

EBOOK

The Hidden Costs of IGA

Stop Sabotaging ROI And Maximize
Platform Value

Saviynt

Table of contents

- 02 Hidden Costs: When Plug-and-Play Becomes Plug-and-Pay
- 02 Hidden Cost #1: Integration
- 05 Hidden Cost #2: Customization
- 07 Hidden Cost #3: Maintenance & Management
- 11 Hidden Cost #4: Business Intangibles
- 14 Conclusion

When Plug-and-Play Becomes Plug-and-Pay

The notion of transforming Identity Governance & Administration (IGA) fuels both excitement and uncertainty. While modernization is attractive, the prospect of a **large-scale transition** is daunting.

In response, some enterprises balk. They worry about sweeping change or reflect on all the time and money invested in a legacy platform. In either case, they convince themselves that the status quo still works. Others settle for IGA solutions that feature both on-premises and cloud components – and eventually struggle with compatibility and management headaches.

In any scenario, enterprises must remember:



IGA solutions carry costs beyond the sticker price. These costs present as hard dollars or, more indirectly, as issues like lost opportunity, inefficiency, and inflated risk.







In this guide, we surface factors that add complexity to IGA programs and reduce long-term program value. Throughout, you'll also discover common cost-of-ownership pitfalls – and gather insights on how cloud innovation helps you avoid each.

Hidden Cost #1

Integration

Acquiring IGA is not simply a matter of buying and installing software. Although significant resource and cost utilization savings **exist in cloud-architected** IGA solutions, “companies underestimate the impact of the efforts and costs of legacy IGA relative to cloud alternatives,” shares Saviynt’s VP, Products and Experience, Anirudh Sen.

Compared to organizations deploying IGA on-premises, companies that adopt cloud platforms tend to invest less on application and system integration – particularly for enterprise tools. So when assessing modernization cost, **companies must consider the number and depth of integrations – and the availability of out-of-the-box modules to support application, data, or infrastructure access governance.** To avoid costly integration troubleshooting and custom engineering, determine availability of direct integration for applications and infrastructure like:

| | | | | |
|---|---|-------------|--|---|
| ORACLE |  | <i>Epic</i> |  | aws |
|  |  | servicenow |  |  |

Without means for simple, direct integration, enterprises endure exorbitant effort and costs for custom connections and manual security controls. Extra investment in architecture is often required to support integration builds – including a need for agents or infrastructure components to connect on-premise systems and cloud tools.

While dissecting integration costliness, Forrester acknowledges a need for unified, cloud-based platforms to integrate governance of multiple identities and access management. In their recent **Total Economic Impact** report on Saviynt’s Identity Cloud, Forrester describes the integration challenges that a company with legacy IGA solutions must overcome.



“[The enterprise] performed identity and access governance duties manually, or they relied on separate point solutions from multiple vendors.

Lacking cross-platform visibility, the customers described their regular tasks as time-consuming, incomplete, error prone, and less frequently performed, which offers bad actors the opportunity to take advantage of excessive permissions...”

The Total Economic Impact™ of Saviynt Cloud Enterprise,
Forrester, 2020

Costs of Compensating for Weak Integration

Modern workforces demand frictionless access (and often self-serve capabilities) within business applications. Naturally, companies harbor concern about compromising access governance while delivering this access. **In response, security leaders may overcompensate and introduce multiple monitoring solutions, overextending tools and support resources.** Cloud-architected platforms fix this, and enable consolidated management, which is a boon to cost savings.

Traditional offerings cannot support “single-pane-of-glass” management, whereas modern offerings allow administrators to monitor and manage multi-cloud strategies by centralizing identity management onto a single platform. This reduces administrative burdens and management fatigue.

By example – Saviynt’s Identity Cloud platform integrates with a federation solution to extend Single Sign-On (SSO), or directly provision console users with granular access (including time-bound rules) to prevent orphaned and excess access.

To reduce maintenance costliness, Gartner notes how enterprises should “prioritize fulfillment capabilities, including a comprehensive list of out-of-the-box connectors that is aligned to the main target systems in the organization¹.” Their research warns enterprises that are evaluating IGA solutions to remember that “[IGA] is heavily dependent on integration and consulting services.” As such, organizations must consider “the ability of the vendor to offer out-of-the-box integrations” for both economic and technical reasons.



SMART SAVING TIPS

Reduce application onboarding time by up to 90%*

Assess availability of pre-built templates, robust control libraries, and intuitive wizards to reduce application onboarding time and improve user experience.

*Total Economic Impact of Saviynt Identity Cloud, Forrester Research 2021

¹ Buyer’s Guide for IGA: Top 4 Elements of a Successful RFP, Gartner, 2020

Customization

Excessive customization costs enterprises in two ways: increased spend and reduced agility in the future.

CEO World Magazine **highlights** how traditional IGA carries significant custom development baggage—and imposes troubling operational ‘gotchas.’ Consider the surprise one unassuming enterprise felt during procurement:



“What was unclear at the time was that all the customization required to get value out of the solution made future upgrades costly endeavors.”

According to Saviynt’s Ivan Childress, Director, Industry Identity Cloud (Healthcare) the problem with hyper-customization is that you develop yourself into a corner:

“Future requirements pile up, and basic blocking-and-tackling like troubleshooting bugs or security and compliance updates become complex and costly.”

Legacy solutions that were conceived prior to new data integration standards exacerbate the issue. Conversely, ground-up new builds likely have open data models built around modern connectivity standards.

Impact of (Excessive) Engineering

When enterprises limit customization, they tend to enhance value return. For example, when a modern identity platform consumes and exchanges risk data across information security risk monitoring tools (including SIEM and UEBA), **IT departments increase their effectiveness, reduce risk-monitoring fatigue, and decrease operational cost.**

Of course, some customization is expected because every organization has different workflow requirements; a healthcare provider may need HIPAA-specific workflows that a manufacturer won't use. Because of this, organizations should look for a flexible SaaS-delivered IGA solution that provides customizable workflows and is robust enough to address all of their needs while still providing room for growth.

This doesn't mean reject configurability because of customization concerns.



“Organizations need flexible solutions but also ones that maintain guardrails to prevent excessive customization and maintenance or update overheads.”

Yash Prakash,
Chief Strategy Officer, Saviynt

To support intended ROI, eWeek Data Points **suggests** enterprises find IGA solutions that are “configured to your business needs with enough flexibility to provide the features you need within the standard product.” This flexibility must be centered on standards and extensions that make it easy for customers to build on and integrate with other enterprise systems.

They note how it should be possible to define and modify business processes and controls through configuration (which is different from customization and virtually impossible with on-premises deployments) without the need for compilation.

Vigilance Around Customization in Any Delivery Model

Do note: Even within SaaS solution options, rigidity may exist. Customization assessments ought to be performed across cloud platforms too. Otherwise **organizations may** “compromise security and functionality when cornered into rigid, pre-set workflows” or end up piece-mealing their own siloed workarounds and “reinvent governance” in a costly, compromised way.

Enterprises must also understand upgrade model demands for solution APIs, including how many versions need support and how often they will change.



SMART SAVING TIPS

To avoid customization cost overrun...

Assess the availability of extensions, APIs, and SDKs within an IGA solution for privileged access management functionality.

Hidden Cost #3

Maintenance & Management

Maximizing ROI must also include capitalizing on indirect benefits. As the Identity Management Institute suggests, **these include** activities such as:

- ✓ Improving compliance
- ✓ Reducing IT administrative workloads
- ✓ Lowering breach-related expenses



“Companies must consider total-cost-of-ownership (TCO) factors. Legacy IGA solutions stick enterprises with hardware purchasing, ongoing maintenance expenses, and complex — or potentially impossible — upgrades.”

Anirudh Sen,
VP, Saviynt Products and Experience

While enterprises generally budget for direct costs, **few understand how difficult it is to actually assess spend across applications, data center hardware, connectors, and professional services.**



Unfortunately, the 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,” says Sen.

Also neglected in budgeting are supplemental support requirements: “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,” guides Sen.

Constrain Your Costs With Cloud

Modern “IGA-aaS” automates manual processes and accelerates employee efficiency, proving that identity governance via a cloud-architected approach **saves time and money**.

According to interviewed customers deploying Saviynt’s Identity Cloud, manual review and reporting of application user access privileges once required over three weeks per application to complete. In many cases, enterprises now complete application access reviews automatically – eliminating three weeks of staff time and generating nearly \$3 million in annual savings².

With Saviynt's IGA-aaS in place, enterprises can:



Experience Rapid TCO

The fastest initial implementation speed in the enterprise and a rapid, continual onboarding model ensures swift ROI. Be ready to go live in six weeks and keep moving forward.



Reduce Costs

Automated identity governance saves time and money. Saviynt’s IGA-aaS automates manual processes and accelerates employee efficiency, and our risk-based access requests can reduce the number of approvals requiring oversight by up to 60%.



Enable Agility

Centralize identity to streamline retiring legacy systems. Saviynt’s agility enables swift onboarding of new applications and user populations.



Repurpose Headcount

Reduce administrative overhead and maximize value. With Saviynt’s no-code/low-code solution, managing governance no longer requires significant staff, freeing your employees up for more valuable activities.



Eliminate Technical Debt

Lower your on-premises footprint with Saviynt’s SaaS-like model. You never have to manage the system, only your users and data. Move from the heavy weight of bare metal to the light, lean cloud.

²The Total Economic Impact™ of Saviynt Cloud Enterprise, Forrester, 2020

These efficiencies also account for savings from reduced IT overhead and hiring and training of new employees.

In a recent study, PwC **highlighted** cloud's untapped potential to propel strategy – and emphasized how much unrealized value is still out there. According to their findings, “now is the time for executives to coalesce around a broader definition of cloud and the value it can bring to drive business transformation.”

Every enterprise interacts with these cost avoidance arenas differently. However, we feature a few of the likeliest savings outcomes below. Keep in mind, while these represent potential savings, the inverse is also true: Companies who deploy legacy solutions may not only miss out on savings, but will incur unexpected expenses related to each.

Three notable value clusters surface in their report:

- ✓ **Improved operational resilience, safety, and soundness**
- ✓ **Increased revenue**
- ✓ **Cost savings and efficiencies**

\$1.6M

Three-Year Benefit PV Coding Talent Cost Avoidance



Coding talent cost avoidance. When identity and access governance responsibilities are managed automatically, enterprises eliminate costs to onboard coding talent. For some enterprises, this merits \$1.6 million to the organization over three years³.



Automated provisioning savings. One industry report **finds that** automated provisioning can reduce security administration involvement by 14,000 hours per year – and free up 6,000 hours of help desk time.



Time-to-work productivity. With legacy IGA, 10-day provisioning for new employees or contractors is common. According to one Saviynt customer, cloud-architected IGA reduced this joiner-mover-leaver delay by 90%. Organizations may even embrace pre-provisioning for further efficiency⁴.

³ Ibid.

⁴ Ibid.

The Total Economic Impact™ of Saviynt Identity Cloud

Through 4 customer interviews and data aggregation, Forrester concluded that Saviynt Identity Cloud has the following three-year financial impact.

**BEFORE
10 DAYS**



Time to provision a new employee or contractor

**AFTER
1 DAY**



Time to provision a new employee or contractor with the Identity Cloud



Prior to deploying Saviynt, we were using a lot of homegrown tools for provisioning and governance. Saviynt allows us to manage identity governance and administration across divisions and applications.

Global identity management leader, Multinational chemical processing company

Saviynt Identity Cloud by the Numbers



9 working days saved per year per onboard user



3 weeks required for user access review eliminated with automation



10 minute reduction in access provisioning time per use per app

FINANCIAL SUMMARY



ROI
240%

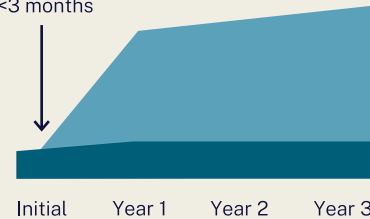


NPV
\$24.3M



PAYBACK
<3 months

Payback Period
<3 months



Benefits
\$34.4 Million

Costs
\$10.14 Million



SMART SAVING TIPS

Consider the technical debt and widened on-premises footprint generated by legacy tools.

Reduce system management requirements and redirect this energy and cost to user and data management instead.

Hidden Cost #4

Business Intangibles

Enterprises also contend with the hard-to-quantify (but damaging) outcomes associated with legacy IT infrastructure. Although these are not guaranteed, they are as expensive as they are hidden.

Data Breaches

As data breaches increase in severity and volume, organizations need **to secure** their mission-critical systems, networks, software, and applications. When companies assess IGA solutions, they must be aware of infrastructure concerns aggravated by on-premises or homegrown tools. These include:



Additional complexity from operating modern IT infrastructures in legacy environments



Reduced management ability from disconnected services across the IT ecosystem



Expanded entry points due to legacy IT infrastructures connected to the cloud



Separation of duties and “least privilege necessary” violations driven by gaps from fragmented identity systems

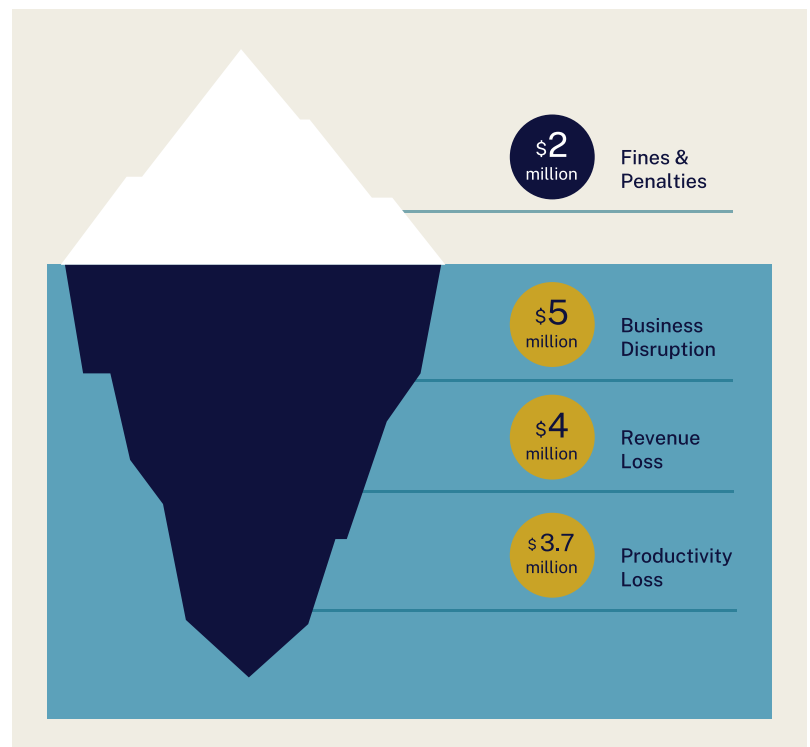
Maintaining data integrity requires an enterprise to control data access and use. Legacy on-premises identity access management systems often fail because they are ill-equipped for the increased connections required by internal and external users. Solutions boil down to intelligence. Enterprises must deploy solutions that simultaneously identify risky user behavior, deliver just-in-time access and removal, and take action when security controls are violated.

Not only does intelligent technology drive safer decisions, but it **frees up resources** so risk managers can focus on higher-value projects and initiatives.

Non-Compliance

Although significant, non-compliance costliness extends beyond simple fines. Consider other “costs” **associated with** non-compliance events:

- Business disruption
- Productivity losses
- Revenue losses
- Fines, penalties, and settlement costs
- Reputation damage



According to the **True Cost of Compliance with Data Protection Regulations** study, in the last decade there was a 45% increase in non-compliance costs. One study pegs the total cost of an information security and data privacy-related non-compliance issue at \$14 million.

Compliance maintenance is quite “cheap” when compared to the expense of resolving non-compliance. On average, smaller organizations spend about \$2,000 per employee annually on compliance initiatives. Organizations with over 5,000 employees spend \$700 per person. For large enterprises in particular, the returns and economies of scale are compelling.

Fortunately, organizations of every size save nearly 3x what they spend to implement compliance programs.

To limit expense damages, consider the following compliance hygiene steps in concert with your IGA solution:

- ✔ **Apply risk-based controls based on applicable frameworks and preventative SoD checks to meet compliance requirements**
- ✔ **Track the application of these controls. Organizations must show evidence of continuous compliance and streamline audit processes**

Keep in mind, many IGA products tout automation, but don't meaningfully apply automation around meeting compliance mandates. Report generation, for example, may be automated, but require manual follow-up to achieve compliance.



SMART SAVING TIPS

Saviynt's Identity Cloud platform offers a control library.

The control library incorporates common application and compliance requirements including HIPAA, HiTRUST, SOX, PCI DSS, CPPA, GDPR, ISO 2000 series, and NIST.

Diminished Agility

Cloud-based solutions enable degrees of operational flexibility that won't show up day one in a corporate profit and loss (P&L) statement. One former Identity and Access Management manager reflects how constrained his enterprise became as customizations, siloed products, legacy infrastructure, and aging processes stacked up:



“We became paralyzed to the point where we were afraid to change anything. We just didn’t know what risks we’d uncover in our software. Modernizing security wasn’t an option – it was disempowering.”

Manager,

Identity and Access Management at Mass General Brigham

The value of flexibility surfaces in other areas as well. Enterprises may be able to introduce new workforce modalities, for example, and embrace remote work models while safely managing the identity perimeter beyond traditional operations.

Conclusion

In IGA improvement discussions, financial assessments often default to a simplistic construction of TCO. Absolutely, plan investment in hardware or networking systems, and capture human capital costs for database, server, firewall, and help-desk resource management. But consider both the difficulty in capturing these – and the certain presence of hidden expenses.

For most enterprises, these unexpected costs primarily curb IGA value. This includes the opportunity cost of lost productivity, failed automation, and weakened security. As you budget, plan, and prepare to implement or support a new solution, remember the value of predictability and clarity. For these, the evaluation journey leads back to the cloud.

Saviynt

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Saviynt Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution. Learn more at [Saviynt.com](https://www.saviynt.com)

Want to talk to an identity and security expert?

[SCHEDULE A CALL TODAY](#)