

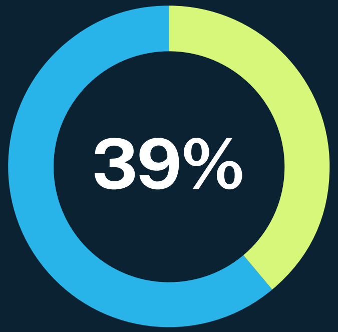
This is a problem if you're fundamentally unable to answer seemingly straightforward questions such as:

- What are all the applications and permissions that a particular user has access to?
- Which users, including machine users, have privileged access to the following list of applications?
- What are all the critical applications and privileged users in my organization?

2 You've had unfavorable audit findings or excessive back-and-forth

Unfavorable audit findings are reflective of deficiencies in governance and security — plus they're embarrassing. And even when there are no problematic findings, excessive back-and-forth with auditors is disruptive and expensive. Everything "under the hood" might be executed correctly, but you may still have an insufficient amount of evidence being collected to establish that fact.

Modern IGA not only helps maintain controls properly, it documents each update, and it helps collect evidence in a package that can be easily consumed by an audit team.



Identity leaders say the effort required to satisfy auditors is high, 39% struggle to keep up, and it's getting harder.[2]

[2] Cyberark, 2025 State of IGA Survey Report, 2025

3 You’re doing IGA by hand, e.g. with spreadsheets

Ah, the tool with 1,000 uses — the glorious spreadsheet! But if you try to use it to perform IGA for hundreds of applications, dozens of permissions each, managed by hundreds of owners, and accessed by thousands of users, you essentially end up with “death by 1000 tables”. Spreadsheets simply don’t scale well. They especially don’t do a good job of tracking changes over time, which is a big problem in the real world of identity management.

4 Your user access reviews are limited to an “as-needed” basis

If you’re seeing some of the other signs on this list, such as manual user access reviews, you might encounter this one as well — user access reviews that are performed on an ad hoc basis or are very limited in scope. While highly privileged application administrators deserve extra attention, they can’t be the sole focus of user access reviews. Similarly, while you need to ensure that you’re quickly revoking access for terminated employees, you also need to make sure existing employees and contractors have the right permissions. This is harder to verify, but necessary.

Then there are machine users and shared accounts — both of which are important to review.

84% of organizations rely heavily or entirely on manual processes for performing activities such as user access reviews and provisioning.[3]

5 You’re relying on “Light IGA” via an SSO solution

Single Sign On (SSO) and multi-factor authentication (MFA) solutions manage authentication centrally, but they don’t do real IGA. Consider the following:

- Legacy applications often don’t fully integrate with an SSO solution.
- SSO can lack a model of complex entitlement information, which can vary from application to application.
- Distributed application ownership can be a problem — especially for all those SaaS applications that are operating outside IT.
- Integration with workflow management solutions is challenging for user access reviews and provisioning activities.

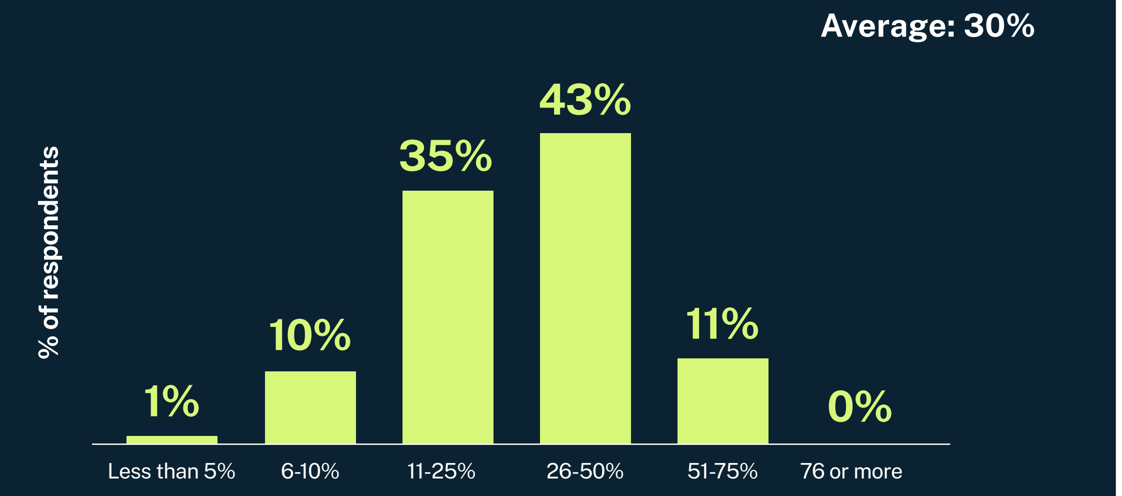
[3] Cyberark, 2025 State of IGA Survey Report, 2025

6 You have an IGA solution, but it isn't integrated with all your applications

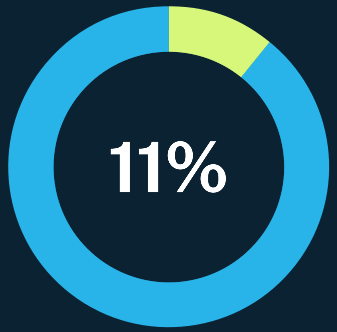
There's an old story about a man, out at night, looking for his lost car keys under a streetlamp. Someone else comes by and asks him if that's where he lost them. He replies, "I don't know, but this is the only place where I can see anything." Having an identity governance solution that doesn't cover your applications is like only looking where you happen to have some light to see by. For effective IGA, you need broad daylight — full coverage of all your applications.

Afterall, identity governance is only as good as the applications it covers.

Organizations in 2024 average the use of 112 SaaS applications, up from only 16 in 2017. And organizations with over 5000 employees average use of 158 SaaS applications.[4]



Percentage of Cloud, SaaS, and On-Prem Applications Integrated with IGA



Only 11% of identity leaders that have deployed an IGA solution have managed to integrate 50% or more of their applications.[5]

[4] BetterCloud, The 2024 State of SaaSOps Report, 2024
[5] Cyberark, 2025 State of IGA Survey Report, 2025

7 Your IGA consulting services are a major annual budget item

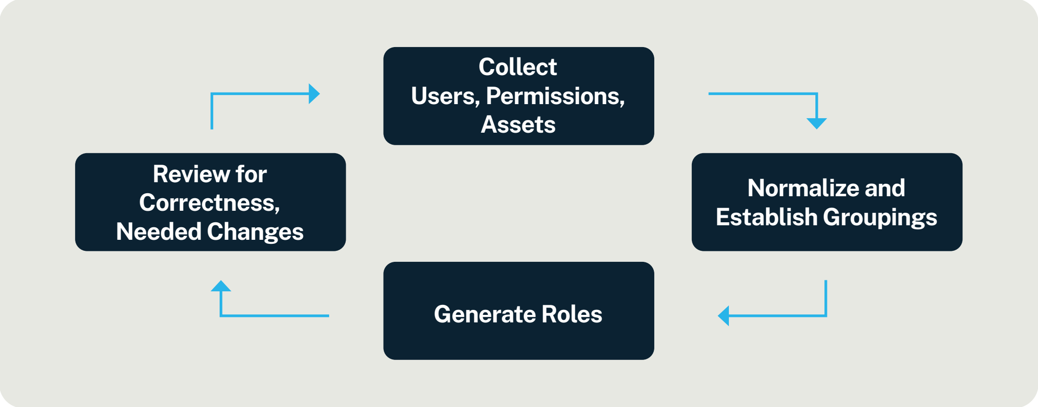
It's natural that you might need some help getting up and running with an IGA solution — for initial installation, setup, integration, and training. But why should you need consulting services on an ongoing basis, year after year? Unfortunately, according to Mordor Intelligence, IGA services represented 57% of the market — a reflection of the continuous services requirements of legacy IGA solutions.

A modern IGA solution can minimize your need for extensive out-of-the-box integrations as well as sophisticated automation so you can add new and custom applications when you need to — without outside help. Getting off the consulting services treadmill is a realistic and rewarding option.

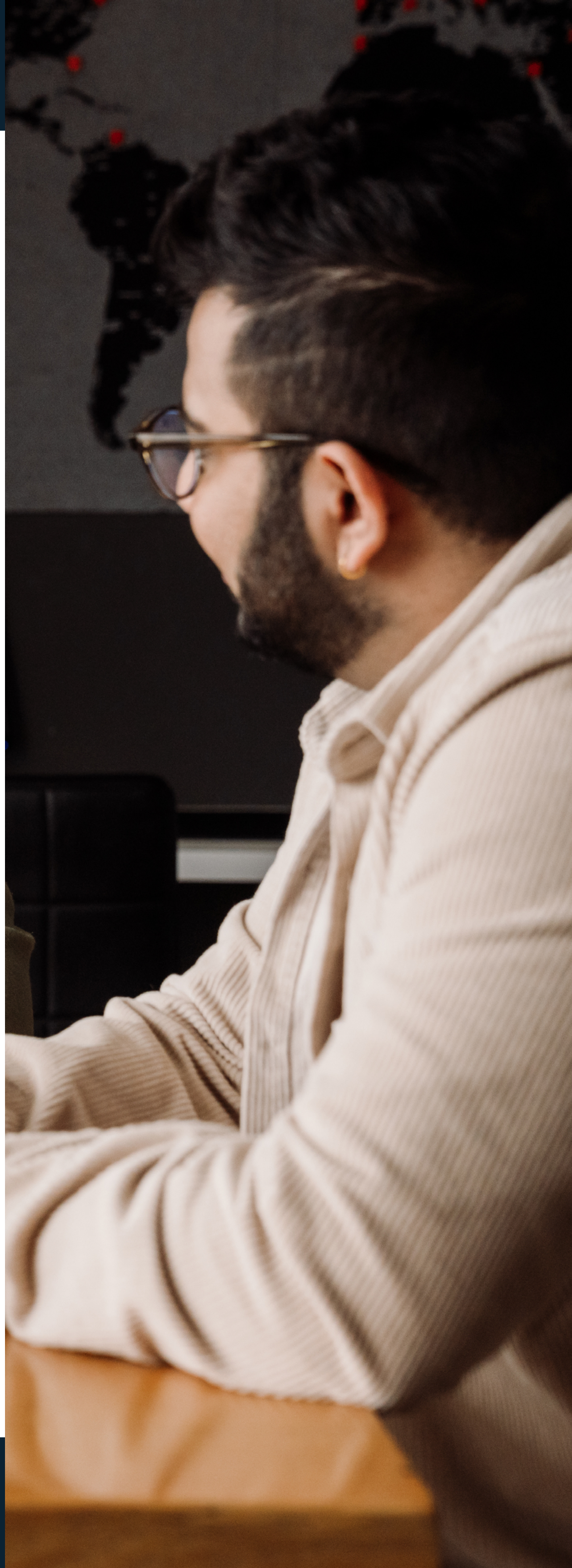
8 Managing roles is too daunting (or is a substantial headache)

You want to get started with an IGA solution, but it may seem too daunting because you're terrified of managing roles. Or you've already started with roles and found it to be a headache. A role-oriented approach can be complicated, involving:

- Collecting and analyzing information on all your employees, contractors, machine users, applications, application owners, and permissions.
- Establishing clear groupings of users, applications, and permissions.
- Turning those into roles that can be administered.
- Continuously updating all this as necessary to reflect your changing environment.


Collect Users, Permissions, Assets
Normalize and Establish Groupings
Generate Roles
Review for Correctness, Needed Changes

A modern IGA solution has alternatives — namely an AI approach focused on machine learning (see below).



9 Making user access changes is slow and unreliable

Executing user access changes well isn't just a matter of maintaining proper governance — it's critical to employee productivity. Who hasn't joined a new organization and faced some frustration with having all the basics in place — email, calendaring, collaboration applications, CRM, IT help systems, etc.? Usually, permissions aren't provisioned on day one, and the resulting hit to productivity is a substantial business expense.

Then, on the other end of the process, who hasn't witnessed situations where accounts are still active for people who've left the organization? That's a major security and governance problem.

More than half of businesses can't provision a new employee's access and app permissions in under 7 days.[6]

98% of identity and security leaders report that 6% or more of all entitlement permissions checked during periodic reviews require revocation because they are orphaned, unnecessary or excessive.[7]

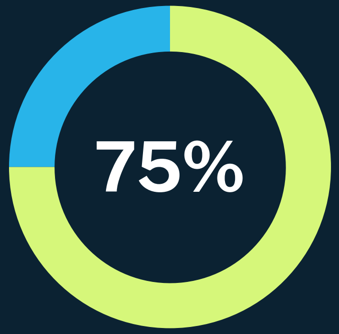
10 You've had an identity-related breach or pen test failure

Shocker — you've had a security issue rooted in an identity vulnerability. There's a reason that identity is the #1 vector for an attacker: legacy identity management can be highly complex, highly dynamic, and doesn't lend itself to simple scanning and patching approaches. But a modern IGA solution can make a large contribution towards identifying and remediating identity-based vulnerabilities.

[6, 7] Cyberark, 2025 State of IGA Survey Report, 2025

11 AI with your IGA? Not even on your radar.

AI is being leveraged effectively in many types of business applications, and IGA is no exception. In fact, machine learning is the perfect approach to deal with the ever-changing morass of employees, contractors, and machine users, complex and extensive permissions, distributed applications, machines, and cloud environments; and there's no one person (or team) that understands it all. The complexity cries out for highly sophisticated AI-based learning.



CyberArk AI Profiles can reduce review effort by up to 75%.

Problems With Most Existing IGA Programs

The “reboot issues” above illustrate the kinds of problems that organizations encounter when they have a legacy or ineffective IGA program. And no wonder — IGA solutions have been available in one form or another for over 20 years. But the demands of compliance and security, as well as the dramatic changes in the IT environment, have made legacy IGA obsolete. Manual methods and legacy IGA simply can’t keep up with the explosion of applications that are managed outside of IT, which may be accessed by employees, contractors, and machine users.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides themost comprehensive security offering for any identity — human ormachine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world’s leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit https://www.cyberark.com, read the CyberArk blogs or follow on X (Formerly Twitter) via @CyberArk, LinkedIn or Facebook.

Ready to Reboot With CyberArk Modern IGA?

CyberArk modern IGA is purpose-built for the cloud and app era. It combines complete and automated application integration, AI capabilities, a more comprehensive identity data model, and security capabilities to defend against modern threats. Reboot your IGA approach with CyberArk modern IGA.

Need help with your IGA Program?

Leverage the modern IGA approach with CyberArk and MajorKey. .

Learn More