Making the Move to Modern IGA

Expert insights to transition your legacy identity platform

Saviynt

Table of contents

Saviynt

Uncertain times, whether led by recession, regulation, or competition, are catalysts for change.

Some businesses grow defensive, shying away from innovation to preserve the status quo. Others adapt and embrace transformation, including cloud-driven agility and scalability as means to survive or thrive. Central to this is modern Identity Governance & Administration (IGA). But while the promise of an agile new platform is attractive, the prospect of large-scale transition is daunting.

Business transformation shouldn't suffer because of migration fears. 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, and measuring success.**

Importantly, we also feature real-world examples from practitioners on the other side of successful transitions – leaders just like you.

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.

PERSPECTIVE FROM THE PROS

"It's OK to have naysayers and take criticism. Always welcome feedback and you'll improve your program."

– Batool Aliakbar, Vice President at Simeio

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."

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.

> PERSPECTIVE FROM THE PROS
>
> **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, 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 Lewis-Gross.

Set Clear Goals and Establish Relevant Metrics

KPIs must connect to – and prove – the improvement story that project sponsors tell. Campbell's Gorman often **finds** that companies 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 or targets that add momentum via early wins. Consider organizing goals 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.

Ultimately, any goal or metric must connect with executive leaders' priorities. Thus, understanding critical stakeholders' goals (both general and specific) is a priority. At Saviynt, we've seen goals range from quantifiable cost savings, to squishier targets like *continuous compliance* or *no standing privilege.*

The C-suite provides strategic air cover via critical budget and support. Modernization is not a grass-roots effort. Ask yourself: *Do plans address executives' business goals?*

Target improvements that matter to senior leaders early on. These might be business 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 to back issue resolution and decision making. Good news...this may be easier than you think: According to StateTech, *Identity & Access Management* is the **number one priority** in terms of technology, application, or tool investment for CIOs in 2023.

Developing a Roadmap for Modern IGA

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

Businesses 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.
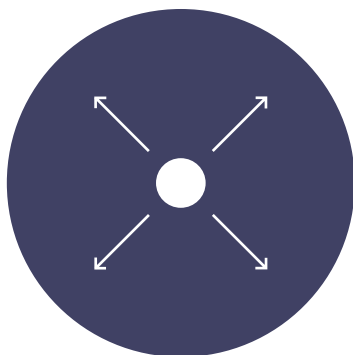
"Cloud has destroyed this separation," guides VP of Professional Services, APAC at Saviynt, Karthik Kumar. "Legacy platforms, even hosted-ones, can't scale to support IGA across both landscapes." The Covid era exposed these limitations – particularly around distributed workforces. Today, remote is officially **the office** of the future.

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 provide access and operate within the work-from-home mandate without having to invest in additional VPN licenses. Further, the effort reduced breach concerns by securing privileged and non-privileged accounts.

Rarely do enterprises re-architect infrastructure all at once. To be genuinely 'future proof,' IGA must immediately bring seamless, secure access to resources – whether in the cloud, on-premises, or in hybrid environments. The stakes are sky-high: Today, up to 10% of an enterprise's cloud identities **have enough permissions** to delete that organization's entire cloud.

Steve Edford, Analyst, Identity and Privileged Account Management at Phillips 66, **points out how a cloud-native model** supports enterprises regardless of the state of their architecture:

"Our on-prem solution could only manage other things on-prem, and Saviynt has the ability to manage things both on-prem and in the cloud, so that was one of the things that made us realize that this is really a good solution for us in both realms."

– Steve Edford, Analyst, Identity and Privileged Account Management – Phillips 66

For companies journeying toward IGA modernization, these examples reinforce the why behind transformation – and remind us how the roadmap must drive success in a cloud-first world.

Start (and stay) stakeholder-centered

Leaders at VMware caution against IT teams diving into 'implementation mode.' Instead, they encourage a robust planning stage punctuated by **in-depth collaboration** with stakeholders, including HR.

"**Pulling in business units to form a VP-level governance committee, is essential to guide the direction of the transformation program and to help manage through organizational challenges and changes.**"

– Tim Mooney, Sr. Director, Infosec at VMware

Every roadmap is different, so let business needs dictate your starting place. This demands a data-informed evaluation. Some **activities** like access provisioning or certification campaigns are useful – but only to the degree that they address 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 separation of duties), understanding new event sources, or where sensitive data lives.

In the case of Phillips 66, **the security team wanted** to unlock standardization and consistency of control execution, processes, and tools to improve user experience and enforce governance and regulatory compliance. For them, this became the critical starting place.

We see this as a key example of scoping projects correctly by acknowledging IGA maturity needs and gaps.

This video, From Zero to Sixty: A Case Study in IGA Transformation, illustrates a successful IGA modernization project at VMware.
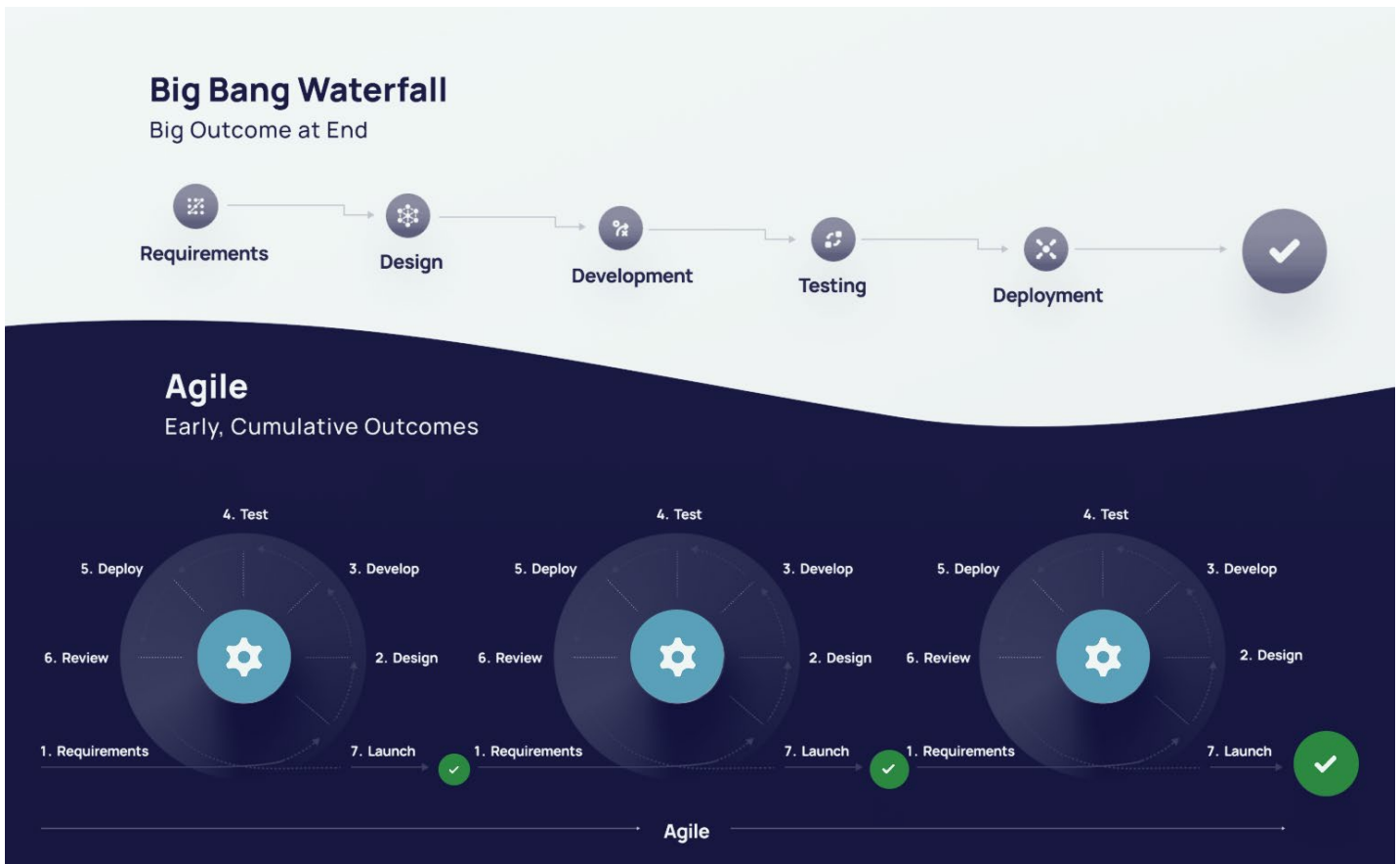
In all things, remain agile

Once companies 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 companies realize benefits.

Big Bang Waterfall
Big Outcome at End

Requirements → Design → Development → Testing → Deployment

Agile
Early, Cumulative Outcomes

Agile

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 business changes – from managing cloud identities to securing SaaS applications. Along this path, Saviynt's Chief Product Officer, Vibhuti Sinha, suggests **companies reconsider** how extensible their solution is:

"Prior IGA concepts revolved simply around identities belonging to humans. With the acceleration in Cloud adoption and growth, there is an exponential proliferation of machine identities. With a 1:10 ratio between humans and machine identities, securing and governing machine identities is paramount which is comprised of bots, service accounts, IoT devices, serverless functions and many more."

– Vibhuti Sinha, Chief Product Officer at Saviynt

While 'identity' once meant human users inside four walls, the term encompasses everything from bots, APIs, and workloads, to vendors, customers, and partners. If an entity can be discretely identified – and has a consistent set of attributes, it needs securing. Truly **modern IGA** delivers this across identity types.

During evaluation, KuppingerCole **points out** that enterprises must cut through the noise and assess a platform's ability to streamline fundamental activities:

"Key to achieving both data security and regulatory compliance is the ability to manage identities effectively and enforce policy-based access controls to ensure only authorized people and things have access to IT systems and data under the correct circumstances."

– KuppingerCole Analysts

With respect to recent IGA platform innovations, we're excited about machine-learning and analytics. ML capabilities **streamline workflows** including around access reviews, requests, and recommendations – and help minimize administrator frustrations.

Machine Learning Provides:

- Access recommendations

- Role analysis and recommendations

- Lifecycle automation

- Access activity reviews/assessments

- Outlier detection

- Access approval and revocation

- Orphan account identification and remediation

- Separation of Duty (SoD) identification

- Risk-based insights

Enterprises are also leveraging strong analytics engines to perform ML-based activities like identifying anomalous behavior and finding outliers that increase enterprise risk.

Many identity platforms promise lower risk profiles, improved decision making, reduced compliance violations, and hardened security postures built around Zero Trust. Yet most don't deliver. However, intelligently built platforms can spark the future-proofing businesses want.
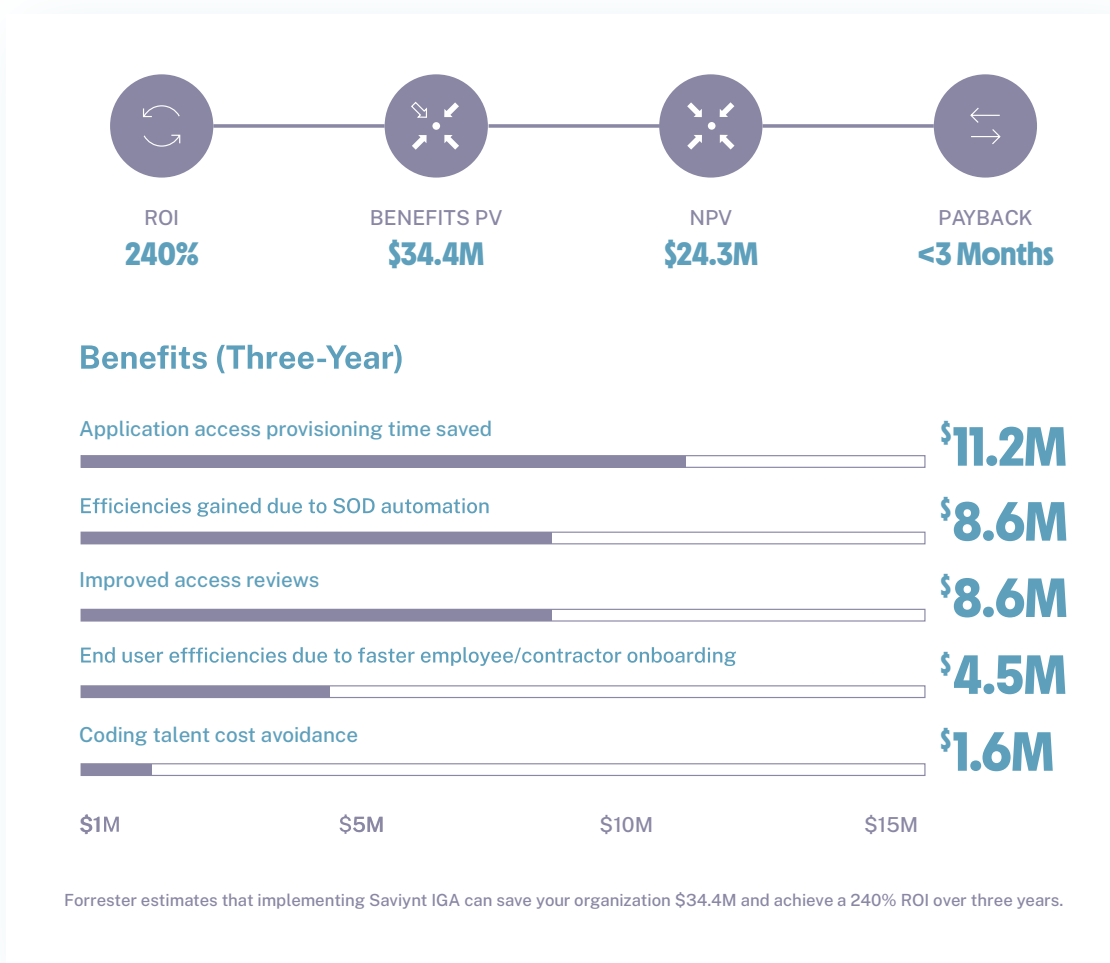
5 Must Ask Questions for Evaluating IGA Solutions

WANT TO LEARN MORE? CHECKOUT OUR NEW BUYER'S GUIDE ⟶

Consider your costs (both obvious, and not-so-obvious)

Companies must weigh total-cost-of-ownership (TCO) factors. Legacy IGA solutions stick enterprises with hardware purchasing, ongoing maintenance expenses, and complex — 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.

Many underestimate the impact of these efforts and costs relative to cloud alternatives, shares Saviynt's VP of Solutions Engineering, Jonathan Neal. "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."

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

Benefits (Three-Year)

Application access provisioning time saved	$**11.2M**
Efficiencies gained due to SOD automation	$**8.6M**
Improved access reviews	$**8.6M**
End user effficiencies due to faster employee/contractor onboarding	$**4.5M**
Coding talent cost avoidance	$**1.6M**

$1M $5M $10M $15M

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

These factors create complexity and ultimately reduce long-term value. Neal suggests C-level 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?'"

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 a healthcare company under HIPAA or a financial services company under SOC or PCI DSS mandates, you need to know the controls, metrics, and capabilities a modern IGA platform enables," shares Neal.

PRO TIP

Saviynt's Identity Cloud platform offers a control library that incorporates common application and compliance requirements including

HIPAA   HiTrust   SOX   CPPA   GPDR   ISO 2000   NIST

Intelligent solutions, higher returns

In its Total Economic Impact report on Saviynt's Identity Cloud, Forrester notes how many companies 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."

According to Forrester, benefits with modern, cloud-based IGA platforms include:

- 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

When evaluating a platform, 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.

An emerging marker of modernization is also key security functionality convergence. Modern IGA solutions ingest information from essential security and GRC platforms including PAM, SIEM, UEBA, and vulnerability management tools.

Leading platforms **also converge core technologies** like PAM and IGA. This capability convergence means that security leaders can provide the "right" access levels to all user types. Don't underestimate the importance of this: Today, only **35% of IT security practitioners** have confidence in the ability of their current security controls to prevent internal threats from accessing privileged credentials.

FORRESTER®

Saviynt has some very unique features that their competitors don't offer. The combination of their bigger governance application offerings, direct connectors, and user access review capability, all in a cloud-based solution...it's been a game changer for us."

- **Senior manager of identity and access management**

READ THE STUDY

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 perform 'identity-like' tasks.

Jaime Lewis-Gross, VP of Solutions Engineering at Saviynt, finds that the hardest part of migration and implementation is dealing with human emotion. She guides leaders not to execute in isolation, but to regularly remind stakeholders about 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."

– Jaime Lewis-Gross,
Director, Sales 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 companies to underutilize the capabilities of modern tools and suboptimize compliance.

"Many companies have a habit of running access certifications quarterly or half-yearly," notes Saviynt's Neal. "Instead of mimicking this in a new environment, be aware of optimization opportunities like triggering immediate access certifications, or 'microcertifications' 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. Neal cautions companies against trusting too heavily in prescriptive, step-by-step guidance from any external party, though:

"Only you truly understand your business. You know how your backend integrates into applications, active directory, and databases. You know if there are multiple tools for requesting certain access or how a certain application owner runs certifications."

– **Jonathan Neal,** VP, Solutions Engineering at Saviynt

No expert can address every situation for you.

For instance, 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 was routed in the legacy platform needs to transfer over or you may have unintended issues of persistent access.

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

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.

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.

But avoid turning this into a passive wait-and-see period. Start by transitioning front-end capabilities like user experiences and analytics. By moving these first, you can gain insights into your 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. This sequencing will surface previously unknown audit issues and guides what remediation areas to focus on next.

Another piece of a start simple ethos is using "BYO-capabilities"–like *Bring Your Own Keys* and *Bring Your Own Vault.* These allow companies to leverage past investments, and mitigate the cost, complexity, and regression worries that can spoil modernization.

Lift, *refine*, and shift

Review existing processes, and validate or refine them before adopting them in the new IGA platform. Often, companies 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!

> **"You've done the hard work, now it's time to capitalize on new opportunities for privileged access management. For example, embark on a zero trust journey with Just In time and just enough access or get the ball rolling with check in check out of credentials securely from the vault."**
>
> **– Vibhuti Sinha,** Chief Product Officer at Saviynt

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.

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.

- 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 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 Kumar suggests companies consider insight availability and ease of data retrieval when measuring implementation success. "Companies 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 measure of value."

– Karthik Kumar, VP of Professional Services, APAC, at Saviynt

Kumar also encourages companies to 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.

PRO TIP

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

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.

WATCH WEBINAR   **READ BLOG**

Conclusion

Both transformative business models and robust defense demand agility, scalability, and improvement at the new security 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–but anything that impacts people and processes never is. So empathize with users' needs, evangelize value-based change, and leverage expert help. Remember: intelligent identity is cloud-architected and fast-tracks business in the digital age.

1 https://saviynt.com/2020-forrester-total-economic-impact-report/

Saviynt

Saviynt's Identity Cloud helps modern enterprises scale cloud initiatives and solve the toughest security and compliance challenges in record time. The platform 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 brands trust Saviynt to accelerate digital transformation, empower distributed workforces, and meet continuous compliance, including BP, Western Digital, Mass Mutual, and Koch Industries.