EBOOK

Making the Move to Modern IGA

Expert private sector insights for Government agencies to transition legacy identity platforms

Saviynt

Table of contents

02 **Building Consensus**

Set clear goals and establish relevant metrics

04 **Developing a Roadmap for Modern IGA**

Be cloud-first (or at least curious) and data-guided

In all things, remain agile

06 **Evaluating Modern IGA Solutions**

Intelligent solutions, higher returns.

Minimize business disruption, maximize platform capabilities

Trust the experts, but own your experience

Execute a coexistence strategy

11 **Proving Success and Ensuring Ongoing Value**

Establish a post migration strategy

Measuring success

Saviynt

Uncertain times are catalysts for change. Some federal agencies turn inward and shy away from innovation to preserve the status quo. Others adapt and embrace cloud transformation, including operational agility and scalability as means to provide critical services or complete their mission. Central to this is cloud-architected and modern Identity Governance & Administration (IGA). But while the promise of an agile new platform is attractive, the prospect of large-scale transition is daunting, especially given the scope of many government operations.

Transformation shouldn’t suffer because of migration fears. In many cases, the private sector is the first to move and transform to remain competitive in their markets. Being on the leading edge can teach many lessons – good and bad. In this guide, we share expert advice on preparing for, executing, and measuring a modernization campaign’s success. Insights surround critical themes, including.

- Building Consensus
- Evaluating Platforms
- Managing Migration
- Measuring Success

Importantly, we also feature real-world examples from private-sector practitioners on the other side of successful transitions – leaders just like you. It is our hope that these examples will help influence the success of your government agency transformation.

Building Consensus

Modernizing legacy IGA requires buy-in from a variety of stakeholders. Without it, identity professionals may turn internal allies into resistors. Simeio Vice President, Batool Aliakbar, **suggests leaders** start by taking inventory of impacted roles before building consensus. “Be transparent with everyone from auditors, risk managers, application owners, and end users.” In this, project leads must do their research and understand constituents’ needs.

From there, Campbell's Soup Co. Senior Information Security Architect, Anne Gorman, recommends building a story about life being easier – not just different. "Stakeholders often hold processes too closely, like a baby with a binky. The fastest way to break down a silo is a story about how [modern IGA] makes lives easier."

> "It's OK to have naysayers and take criticism. Always welcome feedback and you'll improve your program"
>
> **Batool Aliakbar,**
> Vice President at Simeio

Don't push ahead alone; enhancing IGA processes requires multiple champions in areas where modern IGA intersects – areas like cloud infrastructure and security, data privacy, and enterprise SaaS management. Find friendly evangelists, **recommends** Simeio's Aliakbar, and trial new processes and programs in a controlled way in their respective departments or functions. By "demonstrating success on a small scale," leaders improve their credibility before a larger scale rollout.

This doesn't mean forging ahead inflexibly, however. Often, opportunities exist to make concessions around a key stakeholder's concern without compromising the bigger modernization vision. Offering choices is a way to let stakeholders feel involved.

> "Acknowledge all the different stakeholders that you have to bring to the table and understand what makes them tick — and determine what category they fit themselves within."
>
> **Jaime Lewis-Gross,**
> Director of Sales Engineering at Saviynt

Additionally, by **rallying other sponsors** or advocacy committees, project leaders will "...increase adoption at a higher speed and boost compliance and momentum," says Jamie Lewis-Gross, Director, Sales Engineering at Saviynt.

Set clear goals and establish relevant metrics

Critically, KPIs must connect to – and prove – the improvement story that project sponsors share. Often, as Campbell's Gorman finds, agencies don't "establish that a program can do what they say it will do." This erodes buy-in. Don't get lost in the 'art of the possible' – instead, pick metrics that promote momentum via early wins. Consider sequencing metrics by complexity and project stage. For example, you may start with day-one availability and then move to a reduction in ad-hoc access requests. Here, the first target provides momentum toward the second.

Ultimately, any goal or metric must connect with executive leaders' priorities. The agency leaders provide strategic air cover via critical budget and support. Modernization is not a grass-roots effort. Ask yourself: do plans address executives' agency goals?

Target improvements that matter to senior leaders early on. These might be agency outcomes (audit/compliance performance or lower costs) or operational changes (fewer deficiencies, faster access review cycles and remediations). At a minimum, identify an executive champion who is a single point of contract for issue resolution and decision making.

Developing a Roadmap for Modern IGA

Be cloud-first (or at least curious) and data-guided

Agencies now operate at the speed of the cloud. This requires flexibility and scalability across IGA processes. Here, legacy solutions fail as traditional boundaries between information technology (IT) and operational technology (OT) dissolve.

"Cloud has destroyed this separation," guides Saviynt Practice Director, Karthik Kumar. "Legacy platforms, even hosted-ones, can't scale to support IGA across both landscapes." The Covid-era exposed these limitations – particularly around remote work.

Kumar highlights the recent example of an Australian-based global company with limited VPN access that needed to scale rapidly to support an entirely-remote workforce. Because of their cloud-based IGA platform, however, they could broadly provide access and operate within the WFH mandate without having to invest on additional VPN licenses. Further, the effort reduced breach concerns by securing privileged and non-privileged accounts.

For agencies journeying toward IGA modernization, this example reinforces the why behind transformation – and reminds how the roadmap must direct success in a cloud-first world.

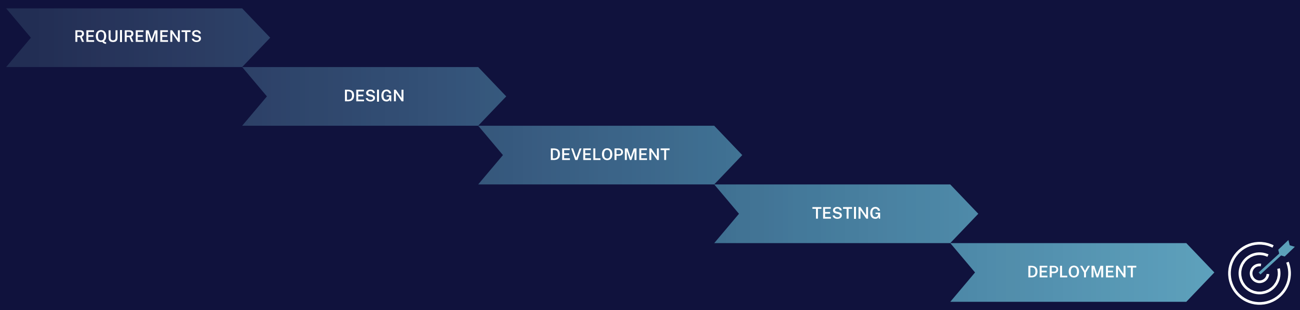
Every roadmap is different, so let organization needs dictate your starting place. This demands a data-informed evaluation. Access provisioning or certification campaigns are useful – but only to the degree that they address specific, identifiable risks. As plans progress, enrich planning with new data to guide future modernization steps. For example, using SIEM and CMDB insights to improve governance practices (like segregation of duties), understanding new event sources, or where sensitive data lives.

Additionally **scope projects** correctly by taking IGA maturity and gaps into consideration. David Kendrick, Manager and Technical Solution Owner of Identity Access & Governance for Cerner, **notes how** this approach led his team to settle on reducing provisioning errors. From there, roadmapping was about "envisioning what we wanted provisioning workflows to be."

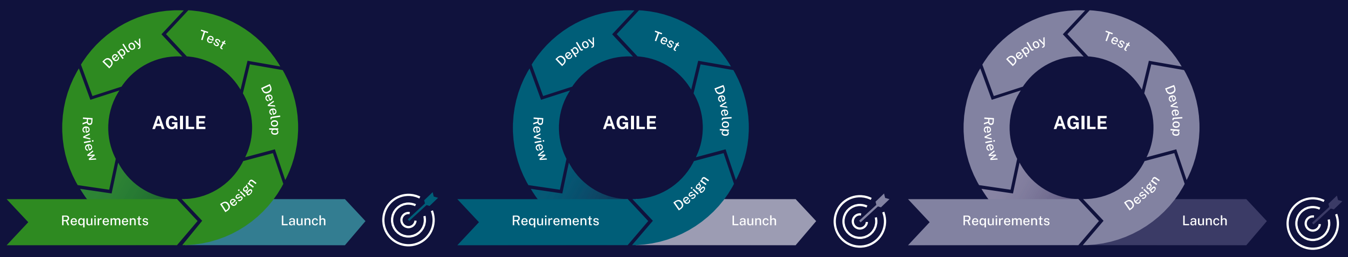
In all things, remain agile

Once agencies define a vision for an improved end-state, they must break down modernization into bite-sized chunks. Saviynt's Kumar sees agility as the foundation. "Plan minimum-viable-projects (MVPs) and a staged rollout over time." Multiple experts caution against a "big bang" approach; that is, the classic all-or-nothing cutover approach that overwhelms systems and staff. This approach takes time, prolongs costs and migration pains, and increases the likelihood of needs changing before agencies realize benefits.

Big Bang Waterfall — Big outcome at end



Agile — Early, cumulative outcomes



Cerner’s Kendrick also champions a staggered approach. “We broke [modernization] down into different components, starting with configuring our environments and reviewing HR workflows.” By documenting various onboarding and offboarding activities, the company was able to “identify bottlenecks in the process” to address in future migration phases.

“Take advantage of package offerings from partnered service and implementation providers,” notes Saviynt’s Kumar. These align with the MVP delivery style and are built around a foundation of templates. Templates simplify activities like onboarding applications and workflows, as well as user access reviews.

Evaluating Modern IGA Solutions

Modern IGA solutions – those that are cloud built with adaptable & frictionless design – deliver agility in a variety of ways. Importantly, they are modular and customizable. This is a departure from traditional static, monolithic design. Cloud-native solutions in particular support agency changes – from managing cloud identities to securing SaaS applications. Along this path, Saviynt’s Chief Strategy Officer, Yash Prakash, suggests **agencies reconsider** how extensible their solution is:

> “Prior IGA concepts revolved simply around identities belonging to humans. As we move towards more cloud and automation, the concept of machine-based identities such as service accounts, robotic process automation (RPA) or internet of things (IoT) devices, grows in importance.”
>
> **Yash Prakash,**
> Chief Strategy Officer at Saviynt

Many identity platforms promise lowered risk profiles, improved decision making, reduced compliance violations, and hardened security postures built around Zero Trust. But most don’t deliver. However, innovative platforms built with intelligent design, including **AI/ML and robust analytics**, will help future-proof your agency.

Further, agencies must consider total-cost-of-ownership (TCO) factors. Legacy IGA solutions stick enterprises with hardware purchasing, ongoing maintenance expenses, and comlex — or potentially impossible — upgrades. The standard data center paradigm is a constant loop of replacing old systems and supporting backup hardware to swap out when old systems fail. The cloud paradigm **eliminates** the upgrade cycle trap.

Agencies often underestimate the impact of these efforts and costs relative to cloud alternatives, shares Saviynt's Director of Product Management, Harvi Nagpal. "On top of the costs for underlying servers and hardware, there are teams dedicated to maintaining the infrastructure and expensive contracts with third-party service providers to support maintenance packages."

These factors create complexity and ultimately reduce long-term value. Nagpal suggests agency leaders ask themselves, "'Do I invest in a platform that will take months to implement, or are there solutions available that let me focus on workflow migration versus installation?'"

ComputerWeekly also **suggests assessing** whether the platform can meet the regulatory requirements for consent management, access requests and approval, regular access review, and the management and enforcement of SoD rules.

Focus on the original premise of improvement too, knowing that your IGA platform is the primary means for enforcing critical governance and compliance policies. "Whether you're trying to meet CMMC certification or achieve Zero Trust objectives, you need to know the controls, metrics, and capabilities a modern IGA platform enables," shares Nagpal.

Intelligent solutions, higher returns.

In its recent Total Economic Impact report on SaviyntIdentity Cloud, Forrester notes how many agencies contend with onerous identity and access governance responsibilities using a "combination of on-premises, homegrown tools that require internal coding, regular maintenance and upgrading, and significant management time."

During platform evaluation, look for differentiators like "bigger governance application offerings, direct connectors, user access review capabilities", as well as low-code/no code environments and access hub functionality to monitor and control applications. According to Forrester, benefits with cloud-based IGA platforms include:

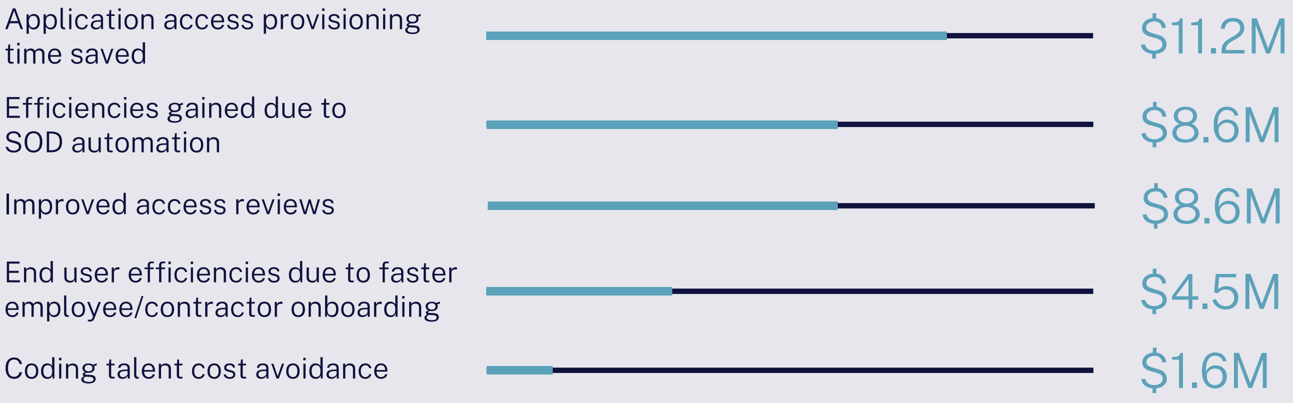
Pro Tip

Saviynt Identity Cloud platform offers a control library that incorporates common application and compliance requirements including HIPAA, HiTRUST, SOX, PCI DSS, CPPA, GDPR, ISO 2000 series, and NIST.

- Time saved with application access provisioning
- New efficiencies due to SOD automation
- Improved access reviews
- End-user efficiencies due to faster employee and contractor onboarding
- Coding talent cost avoidance
- Reduced IT resolution time
- Timely, on-demand privileged access management

ROI	BENEFITS PV	NPV	PAYBACK
240%	$34.4M	$24.3M	<3 months

Benefits (Three-Year)



Forrester estimates that implementing Saviynt IGA can save your organization $34.4M and achieve a 240% ROI over three years.

Minimize business disruption, maximize platform capabilities

Unlike traditional PAM or even IT projects, IGA modernization cuts across a variety of stakeholders. Be aware of wholesale process or experience breakages that disrupt user experiences and operations. To the degree that changes come, leaders must evangelize how modernization frees workers to do their real jobs and not just 'identity-like' tasks.

Adam Barngrover, Principal Solution Strategist at Saviynt **agrees that** the hardest part of the migration and implementation phases is dealing with human emotion. He guides project leaders to not execute in isolation, but share continuous reminders of project benefits.

> “Don't just tell someone about the new access they'll receive. Remind them what this access is for and why it matters.”
>
> **Adam Barngrover,**
> Team Lead – Solutions Engineering at Saviynt

In addition, while expediting migration and implementation is admirable, don't just transfer 'as is' legacy processes to your new platform. This leads agencies to underutilize the capabilities of modern tools and suboptimize compliance.

“Many agencies have a habit of running access certifications quarterly or half-yearly,” notes Saviynt's Nagpal. “Instead of mimicking this in a new environment, be aware of optimization opportunities like triggering immediate access certifications, or 'microcertificaitons' around critical identity or joiners-movers-leavers events.”

Another optimization opportunity area is preventative SOD violation checks. Not only does this harden security, but it brings benefits to other offices and leaders–accelerating buy-in in an otherwise uncertain time of platform change.

Trust the experts, but own your experience

Migration automation tools are critical to moving capably through platform transition. Partnering with a systems integrator (SI) offers meaningful return in terms of reduced drain on internal resources, stakeholder morale, and overall deployment speed and time-to-value.

Lean on leading SIs' orchestrator tools to help automate platform configurations. Many have programs to analyze migration efforts and determine reasonable roadmap, milestones, and timing. Nagpal cautions agencies against trusting too heavily in prescriptive, step-by-step guidance from any external party, though:

> “Only you truly understand your IT ecosystem. You know how your backend integrates into the variety of applications, active directory, and databases. You know if there are multiple tools for requesting certain access or how a certain application owner runs certifications.”
>
> **Harvi Nagpal,**
> Sr. Director of Product & Partner Success at Saviynt

No expert can address every situation for you.

For example, identifying what tool access rules need migrating as you reestablish lifecycle management processes on the new platform is something only internal leaders know. These are critical issues, however. What is routed in the legacy platform needs to transfer over or you may have unintended issues of persistent access.

His takeaway: “Seek advice from partners and solution providers, but own the hard work of developing a programmatic approach yourself.”

Execute a coexistence strategy

Migration, implementation, and deployment issues can overwhelm even experienced implementation teams. To improve modernization outcomes, transition around three guiding principles:

Begin bite-sized: Don’t anticipate a single, major cutover. Instead, focus on a “coexistence” period between the modern IGA solution and your legacy platform. Don’t turn this into a passive wait-and-see period though. Transition modern user experience, analytics, and machine learning capabilities to “front end audit” data in your existing legacy platform.

Pro Tip

As your cutover date nears, mind the execution level details that affect user experience. One example: addressing access requests or other processes that are in-flight on the old platform.

By moving these capabilities first, agencies gain new insights into their audit posture using data that already exists. This may feel like using the new platform as a facade on your old solution–and it should. Doing this brings rapid value by surfacing previously unknown audit issues. In this, it qualifies business outcomes and remediation areas for the next migration phase.

Lift, *refine*, and shift: Review existing processes, and validate or refine them before adopting them in the new IGA platform. Often, agencies apply a "like-for-like" lift and shift strategy–and unwittingly introduce bad habits or manual steps into new workflows. For example, every company has those time-sucking "ten step access request and approval processes." Look for ways to consolidate into two to three steps and introduce the reimagined and potentially AI-driven processes instead.

Focus on experience, but be data aware: While your systems briefly co-exist, plan a cutover strategy with user experience at the center. Early user adoption sets the trajectory for further IGA platform use. So, focus on operational efficiencies and process areas that tangibly aid users' work. These may include automated user lifecycle management, birthright access, or priority app onboarding. In your eagerness, don't neglect multi-way data synchronization issues between your old and new IGA platforms. This shows up when you manage data, a process, or an application in two separate locations. Once an application onboards, cutover all associated processes to avoid data integrity or synchronization pitfalls.

Pro Tip

Consider specific compliance mandate requirements to determine how long you need to support/maintain legacy databases.

Proving Success and Ensuring Ongoing Value

Establish a post-migration strategy

Now is the time to look for enhancements to build on the foundation you created. This is the fun stuff!

Ask yourself what else can you converge into your modernized IGA program? Layering new, critical endpoints and adding functionality for more analytical capabilities can add significant value to your program. You've done the hard work, now take advantage of new opportunities for privileged access management. For example, store credentials for certain access inside a vault and let users check them out.

Similarly, because the modern IGA platform is flexible, reorient how you roll out updates and releases. Consider co-opting the DevOps model of micro-releases to keep your identity and digital transformation journey moving.

As Saviynt's Barngrover notes, "You put thousands of users on Microsoft Teams overnight. You have the right data points to give users the right access and make faster improvements – use them!"

Measuring success

While modernization 'success' is broadly defined, a few key metrics typify real improvement. Plan toward these so that your migration, implementation, and deployment efforts lead to target outcomes.

Pro Tip

Reference platform dashboards for a before-and-after view of issues like audit exposures and incidents.

- How quickly were you able to onboard?
- How many new services or capabilities were you able to introduce?
- How many applications were you able to onboard?
- How did your compliance posture rate increase?
- Did audit findings decline and compliance posture improve? By how much?

Depending on your operational use case, also consider –

- How significant was the reduction in tickets?
- What process issues are now eliminated?
- How much FTE and/or contractor time is saved related to supporting legacy platforms?
- How much time is saved during access provisioning per user?
- How much time is saved by automating joiner/mover/leaver processes?
- Other productivity captured?

Savyint's Karthik suggests agencies consider insight availability and ease of data retrieval when measuring implementation success. "Agencies should use platform controls to quickly understand their audit posture with simple before-and-after views. Dashboarding makes it obvious what audit issues were remediated."

> “Awareness around which audit issues existed and were resolved is a baseline to measure value.”
>
> **Karthik Kumar,**
> Practice Director at Saviynt

Karthik also suggests that agencies consider returns in the area of human and machine identity onboarding. “Yes, this is a speed and time-savings issue, but it also proves cost-efficiencies” because of reduced skill, training, and support requirements related to managing onboarding. Forrester notes how time savings for identity access administrators saved one enterprise client approximately $11.2 million over three years.

Don’t forget harder-to-quantify areas like user experience. Cerner’s Kendrick, **found that** automating as much as possible, reducing complexity, and targeting specific user experience outcomes simply reduces “the number of things that can go wrong.”

Want to learn more about measuring the ROI of your identity investment?

Sean Ryan of Forrester shares five of his best practices for maximizing return on identity management investments.

READ BLOG WATCH WEBINAR

Sean Ryan
Senior Analyst
Forrester

Conclusion

New transformative business models for federal agencies demand agility, scalability, and improving security at the new perimeter–identity. But don’t let legacy platforms and mindsets limit your pursuit of more modern IGA.

Changeover to a new solution isn’t easy–anything that impacts people and processes never is. So understand users’ needs, evangelize value-based change, and leverage expert help. Remember: intelligent identity is cloud-architected and fast-tracks business in the digital age.

Saviynt

Saviynt Identity Cloud helps modern enterprises and Federal agencies scale cloud initiatives and solve the toughest security and compliance challenges in record time. The company brings together identity governance (IGA), granular application access, cloud security, and privileged access to secure the entire business ecosystem and provide a frictionless user experience. The world's largest companies trust Saviynt to accelerate digital transformation, empower distributed workforces, and meet continuous compliance, including BP, Western Digital, Mass Mutual, and Koch Industries. For more information, please visit **saviynt.com**.

Want to talk to an identity and security expert?

SCHEDULE A CALL TODAY

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com