



Identity Governance Buyer's Guide: How to Evaluate IGA Providers

Evaluation Criteria: Key IGA Capabilities, Definitions, and RFP Questions



BUYER'S GUIDE

Table of Contents

02

Introduction

04

How to Evaluate IGA Providers for Today's Workforce Requirements

Step One: Review Providers for Basic IGA Capabilities

Step Two: Evaluate IGA Providers for Intermediate Capabilities

Step Three: Evaluate IGA Providers for Advanced Capabilities

18

Quickly Support Your IGA Requirements with Ping Identity

Leverage A Single, Unified Identity Platform for All IGA and IAM Use Cases

Meet Modern Identity Demands Without Ripping and Replacing Legacy IGA and IAM

19

Learn More About Ping Identity for Your Organization



Introduction

In today's rapidly evolving digital landscape, robust, enterprise-grade Identity Governance and Administration (IGA) platforms are more critical than ever. Businesses face myriad challenges that underscore this need. IGA platforms are essential for managing digital identities, ensuring security, and maintaining compliance. Here are some key reasons organizations invest in sophisticated IGA platforms:

- 1. Skilled Employee Shortage and Turnover:** The global shortage of cybersecurity professionals is a significant challenge - with millions of critical positions unfilled at any given time. Yet, attracting and retaining skilled employees is essential for maintaining robust security postures and ensuring continuous compliance with evolving regulations. A sophisticated IGA platform can help mitigate the impact of this shortage by automating routine tasks such as user provisioning and deprovisioning, thereby freeing up valuable human resources to focus on more strategic security initiatives.
- 2. Regulations and Compliance:** The global shortage of cybersecurity professionals is a significant challenge - with millions of critical positions unfilled at any given time. Yet, attracting and retaining skilled employees is essential for maintaining robust security postures and ensuring continuous compliance with evolving regulations. A sophisticated IGA platform can help mitigate the impact of this shortage by automating routine tasks such as user provisioning and deprovisioning, thereby freeing up valuable human resources to focus on more strategic security initiatives.
- 3. AI and Machine Learning:** Integrating AI and machine learning in security systems enhances threat detection, behavior analysis, and automated responses to security incidents. An advanced IGA platform leverages these technologies to provide continuous monitoring and automated remediation of access risks, thereby strengthening the organization's security posture against sophisticated threats.
- 4. Insider Threats:** Each year, millions of dollars are lost to data breaches, with insider threats and negligence posing significant risks. Ensuring that employees only have the access necessary for their roles and that access is promptly revoked when no longer needed is crucial. A modern IGA platform offers capabilities like automated identity lifecycle management and role-based access control to minimize these risks and prevent unauthorized access.
- 5. Hybrid Workforce and BYOD Policies:** The shift towards a hybrid workforce and the adoption of BYOD policies require solutions that can securely manage access from various personal devices. An enterprise-grade IGA platform supports these changes by offering centralized access control, multi-factor authentication, and secure single sign-on. In turn, employees can work securely from anywhere without compromising corporate security.



- 6. Cloud Adoption:** The increasing adoption of cloud technologies has enabled organizations to develop and deploy applications faster than ever. This trend is particularly evident in regulated industries such as financial services, where cloud adoption is becoming ubiquitous. Identity governance frameworks are essential for securing cloud environments, ensuring that access controls are enforced consistently across all applications and services.
- 7. API Economy:** The widespread adoption of cloud services and the rise of the API economy necessitate robust identity governance to manage and secure access across diverse environments. A modern IGA platform facilitates seamless integration with cloud services and supports API-based access controls, ensuring consistent security policies across all platforms and applications.
- 8. Cybercrime:** As cybercrime continues to rise, managing and securing employee access becomes increasingly crucial. An IGA platform helps organizations implement stringent vetting processes and continuous monitoring of employee activities, thus reducing the risk of breaches.
- 9. Third-Party Risk:** As businesses rely more on third-party vendors and business partners, managing and securing third-party access has become crucial. This includes stringent vetting processes and continuous monitoring of third-party activities. 75% of those who responded to the 2023 Gartner Reimagine Third-Party Cybersecurity Risk Survey reported spending more time on third-party cybersecurity risk management initiatives, compared with 2021.
- 10. Insurance and Risk Management:** The growing cyber insurance market is influencing businesses to adopt stringent security practices in hopes of qualifying for favorable insurance terms and reducing premiums. Effective identity governance is a key component of these practices, assuring that access controls are robust and that security measures are consistently enforced.

A modern, enterprise-grade IGA platform is required to address the challenges of today's rapidly evolving digital landscape. Such a platform not only enhances security and compliance but also improves operational efficiency, making it a critical investment for any forward-thinking organization.



How to Evaluate IGA Providers for Today's Workforce Requirements

Unfortunately, meeting today's workforce and organizational demands presents real challenges to current IT architectures and legacy IGA systems. What's needed are identity governance capabilities purpose-built to meet the challenges of today, as well as tomorrow. However, not all IGA platforms are the same. This makes the selection process more difficult.

When evaluating IGA providers, Ping Identity recommends a three-step evaluation process organized by basic, intermediate, and advanced capabilities.

1. Basic components cover the most common and simple workforce use cases.
2. Intermediate capabilities should be included by most IGA platform providers.
3. Advanced capabilities are those that only enterprise-grade IGA platforms offer.

Together, basic, intermediate, and advanced IGA features enable leaders to address today's challenges and future-proof their organizations – all while reducing costs.

This evaluation guide lists key basic, intermediate, and advanced IGA capabilities. It also provides definitions and suggests questions for your request for proposals (RFP) to help you differentiate IGA providers during your evaluation process.

For Ping Identity's answers to the RFO questions, a competitive matrix, and more, please request a copy of the [**Workforce IGA RFP Guide**](#) .xls spreadsheet.



Step One: Review Providers for Basic IGA Capabilities

As a first step in your evaluation process, compare IGA providers for basic capabilities using the following RFP questions.

Basic IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Identity Data Store	An identity store is a repository for identity (user or connected thing) attribution data. Stored identity data should be encrypted both while at rest and in transit. Also, as a best practice, it is good to have an embeddable repository that can easily share real-time employee, device, and user identity data across multiple environments. Additionally, from a hosting perspective, identity stores should include high availability, performance, and security.	• Does the IGA platform model the profile, accounts, and access for identities that need to be governed? • Does the platform support flexible identity attribute schema for modeling identities and offer the ability to add custom attributes for the identity data? • Does the platform have the ability to import for all data entities like roles, users, permissions, subject of permissions, assignment user to groups, roles, and permissions from open format e.g. csv or json?
Application Integration	In the early days of IAM, application integration onboarding was a resource-intensive activity because it relied heavily on point-to-point integrations. This created a bottleneck for organizations that wanted a large volume of applications integrated. Additionally, the entire process was time-consuming and expensive.	• Does the platform have the ability to import for all data entities like roles, users, permissions, subject of permissions, assignment user to groups, roles, and permissions from open format e.g. csv or json? • Can the platform be configured to support configuring multiple authoritative sources? • Does the platform have the ability to monitor source systems (e.g. databases and applications) and identify changes to data?

Basic IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Application Integration	Today's modern approach is to enable application onboarding with templates that are pre-filled with default values that can be customized if needed. Wizard-driven approaches to application onboarding also make it faster, more cost-effective, and more scalable from a roll-out perspective.	• Do administrators have the ability to on-board applications using guided processes/wizards in the IGA platform? • Can the platform manage disparate data repositories, network applications, and user data stores anywhere in the infrastructure stack? • Does the platform reconcile objects within target systems in order to verify object properties, identify orphaned (unmanaged) objects, etc? • Does the platform handle unexpected problems with source or target systems (e.g. a system becoming unavailable)? • Does the platform have out-of-box application templates that support standard account provisioning operations - create, modify, delete, enable, disable, and unlock? • Do the application templates support adding and removing access to accounts on target sources?
Provisioning	Provisioning is the process of managing roles and entitlements that are assigned to specific users, devices, or things based on organizational policy and structure (such as job function, title, and geography). It also includes creating accounts with roles and entitlements during onboarding, updating them when they change roles, and removing them when they no longer work at the organization. Importantly, more sophisticated workforce IAM platforms offer automated provisioning and workflow-driven provisioning. See the intermediate and advanced sections below for details.	• Does the IGA platform support role-based provisioning? • Does the IGA platform support rule-based provisioning? • Does the IGA platform support request-based provisioning? • Can the IGA platform define a unique identifier, both within the governance platform and when provisioning application accounts on targets? • Can the platform provision and assign relationships to users, devices, and things? • Can the platform process event-driven identity life cycle changes that are detected and processed in real-time?



Basic IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Self-Service Access Request	Enabling self-service access request for employees streamlines user provisioning, empowers employees, and reduces IT and help desk overhead. It improves efficiency, enhances security, scales easily as an organization grows, and ultimately promotes agility and productivity within the organization.	• Do users or managers have the ability to browse and search a catalog of access available to be requested in the connected applications to the IGA platform? • Does the platform allow users to request roles for themselves or other users/role owners (e.g. can managers request roles for their subordinates)? • Does the platform have the ability to allow requesters or approvers to enter effective dates for the requested access? • Do users or managers have the ability to request multiple access (applications and/or roles) at once, such as application, roles, and entitlements/permissions in the IGA platform? • Do users or managers have the ability to request access for multiple users at one-time in the IGA platform? • Can users or managers view access request progress status in the workflow, as well as key subjects such as approver(s) and support personnel in the IGA platform? • Do users have the ability to view their own profile and accesses, such as applications, data (files), roles, entitlements, permissions, etc. in the IGA platform?
Dashboards & Reporting	Dashboards and reporting are critical for a governance platform to provide visibility, insight, and monitoring of compliance, risk, and performance. They enhance operational efficiency, promote transparency, and facilitate communication, enabling informed decision-making and effective governance.	• Does the IGA platform support user-friendly reporting with online dashboards and out-of-box reports? • Does the IGA platform have provisioning KPI dashboards - number of identities provisioned/de-provisioned, SLA adherence, etc? • Does the IGA platform provide dashboarding for certification KPIs relating to reviewers - e.g. rubber stampers, laggards, reviewers having too many decisions to make, etc? • Does the IGA platform provide dashboarding for certification KPIs relating to applications - e.g. applications with highest revocations, etc? • Does the IGA platform provide a report that shows the status of any revoked access items? • Does the IGA platform provide the ability to export reports to CSV, PDF, Excel, and XML?



Basic IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Role Management	Role management enables organizations to map business functions to IT access. This is typically managed by defining business and IT roles and mapping them with policies driven by HR attributes like user title, group, or location. At the basic level, the governance platform should provide an easy way to create and manage roles and assign policies so that they can be granted to users during onboarding and role changes.	• Does the IGA platform allow for both business (constituent type, job family, department) and technical (logical grouping of entitlement) roles and policies to be defined and assigned? • Does the IGA platform allow for a mechanism to re-apply roles and policies to users when a policy has been updated?
SaaS Platform	Traditional governance platforms have been designed for on-premises deployment models. However, organizations are increasingly shifting to SaaS services for Governance because of the cost benefits of cloud and automatic upgrades. It's crucial to evaluate the architecture of the SaaS service during selection. The service must meet the organization's data residency, uptime, and recovery time objectives.	• How can the IGA platform support System Availability of a minimum of 99.99% availability? • Does the platform support a Recovery Time Objective (RTO) that does not exceed 4 hours? • Does the platform deliver a Recovery Point Objective (RPO) of four hours or less? • Does the platform deliver KPIs that ensure the system is healthy and working well? • Does the platform provide industry best practices around monitoring for both availability and performance? • Does the platform support HA (high availability)? • Does the platform have a distributed architecture so components can be replaced if needed? • Does the service offer a separate development environment/tenant as part of the offering?



Step Two: Evaluate IGA Providers for Intermediate Capabilities

Enterprise organizations require IGA platforms that go beyond the basics. Use the following criteria to evaluate providers for intermediate IGA capabilities.

Intermediate IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Identity Data Store	Organizations are increasingly required to centrally manage and govern vendors, contractors, and non-human identities. These requirements are primarily driven by security and regulatory considerations that go beyond standard employee identities. An effective governance solution should feature a flexible identity data model. This enables the management of profile information across diverse user populations, the recognition of unique profile characteristics, and the establishment of secure relationships among them.	• Do administrators have the ability to store and use custom user identity data (such as geographical region, office location, function, department, role, title, etc.) for access provisioning in the IGA platform? • Does the IGA platform support multiple user populations, including human identities such as employees, vendors, and contractors, as well as non-human identities such as service accounts and RPAs (bots)? • Can the IGA platform act as a system of record for user populations when there is no authoritative source? • Can the identity store scale to support data from hundreds to millions of identities, including devices and things that employees may use?
Cloud Application Integrations	The IGA platform should provide native integrations or support industry-standard protocols such as SCIM for modern cloud-based applications. These integrations allow for automated user provisioning, streamlined user onboarding, access request, and access request processes.	• Can the IGA platform integrate with major cloud providers such as AWS, MS Azure, and Google Cloud Platform? • Can the IGA platform integrate with Salesforce and other cloud applications?

Intermediate IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Cloud Application Integrations	Workflow-driven provisioning involves a sequence of structured steps that must be executed during the creation, modification, or termination of a user's account. These workflows may range from simple managerial approvals for granting new access privileges to intricate multi-step procedures that involve extracting data from various systems to authenticate the user and seek multiple levels of approval. Workflows also systematically organize identity synchronization, reconciliation, and provisioning into repeatable processes, complete with logging and auditing capabilities for reporting purposes. This mechanism ensures adherence to a standardized policy when granting or revoking user access, eliminating the need for email or paper-based approvals. Importantly, within identity governance, workflow	• Can the IGA platform integrate with third-party Integration Platform as a Service (IPaaS) solutions, like Mulesoft, external workflows, or other event-buses? • Can the IGA platform integrate with SCIM-based endpoints supported by many modern cloud applications? • Does the IGA platform have a simple user experience for administrators to configure their connectors and integrations to target sources? • Does the IGA platform have the ability to manage passwords for provisioning connector service accounts? Who owns the keys to these sensitive items? • Does the IGA platform support different workflows for the management of different types of identities - employees, suppliers, externals, agencies, system accounts, technical accounts, shared accounts, and robot accounts? • Does the IGA platform allow you to define end-to-end workflows with both automated and human intervention, including the ability to call out to external services like IDV, ITMS, LMS? • Can the platform trigger workflows based on any governance entity - Identity, App, users, policy, rule and even orgs? Does it support federated or delegated app onboarding workflows where business users can onboard apps with approval - before apps show up in production? • Can the platform send workflow requests to managers for approval, allowing full approval or partial rejection? If rejected, are the individual roles then sent to owners for further approval, who can approve, reject, or request justification? • Does the platform support workflows for various identity lifecycle events, such as creation, changes, and termination, with multi-level approval based on organizational structure and defined groups of approvers at each step? • Can the platform send email notifications with the results of each workflow step after the step is approved or denied? • Does the platform allow administrators to override or block notifications per the workflow step?

Intermediate IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Access Certification	Organizations must ensure user access is aligned with regulations, business policies, and standards to reduce the risk of insider threats and maintain compliance. This process can be time-consuming and expensive. An IGA platform should offer pre-built certification templates, ad hoc micro-certifications, and an easy-to-use and flexible UI for reviewers to streamline access reviews that enforce the principle of least privilege. Pre-built certification templates provide a standardized framework and industry best practices for access reviews, while ad hoc micro-certifications allow for targeted and flexible reviews.	- Is the IGA platform capable of generating access review and certification campaigns with flexible scheduling: full certification, delta certification, ad-hoc certification, user-transfer certification, annual certification, semi-annual certification, etc.? - Is the IGA platform able to generate different types of access reviews and certifications for target applications: - User access review and certification - Resource review and certification - Role review and certification - Accounts and entitlements review and certification - Can the IGA platform initiate out-of-the-box remediation activities when access is judged to be no longer appropriate by the reviewer to the target or other applications? - Does the IGA platform provide the ability to offer an "Approve All" option in access certifications, and monitor its usage?
Access Request Automation	Access Request elevates end-user productivity with a user-friendly, shopping cart-like experience when making requests. Low-risk requests are automatically approved and provisioned without manual review and fulfillment. This ensures users are productive from day one while reducing help desk calls and tickets. Yet, high-risk entitlement requests can undergo one or more approval levels - thus adding additional layers of security and improving compliance.	- Does the IGA platform have a shopping cart-like user experience for self-service so the user can request multiple roles in different managed systems simultaneously? - Can the UI display the role/entitlement/permission information of the access request in a business-friendly language (eg. avoid AD group names or target application role names in the IGA platform)? - Does the platform alert the requestor, approvers, and the person submitting the request, when a request is blocked? Is it capable of suppressing the notifications if needed? - Does the platform document and display request approval for any workflow step where the approver is the same as the submitter? - Can users or managers view access request history? Can approvers view their approval history in the IGA platform?



Intermediate IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Segregation of Duties	Segregation of Duties (SoD) involves enforcing checks to prevent toxic combinations of roles or entitlements. A governance platform should enable organizations to centrally define SoD policies and evaluate them during the access request process as a preventative control to prevent violations or improper access grants.	- Can the IGA platform define segregation of duty (SOD) policies both within and across applications? - Does the IGA platform allow administrators to search for entitlements to define SoD policies? - Does the IGA platform enhance the SoD policies with meta-data that can be added for further SoD policies (For example, owner, violation owner, mitigating controls, etc)? - Does the platform include preventive controls to prevent potential SoD violations during access requests? - Does the platform have the ability to alert the requester when the request generates a policy violation? - Does the platform alert request approvers when approving the request generates a policy violation?
Self-Service Reporting	Custom report-building capabilities in an IGA service allow users to tailor data analysis to their specific needs. By customizing reports, organizations can gain deeper insights, track KPIs, comply with regulations, and make swift, informed decisions. This flexibility enhances operational efficiency, supports strategic planning, reduces compliance costs, and fosters a data-driven culture.	- Does the platform provide access history reports that show a user's access and profile changes over time? - Does the platform offer remediation reports that show the closed-loop processing of certification revoke decisions? - Does the platform provide reports on SoD violations? - Can the platform email reports at regular schedules with customizable intervals? - Does the platform generate customizable reports?
Security	Instead of managing IAM solutions and infrastructure, organizations should prioritize enhancing their business strengths, user experiences, and security. Therefore, IGA vendors provide essential security services in today's market. To meet business demands, these services should ensure enterprise-grade security, availability, confidentiality, and privacy for customer data. One effective method for evaluating the reliability of IGA vendors is by examining their third-party industry validations. These certifications are proof that customer data is handled with the utmost security and compliance standards.	- Can the IGA platform connect to internal applications without a VPN required? - Do you have a dedicated security staff to test the platform? - Do you offer a single code base, which isn't customized - allowing for vulnerability / penetration testing that would apply to all customer tenants? - Do you have outside firms perform white-box and black-box security assessments at least once per year? - Does the platform architecture prevent the identity vendor from accessing the private encryption keys? - Is the platform accessible from any network, while also offering dedicated, direct, and secure communication between IGA and the corporate on-premises network?



Step Three: Evaluate IGA Providers for Advanced Capabilities

Advanced capabilities are the main differentiator between IGA providers. Comprehensive IGA platforms are future-minded and built to handle the organizational complexity of the world's largest enterprises.

For Ping Identity's answers to these questions, please request a copy of the [Workforce IGA RFP Guide .xls](#) spreadsheet.



Advanced IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Legacy Application Support	Many organizations rely on legacy systems and applications to store critical user data and credentials. An IGA platform must be capable of managing the user lifecycle and enabling governance for these applications - thus ensuring compliance and security. This is done through the support of legacy application connectors and standards-based connectors. Legacy application support allows organizations to extend their current digital investments, resulting in increased ROI and reduced costs without having to perform a huge rip-and-replace project.	• Can the platform manage disparate data repositories, network applications, and user data stores anywhere in the infrastructure stack? • Can the platform provision to on-premises applications without opening inbound firewall ports? • Can the platform provision to on-premises applications without requiring VPN tunnels? • Can the platform connectors be updated without downtime? • Can the platform integrate with multiple Active Directory domains/forests and multiple LDAP directory technologies beyond just a single Active Directory domain? • Can the platform work completely without plugins or other software installed directly on the Active Directory Domain Controller? • Does the platform support technology or protocol-based connectors such as Mainframe, JDBC, REST, LDAP, and SOAP? Does the platform support provisioning to custom homegrown applications?

Advanced IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Access Certification	AI-assisted decision-making leverages advanced data analytics to provide recommendations for reviewers. Not only does this help them make informed decisions, but it also reduces certification fatigue.	- Can the IGA platform use identity analytics and machine learning (ML) to recommend whether access should be certified? - Does the platform deliver explainable AI/ML analytics and recommendations during access certification? - Can the IGA platform auto-certify low-risk access to the applications without human intervention?
Segregation of Duties	With the ability to schedule policy evaluations, organizations can proactively scan all identity data as a detective control to find rogue accounts or inappropriate user access. By automating policy enforcement, enterprises can reduce security access risks and maintain regulatory compliance across the entire organization.	- Does the IGA platform allow SoD policies to be tagged with regulations (SOX, PCI DSS, etc.) or business criteria ("Region: AMER/EMEA/APJ" or "Bus_Unit: Finance", etc.)? - Does the IGA platform have detective controls for scanning identities to detect violations of SOD policies? - Does the platform alert violation owners of policy violations after a detective scan? - Does the platform enable violation owners to correct the violations after a detective scan?
Auditing	Auditing allows for continuous monitoring and recording of identity and access management activities, such as user authentication, access requests, permissions changes, and system events. It focuses on capturing detailed information about who accessed what resources, when, and for what purpose. Auditing provides a real-time or near-real-time view of user activities and access controls, enabling organizations to promptly detect and respond to security incidents, policy violations, and compliance issues. This capability works closely with reporting and analytics auditing, focusing on real-time monitoring and recording of identity and access management activities to derive insights, demonstrate compliance, and support decision-making.	- Does the IGA platform have extensive logging and auditing capabilities? - Does the auditing framework enable the continuous evaluation of key controls, business rules, data integrity, and performance? - Does the platform provide an intuitive user interface for defining and configuring audit controls that can be evaluated or enforced through the system? - Does the platform support a "least privilege" security model by decentralizing control with delegated administration?



Advanced IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Role Mining	Role mining is a process within Identity Governance that automatically analyzes user permissions and activities to identify common patterns. By uncovering these patterns, role mining helps organizations create more efficient and secure access control structures. This proactive approach enhances compliance, streamlines user access, and mitigates security risks by aligning permissions with job roles and responsibilities.	• Can administrators discover roles and entitlements/permissions using connectors to other applications in the IGA platform? • Does the platform provide an intuitive UI/UX for the Role Administrator for the refinement of discovered roles and saving role candidates to refine later? • Does your platform use true AI / ML to discover roles? • Does the platform have role maintenance capabilities so they don't become stale and outdated? • Does the platform ensure existing roles are maintained when new applications are onboarded after roles have already been defined? • Does the platform update roles to add access and ensure the new access is granted to current (and all future) members of the role?
Security	To effectively address the security requirements of large organizations, a platform must offer more than just encryption and industry certifications. An enterprise-grade identity governance solution should provide architectural and platform-level differentiating features that deliver capabilities like tenant-isolation and data sovereignty to mitigate common cloud platform issues, such as nosey and noisy neighbors.	• Does the platform have SOC 1 Type II (CSAE3416 or SSAE16), SOC 2 and/or SOC 3 reports in place for all the solution's components, whether managed by you or a service provider (e.g. 3rd party data center, etc.)? • Does the IGA platform support data residency requirements and protection of Personal Identifiable Information (PII) ? • Does the platform support a “least privilege” security model by decentralizing control with delegated administration? • Does the IGA platform protect logs against tampering, deletion, or unsolicited access (e.g. by users not required to access the audit logs and target applications)? • Does the platform provide brute-force protections?



Advanced IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
Identity Analytics with AI/ML	Identity analytics capabilities offer organizations valuable insights into user behavior and access patterns. Given the vast amount of identity and access data generated by large enterprises, traditional methods of analysis often fall short. Specialized AI/ML engines, finely tuned for rapid pattern recognition, are now a critical need. These advanced systems should not only assign confidence scores but also provide detailed explanations for flagging certain access or users as outliers. AI and ML take IGA to the next level by enhancing the ability to identify outliers within a huge volume of data. These technologies also produce confidence scores to assist managers and approvers charged with conducting access reviews and approvals. All-inclusive modern IAM platforms that offer IGA with AI and ML increase efficiency and provide more time for IT staff and access approvers to focus on risky and anomalous access rights. The result is improved security and reduced administrative burdens.	• Does the platform have AI/ML capabilities for Identity analytics? • Can the AI engine consume data from other sources? Is it flexible enough to work with other IAM solutions and data sources, or is it limited to the provider's platform only? • Does the platform have pre-defined analytics as part of the offering? • Does the platform support AI/ML based confidence scoring? • Does the IGA platform support usage and behavioral analytics? • Is the IGA platform able to gain new insights from the large amounts of data that the system generates?
API & SDK	The API First Model is a developer-centric method of creating a solution. Within this model, a provider first creates the API and then builds the platform around it. This results in less complexity for external developers and organizations. To ensure ease of use, scalability, and flexibility, digital identity providers should adopt an API-first development approach. This involves creating a unified REST API framework across the entire platform, enabling a single, consistent method for invoking any identity service. The result is a simple and secure way to extend identity to all realms, including social, mobile, cloud, and IoT.	• Does the platform support web service interfaces/APIs to import data to the IGA platform? • Is the IGA platform capable of accessing other systems through documented API?



Advanced IGA Capability	Capability Definition and Context for Why It's Important	Questions to Ask Providers
API & SDK	It's also important to be sure that your IGA provider includes the necessary instruments like Software Development Kits (SDKs) for implementing their technology. An SDK is a toolkit that consists of prebuilt software components, tools, and documentation that enable developers to build applications for a specific platform more efficiently. SDKs help speed time-to-market by eliminating laborious coding work like building out specific capabilities themselves. They also help to standardize the development of applications.	Does the platform have a well-documented SDK for building custom connectors to third-party applications?

Quickly Support Your IGA Requirements with Ping Identity

Ping Identity is the leading enterprise-grade IGA provider, helping enterprise leaders manage, secure, and govern their businesses. Global leaders use Ping Identity to modernize and accelerate digital transformation and support digital initiatives while securing users and partners across their organizations.

Leverage A Single, Unified Identity Platform for All IGA and IAM Use Cases

Ping Identity delivers the industry's only unified identity platform that seamlessly integrates enterprise-grade IGA with IAM, streamlining identity lifecycle management and access control across the entire enterprise.

Ping's unified approach reduces complexity, eliminates redundant processes, and enhances security by providing comprehensive oversight and auditing capabilities for all identities and access rights. By leveraging a single platform, organizations can achieve cost savings, improve operational efficiency, and ensure regulatory compliance - while also providing frictionless and secure user experiences for employees, IT staff, partners, and customers. The unified approach also supports the implementation of a Zero Trust security model, including adaptive authentication and dynamic authorization to protect against evolving threats and insider attacks.

Meet Modern Identity Demands Without Ripping and Replacing Legacy Identity Systems

Time is of the essence for implementing modern IAM capabilities. Unlike most providers, with Ping Identity you don't need to suffer the pain, risk, and expense of ripping out existing legacy identity solutions to get the features and benefits of IGA modernization needed to support workforce initiatives at scale.

Ping Identity provides a flexible approach that enables you to augment first, and then coexist. In turn, you can consolidate or retire disparate, legacy identity systems when needed.

Learn More About Ping Identity for Your Organization

Get your questions answered!

Request a copy of the **IGA RFP Guide** .xls spreadsheet with Ping's answers to the RFP questions. Or, **contact us** directly to learn how Ping Identity can help your organization.

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. Ping enables enterprises to combine our best-in-class identity solutions with third-party services they already use to remove passwords, prevent fraud, enable Zero Trust, or anything in between. And they can do it all with a simple drag-and-drop canvas. That's why more than half of the Fortune 100 choose Ping Identity to protect every single digital interaction from their users, while making experiences frictionless. Learn more at www.pingidentity.com.

#4054 | 09.24 | v02

