|  |
| --- |
| **RFP GUIDE**  **Modern Identity Governance and Administration** |

# Essential Questions for Evaluating Modern Identity Governance and Administration Solutions

As organizations prioritize security, compliance, and streamlined access management, selecting the right Identity Governance and Administration (IGA) solution is critical. This list of key RFP questions is designed to help prospects thoroughly evaluate potential IGA solutions, ensuring they meet both current and future needs. Whether you're looking to enhance user access controls, improve audit capabilities, or drive operational efficiency, these questions will guide you in making an informed, strategic decision.

# Questions to Assess Rapid Time-to-Value

## **Deployment and Implementation**

* What is your average deployment time from contract signing to full solution implementation for organizations similar in size and complexity to us?
* Can you provide a breakdown of the key milestones and expected timelines for each phase of the deployment process?
* Do you rely on a partner system integrator (SI) for implementation or is everything done in-house? If so, how much IGA deployment experience does that partner have?
* How quickly can organizations expect to see tangible security and operational improvements?
* What metrics do you use to measure implementation success and time-to-value?
* Can you provide case studies demonstrating rapid deployment in organizations similar to ours?
* What is your approach to risk mitigation during the implementation process?

## **Accelerated Deployment Package**

* Do you offer an accelerated deployment package? If so, what specific components are included? And what deliverables are excluded?
* What specific customizations or configurations can be done within the accelerated deployment package? E.g. reports, dashboards, workflows
* Is your accelerated deployment package offered at a fixed cost?
* What guarantees are provided regarding implementation timeline and performance?
* Do you offer a shared risk model with the accelerated deployment package? If so, please explain.
* What is your approach to knowledge transfer and training during and after the implementation?

## **Industry Experience**

* How many years has your organization been specializing in IGA implementation and deployment? Is IGA your key business?
* In how many industries and verticals have you implemented IGA solutions?
* Can you share the number of successful implementations in our specific industry?
* Can you share specific examples of successful IGA implementations in organizations similar to ours, highlighting the challenges faced and solutions implemented?
* How do you ensure that your implementation methodology aligns with industry-specific regulations and standards?
* What percentage of your customer base represents repeat or long-term clients?

## **Best Practices Framework**

* Do you have a standardized implementation methodology or framework to ensure consistency and efficiency?
* How do you ensure that your implementation methodology is adaptable to different organizational structures and business processes?
* How do you support organizations in adapting the IGA solution to evolving business needs?
* Do you have pre-configured templates or workflows specific to our industry?
* How do you stay current with evolving identity governance best practices?

# Questions to Evaluate TCO

## **Initial, Ongoing, and Hidden Costs**

* Can you provide a detailed breakdown of your pricing model, including any base fees, per-identity charges, and additional costs for features like reporting, workflow customization, and integration with other systems?
* What are the upfront costs associated with the implementation, including container/virtualization orchestration, licensing fees (databases, operating systems, firewalls, anti-virus etc), hardware, and software requirements?
* Are there any additional costs for customization or integration with existing systems?
* What is the estimated timeline for implementation, and what resources will be required from our organization?
* What are the ongoing licensing costs, and how do they scale with our organization’s growth?
* Are there any maintenance or support fees, and what level of support is included?
* What are the potential costs associated with training and onboarding new administrators and end-users?
* How much time and effort will be required for ongoing administration and maintenance?
* What are the potential costs of security incidents or data breaches that could be mitigated by a robust IGA solution?

## **Cloud IGA and Maintenance/Upgrades**

* Is your solution cloud-native? Does it include a dedicated database per customer or is it a shared database service?
* How often are security patches and feature updates released?
* What is the process for deploying these updates, and how much downtime is typically required?
* Are there any additional costs associated with upgrades or maintenance?
* What level of support is provided during upgrades and maintenance windows?

## **Cloud-Native Architecture**

* Is your solution built on cloud-native architecture?
* How does your solution ensure scalability and performance as our organization grows?
* What are the specific cost savings associated with your cloud-based solution compared to traditional on-premises deployments?
* How do you ensure data security and compliance in a cloud environment?

## **Cloud Operation Management Capabilities**

* What level of cloud environment operational self-service capabilities does your platform offer for administrators?
* How does your platform support a DevSecOps model for rapid deployment and configuration changes?

## **Self-Service Capabilities**

* What level of self-service capabilities does your platform offer for administrators and end-users?
* Can we independently manage user provisioning, de-provisioning, and access rights without relying on vendor support?

## **Operational Resiliency**

* Where are your data centers located? What certifications exist?
* What redundancy and failover mechanisms do you have in place?
* How do you ensure the security of your data centers and infrastructure?
* What are your service availability metrics? Please provide specific metrics on your service's historical uptime, including average uptime percentage, mean time to repair (MTTR), and any significant outages.
* What is your disaster recovery plan, and how often is it tested? What are your SLAs for system uptime and response times?
* What is your process for handling service disruptions and outages?

## **User Interface and Workflow Design**

* How intuitive is the user interface, and what level of training is required for administrators and end-users?
* What kind of customization options are available to tailor the platform to our specific needs?
* How does the platform support role-based access control and user provisioning automation?
* How do you ensure business continuity in the event of a major disruption, such as a natural disaster or cyberattack?

## **Configuration over Code**

* What is the extent of code-free configuration capabilities? Can we customize workflows, policies, and integrations without writing custom code?
* If code is required for custom configuration, what does that process look like? Are you required to review code before it’s published? If so, are there any fees associated with that?
* How does the platform support rapid application development and integration with other systems?

# Questions to Assess Vendor Commitment to Customer Success

## **Customer Support**

* Do you provide a dedicated account manager or support team for each customer?
* What is your standard response time for support inquiries?
* What is the average response time for critical support issues?
* What are the SLAs for different support ticket severity levels (e.g., critical, high, medium, low)? Please provide details on response times, resolution times, and escalation procedures.
* What are your support hours of operation? Do you offer 24/7 emergency support?
* What is your approach to knowledge learning and self-service support?
* How do you measure and track customer satisfaction with support services?
* How do you provide ongoing support and maintenance to ensure optimal performance and security?

## **Customer Success**

* What is your customer success model, and how does it help customers achieve their business objectives?
* How do you collaborate with customers to develop long-term IGA strategies?
* How often do you conduct customer reviews and business reviews?
* What kind of proactive guidance and best practices do you provide to customers?
* How do you measure the success of your customer success initiatives?
* How do you ensure a smooth transition and ongoing support throughout the customer journey?

## **Relationship Management**

* How do you foster long-term relationships with your customers?
* What is your approach to customer feedback and suggestions?
* How do you handle escalations and resolve customer issues?
* How do you measure customer satisfaction and loyalty?

## **Integration Support**

* Do you provide guidance and support for integrating your IGA solution with various applications and systems?
* Do you offer pre-built integrations with popular business applications?
* What is your approach to handling complex integration scenarios?

## **Product Feedback**

* How does your company gather and prioritize customer feedback?
* Do you have a formal customer advisory board (CAB)? If so, how often does it meet, and how are members selected?
* How do you ensure that customer feedback is considered in your product development process?
* What mechanisms do you have in place for customers to submit and vote on feature ideas?

# Questions to Evaluate Vendor Identity Security Capabilities

## **Zero-Trust Architecture and Least Privilege Access**

* How does your solution align with Zero Trust principles, such as continuous verification, least privilege access, and micro-segmentation?
* What specific features and capabilities does your solution provide to support Zero Trust architectures?
* What are your capabilities for granular access controls and role-based access control (RBAC)?
* How does your solution support dynamic access controls based on user attributes, device context, and risk factors?
* How do you ensure continuous monitoring and enforcement of access policies?
* How does your solution help organizations comply with regulatory requirements for incident reporting and data privacy?
* What tools and processes do you have in place to efficiently collect, analyze, and report on security incidents?
* How does your solution integrate with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools to streamline incident response?

## **Identity Lifecycle Management**

* How do you ensure timely and accurate provisioning of user accounts and access rights?
* What are your capabilities for managing user identities across multiple systems and applications?
* How do you enforce strong password policies and promote multi-factor authentication (MFA)?
* Explain how your solution can operate in an identity landscape with multiple authoritative systems, how does it cope with duplicate Identities and prioritize duplicate or dirty data attributes?

## **Identity Security Posture Management**

* How does your solution help identify and remediate orphan and dormant accounts?
* What are your capabilities for continuous access reviews and certification?
* How do you monitor user behavior for anomalies and potential threats?
* How do you enforce data hygiene practices to ensure accurate and up-to-date identity information?
* How does your solution expose the level of Identity Security Posture Management for physical systems and logical applications?

## **Reporting and Analytics**

* How do you track and measure key identity security metrics, such as access requests, authentication failures, and security incidents?
* How do you visualize and analyze identity security data to identify trends and potential risks?

## **Integration and Automation**

* How does your solution integrate with other security tools and systems, such as SIEM, SOAR, and UEBA platforms?
* What are your capabilities for automating identity and access management tasks, such as provisioning, de-provisioning, and password resets?

## **Compliance**

* How does your solution ensure compliance with regulatory specifications?

# Questions to Evaluate Business Agility Capabilities

## **General Business Agility**

* How does your solution help organizations adapt to changing business needs?
* How flexible is your solution when it comes to adapting to changing business needs?
* What are the key metrics and KPIs that your solution helps organizations track to measure business agility?
* How does your solution support a continuous improvement approach to identity and access management?
* Can you demonstrate how your solution can adapt to our evolving organizational needs?
* How quickly can your solution respond to changes in regulatory requirements or organizational structure?

## **Orchestration**

* Does your solution offer code-free automation capabilities? If so, what does that process look like?
* What types of routine tasks can be automated through your orchestration framework?
* How robust is your solution’s orchestration engine in automating complex identity and access management workflows?
* Can your solution orchestrate workflows across multiple systems and applications, including legacy and cloud-based systems?
* How does your solution handle errors, retries, and exceptions in automated workflows?

## **Rapid Application Onboarding**

* What integration methods do you support for connecting new applications to your IGA solution?
* What protocols (SAML, OAuth, SCIM) do you support for application integration?
* How quickly can your solution onboard new applications into the identity and access management environment?
* What is the level of automation and manual effort required for application onboarding?
* Can you explain your approach to integrating legacy systems, cloud services, and new applications?
* Does your solution support the discovery and integration of shadow IT applications?

## **Transformative Data Modeling**

* How does your solution handle complex identity and access management data models, including hierarchical and attribute-based models?
* Can your solution adapt to evolving data structures and business requirements?
* How does your solution ensure data quality and consistency across different identity sources?
* Can you demonstrate your capabilities for mapping and synchronizing identity attributes across diverse platforms?
* How do you break down data silos and ensure a consistent view of identity data?

## **Policy-Driven Access Governance**

* How flexible is your solution’s policy engine in defining and enforcing access policies?
* Can your solution dynamically adjust access policies based on changes in business needs and risk profiles?
* How does your solution support role-based access controls and risk-adaptive authentication?
* How does your solution ensure compliance with industry regulations and internal security standards?
* How quickly can policies be modified to adapt to changing organizational requirements?

## **Self-Service Capabilities**

* How does your solution reduce administrative overhead for IT and security teams?
* What self-service capabilities does your solution offer to end-users, such as password resets, access requests, and profile updates?
* How does your solution ensure that self-service requests are secure and compliant with organizational policies?
* Can your solution be customized to meet specific self-service needs of different user groups?

## **Delegated Administration**

* How does your solution enable the delegation of identity and access management tasks to business units and resource owners?
* How granular are the delegation controls in your solution?
* What controls and policies are in place to ensure secure and compliant delegation of authority?
* How does your solution support the rapid provisioning, modification, and de-provisioning of access rights at the business unit level?

## **Flexible Integration with Target Business Systems**

* How robust is your solution’s integration framework in connecting with a variety of target systems, including legacy and cloud-based systems?
* How do you ensure consistent identity management across hybrid environments?
* What is the level of customization and extensibility offered in your integration framework?
* How does your solution ensure data consistency and security during integration with target systems?
* Does your solution offer the ability to validate (review) provisioning operations prior to them being performed?

# Questions to Evaluate Vendor Intelligent Decision-Making Capabilities

## **Intelligent Decision-Making Capabilities**

* How does your solution leverage data analytics to provide actionable insights into user behavior, access patterns, and security risks?
* What types of real-time analytics do you provide to support risk-aware access governance?
* How does your solution use risk assessments to dynamically adjust access controls and minimize security risks?
* How does your solution proactively identify and address potential security threats before they can cause harm?
* How do your predictive intelligence features help inform access certification and recertification processes?
* What contextual factors does your platform consider when assessing access requests?

## **AI and ML**

* Does your solution leverage GenAI and/or ML? If so, how? What safeguards are in place to ensure that GenAI is appropriately being used?
* Does your solution leverage machine learning to identify anomalies, trends, and potential risks in user behavior and access patterns? If so, how?
* Does your solution use GenAI and ML to assess risk in real-time, adjusting access controls as needed?
* Can your solution predict future access needs and potential security threats based on historical data and current trends?
* Does your solution continuously learn and adapt to changes in the organization’s structure, policies, and threat landscape?
* How does your solution ensure the privacy and security of sensitive user data, especially when using AI for analysis and decision-making?
* What specific measures are in place to protect user data from unauthorized access, breaches, and misuse, particularly when AI models are involved?
* How do you comply with relevant data privacy regulations (e.g., GDPR, CCPA, HIPAA) when processing user data with AI?

## **GenAI and NLP**

* Does your solution have GenAI and/or NLP capabilities? If so, explain these capabilities and the benefits they have
* Does your solution support natural language queries for requesting access, troubleshooting issues, or seeking information about access policies?
* Does your solution use GenAI to provide intelligent recommendations for access requests, based on user roles, context, and historical data?
* Can your solution understand the context of a user’s request, such as their role, department, and project, to provide accurate and relevant recommendations?
* How does your solution continuously learn from user interactions and feedback to improve its understanding of natural language and its ability to provide accurate and relevant recommendations?

# Questions to Evaluate Vendor Approach to Discovery, Visibility, and Intelligence

## **Data Discovery and Inventory**

* How comprehensive is your solution’s ability to discover and inventory identities and entitlements across various systems and applications?
* What techniques does your solution use to identify shadow IT and unauthorized access points?
* How does your solution handle dynamic environments where systems and applications are frequently added or removed?
* Explain how your solution can assist with the classification of resources such as accounts, entitlements and Identities.

## **Audit Trail**

* What level of detail does your solution provide in audit logs? Can you track changes at the attribute level, or is it limited to high-level actions?
* How long does your solution retain audit logs? Can this retention period be customized to meet regulatory requirements?
* What tools and capabilities does your solution provide for searching and analyzing audit logs? Can you filter and sort logs by user, action, or time period?
* Can your solution generate alerts for specific audit events, such as unauthorized access attempts or changes to critical user attributes?

## **Merging Multiple Accounts into a Single Identity**

* How does your solution identify and match multiple accounts associated with the same identity? What criteria does it use to determine if two accounts should be merged?
* How does your solution handle data inconsistencies between multiple accounts, such as conflicting email addresses or phone numbers?
* What workflows and approval processes are in place to ensure accurate and secure account merging?
* How does your solution assess the potential impact of merging accounts on downstream systems and applications?

## **Machine Identity Management**

* How does your solution discover and inventory machine identities across your IT environment?
* How does your solution manage and automate the lifecycle of machine certificates, including issuance, renewal, and revocation?
* How does your solution enforce granular access controls for machine identities based on predefined policies and roles?
* How does your solution assess the security posture of machine identities, identify vulnerabilities and recommend remediation actions?
* How does your solution assign ownership of technical machine identities?

## **Dashboards and Reporting**

* Is reporting performed by a third party provider, such as a third party cloud provider, explain the data flow for reporting?
* What kind of dashboards and reports are available out-of-the-box? Provide a list of reports and dashboards.
* Can your solution create custom dashboards and reports?
* Can users drill down into specific data points to gain more detailed insights?
* Can users share specific dashboard configurations, including custom filters and visualizations, with other users?
* How does your solution help organizations meet compliance requirements and reduce audit fatigue?
* Does your solution provide pre-built reports for specific regulations, such as GDPR, HIPAA, or PCI DSS?
* How does your solution leverage AI and machine learning for reporting?
* Can reports be exported in various formats (e.g. PDF, CSV, Excel) for further analysis and distribution?
* Are there additional charges for reporting, and/or downloading of data contained within the reports?

# Questions to Assess Integration into the Security Fabric

## **Security/Identity Fabric(s)**

* How does your solution integrate with other security tools and technologies, such as SIEM, SOAR, and endpoint protection platforms?
* Does your solution provide robust APIs to enable integration with other security tools and platforms? What modern authentication protocols are supported?
* How does your solution share threat intelligence with other security tools and platforms?
* How does your solution automate incident response workflows, leveraging integration with other security tools?

## **Shared Signal Framework (SSF)**

* Is your solution compliant with the OpenID SSF standards and specifications?
* How does your solution consume threat intelligence from the SSF?
* What kind of threat intelligence does your solution share with the SSF?
* How does your solution integrate with the SSF through APIs to share and consume information?