SAVIYNT

Identity Governance & Administration Solution Buyer's Guide

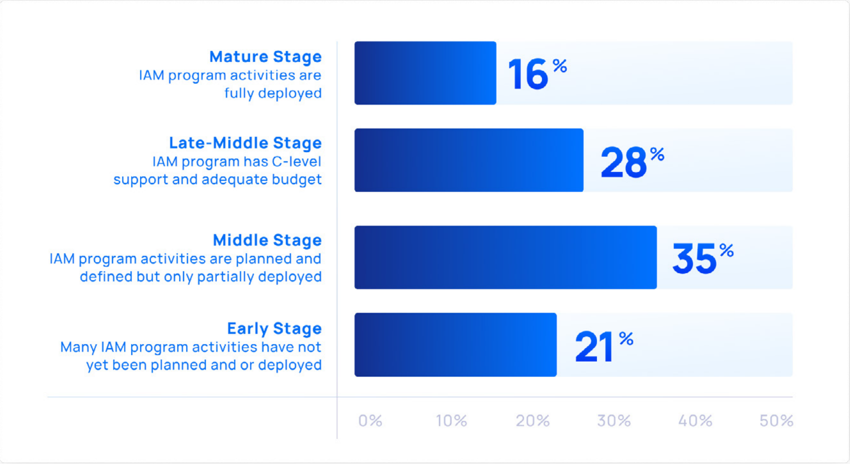
5 MUST-ASK QUESTIONS FOR EVALUATING IGA SOLUTIONS

Why IGA Modernization is No Longer Optional

Over the last few years, cloud acceleration, security threats, and constant technology transformation, bombarded enterprises. More than ever, they lived the adage that 'the only constant in life is change.' For many, inflexible IGA technology worsened the challenges brought on by constant business shifts. Security leaders struggled to adapt, embrace cloud, and manage risk among growing identity bases.

In fact, according to a **study** by the Ponemon Institute, "Most identity and access (IAM) programs have not achieved maturity which is affecting organizations' ability to reduce identity & access risks." Only 16 percent of the 1000 IT professionals surveyed say their organizations have reached the mature stage.

What best describes the maturity of your organization's IAM program?



The State of Enterprise Identity, The Ponemon Institute, May 2022.

TABLE OF CONTENTS

The lack of comprehensive identity controls or policies puts organizations at risk. The study found that in the past two years, 56 percent of respondents say their organizations had an average of three data breaches or other access-related security incidents in the past two years. Fifty-two percent of these respondents say the breach was due to a lack of comprehensive identity controls or policies.

IGA is fundamental to modern enterprise security. Properly deployed, it regulates access to data and business transactions for human and machine identities. Importantly, IGA builds a foundation for Zero Trust across cloud, hybrid, and on-prem environments.

Below, we highlight key macro trends facing global enterprises. As you review each, ask yourself, *"Does my current solution offer the agility, scalability, and security benefits my enterprise now needs?*

Accelerating Cloud Adoption

Every day, more apps and workloads move to the cloud. Workforces operate beyond the confines of corporate offices, and converging IT and operational technology (OT) expand the threat landscape. As these dynamics play out, legacy systems flounder.

Legacy systems limit visibility and rely on manual upkeep and custom coding. Further, SaaS proliferation makes enforcing identity policies (and identifying risky users) more difficult. Additionally, while leaders push the cloud for agility and productivity, maintaining security in the midst of rapid digital services adoption stretches IGA processes.

> **"The shift to cloud-based IGA is accelerating, with many smaller organizations insisting on SaaS-only solutions. Gartner sees this direction moving into the larger organizations that are typically assessing the feasibility of IGA offerings based in the cloud or looking at cloud-first if possible."**
>
> *– Market Guide for Identity Governance and Administration, Gartner© 2020*

Growing Identity Complexity

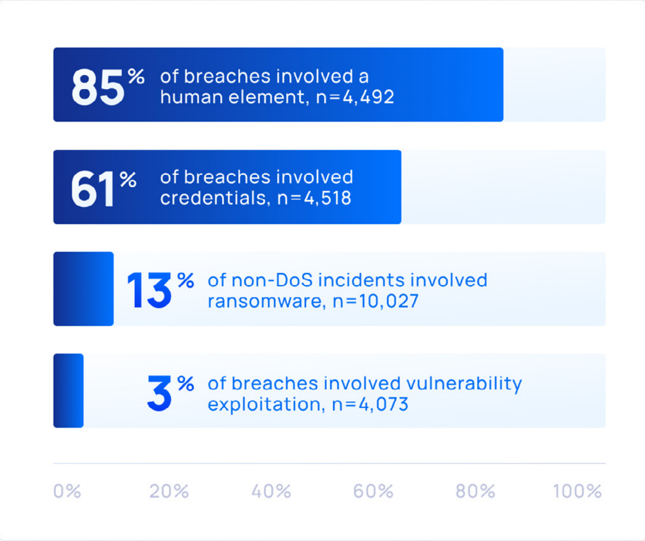
'Identity' once meant human users within an organization's walls. Today, the term represents a host of entities including bots, APIs, workloads, vendors, contract workers, customers, and partners.

If an entity can be discretely identified – and has a consistent set of attributes, it needs securing. Constant digital transformation campaigns spawn legions of these new machine identities and widen attack surfaces. Meanwhile, poor access management and visibility multiply risks. Just 40% of CISOs and IT leaders say they have an enterprise-wide strategy to manage machine identities.

Rising Cyberthreats

The evolution of cyberattacks and growing use of cloud workloads and applications creates a “perfect storm” for IT leaders, **suggests** Gartner. According to **one estimate**, cybercrime will cost companies an estimated $10.5 trillion annually by 2025.

Complications from introducing new technologies including IoT, open-source code, digital supply chains, and cloud applications increase threats. Companies must progress agile identity management, visibility, and monitoring–in particular, to limit compromise connected to application adoption, user permissions, system configuration, and new workloads.



Source: Verizon 2021 Data Breach Investigations Report

Evolving Regulatory Landscape

At both state and national levels, lawmakers are pushing ambitious security legislation. As **we’ve predicted**, non-compliance issues worsen as companies sort through revisions and try to harden a variety of processes – from HR onboarding to customer offboarding – that touch data protected by various rules.

Companies need systems to enable least privilege and privacy by design, while focusing on pathways to simplify audit compliance, address consent management, and an individual’s right to erasure, for example.

These trends increase decision-making complications for security leaders. However, they may also provide the impetus enterprises need to introduce modernization.

So what does a flexible IGA solution look like? Our guide explores this question.

Read on as we outline key features and capabilities, and share an insider view of must-ask platform evaluation questions.

What Defines a Modern Cloud IGA Platform?

According to a recent Forrester Report, "In replacing their manual identity management environments, organizations seek a flexible, comprehensive solution to improve workflows, eliminate compliance risk, and adapt to future IT trends."

TO DELIVER THIS, A MODERN IGA SOLUTION MUST:

- Be built on cloud-native architecture
- Incorporate automation
- Emphasize adaptability
- Converge technologies and functionality

KEY CHARACTERISTIC #1

Born in the Cloud

A modern IGA solution should be cloud-native, full stop. This architecture is essential to reduce infrastructure spending and management complexity, and to realize the cost savings and flexibility of SaaS.

In a cloud-first paradigm, your IGA solution can grow and scale as the business changes. Through auto-scaling, for example, companies embrace real-time scale and can lower ongoing expenses. This approach also eliminates the guesswork from downstream hardware investments.

> **"With accelerated cloud adoption, digitization, and the need for constant, anywhere access, the number one capability your organization requires is the ability to scale. The number of digital identities—and their complexity—is only going to grow in the future."**
>
> *– Paul Mezzera, VP of Strategy, Saviynt*

Companies should also consider total-cost-of-ownership (TCO) factors. Legacy IGA solutions stick enterprises with hardware purchasing, ongoing maintenance expenses, and complex — potentially impossible — upgrades. The standard data center approach brings with it 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.

KEY CHARACTERISTIC #2

Emphasizes Adaptability

The modern IGA solution should be configurable rather than static, monolithic, or needing extensive customization. Solutions must be able to adapt to unknowns, including changes in adjacent technologies and IGA processes. For example, when a cloud provider releases a new product, IGA solutions will be able to integrate with it more quickly – improving application onboarding and governance.

Today, IGA (and related IAM capabilities) must account for new identity concepts like machine-based identities including service accounts, robotic process automation (RPA), or internet of things (IoT) devices.

KEY CHARACTERISTIC #3

Accelerates Automation

Legacy solution inefficiencies increase costs and introduce risks. One common issue is manual access provisioning and deprovisioning. Another includes manual separation of duties (SoD) management where overburdened security staff can overlook toxic permission combinations.

According to Mezzera, the explosion of identity types, and application access makes determining appropriate access levels convoluted. “It’s impossible to manually review now – we need analytics coupled with machine learning to stay safe.”

Automation makes IGA solutions faster and more efficient – and adds incremental business value. “Why waste time researching permissions and searching for toxic combinations? Focus instead on real, revenue-driving processes,” shares Mezzera.

One of the most powerful automation use-cases surrounds intelligent approvals and access reviews. Instead of manually combing through dozens – or even hundreds – of access requests, modern platforms enable smart review and filtering. This means: automation of low-risk/no risk access approvals to remove friction, boost productivity, and lower risks

KEY CHARACTERISTIC #4

Converges Technologies & Functionality

Modern IGA solutions must be able to ingest information from key security and GRC platforms including PAM, SIEM, UEBA, and vulnerability management tools. By utilizing data from other security technologies, enterprises improve security posture and improve TCO/ROI. For instance, by converging all risk signals in a single dashboard, IT departments reduce risk-monitoring fatigue and decrease operating costs.

Significantly, modern platforms also converge core technologies like PAM and IGA. In cloud-first business, the distinction between privileged and non-privileged users gets blurred. Traditional PAM solutions can’t handle the transient nature of the cloud as workloads are spun up and down within hours, or as admins perform privileged activities (via direct console access, RDP, command line) and introduce new access points.

Capability convergence means that enterprises can provide the “right level” of access to new and existing users. No longer is privileged access only an IT problem – meaningful governance controls, policies, and reviews reduce management silos and bring this back into the businessThis means: automation of low-risk/no risk access approvals to remove friction, boost productivity, and lower risks.

> **“A converged identity platform helps make organizations more secure, compliant with regulations and provides a faster return on investment.”**
>
> *– **Security Magazine**, Will the convergence of IGA, PAM and AM fix the fractured identity landscape?*

The Big 5: Questions to Ask When Choosing an IGA Solution

According to the **Gartner Buyer's Guide for IGA**, "…the majority of IGA projects start as a result of a production issue, like an audit finding or a data breach, and buying initiatives follow a firefighting pattern, often skipping ideal planning steps."

Ideally, enterprises start before an emergency arises; this requires proactive planning and internal championing. To support the procurement journey and help leaders secure platforms that meet business and security KPIs, we've put together five questions to ask when evaluating IGA options.

1 How Does the IGA Platform Fit Into My Risk Reduction Strategy?

Why It Matters

Managing the digital workforce across modern ecosystems requires better identity governance and administration. Because identity is a favorite attack vector for bad actors, IGA is crucial to risk reduction.

Most organizations have some Governance, Risk, and Compliance (GRC) program relying on patchwork technologies to reduce risk. These range from multi-factor authentication (MFA) to user and entity behavior analytics (UEBA), and security information and event management (SIEM). IGA supports deeper risk reduction; in particular, because modern solutions extract data from other tools for more holistic security.

Many identity platforms promise, but don't deliver, lower risk profiles, improved decision making, reduced compliance violations, and Zero Trust. But the right IGA platform is central to coordinated risk reduction and provides a framework for ongoing security effectiveness.

What To Look For

A robust IGA solution applies the following techniques to reduce risks:

Risk-Based Approach – To address "excessive access" risk, use an identity platform that incorporates risk-based decision-making to determine user privilege levels. This helps simplify compliance and reduces labor costs. For risk-based decision making, modern tools can also leverage data from disparate security systems to set risk thresholds and remediate risky behaviors.

Lifecycle Management – Both human and machine identities need proper management when joining, moving, or leaving an environment. Rationalizing these identities also allows access consistency across the IT ecosystem. To do this effectively, IT leaders need to be able to directly link accounts to identities within a single, centralized repository. This allows automated provisioning and deprovisioning, ensuring that credentials never end up orphaned.

Just-in-Time (JIT) Provisioning and "No Standing Privilege" – To support Zero Trust (or least privilege), solutions must continuously verify user access during a session. Traditional password-based "one and done" systems that require credentials once to permit access put enterprises at risk.

Solutions that employ least privilege ensure users only receive the minimum access required to perform their job.

Automated Access Review Processes – Manual access reviews often lead to issues of orphaned accounts and excess access. These reviews are often time-consuming and error-prone: When faced with hundreds or thousands of users and accounts, managers may be tempted to select Approve All. A risk-based system automates this; escalating high-risk situations for manual review.

Analytics and Continuous Compliance – An identity platform employing data-rich analytics surfaces the right metrics to quantify organizational risks. It also proves whether your security program moves the needle with respect to monitoring, managing, and reducing these risks. Do not underestimate this with respect to securing executive program buy-in.

With built-in AI and machine learning, enterprises enable continuous compliance monitoring, documentation, and access violation remediation from day one. Alongside this, to enhance risk monitoring, context, visibility, and remediation, look for a solution that integrates with adjacent security tools like ZTNA, XDR, SIEM, and UEBA platforms.

2 What Business Needs Must Be Considered in the IGA Evaluation?

Why It Matters

IGA modernization crossects multiple stakeholder interests. Thus, it is important to understand business needs before choosing a solution.

Generally, transformation projects change users' workflows; make sure to anticipate wholesale process or experience breakages. Once you map these, create your "business case" – that is, plan how to evangelize modernization and present how changes free staff to do meaningful work, not just "identity-like" tasks.

The right solution brings efficiencies that lower total cost of ownership (TCO), strengthen your security posture, and improve stakeholders' contributions. So begin with the business in mind. Not only will you deploy a better platform, but you'll have champions behind your deployment.

What To Look For

Before selecting an IGA solution, establish a full understanding of business goals, applications, and workflows. Start this process by interviewing impacted stakeholders. As you receive feedback, validate findings against vendors' solutions:

How is the current system being used?

What new capabilities are required?

How do each platform's strengths match up with our priorities?

In a presentation titled “How to Choose and Deploy an Identity Governance and Administration Solution” at a recent Identity and Access Management Summit event, Gartner cautioned enterprises to begin by defining their most important IGA use cases and capabilities. They recommend solution champions get answers to questions including:

- **Is this solution supported out of the box? Or does it require configuration?**
- **How does the product achieve our described goals?**

They also emphasize that enterprises must “provide use case scenarios” and ask vendors how their solutions specifically solve them.

Establishing this takes time and effort up front, but saves resources in the long run. Involving business stakeholders also improves the odds that your solution delivers the ROI leaders expect.

Learn how VMWare prepped, planned, and executed an identity modernization campaign

✓ Adopt **Hybrid Agile** Approach

✓ **Solidify Foundation Design Early On**

✓ Provide **Early Demos** to Stakeholders

✓ Build Healthy App **Onboarding Pipeline**

✓ **Train** IAM Staff Throughout Implementation Engage **OCM** Frequently

✓ Choose the Right Implementation **Partner**

CUSTOMER STORY

3 What Is the Total Cost of Ownership of My Existing (Or Future) Solution?

Why It Matters

Legacy IGA solutions involve hardware purchasing, ongoing maintenance expenses, and complex upgrades. But even if a company isn't replacing a legacy solution, it is easy to underestimate savings from a cloud-architected IGA platform.

In addition to server and hardware expenses, companies must account for staff and third-party maintenance contract costs. Leaders will also want to monitor morale issues stemming from propping up legacy systems to meet new security standards. This effort burns out staff, compounding retention and hiring problems.

Surprisingly, some newer platforms may rely on legacy technologies or their older products. To identify these systems, compare features between their on-premises and cloud components – notice any dissimilarity. Mismatch likely means heavier management costs and reliance on physical components. So while the solution might be sold as "converged" this may be 'marketer-speak.'

What To Look For

The optimal cloud-based IGA solution introduces full-fledged automation for lifecycle provisioning, role-based access controls, user access reviews and SoD management. Not only does this boost security, it also simplifies IGA processes and ongoing management.

Post-pandemic security teams tend to be understaffed and are regularly asked to "do more with less." Capabilities like continuous monitoring and controls tracking ease efforts to prepare or respond to audits – and free staff for more strategic project work.

In its recent **Total Economic Impact report** on Saviynt's Enterprise 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."

TO COMBAT THIS, LOOK FOR PLATFORM DIFFERENTIATORS:

- Comprehensive governance capabilities
- Continuously monitor and remediate identity controls
- Extensive and granular integrations
- Risk-based access review capabilities for all objects
- Low-code/no-code environments

Cloud-based platforms also allow organizations to shift from a capital expenditure (CapEx) model where they buy a product upfront and pay for maintenance and upgrades to an operational expenditure (OpEx) model where the vendor delivers services on a subscription basis. This shift also simplifies budget forecasting.

4 Will This Solution Scale To Meet Future Business Needs?

Why It Matters

On-prem legacy IGA systems may be able to scale, but the question is, at what cost?

To add capacity to an on-prem system, you will need servers, networking equipment, routers, switches — the list goes on! In terms of personnel, scaling requires a multidisciplinary team for infrastructure monitoring, database, application, and compute management.

Don't forget physical space requirements: Your enterprise will buy or lease space, and invest in temperature control and miscellaneous upkeep.

Cloud deployments also improve user experiences, allowing enterprises to launch new products and services quickly. In general, reporting and analysis are also simplified. Modern solutions will surface key, concerning metrics and let administrators respond quickly – for example, terminating access for users performing unauthorized actions or access assigned out of band.

What To Look For

IGA "as a service" (aaS) solutions enable pay-as-you-go, reducing capital expenditures from day one. This model abstracts hardware purchasing concerns away from customers – one less thing to budget and forecast for!

Since you won't know all of your needs down the road, prepare with as much "future proofing" as possible. For example, assess whether a solution will scale as you add additional identities or whether vendors limit the number of applications or users you can onboard (particularly for non-employee users).

Consider a platform's ability to automatically identify and onboard new applications to reduce IT capacity and resource forecasting. Also, understand the backup and recovery agreement to ensure that it fits with planned risk objectives.

5 Does This Solution Deliver Visibility Across an On-Premises, Cloud and/or a Multi-Cloud Environment?

Why It Matters

To support a Zero Trust framework, enterprises need visibility into all resources and users, both in the cloud and on-prem. This requires a solution that simultaneously discovers, onboards, and monitors access to these resources – without onerous staff intervention. Formulating a visibility strategy for hybrid or multi-cloud environments can be complicated, particularly when multiple cloud providers are used.

Many organizations employing cloud technology (and hybrid environments) rely on separate teams to manage architectures. Often, they suffer from poor visibility and collaboration — especially when provisioning and deprovisioning access to resources as users move throughout the identity management lifecycle.

Security risks also intensify when enterprises rely on manual discovery and management to monitor and control user access across varied environments. Adding automation here unlocks visibility into who (or what) has network access – including the time, location, and applications associated with every interaction.

What To Look For

Verify that a solution integrates with hybrid ecosystems and can bring governance to all identity types. This ensures seamless migration to SaaS applications or management of new cloud identities.

A solution providing visibility across IT environments also adds a multidimensional risk profile of all user access. An optimal security system flags unusual behaviors and Separation of Duties (SoD) conflicts, while tracking all activity. Platforms should provide a detailed view of all activity in your environment; this helps reduce costs, surface application performance issues, and expose security vulnerabilities.

In addition, you should assess whether solutions require complex IGA platform implementation, customization, and administration. You want a solution that will allow you to mitigate risk, control access, govern identities, and secure assets – quickly, intuitively, and confidently.

Finally, ensure capabilities for centralized monitoring across the entire ecosystem. This allows you to monitor access and usage for control violations, including those granted during emergency elevation or through a backdoor. The solution should also allow you to control risk across multiple applications – ideally with visibility drawn from fine-grained entitlement management.

IGA Features and Functionality: Evaluation Checklist

- User Experience
- Automation Capabilities
- Continuous Compliance
- System Management
- Application Management
- Architecture and Security

As you evaluate governance and administration platforms, consider capabilities through the lenses of *user experience, automation, compliance, platform management, application management,* and *architecture.* We highlight essential criteria for each of the capability areas below.

User Experience

- 360° view of all applications and identities regardless of location
- Access requests and approvals from anywhere (mobile, browser, ITSM, collaboration tools, etc)
- Flexible workflows, unified across all applications
- Access and provisioning recommendations based on policies, dynamic peer analytics, and historical requests
- Time-based, just-in-time access to support least privileged access/Zero Trust
- Seamless user experience across web and mobile platforms
- "One identity for life" capabilities
- Policy and role preview/sandboxing
- Inline collaboration for access decisions
- Role and attribute-based policy management:
    - Role and rule management across composition, lifecycle, attributes, and application usage
    - Role and rule management across composition, lifecycle, ownership, and version control

Automation Capabilities

- Application discovery and onboarding
- Lifecycle management (Joiner, Mover, Leaver)
- Ownership and succession management
- Policy workflows based on changes to user identities
- Built-in RPA for automated provisioning
- Assignment and revocation of access based on changes to user attributes
- Detection and auto-remediation of control failures
- SoD violation identification and remediation
- Machine learning (ML) and artificial intelligence (AI) delivering role and policy definition recommendations

Continuous Compliance

- ✓ Out-of-the-box controls library mapped to relevant regulations (PCI-DSS, HIPAA, GDPR, FedRAMP, etc)
- ✓ Single-tenant architecture for better data isolation and meeting data sovereignty needs
- ✓ Ongoing micro-certification campaigns triggered by changes in job, attributes, or time-bound access needs
- ✓ Real-time, consolidated reporting for actionable investigations and audit reviews
- ✓ Cross-application SoD conflict detection, management, and remediation
- ✓ Risk-based insights to identify and prioritize remediation

System Management

- ✓ Modern UI with a single pane of glass to manage the platform:
  - ✓ Complete visibility and KPIs
  - ✓ Service health
  - ✓ Actionable reporting
- ✓ Low/no code experience with robust configurability (not high customization)
- ✓ Risk modeling
- ✓ Training AI models
- ✓ Dynamic persona creation and management for tailored experiences
- ✓ Analysis of dynamic peer groups

Application Management

- ✓ Out-of-the-box connectors to popular enterprise applications
- ✓ Last-mile application integration and provisioning for disconnected applications
- ✓ Strong SoD identification and remediation
- ✓ Built-in robotic process automation (RPA)
- ✓ Fine-grained entitlement management
- ✓ AD and service account management

Architecture and Security

- ✓ Single- or multi-tenant deployment flexibility based on needs/regulations
- ✓ Extensible platform that lets you bring existing connectors, keys, vaults, etc., to enhance data security
- ✓ 100% cloud-based and architected SaaS platform
- ✓ Security certifications and authorizations
- ✓ Support for different clouds to extend your hybrid enterprise
- ✓ Limited on-premises deployment

For a more in-depth assessment, consider the Gartner 318-point Solution Criteria **evaluation**.

Schedule a Demo

Ready to see our IGA solution in action?

REQUEST A DEMO

SAVIYNT