Getting a Handle on Identity Governance and Administration for Remote Workers

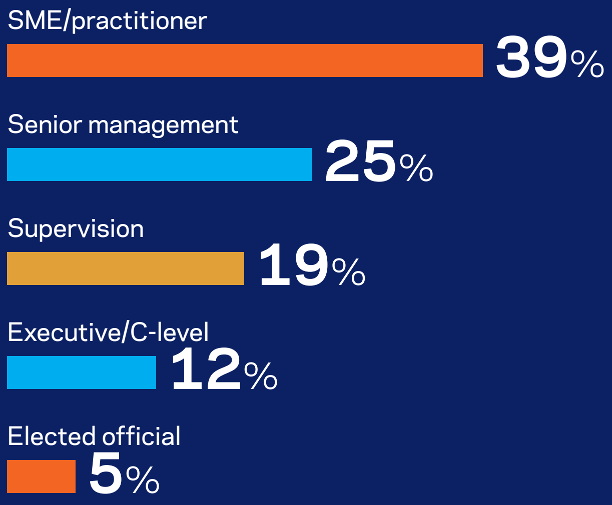
The Center for Digital Government recently conducted a survey of 263 state and local government leaders to assess how the COVID-19 pandemic has impacted their identity governance and administration (IGA) priorities, practices and concerns. The goal was to understand the challenges the pandemic has presented to government IT agencies and departments, gauge respondents' short- and long-term priorities post-COVID-19, and explore their unmet needs related to remote work.

IGA refers to the tools used to manage and secure digital identity and access rights for all users and digital assets across the extended enterprise. As described by Gartner, "These tools help ensure that only the right people get entitlements to the right resources (e.g., applications and data) at the right time for the right reasons." Mature IGA solutions go beyond basic credential provisioning and identity and access management (IAM) solutions. Besides using artificial intelligence (AI) and machine learning (ML) to automate and enhance credential provisioning and other identity access management tasks, they automate labor-intensive governance processes to help organizations meet compliance and auditing requirements.

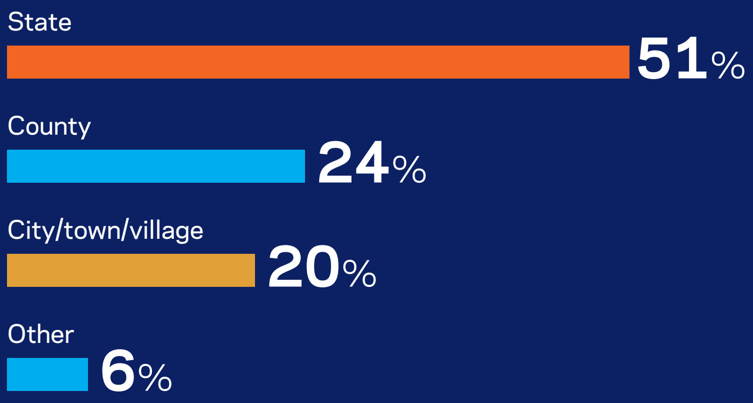
RESPONDENT DEMOGRAPHICS

The Center for Digital Government surveyed 263 state and local government professionals in July 2020. The following data shows respondents' demographics by role and level of government they work in.

What is your job role?



What level of government do you work for? *



** Some percentages will not add up to 100 due to rounding.*

MORE THAN HALF OF ORGANIZATIONS LACK BASIC IGA FUNCTIONALITY TO MANAGE REMOTE WORKERS' IDENTITY AND ACCESS TO RESOURCES.

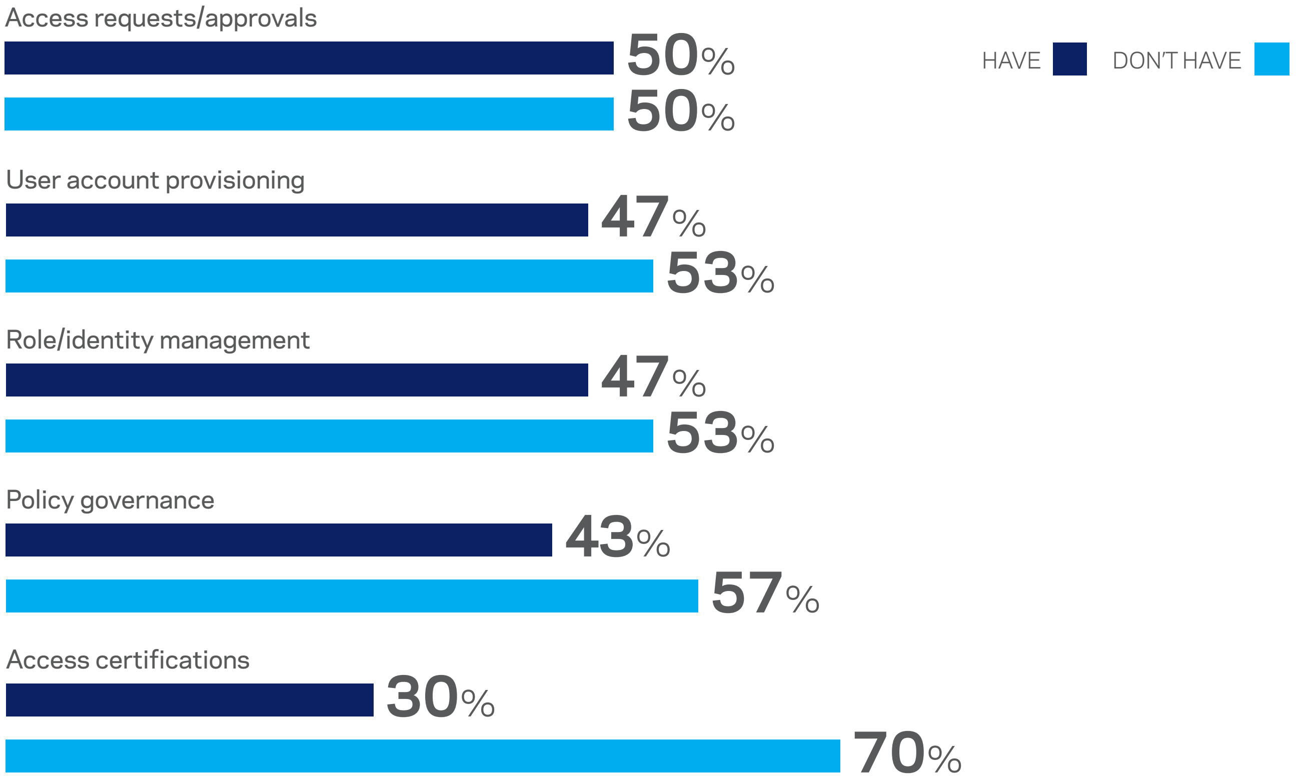
Only 50 percent of respondents said their organization's IGA strategy includes access to requests and approvals, and only 47 percent said user account provisioning and role/identity management are included.

Respondents' organizations moved mountains to quickly provision equipment and identities to remote workers. Now that they are catching their breath, it's time to take a closer look at identity governance and administration practices as they relate to remote work.

Like many IT operations today, remote work pushes the boundaries of the enterprise perimeter to include the cloud, home offices, mobile devices and more. While traditional perimeter defenses are still essential, they cannot protect against breaches related to compromised or misused identities. These vulnerabilities are the source of many breaches today. For this reason, formally certifying users, assigning the correct access rights and performing ongoing assessments of the validity of authorized users is essential.

An effective identity and governance program provides these capabilities, enabling organizations to determine who has access to what data and applications, who should have access and how they are using that access. In addition, it allows organizations to more easily provision and manage user accounts as workers' access requirements change.

If any, what is included in your agency's or department's IGA strategy to remotely support its employees?



MORE THAN 20 PERCENT OF RESPONDENTS' ORGANIZATIONS STILL LACK A CENTRALIZED USER DIRECTORY.

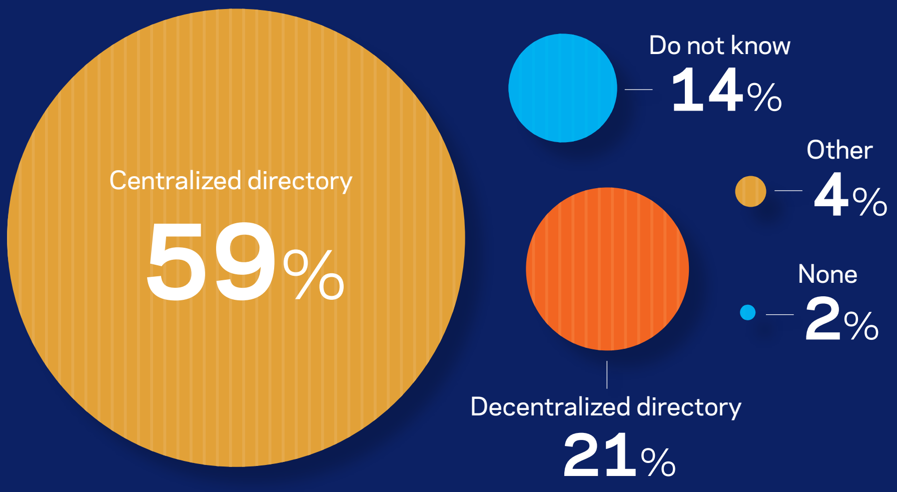
While nearly 60 percent of agencies or departments use the same user directory, 21 percent still use a decentralized directory.

A centralized user directory provides a single, authoritative view of users and what applications and resources they have access to — regardless of where they are working. By allowing organizations to control user access centrally and apply policies consistently, a centralized directory helps prevent breaches, supports compliance and simplifies auditing.

By contrast, with decentralization, user directories exist in multiple, siloed environments. Individual departments or agencies may issue credentials and govern user policies without coordination across the enterprise, and a single user or a single user role may have different, incompatible access rights in different directories. These inconsistencies open the door to improper access and breaches, policy or compliance violations, and weak controls. In addition, decentralization makes it more laborious to provision the right credentials to the right users as well as review users' access rights periodically to ensure they are appropriate and compliant.

IGA gives organizations with decentralized user directories more control over access by compiling and correlating disparate user identity data from across the enterprise. It's important to note, however, that IGA technology is most effective when used in tandem with strong leadership that drives the move to a more centralized model. This includes setting clear goals; working with stakeholders; and managing, monitoring and measuring progress toward those goals.

Do individual agencies or departments use their own user directories (decentralized directory), or do all agencies use the same user directory (centralized directory)?



MANY IT PERSONNEL LACK SUFFICIENT VISIBILITY INTO USER ACCESS AND USER ACTIVITY.

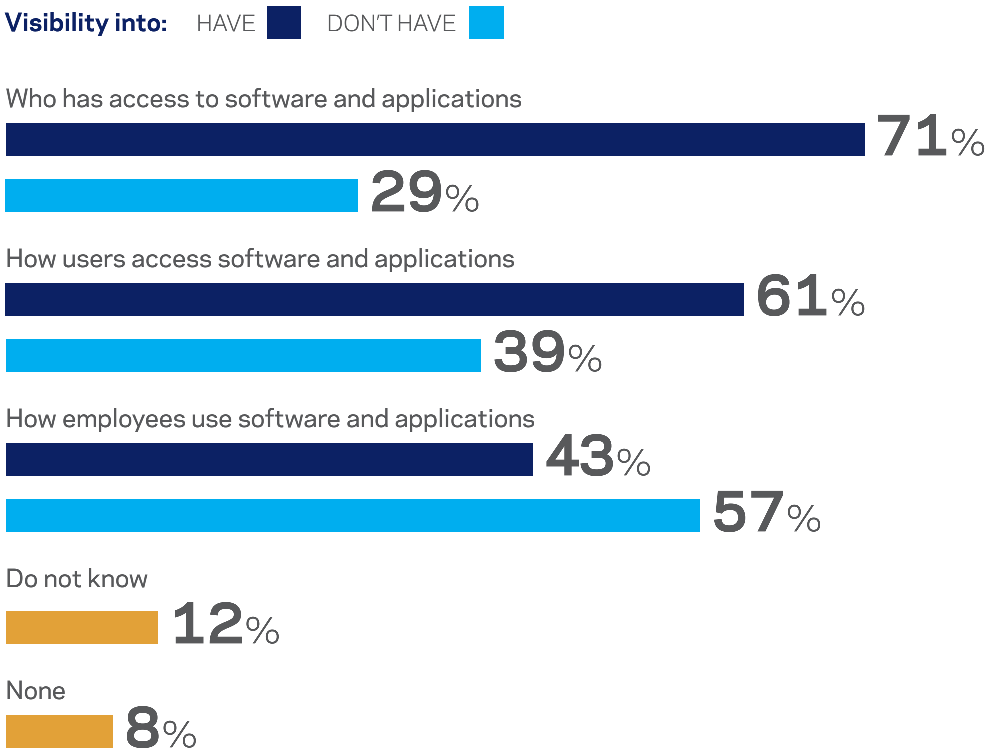
More than one-quarter of IT respondents do not have visibility into who has access to software and applications. Nearly 40 percent do not have visibility into how users access these resources, and nearly 60 percent lack visibility into how employees use the resources they access.

As more employees work remotely and the enterprise becomes increasingly distributed, achieving visibility into who has access to resources and how they are being used becomes more complex. Organizations must have visibility across the entire enterprise, including the cloud, mobile devices and decentralized user directories. In addition, they must have visibility into the access rights and behavior of non-human resources such as chatbots and other automated tools that have identities assigned to them.

Given the lack of visibility reported by survey respondents, organizations may have exposed themselves to greater risk of breaches and non-compliance when they initially allowed users to access resources remotely. Some workers may have been given broader access rights than were necessary or safe, or their access rights were not revoked when they were furloughed. Some devices used by workers may not have been properly provisioned or protected. Some organizations may have drawn from outdated, non-standardized decentralized user directories to roll out identities and access rights.

To ensure they can meet identity and access-related security, compliance and auditing requirements as they move forward with remote work and other initiatives, organizations will need the visibility and insight provided by mature IGA solutions. These solutions start with a platform that aggregates data from the entire enterprise ecosystem; provides a unified, real-time window into users, their access rights and behavior; and incorporates AI-driven insights, governance recommendations and automation to inform decision-making and expedite tasks.

What type of visibility into users' identities do you have within your system?



REGULATORY MANDATES REQUIRING IAM OR IGA MAY NOT BE A FOCUS — OR THEY MAY NOT BE WELL UNDERSTOOD — WITHIN IT AND BUSINESS OPERATIONS.

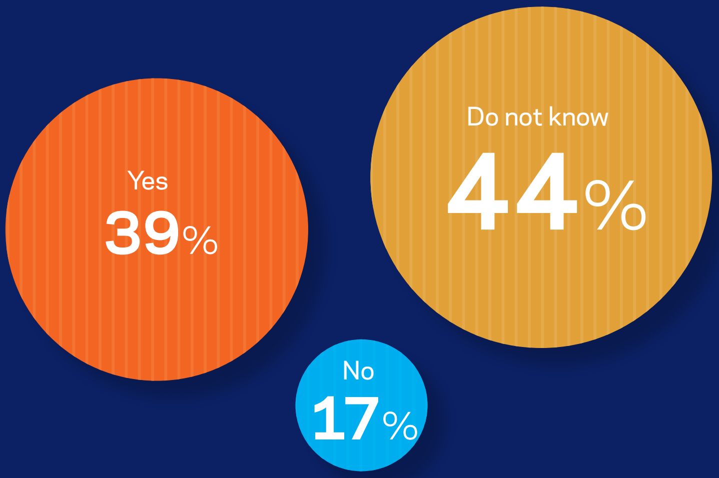
Only 39 percent of IT and business respondents say their regulatory mandates require IAM or IGA; nearly 44 percent say they do not know.

Identity management/IGA capabilities are essential to support compliance and streamline auditing. These responses raise important questions about staff perceptions and behavior related to security, compliance and auditing. The responses indicate that organizations may need to more fully educate staff on the importance of regulatory compliance; the difference between security and compliance; and the role of IGA tools, processes and policies in maintaining compliance and demonstrating it.

It's not enough to simply implement mechanisms and processes and say they are giving the right people the right access at the right time. Organizations must be able to document compliance on an ongoing basis and prove it to auditors. While the pandemic may have given organizations a momentary "pass," audits are not going away. In fact, a distributed workforce and the number of additional devices will make auditing more complex.

Mature IGA allows organizations to verify the right controls are in place to meet regulatory requirements related to security and data privacy. It provides consistent, repeatable and automated processes — built on top of a common policy, role and risk model — to manage passwords, evaluate and control user access, and verify and document user identity and access controls.

Do your regulatory mandates require IAM/IGA?



ONE OUT OF FOUR RESPONDENTS SAY THEY HAVE NO SYSTEMS IN PLACE TO SUPPORT THEIR IGA PROGRAM.

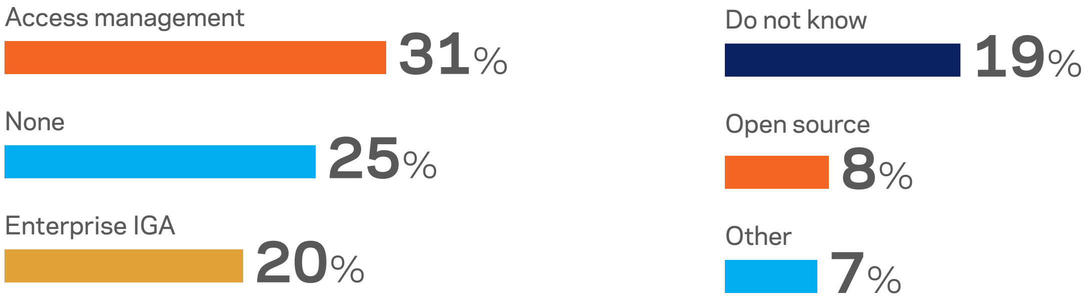
Thirty-one percent of respondents are using access management tools; 20 percent are using enterprise IGA; about 15 percent are using open source or something else; 25 percent are using nothing; and 19 percent don't know.

IT and business staff may be missing out on the value of IGA. IGA doesn't just allow organizations to define, enforce, and enhance provisioning and IAM. It also connects, unifies and extends IAM functions to meet compliance and auditing requirements. As detailed in Gartner's Magic Quadrant, IGA tools provide the following functions: identity life cycle maintenance, entitlement management, access requests through a business-friendly user interface, workflow, policy and role management, access certification, fulfillment, auditing, and identity analytics and reporting.

IGA also helps address complex business challenges. Besides reducing risk, strengthening security, and improving compliance and audit performance, IGA lowers operational costs by automating labor-intensive processes such as access certifications, access requests, password management and provisioning. It also enables organizations to quickly empower workers with the access they need to do their jobs and be productive wherever they are — and regardless of how their roles and access requirements change.

To deploy IGA quickly and effectively, many organizations are turning to third-party experts for help with either in-house deployments or cloud-based solutions. For many, software as a service (SaaS) will be the best route, given tight budgets, IT staffing shortages and the urgencies of the moment. According to Gartner, "Through 2021, customers using a cloud-architected IGA solution will save an average of 30 percent in initial integration costs and 40 percent in overall professional services over a three-year period, and accelerate time to value by an average of 25 percent."

What systems or tools does your agency or department currently use to support your IGA program?



GETTING STARTED

Many organizations struggle with how to get started on their identity governance and administration journey. In partnership with UberEther, Sailpoint has developed an identity governance and administration maturity calculator. This will help you identify where your organization can quickly make improvements to better secure your organization. UberEther's Identity and Access Management experts have successfully brought hundreds of solutions to production for SailPoint customers. Upon completion of the survey you'll have a high-level plan for your organization, but UberEther is also offering a 30-minute free consultation to review your results and make personalized recommendations on next steps. To access the survey, email identity_assessment@sailpoint.com.

Endnotes:

1. Gartner. Magic Quadrant for Identity Governance and Administration. October 2019. https://www.gartner.com/doc/reprints?id=1-1S6W2MQ5&ct=191011&st=sb
2. Ibid.
3. Ibid.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com**.

Underwritten by: SailPoint

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity^{TM} platform. The platform is designed to securely accelerate mission objectives while delivering adaptive security and continuous compliance. SailPoint provides a comprehensive view of access to all resources across multi-cloud infrastructure, and helps make faster, more informed access decisions, detect potential risks and easily enforce access policies for all users. **https://www.sailpoint.com/identity-for/government**