Omada

RFP GUIDE

# Modern Identity Governance and Administration

A comprehensive guide to selecting the right IGA vendor for your business

# Contents

# Introduction

To help you navigate the vendor selection process, we've created a comprehensive RFP guide. This guide includes essential questions to ask vendors about key factors, features, and capabilities that will determine if they can meet your specific needs and provide long-term success. This guide will empower you to navigate the IGA landscape with confidence, asking the right questions and aligning with the ideal vendor for your needs.

# Executive Summary

Selecting the right Identity Governance and Administration (IGA) solution is crucial for organizations aiming to enhance security, compliance, and operational efficiency. This guide provides a comprehensive framework to help companies navigate the vendor selection process by offering key questions and critical considerations for evaluating IGA solutions.

Before beginning your evaluation, it is important to first understand your desired outcomes. By clarifying your business goals upfront, you can ensure the IGA solution you select aligns with your needs.

The guide highlights the importance of integrating identity security into broader risk management strategies and ensuring the solution supports business agility and intelligent decision-making. It also addresses the need for discovery, visibility, and intelligence in identity management and the role of a robust security fabric in protecting organizational assets.

By using this guide, organizations will be empowered to select an IGA solution that delivers long-term value, security, and flexibility to meet their evolving needs.

# Full-Featured vs. Light IGA: The Importance of Separation of Duties (SoD)

When selecting an Identity Governance and Administration (IGA) solution, one of the most critical factors to consider is Separation of Duties (SoD). SoD is a key principle in identity governance that ensures no single individual has enough access or control to perform high-risk actions without oversight, which helps mitigate the risk of fraud, error, and security breaches. Understanding how SoD is addressed in full-featured versus light IGA solutions can be a deciding factor in ensuring your solution supports the security and compliance needs of your organization.

## Separation of Duties in Full-Featured IGA

Full-featured IGA solutions are designed to support robust Separation of Duties policies by offering comprehensive tools for identity and access governance. These solutions are well-suited for organizations with complex requirements, as they provide the necessary controls to enforce SoD across various roles, applications, and systems.

## Separation of Duties in Light IGA

While light IGA solutions may offer basic identity management capabilities, they often lack the comprehensive SoD enforcement features needed for organizations with higher security or compliance needs. These solutions typically focus on simpler, more cost-effective identity lifecycle management without providing the depth of controls required for complex SoD policies.

## Choosing the Right Solution Based on SoD Needs

The importance of Separation of Duties cannot be overstated when selecting an IGA solution, especially for organizations with complex workflows or regulatory requirements. Full-featured IGA solutions are better equipped to handle advanced SoD needs with automated enforcement, real-time violation detection, and the ability to scale as your business grows.

For organizations that require strong controls to prevent fraud, reduce security risks, and meet compliance standards, a full-featured IGA solution is likely the best choice. These solutions provide the granular controls and automation necessary to enforce SoD effectively across your organization.

On the other hand, if your organization has simpler governance needs and can manage SoD through manual processes or basic controls, a light IGA solution may suffice. However, it's important to understand the trade-offs involved, particularly if your organization plans to scale, handle sensitive data, or operate in highly regulated industries.

In your Request for Proposal (RFP), be sure to ask vendors about how their solution handles Separation of Duties, including features like automated violation detection, role-based access control, and compliance support. By prioritizing SoD enforcement, you can select an IGA solution that ensures strong governance, security, and compliance for your organization.

# Know Your Desired Outcomes

Before starting the vendor selection process, it's crucial to identify your organization's specific business drivers and how IGA can support those goals. Understanding these drivers will help you prioritize features and choose a solution that aligns with your strategic objectives. Common business drivers include:

**Compliance:** Meeting regulatory requirements (e.g., SOX, HIPAA, GDPR, NIS2) and aligning with industry standards (e.g., PCI-DSS) and security frameworks like ISO/IEC 27001:2022, CIS-18, and NIST CSF. This involves managing access and entitlements effectively to ensure security, privacy, and compliance with both regulatory mandates and best practices.

**Security Risk Management:** Reducing security risks by gaining comprehensive visibility into your IT environment, identifying and controlling high-risk access (e.g., overprivileged accounts), and enforcing least privilege principles.

**Operational Efficiency and Business Agility:** Optimizing identity and access management processes, to reduce manual effort, improve efficiency, and support ongoing business growth and agility.

By understanding your specific business drivers, you can tailor your IGA requirements and select a solution that delivers the desired outcomes.

# Self-Assessment Questions to Help Determine Your Desired Outcome

To effectively evaluate your current IGA landscape and identify your specific needs, consider the following questions:

## Understanding Your Current IGA Landscape

- What triggered the interest in evaluating a modern IGA solution?
- What are the biggest pain points in the current identity and access management processes?
- Do we have benchmarked actual against goal of our current identity and access landscape?
- What are the biggest challenges we currently face in managing user identities and access privileges?
- Are we looking to solve immediate tactical challenges or planning for long-term identity governance transformation?
- What is the preferred deliverable method for the new IGA solution, is this aligned to the policy and operational environment of the organization?

## Compliance

- Are there specific industry regulations or regulatory initiatives that we need to adhere to? If so, which ones? (e.g., SOX, HIPAA, PCI-DSS, NIS2, GDPR)  What's our actual state of compliance, are there any lessons learned from previous audits?
- What are the current processes used to ensure compliance with these regulations?
- Are there any outstanding audit findings that we need to remediate? If so, how can a new IGA solution help with this?
- How often are access reviews conducted, and how efficient is the current process?
- Are there any recent audit findings or regulatory violations related to access control?

## Security Risk Management

- What are the top security risks facing your organization, and how does identity and access management contribute to these risks? How well is Identity Security understood by the business stakeholders.
- How effectively are you managing privileged access and enforcing the principle of least privilege? Are Zero Trust Architectures a well-known concept, what's the state of adoption within the organization?
- Are there any known vulnerabilities in your current identity and access management systems?
- How often are security assessments and penetration testing conducted?

## Operational Efficiency and Business Agility

- How long does it take to provision and de-provision user accounts of different types such as internals or external identities? What's the expectation from the business?
- What is the current level of automation in our identity and access management processes?
- How efficient are our password reset and account lockout procedures?
- Do we need to support hybrid and remote work environments? If so, how well does our current IGA solution support this?
- Are there any bottlenecks or inefficiencies in our current identity and access management processes?
- How quickly can we detect new SaaS applications in use by the business and onboard them to IGA in order to minimize shadow IT and audit failures ?
- How well is IGA integrated into the Security Operations Response team operational playbook?

# What to Look for in a Modern IGA Solution

When selecting a modern Identity Governance and Administration (IGA) solution, it's essential to focus on key factors that ensure long-term success and align with your organization's strategic goals. A robust IGA solution should not only meet current security and compliance requirements but also provide scalability, flexibility, and efficiency to support future growth.

This section explores the critical capabilities and features that define a modern IGA solution. To help you evaluate potential vendor solutions, we've provided targeted questions for each topic to include in your Request for Proposals (RFPs). By incorporating these questions into your RFP process, you'll be better equipped to select an IGA solution that not only meets today's demands but also supports your organization's evolving security, compliance, and business needs.

# Rapid Time to Value

Accelerate your time-to-value by selecting an IGA vendor that ensures rapid implementation. By eliminating lengthy implementation cycles, you can quickly reduce risks, streamline operations, and maintain security momentum.

## Accelerated Deployment Options

Transform your IGA deployment from  a seemingly endless, unstructured project misaligned with business goals, into a rapid, value-driven initiative.  By selecting a vendor with a fixed-cost accelerated deployment package, you can achieve expected timelines using pre-configured workflows and dedicated support. This strategic approach, combined with a vendor that employs a shared risk model, delivers immediate ROI and measurable security and operational improvements, all while ensuring total financial transparency.

## Partnering with an IGA Expert

Experienced IGA vendors transform rapid time-to-value from a theoretical concept into a tangible reality. Their deep industry knowledge allows them to anticipate implementation challenges, develop pre-configured solution templates, and create streamlined deployment strategies that dramatically compress project timelines. By leveraging lessons learned from numerous previous implementations, these vendors can quickly map your unique requirements to proven solution approaches, reducing discovery, design, and configuration cycles from months to weeks. This accumulated expertise enables faster connector development, more intuitive workflow design, and more precise risk mitigation strategies—ultimately helping you achieve your identity governance objectives with unprecedented speed and precision.

## Knowing Your Implementation Team

Understanding the implementation team is crucial when selecting an IGA vendor, especially for organizations prioritizing rapid time to value. Some vendors offer a range of implementation options, including vendor professional services organizations, system integrators (SIs), or in-house teams. Vendor professional services organizations and SIs often have a deeper understanding of the product and its capabilities, as they work closely with the vendor to develop and deliver implementation methodologies. In-house teams, while familiar with the organization's specific needs and infrastructure, may require additional training and support from the vendor to ensure successful implementation. By carefully evaluating the vendor's implementation model and the qualifications of their team, you can select a partner that aligns with your specific needs and preferences.

## Leveraging Industry Best Practices

IGA best practices developed through years of implementation serve as a strategic accelerator for organizations seeking efficient identity governance solutions. Experienced vendors transform complex implementation challenges into predictable, streamlined processes through standardized integration frameworks, proven identity lifecycle management workflows, and industry-specific configuration templates. These best practices enable you to bypass common implementation pitfalls, reduce configuration complexity, and dramatically compress deployment timelines. Selecting a vendor with a best practice framework allows you to easily align your identity governance strategy with proven methodologies, resulting in faster risk mitigation, more intelligent solution design, and accelerated realization of your IGA solution's full strategic potential.

# 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?

# Total Cost of Ownership

Understanding the Total Cost of Ownership (TCO) of an IGA solution is essential to making informed decisions. By considering both upfront and ongoing costs, you can avoid hidden expenses and optimize your investment. Factors such as maintenance fees, support contracts, upgrade costs, and administrative overhead can significantly impact the overall TCO. Additionally, the complexity of the solution and the required level of customization can influence these ongoing costs. By carefully evaluating the long-term implications of each vendor's solution, you can select a cost-effective and sustainable IGA solution that aligns with your budget and strategic goals.

## Understanding Pricing

Understanding a vendor's pricing model is crucial to accurately assess the TCO of an IGA solution. While the number of identities supported is a significant factor in licensing, it's essential to delve deeper into the pricing structure to identify potential hidden costs. Some vendors may charge additional fees for essential features like reporting, report customization, workflow creation, and data exports. These seemingly minor costs can accumulate over time, significantly impacting the overall TCO. To make an informed decision, it's imperative to request detailed pricing breakdowns, including any additional fees or usage-based charges. By thoroughly evaluating a vendor's pricing model, organizations can avoid unexpected expenses and select a solution that aligns with their budget and long-term goals.

## Evergreen Cloud IGA

Selecting an evergreen, cloud-native IGA solution can significantly reduce your TCO by eliminating the need for costly hardware and software maintenance, reducing operational overhead, and providing continuous access to the latest security features and compliance updates. An evergreen solution is one that is continuously updated with the latest features and security patches, eliminating the need for manual upgrades and minimizing downtime. By leveraging cloud-native architecture, you can benefit from automatic scalability, reduced infrastructure maintenance overhead, minimized downtime, and the elimination of expensive hardware refreshes or complex version migration projects.

This seamless update model ensures you always have access to the most current capabilities without additional professional services costs. Additionally, the elastic infrastructure allows for precise resource allocation that dynamically adjusts to your needs, optimizing operational expenses and reducing the long-term financial burden associated with legacy identity management solutions.

## Cloud-Native Autonomy

Having full autonomy over your instance through a centralized management console is essential for reducing TCO and maximizing flexibility. By empowering you to be self-sufficient, this level of control eliminates the need for extensive vendor support. You can independently manage user provisioning, de-provisioning, access rights, and even clone environments or promote objects from staging to production. This streamlined approach significantly reduces costs, accelerates innovation, and allows you to quickly adapt to changing business needs. By selecting a vendor that offers you this level of control and autonomy, you can optimize your IGA solution and achieve long-term cost savings.

## Simplified Upgrades and Maintenance

Cloud-native IGA solutions can significantly reduce your TCO by simplifying upgrades and maintenance. Unlike traditional on-premises systems, cloud-native solutions often allow for seamless upgrades with a single click, minimizing disruption to business operations. Additionally, cloud-based IGA solutions often maintain high availability during upgrades, ensuring continuous access to critical identity and access management functions. By selecting a vendor that offers a cloud-native IGA solution, you can avoid productivity losses and reduce the associated costs of business disruption.

## Operational Resiliency

Selecting a vendor with strong operational resiliency is crucial for ensuring the reliability and security of your IGA solution. This strategic approach can significantly lower your TCO by minimizing the costs associated with system outages, data breaches, and security incidents. A vendor with strong operational resiliency provides comprehensive capabilities such as robust disaster recovery mechanisms, redundant infrastructure, automated failover systems, and continuous monitoring. These capabilities ensure the uninterrupted operation of your identity governance processes, even during unexpected system failures, cyber incidents, or significant organizational changes. By choosing a vendor with a strong track record of operational excellence, you can safeguard your critical business functions and maintain security integrity, thereby reducing your overall risk exposure and long-term costs.

### Ease of Use

An IGA solution with user-friendly interfaces and intuitive workflows can significantly reduce operational costs. By selecting a vendor that prioritizes ease of use and streamlined administration, you can minimize the need for extensive technical expertise and complex configurations. This translates to lower TCO in several ways: reduced personnel costs, increased efficiency, and faster time to value. A clear and intuitive interface can significantly reduce training time and user error. Self-service capabilities can empower end-users to manage their own access requests, reducing the burden on IT staff.

### Configuration Over Code

Selecting a vendor that offers a code-free configuration approach is another way to significantly reduce your TCO. By eliminating the need for custom development, you can accelerate deployment time, minimize the risk of human error, and reduce implementation and maintenance costs. Intuitive drag-and-drop workflow builders enable you to tailor the solution to your exact needs without writing a single line of code. This approach also enhances security by reducing your reliance on custom code, which can introduce vulnerabilities if not properly vetted and maintained.

# 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?

## 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?

## 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?

## 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?

## 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?

# Customer Partnership

A strong vendor-customer relationship is essential for success in IGA. By prioritizing a vendor dedicated to customer success, you can minimize operational risks, maximize your return on investment, and ensure a seamless IGA experience. A reliable and responsive vendor can provide exceptional support, actively collaborate with you, and help you navigate the complexities of identity and access management.

## Customer Success Model

A robust customer success model, coupled with white-glove vendor support, can maximize the value of your IGA investment. Partnering with a vendor who provides proactive guidance, best practices, and strategic advice helps to minimize disruptions and ensure alignment with your long-term business objectives. Regular check-ins, performance reviews, and actionalble recommendations for improvement ensure ongoing optimization of your IGA implementation. Dedicated support teams provide expert assistance, addressing questions and resolving issues promptly. This personalized approach accelerates the implementation process and minimizes downtime, ensuring a seamless transition to your new IGA solution. Additionally, support for integrations simplifies the process eliminating potential challenges . By leveraging a white-glove vendor relationship, you can  accelerate your IGA implementation and unlock faster time to value.

## Product Feedback

A strong vendor-customer relationship is built on open communication and mutual understanding. A key aspect of this relationship is the ability to provide feedback on the product. This feedback loop is essential for driving product innovation, addressing customer pain points, and ensuring the IGA solution continues to meet evolving business needs. Customer Advisory Boards (CABs) provide a platform for direct interaction between customers and the vendor's product teams, contributing to the product roadmap and sharing insights on industry trends and future requirements.

Product feedback surveys gather quantitative data on customer satisfaction and qualitative feedback on specific features and pain points. Idea portals empower customers to submit and vote on new feature ideas, fostering customer-driven innovation. Regular check-ins and performance reviews facilitate open dialogue and identify areas for improvement. By actively soliciting and incorporating customer feedback, vendors can demonstrate their commitment to delivering a high-quality product and strengthen long-term partnerships.

# 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?

# The Need for Identity Security in Security Risk Management

A robust identity security strategy is essential to mitigate the risk of data breaches, unauthorized access, and other cyber threats. As organizations increasingly rely on digital technologies, the protection of digital identities has become a top priority.
By selecting a vendor who provides comprehensive identity security capabilities, you can safeguard your sensitive information and maintain business continuity.

## Zero-Trust Approach

A zero-trust security model can significantly mitigate identity-related risks by assuming no user, device, or application is inherently trustworthy. This paradigm shift from traditional perimeter-based security to a granular, continuous verification model ensures more precise access governance and creates a dynamic security environment that adapts in real-time to potential threats. A zero-trust approach also prepares organizations to respond effectively to security incidents. By assuming a breach is inevitable, organizations can proactively implement measures to detect and respond to threats quickly, including collecting and analyzing incident response data to share with relevant authorities as needed. By implementing zero-trust principles, you can effectively reduce the attack surface and minimize the potential for unauthorized access or credential misuse.

## Least Privilege Model

The principle of least privilege access is a cornerstone of effective identity security. By granting users only the minimum level of access required to perform their job functions, you can significantly reduce the risk of unauthorized access and data breaches. A robust IGA solution can help enforce least privilege access by defining granular permissions and roles for each user, ensuring that only authorized individuals can access sensitive systems and data.

## Role and Policy Engine

A comprehensive role and policy engine can significantly enhance your organization's security posture. By dynamically mapping identities to precisely defined roles and systematically applying contextual policies, this engine enables organizations to create a flexible yet stringent authorization ecosystem. This approach allows for automated, intelligent access governance that can immediately adjust permissions in response to changing risk conditions, minimizing the potential for unauthorized access and data breaches.

## Identity Security Posture Management (ISPM)

Identity Security Posture Management (ISPM) can significantly enhance your organization's security posture. By continuously assessing, monitoring, and improving your identity security, ISPM enables you to proactively identify and mitigate potential risks, ensuring the ongoing protection of sensitive data and systems. Below are some of the key aspects of ISPM:

## Identity Lifecycle Management (ILM)

By effectively managing the entire lifecycle of user identities, from creation to termination, Identity Lifecycle Management ILM ensures that user identities are created, maintained, and deleted in a secure and efficient manner. Selecting a vendor with robust ILM capabilities reduces the risk of unauthorized access, data breaches, and other security threats.

## Data Hygiene

By regularly reviewing and cleaning up user accounts, removing inactive or unnecessary permissions, and enforcing strong password policies, you can maintain accurate, up-to-date, and consistent identity data. Prioritizing vendors with strong data hygiene processes reduces the risk of unauthorized access, data breaches, and other security threats.

## Orphan and Dormant Account Management

Selecting a vendor who can easily identify and remove unused or inactive accounts, often referred to as orphan or dormant accounts, reduces your organization's attack surface and improves overall security. These accounts, which are no longer associated with active users, can pose a significant security risk as they may be compromised and used to launch attacks.

## Continuous Access Assessment

Regularly reviewing and reassessing user access rights to ensure they align with current job roles and responsibilities is another way to minimize the risk of unauthorized access and data breaches. This involves implementing automated workflows to detect and remediate access anomalies, such as outdated permissions or excessive access privileges.

## Role-Based Access Control (RBAC)

Selecting a vendor that supports a comprehensive Role-Based Access Control (RBAC) model is critical to ensure that only authorized individuals have access to sensitive resources. RBAC policies allow you to enforce strict access policies based on user roles, attributes, and contextual factors to help mitigate the risk of unauthorized access, data breaches, and insider threats.

# 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?

# Business Agility

A flexible and agile IGA solution can help you maintain a competitive edge by supporting rapid business growth, innovation, and digital transformation initiatives. Business Agility refers to a solution's capacity to quickly respond to changes in organizational structure, regulatory requirements, and emerging threats. When evaluating IGA vendors, it is essential to consider their ability to deliver a solution that can adapt to your organization's evolving needs.

## Orchestration

Orchestration can significantly improve the efficiency and flexibility of your IGA solution. By automating routine tasks such as provisioning, de-provisioning, and access requests, you can reduce manual effort, minimize errors, and accelerate time-to-market for new initiatives. Some vendors offer code-free orchestration capabilities, further simplifying the process and reducing the need for specialized technical skills. This increased efficiency and flexibility enables you to respond quickly to changes in business requirements, such as mergers and acquisitions, organizational restructuring, or regulatory updates.

## Rapid Application Onboarding

Selecting a vendor who has a flexible integration framework can significantly accelerate application onboarding and enhance business agility. By providing a standardized, adaptable approach to connecting identity governance capabilities across diverse technological ecosystems, you can quickly integrate new applications, cloud services, and legacy systems into your identity management infrastructure. This reduces time-to-value, enhances IT agility, and maintains a comprehensive, real-time view of user access across your entire application landscape. By supporting multiple integration methods, such as pre-built connectors, API-based integrations, and robust identity management protocols, you can dramatically reduce time-to-value and empower you to respond more dynamically to changing operational requirements and emerging technological opportunities.

## Transformative Data Modeling

Prioritizing vendors with transformative data modeling capabilities can further enhance your organization's agility and efficiency. By implementing advanced schema translation techniques, you can dynamically map, transform, and synchronize identity attributes across different application architectures, data structures, and technological platforms, effectively breaking down traditional data silos. This approach allows you to rapidly onboard new applications, adapt to changing business requirements, and maintain a consistent, holistic view of identity data across hybrid and multi-cloud environments. This ultimately drives operational agility and reduces the complexity and cost associated with manual identity data reconciliation.

## Policy-Driven Access Governance

By selecting a vendor that enforces policy-driven access governance, you can create nuanced, contextually-aware security frameworks that dynamically align identity management with specific business requirements and risk tolerances. This approach ensures consistent, automated enforcement of security policies across complex technological ecosystems, preventing unauthorized access and minimizing potential compliance risks. By developing granular policies that reflect unique organizational contexts, such as role-based access controls, time-sensitive permissions, and risk-adaptive authentication, you can enhance security posture and provide unprecedented business agility, allowing rapid adaptation to changing operational needs, regulatory landscapes, and organizational restructuring without compromising security or operational efficiency.

## Self-Service Capabilities

Self-service capabilities can significantly empower end-users and streamline identity management processes. By allowing end-users to independently perform routine identity-related tasks such as password resets, access requests, and entitlement reviews, you can dramatically reduce the administrative overhead for IT and security teams, minimizing service desk tickets and eliminating unnecessary waiting periods for access. Many modern self-service portals leverage contextual awareness and guided workflows, enabling users to request and receive appropriate access quickly and efficiently.

## Delegated Administration

To enhance business agility and accelerate critical lifecycle events, it's crucial to ensure your selected vendor has delegation administration capabilities in their solution. By decentralizing decision-making authority, you can streamline access management and empower managers and team leaders to directly manage access permissions for their teams. This reduces bottlenecks and accelerates critical lifecycle events like onboarding, offboarding, and access modifications. This approach enables rapid, context-aware access adjustments that align with evolving business needs, ensuring that access management remains dynamic and closely aligned with organizational structures and operational requirements.

## Flexible Integration with Target Business Systems

Selecting a vendor with flexible integration capabilities is essential for business agility and technological adaptability. Vendors with robust integration frameworks can seamlessly connect to a wide range of on-premises, cloud, and hybrid systems. This enables the rapid adoption of new tools and services, accelerating business growth. By maintaining consistent identity and access management across hybrid environments, you can ensure uniform security policies and governance standards. This integration flexibility empowers you to rapidly scale, innovate, and respond to emerging technological opportunities, driving digital transformation.

# Questions to Evaluate Vendor 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?

# Intelligent Decision-Making

One of the many benefits of migrating from legacy to modern IGA is the ability to make data-driven decisions. By incorporating real-time risk insights, behavioral analytics, and predictive intelligence, IGA solutions can dynamically assess access requests, detect anomalies, and proactively mitigate risks. This enables you to make more precise, risk-aware, and adaptive access governance decisions, balancing robust security with operational efficiency. Ultimately, intelligent decision-making empowers you to create a more responsive and context-aware identity management strategy, capable of rapidly adapting to evolving business needs and emerging technologies.

## Leveraging AI and ML

Artificial Intelligence (AI) and Machine Learning (ML) enable more intelligent decision-making in IGA by analyzing complex access patterns, user behaviors, and potential risks. This enables you to make nuanced, context-aware decisions, automatically identify vulnerabilities, flag suspicious activity, and recommend access modifications. This reduces manual effort, minimizes errors, and provides security teams with actionable insights. AI-driven IGA adapts to organizational changes, evolving roles, and emerging threats, making it a strategic capability for organizations seeking robust, agile, and intelligent identity management.

## Generative AI and Natural Language Processing

Generative AI (Gen AI) and Natural Language Processing (NLP) simplify IGA and drive intelligent decision-making. Users can engage with IGA systems through conversational queries, reducing the technical barrier to entry and empowering a broader range of employees.

By selecting a vendor that leverages Gen AI and NLP, you will be able to process vast amounts of data to identify complex patterns, trends, and anomalies, enabling proactive risk mitigation, optimized resource allocation, and improved operational efficiency. Gen AI can also provide intelligent guidance, recommending appropriate entitlements based on roles, historical patterns, and least-privilege principles. This simplifies the user experience, minimizes human error, and enhances security.

# 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 Gen AI and/or ML? If so, how? What safeguards are in place to ensure that Gen AI 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 Gen AI 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 Gen AI 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 Gen AI 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?

# Discovery, Visibility and Intelligence

Modern IGA solutions have significantly advanced beyond their legacy counterparts, offering enhanced discovery, visibility, and modelling capabilities. By automating the discovery of users, and applications, modern IGA solutions reduce manual effort, minimize errors, and ensure that access rights are aligned with your business needs. This heightened control and visibility empowers you to make informed decisions about access governance, strengthen security posture, and improve operational efficiency. When selecting an IGA vendor, it is crucial to choose a solution that can provide advanced discovery and visibility capabilities to achieve greater control over your identity landscape, reduce risk, and improve overall security posture.

## Robust Audit Trail

A comprehensive audit trail provides a detailed, unalterable record of all identity-related activities, enabling organizations to track user behavior, identify security risks, and comply with regulatory requirements. By selecting an IGA vendor that provides a robust audit trail, you can ensure that you can easily investigate security incidents, respond to compliance audits, and maintain a high level of security and accountability.

## Merging Multiple Accounts into a Single Identity

To ensure a clear and accurate audit trail and gain a comprehensive understanding of user access, it's essential to maintain a coherent identity for each identity. By merging multiple accounts associated with a single individual, you can simplify identity management, reduce security risks, and streamline the provisioning and de-provisioning processes. By prioritizing the ability to merge multiple accounts into a single identity during vendor selection, you can improve security posture and maintain regulatory compliance.

## Machine Identity Management

Machine Identity Management can significantly enhance visibility and control over your organization's digital assets. By automating the classification, review, and provisioning of machine identities, MIM helps you ensure that these non-human entities have the appropriate access privileges to perform their functions. This reduces the risk of unauthorized access, improves security posture, and streamlines operations. By selecting a vendor that integrates Machine Identity Management into their IGA solutions, you can achieve a more comprehensive and secure identity governance framework, protecting both human and machine identities.

## Data Ingress Policies

Data ingress policies are crucial for enhancing visibility and monitoring within an organization's identity landscape. By governing how data enters systems, these policies ensure that only authorized data is admitted and properly managed. A robust IGA solution leverages these policies to accurately identify user identities and access rights from incoming data sources. Real-time tracking of data ingress points enables detection of potential security threats and anomalies, while pattern analysis provides insights into user behavior, potential risks, and compliance challenges.

## Priority Policies

Effective priority policies are important to consider in IGA vendor selection, as they determine the processing order and scrutiny of access requests. These policies balance timely access provisioning with robust security risk management. By strategically applying priority policies, IGA solutions can enhance visibility and monitoring, efficiently classifying users and their entitlements. This systematic tracking and analysis enable you to uncover potential bottlenecks, security vulnerabilities, and patterns of potential misuse or unauthorized access.

## Human Resources Integration

Seamless integration with Human Resources (HR) systems enables real-time visibility into your workforce, allowing for more effective monitoring and control of access privileges. By synchronizing employee data between HR systems and access management platforms, you can ensure accurate and up-to-date information about users and their entitlements. This integration also facilitates automated user lifecycle management, streamlining processes and reducing the risk of human error.

## CIEM (Cloud Infrastructure Entitlement Management)

While not a core feature of IGA, CIEM (Cloud Infrastructure Entitlement Management) can significantly enhance visibility and control over cloud resources. By integrating with broader IGA platforms, CIEM enables you to discover, monitor, and control cloud identities, roles, and permissions through a unified governance framework. This integration allows for centralized visibility into cloud access activities, automated risk detection, and consistent policy enforcement across on-premises and cloud resources.

## Dashboards and Reporting

Having complete visibility into your identity environment is paramount for effective identity governance. Prioritize vendors who can provide extensive reporting capabilities and interactive dashboards to visualize your identity data. These tools should provide tailored views of your data, including regulation-specific dashboards to meet industry standards. The ability to easily filter and drill down into specific details within these dashboards, including the ability to save and share filter sets, is also important for proactive risk management and to prove compliance to auditors.

To further streamline reporting, some vendors leverage GenAI to extract reporting material for auditors. This innovative approach can significantly enhance efficiency, reduce the overall burden of audits, and accelerate time to compliance.

# 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?

# Security Fabric

Modern IGA can be thought of as a ‘system of systems’, no longer a silo as per the traditional, now legacy model but rather a player in security operations, sharing security signals and information whilst consuming signals from the connected technology ecosystem. This concept is sometimes referred to as an identity mesh, or fabric(s).

The identity fabric is a comprehensive, integrated approach to security that connects various security tools and technologies to share information and coordinate responses. By seamlessly connecting with other security tools, such as a SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), or endpoint protection platform, IGA solutions can significantly contribute to this fabric by providing a strong foundation for information and security signal sharing and consumption.

## Shared Signals Framework (SSF)

The Shared Signals Framework (SSF) is an open standard that enables organizations to securely share threat intelligence and security event information. By participating in the SSF ecosystem, IGA solutions can enhance their ability to detect and respond to threats, improve identity verification, and strengthen access controls. When selecting an IGA vendor, it's crucial to prioritize solutions that actively participate in the SSF ecosystem to ensure seamless integration and optimal security benefits.

By integrating with SSF, IGA solutions can receive threat intelligence and security alerts from other security solutions, enabling them to proactively identify and mitigate risks. Additionally, IGA solutions can share identity-related events, such as user provisioning and de-provisioning, with SSF to provide valuable context for security analysis. This collaboration between IGA and other security solutions can help build a more secure and resilient digital environment.

SSF also plays a crucial role in enabling Zero Trust. By sharing threat intelligence and security event information, you can make more informed decisions about access control and risk mitigation. By adopting a Zero Trust approach and leveraging shared signaling, you can build a more resilient and secure IT environment.

# Questions to Access 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?

# Conclusion

This guide provides a solid foundation for crafting a comprehensive RFP, conducting thorough vendor evaluations, and ultimately making an informed decision. By leveraging the insights gained , you can ensure that your IGA solution aligns seamlessly with your business objectives and enhances your organization's security posture.

---

**To further assist you we have provided downloadable versions of the questions in both spreadsheet and document formats so you can copy and paste them directly into your RFPs.**

**RFP Questions Word Version**

**RFP Questions Excel Version**

Omada

Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.



V040225