2025 State of IGA Survey Report

Jan 2025

Table of Contents

Introduction and Key Findings

Introduction & Methodology

As the traditional network security perimeter has dissolved, with applications moving to the cloud, it is widely accepted that identity is both the new perimeter and the top vector of cyberattack. Organizations are dealing with increasing compliance mandates, expanding application environments, and more applications owned by a wider range of staff (both IT and non-IT). However, legacy Identity Governance and Administration (IGA) tools have been around for twenty years or more, and they simply weren't built to meet this reality. Increasingly, every entitlement under an organization's roof—granted to both human and non-human users—is subject to user access reviews, providing a significant and growing challenge.

As the leading provider of Modern Identity Governance and Administration, Zilla Security provides a SaaS platform that automates the processes of identity compliance, provisioning, and security. We embarked on this report to uncover the true state of IGA in today's enterprises. Where are identity and security leaders on their automation roadmap? How much of a struggle are they finding everyday tasks such as onboarding a new hire, satisfying auditors, or revoking excessive permissions?

The results shine a light on an industry that's starting to mature, but where just 6% are fully invested in automating IGA processes. Yet the majority are seeing the negative impact of a reliance on manual execution.

Methodology

To get more insight into the state of IGA processes today, we commissioned a survey of 300 Identity Management leaders, with 80% from the U.S. and 20% from the U.K. The respondents were split evenly between companies with 250 to 1,500 employees and those with 1,501 to 15,000 employees. We chose 40% of respondents from organizations in the financial services sector, 25% from healthcare/pharma, and the remainder from other industries, excluding the service industry, logistics, transportation and education.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during October 2024. The average amount of time spent on the survey was 4 minutes and 22 seconds. The ordering of options to the majority of non-numerical multiple-choice questions was randomized, in order to prevent order bias in the answers.

Key Findings

1. ## Manual execution of crucial IGA tasks is the norm – fewer than 6% of companies have full automation in place

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

2. ## 83% say difficulty integrating with IGA systems is the primary cause of manual IGA processes

The cost and difficulty of application integration with legacy IGA solutions is very high. As a result, only 11% of identity leaders that have deployed an IGA solution have managed to integrate 50% or more of their applications.

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

99% of companies complete user access reviews to satisfy compliance regulations, and 55% have 5 or more regulations for which they are required to perform reviews. 91% report an increased scope for this task over the past three years, and 84% are expecting the scope of user access reviews to continue to increase.

4. ## Excessive permissions are a growing risk, with 10%+ of entitlements being excessive at over half of all organizations

Orphaned or excessive permissions create security risk, and 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. In 52% of cases, 11% or more require revocation.

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

Just 10% can provision application permissions in less than two days, and 29% say it takes at least 11 days to complete. Defining and maintaining business roles would enable easier and faster provisioning, but 90% say that the effort involved in this task has held them back until now.

6 Industries with less automation struggle more with access audits and are slower to provision new users

93% of healthcare companies rely heavily or entirely on manual processes for IGA, followed by 84% of financial services organizations. The impact of this can be seen on the outsized effort they need to put into everyday tasks compared to other industries on average. 56% of healthcare respondents say access reviews are a significant effort that their teams cannot support, compared to 39% on average, and in finance — 39% of identity leaders admit that provisioning can take more than 11 days to complete, significantly higher than the 29% average.

Survey Report Findings

IGA Is a Predominately Manual Activity

Just 6% of identity and security leaders say their Identity Governance and Administration (IGA) processes are fully automated.

At the other end of the scale, **84% of organizations rely heavily or entirely on manual processes** for performing crucial tasks such as user access reviews and provisioning granular permissions.

With minimal resources to go around, there are dramatic cost savings available to businesses that can leverage automation to replace manual efforts for these processes. However, IGA solutions have been around for two decades, and the legacy vendors have done little to modernize their solutions to support organizations with the level of automation needed.

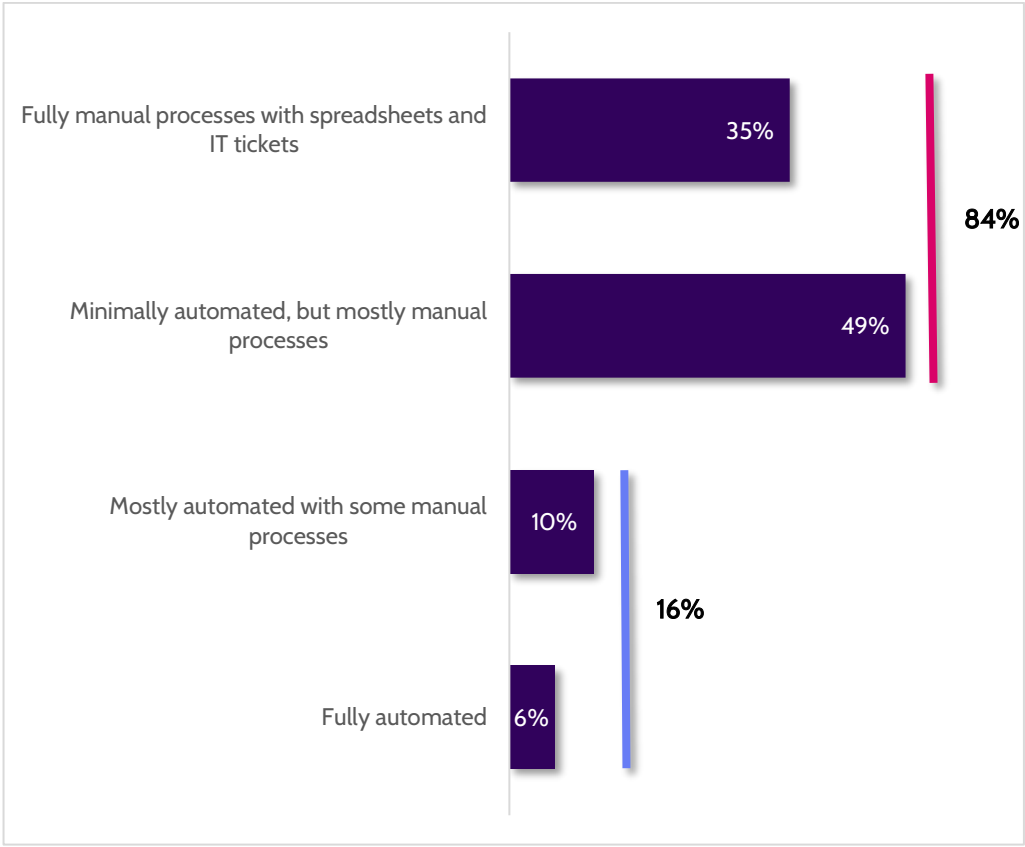

Figure 1: Implementation of IGA Processes and User Access Reviews

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

The UK is Ahead of the US in IGA Automation

By breaking down the responses by region, the data uncovers that identity leaders in the United Kingdom have a higher propensity to automate IGA processes than their peers in the United States. **In the UK, 32% of respondents say their IGA processes are mostly or fully automated, compared to just 13% in the U.S.** This could be linked to the push to achieve GDPR compliance, or could simply be a cultural differentiator.

It's also interesting to note that **Healthcare is more reliant on manual processes than any other industry, followed by Financial Services.** These are highly regulated industries, and have a lot to gain by automating their IGA processes to meet compliance and streamline the way they work.

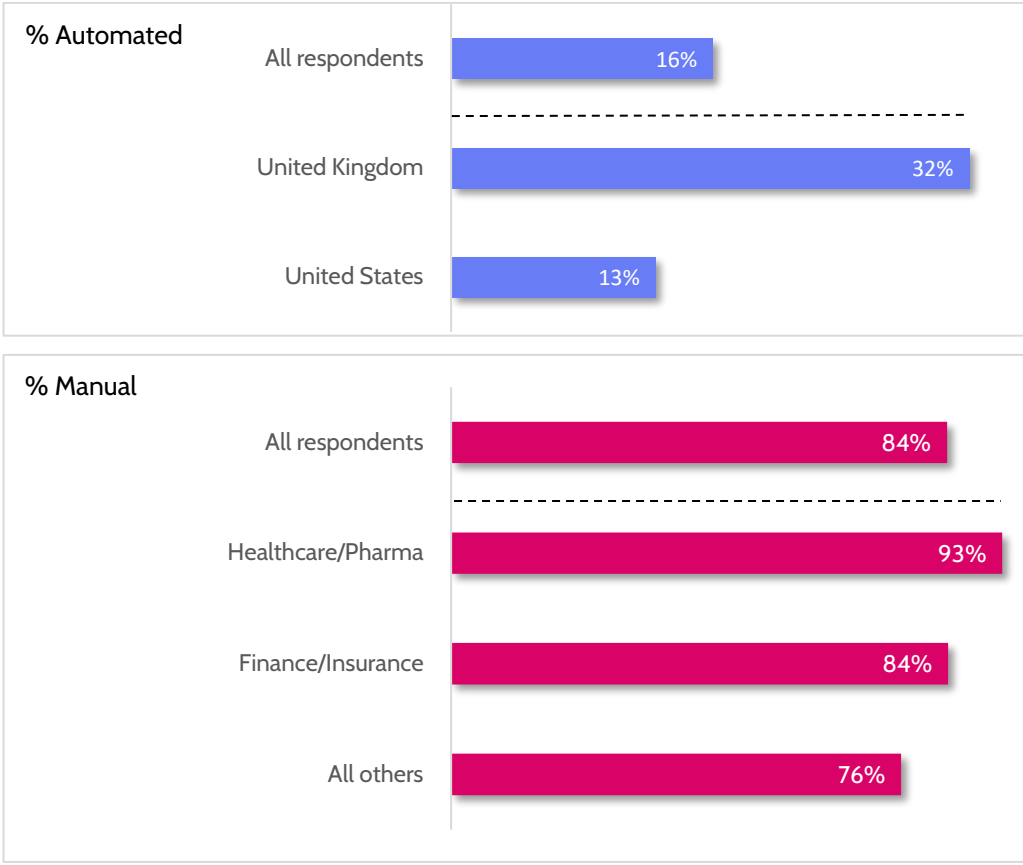

Figure 2: Implementation of IGA Processes and User Access Reviews by Country and Industry

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Integration and Customization are the Roadblocks to Automated IGA

What is keeping identity and security leaders tied to overwhelmingly manual execution of IGA processes?

For 82% of identity leaders, the difficulty of integration and customization is the primary reason for not having automated with an IGA solution. This includes 64% who cite the efforts involved in integrating IGA solutions with SaaS and other cloud applications, as well as 18% hamstrung by the high resource efforts involved in customizing and operating the solutions.

Bottom line? **Integrating data from disparate applications is extremely difficult to do with legacy IGA technology.** Just 6% call out cost as a blocker – suggesting that if a solution could solve the complexity challenge, budget may follow.

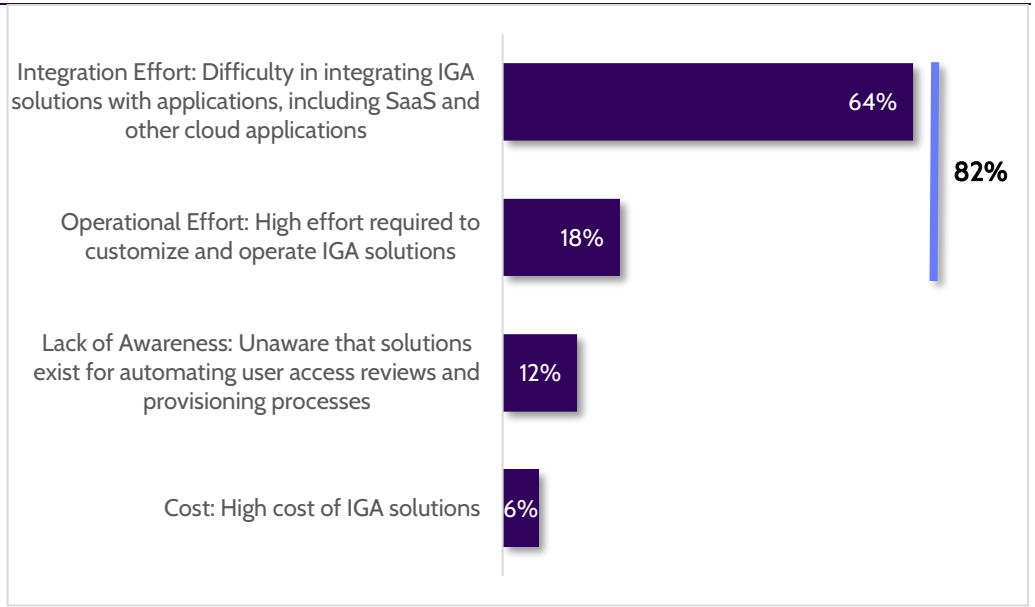

Figure 3: Primary Reason for Manual Execution of IGA Processes

Organizations Struggle to Govern Application Permissions Due to Integration Issues

To understand the success of current IGA solutions when deployed, we asked the 16% of identity and security leaders who have mostly automated processes in place (Figure 1) to share the degree of integration that has been achieved across the business.

Despite modern organizations having hundreds or thousands of applications used across the business, including HR systems, Finance apps, Marketing tools and custom applications, **61% of respondents have only 25 or fewer applications integrated with their IGA solution**. Additionally, just 11% have managed to integrate more than half of their organizations' apps. The substantial gap in integration coverage means permissions are going unmanaged – contributing to a crisis in identity security.

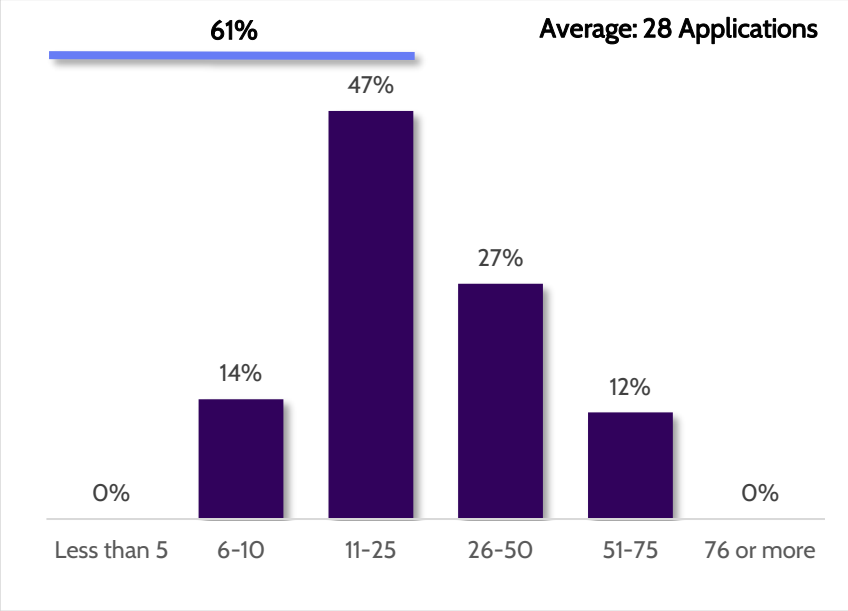

Figure 3: Number of Applications Fully Integrated with IGA Solution

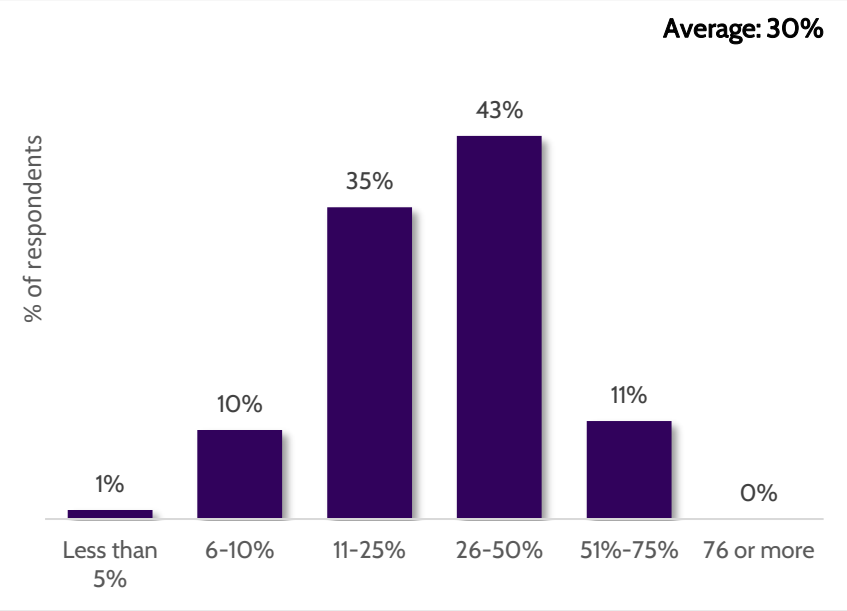

Figure 4: Percentage of Cloud, SaaS, and On-Prem Applications Integrated with IGA

Compliance Drives User Access Reviews, With Most Organizations Having 5+ Compliance Obligations

Whether it's PCI-DSS, GDPR, Sarbanes Oxley (SOX), ISO 27001, NIST, or any other number of extensive and continually evolving regulatory frameworks, compliance is driving the need for regular access reviews. 99% are completing these reviews for compliance rather than security purposes.

However, just 19% have a single regulation to contend with. **55% of identity leaders are required to perform these reviews for five or more regulations**, and in 3% of cases, organizations have upwards of 15 compliance frameworks for which to complete user access reviews.

The cost of managing this commitment is huge, especially with a lack of automation to help complete these reviews.

Figure 6: Reason for Conducting Regular User Access Reviews

The Scope of User Access Reviews is Increasing, With No End in Sight

We asked identity and security leaders to consider how the scope of user access reviews has evolved over the past three years, and to look ahead and estimate how it will be likely to change in the three years to come.

91% of respondents have experienced an increase in scope since 2022, and 84% believe there will be a similar increase before 2028. Just 10% of identity leaders believe there will be no change, and only 6% say they expect a decrease in scope.

It is likely that the need for automation of IGA processes will increase as the requirements for compliance efforts increase.

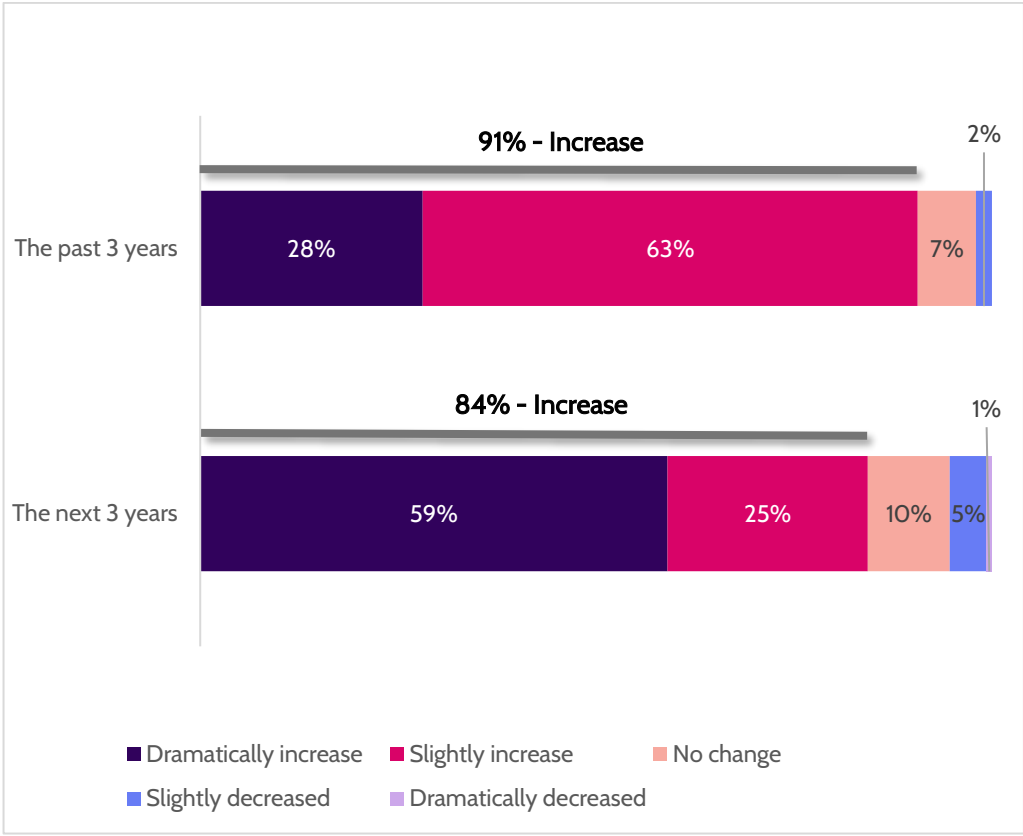

Figure 7: Changes in the Scope of User Access Reviews Over (Past Year, Next 3 Years)

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Large Efforts are Required to Complete User Access Reviews to Auditor Satisfaction

With a growing number of regulatory requirements to meet, identity leaders shared how difficult the associated tasks are to perform.

Just 18% had no issues with the effort of compliance, while the other 82% of respondents indicated that it requires a high level of effort to support user reviews. **For 43% of identity leaders, this significant effort can be managed with existing staff, while 39% struggle with the effort to manage the growing scope of user access reviews,** presenting a significant challenge for identity and security teams.

Looking at the responses broken down by industry, it's clear that **Healthcare is struggling the most.** For 56% of healthcare identity leaders, the high efforts involved in managing user access reviews are greater than their staffing can support without struggling. As we saw in figure 2, 93% of healthcare companies are relying on manual processes for this task – and here we can clearly see the result.

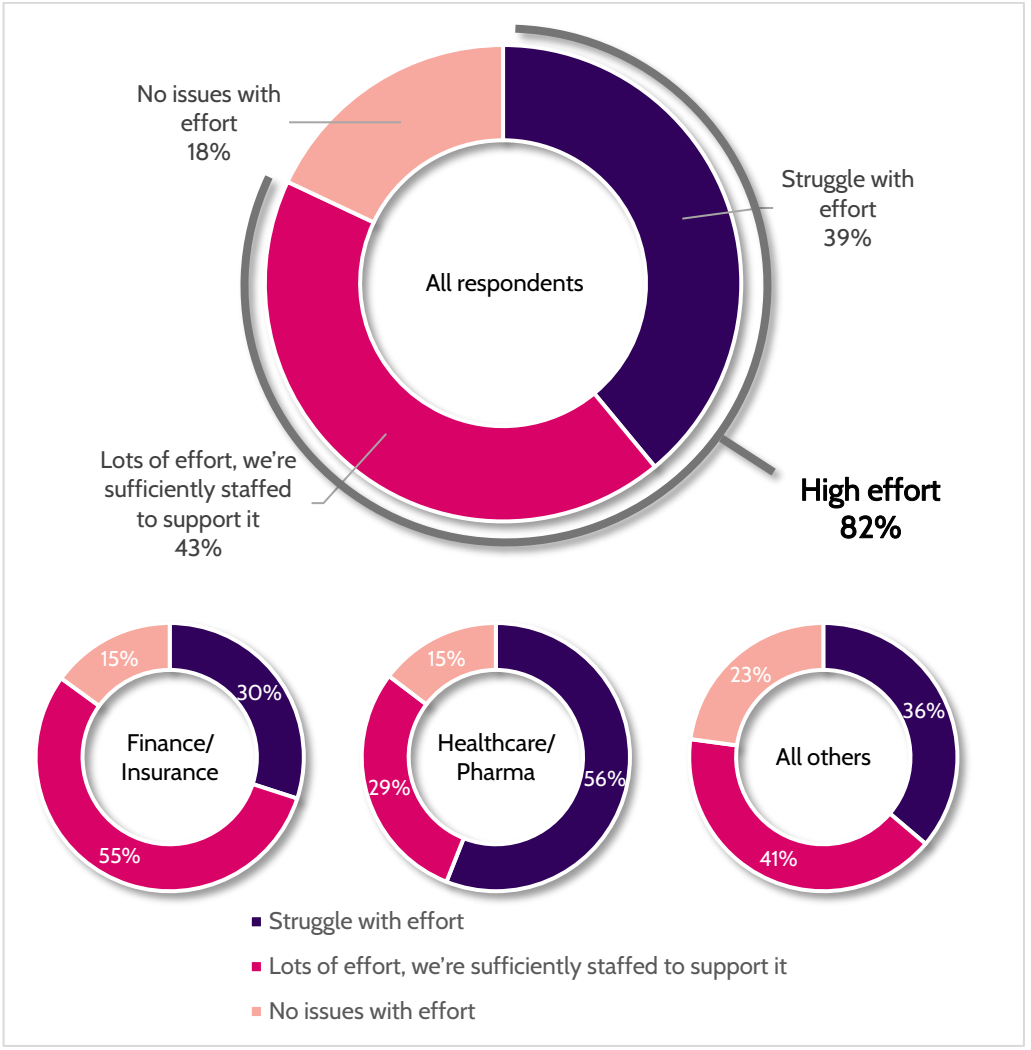

Figure 8: Effort Required to Complete User Access Reviews for Auditor Satisfaction by Industry

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Orphaned and Excessive Permissions are a Pervasive Problem

Orphaned or excessive permissions are a common result to find during periodic reviews. These entitlements are crucial to find and remove, and this functionality is an essential part of an IGA solution. It's important that the scope includes both human and non-human accounts, with the latter including service accounts in cloud environments, automation or script accounts, and service accounts related to logging or monitoring.

98% of identity leaders report that 6% or more of all reviewed entitlements permissions require revocation as part of a periodic review. **More than half (52%) admit that 11% require revocation – greater than one in ten.**

Naturally, discovering excessive permissions at this rate isn't comforting as they are an indication of significant cybersecurity risk. Identity compromise is the #1 vector for cyberattacks.

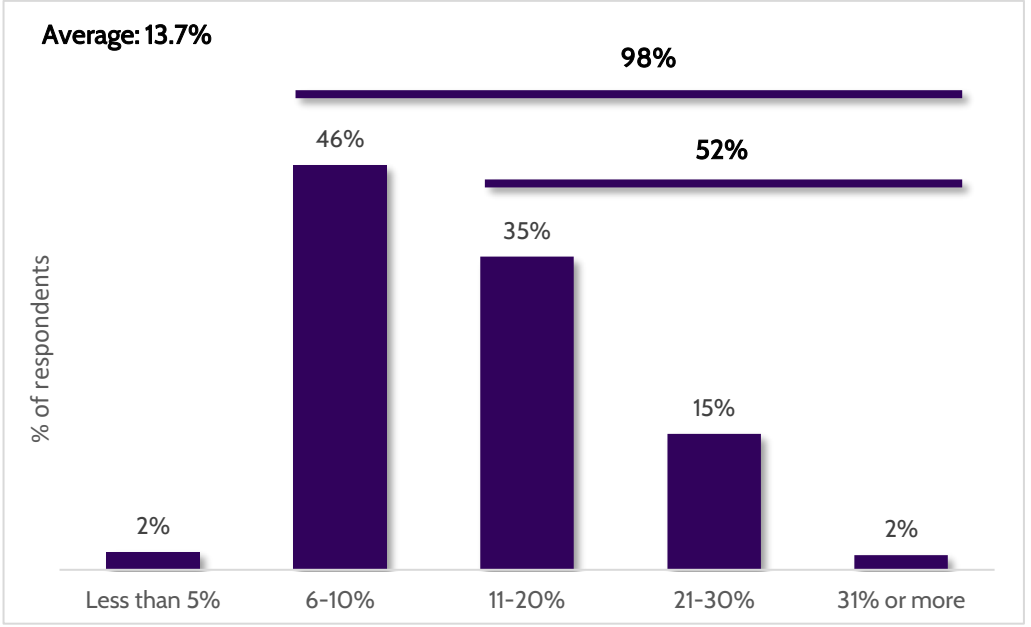

Figure 5: Percentage of Entitlements Identified for Revocation During Periodic Reviews

Provisioning a New Employee Typically Takes a Week or More, Impacting Workforce Productivity

55% of respondents report that it takes seven days or more to comprehensively provide a new employee with the necessary access and application permissions. **Just 10% of identity leaders report the business can provision access in 1-2 days**. In 29% of cases, this takes at least 11 days. This creates both a cost and frustration point for the business, as new employees are unable to be productive as they wait for the access they need to do their job.

The time to provision new users varies largely between industries. In Financial Services—which this survey illustrates relies more heavily on manual processes than the average — 39% of teams take 11 days or more to provision a new hire.

We can also see steep variation by geography. While 34% of identity leaders in the U.S. say it takes at least 11 days to provision new users, in the United Kingdom, this is only the case for 7% of respondents. As we saw in figure 2, the UK is far more likely to have mostly or fully automated IGA processes in place, which may explain why they are able to provision access for users so much faster.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

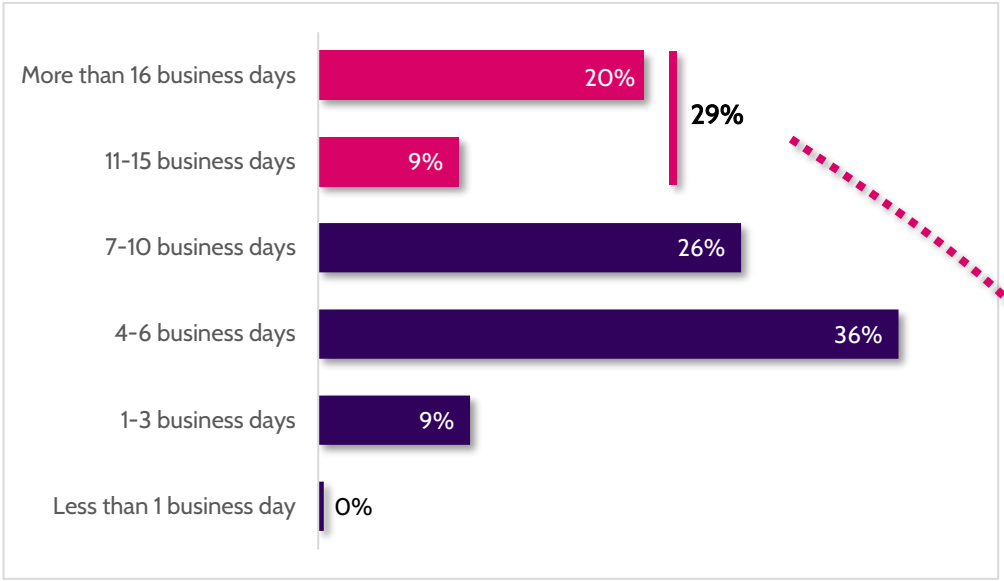

Figure 6: Average Time to Grant Full Application Permissions to New Hires and Contractors

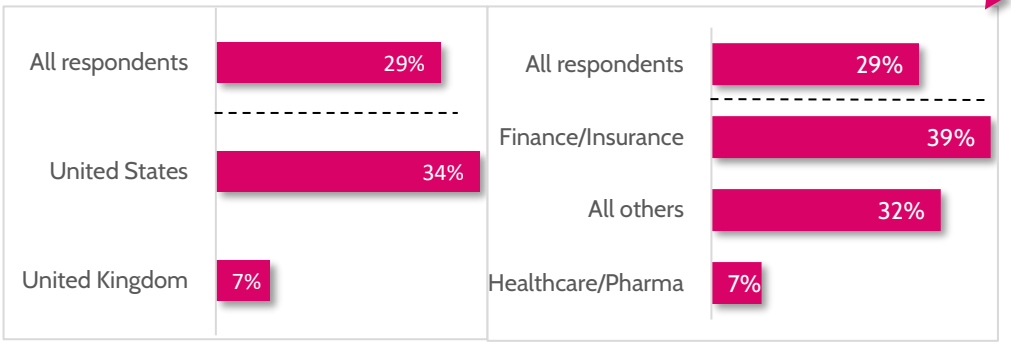

Figure 7: Percent That Take 11 Days or More to Grant Full App Permissions

90% of Organizations Struggle with Managing Roles, Or Have Just Given Up

The lifecycle of users within an organization comprises joiners, movers and leavers. A capable IGA solution should make each of these processes faster, more efficient, and more reliable.

Legacy IGA solutions however, typically require an organization to maintain complex roles and provisioning rules to automate these activities. Unfortunately, **90% of identity and security leaders are struggling to define these roles**, and as a result cannot automate their processes using legacy solutions or can only do so with an excessive level of effort.

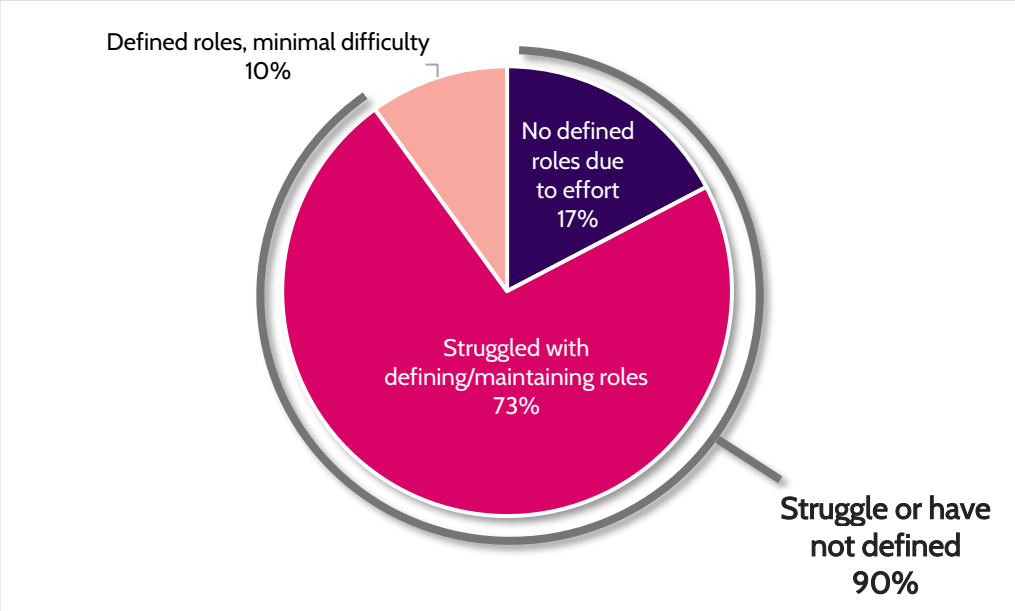

Figure 8: Effort Involved in Defining and Maintaining Business Roles for Efficient Provisioning

The Increased Focus on Identity Security Has Driven Operational Ownership Changes

Traditionally identity management has been the responsibility of IT Teams. As identity management has become a growing security concern, there is a trend to see identity governance responsibilities being overseen by the security organization, led by the CISO.

The larger the company, the more likely IGA activities are to be overseen by the CISO, with companies of more than 10,000 employees the most likely to follow this structure.

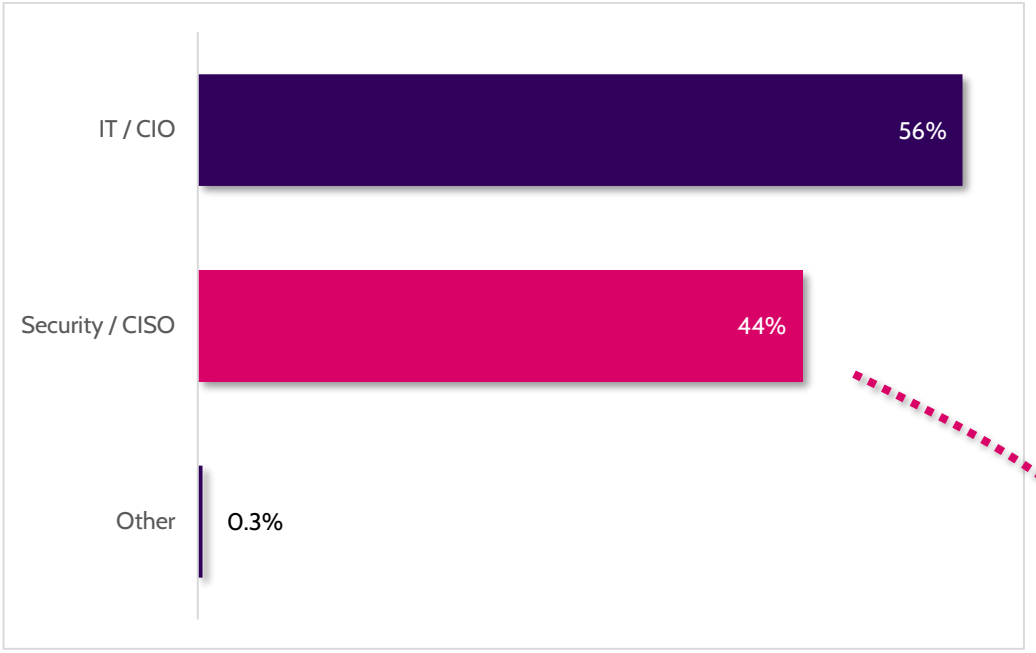

Figure 9: Reporting Structure of the IGA Team Within the Organization

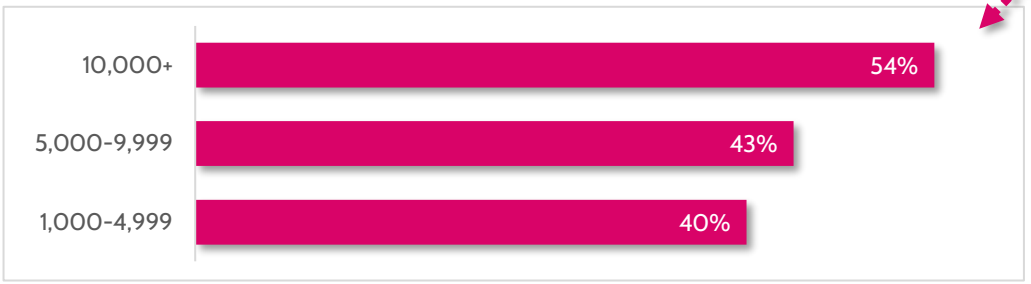

Figure 10: Security/ CISO by Company size

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Demographics

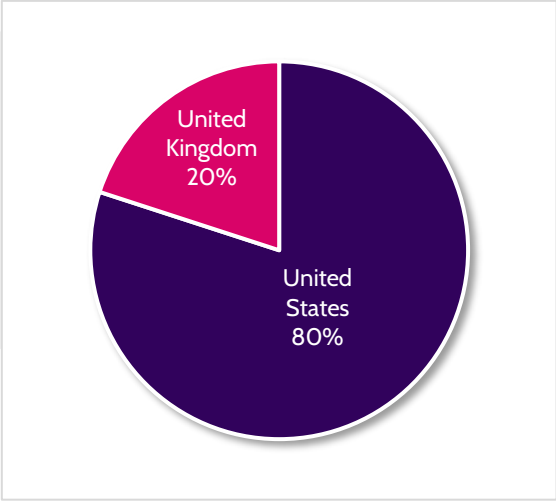

Figure 11: Country

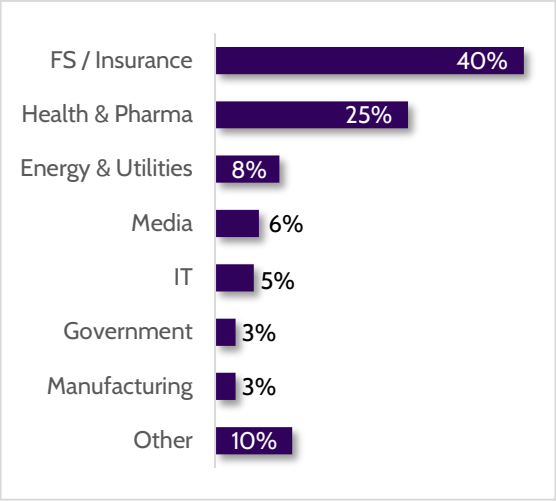

Figure 12: Industry

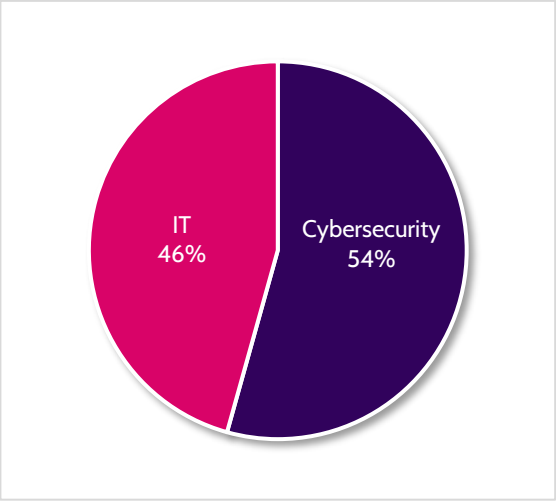

Figure 13: Department

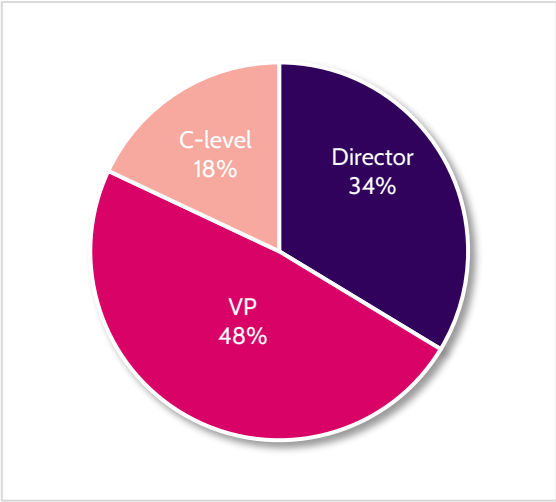

Figure 14: Job Seniority

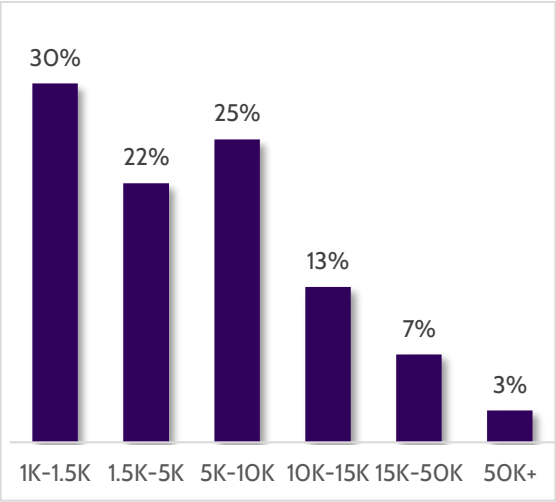

Figure 15: Company Size

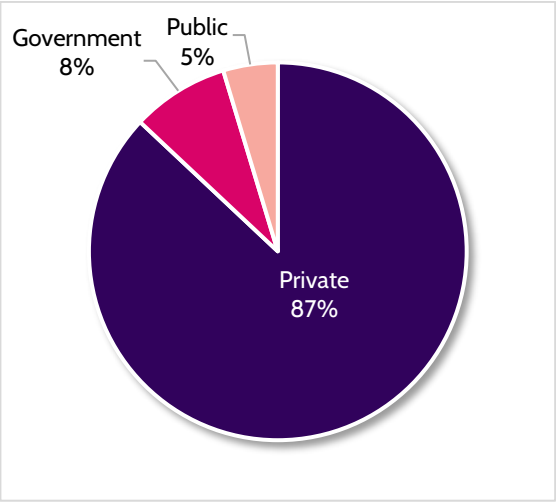

Figure 16: Company Ownership Type

About Zilla Security

Zilla Security is the leading provider of Modern Identity Governance and Administration (IGA), providing a SaaS platform that automates the processes of identity compliance, provisioning, and security. Zilla stands out for its speed to value, offering the most complete set of application integrations capabilities for both commonly used and custom applications. Zilla AI Profiles™ eliminates the tedious, nearly impossible process of creating and maintaining rules that define roles or groups. Through its automations, Zilla clients are able to deploy 5X faster, complete access reviews with 80% less effort, and enable faster provisioning with 60% fewer ITSM tickets.

Request a Demo

For more information, please visit us:

Email: info@zillasecurity.com