www.pwc.com

The Case for Identity Governance and Administration

pwc

Table of contents

1. Introduction

Today's IT solutions increasingly leverage multiple heterogeneous platforms for mission-critical applications. Additionally, just as enterprise applications extend farther into the mobile and cloud space, businesses face an ever-more challenging landscape and tighter regulatory controls in order to protect their brands and meet the demands of the marketplace. Today's enterprises must therefore operate with sophisticated, secure, and scalable means to assign, monitor, and control access to company resources. As the glue between human interaction and business applications, Identity Governance and Administration (IGA) tools provide businesses with the capability to manage access in complex technical environments.

In recent years, the requirements placed on IGA tools have grown exponentially. These days, companies grow fast and furiously; it's important that a company's IGA solution does not hinder it, but rather grows with it, seamlessly supporting its success. IGA should also be thought of as an important business enabler, as it provides firms with agility in terms of both the application of controls and the ongoing monitoring of compliance. Imagine onboarding staff and contingent labor to meet sudden ramp-up needs in hours instead of days, or immediately responding to a controls need with an edit to a policy that is instantly reflected within the applications used to conduct business throughout the entire organization.

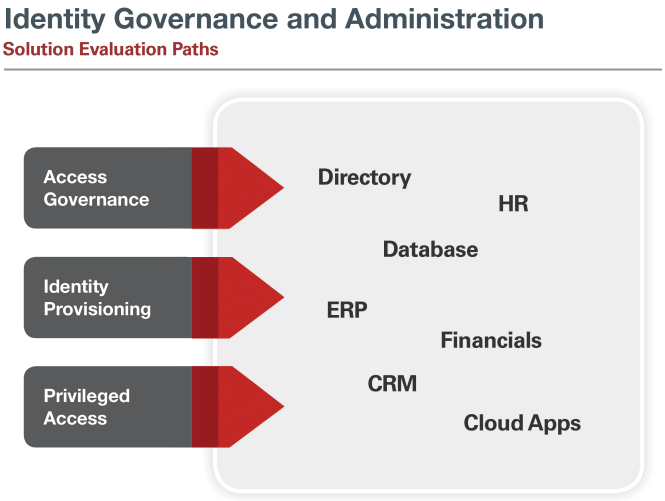
These capabilities are all possible with the right IGA solution. This buyer's guide presents key points to consider when selecting an IGA solution provider, along with evaluation criteria specific to each area of evaluation.

2. *IGA can solve business problems and help achieve significant ROI*

Technology considerations are important in the evaluation of any software tool, and IGA is no different. But the technology considerations should always be in the context of the tool's ability to solve *business problems*, and the IGA space is unique in how these considerations must be made at time of initial purchase.

In almost all cases, buyers initially will look for a solution to solve problems in one of three areas: identity provisioning, identity governance and compliance, or privileged access management. For the purposes of this guide, *provisioning* refers to the process of creating and managing user accounts in various enterprise systems; *governance and compliance* refers to the ongoing, periodic auditing and re-certification process to ensure that user entitlements are appropriate; and *privileged access management* refers to accounts that have administrative or "super user" privileges to components of the IT environment.

It is rare that buyers entering the IGA space consider all three. However, the maximum value of IGA tools is obtained when buyers invest in offerings that play to all three areas of the house, because the data entities involved are common to each type of functionality. Therefore, tools that provide a consistent and integrated data model, coupled with common connectivity frameworks, enable organizations to achieve far greater return on investment (ROI) because by their nature, they include mechanisms that can grow with a business.



When identity and governance tools are tightly integrated, ROI boosts are also achieved, because the need to create custom "bridges" between the provisioning, governance, and privileged access functions is removed. When the connection is not present, the following types of tasks must be performed during initial implementation and as ongoing maintenance when updates are made to any of the areas:

- **Extract, transform, and load between the systems, potentially with complex mapping between data entities.** For example, disparate tools may not allow the same types of relationships between users, their accounts, and the level of access that can be managed. This means that auditors and managers will see different pictures when looking at a user's access privileges in the provisioning system, and reports from the governance system. Auditors and managers therefore cannot truly understand and certify access without gathering additional information.

- **Management of business-friendly entitlement names between the systems.** Many computer systems use codes or abbreviations to "name" a given account type or access level. These abbreviations often do not provide a business context that a manager or reviewer can understand. For example, "AP1" does not help a manager or reviewer understand that the access right in question is equivalent to an "Accounts Payable Approval role with signoff authority greater than $100,000." Poor entitlement names often explain why IGA tools fail to provide businesses with the data and confidence needed to know that access rights are well-managed.
- **Configuration or customization to achieve closed-loop remediation during identity certification.** Getting through a review of access rights for users is only one part of the story. When managers use an IGA tool to determine that a given entitlement is no longer appropriate for a given employee, it is critical that the non-compliant access be removed immediately. A well-integrated IGA tool will instantly react to the decision and begin a workflow to cause the entitlement to be removed, and provide reporting and escalation to ensure that the action is taken.
- **Reconciliation and documentation of data movement between the systems**. This is directly related to the concept of closed-loop remediation above. In the absence of out-of-box integration within the IGA tool, auditors and compliance managers must rely upon comparison counts between the provisioning and recertification tools as a check for compliance. For example, managers should look at the total entitlements that exist in the provisioning tool and compare it to the total number of entitlements reviewed in the recertification tool. Then, a step must be taken to compare the number of items that were flagged as inappropriate with the total number of entitlements remaining in the provisioning system after access was removed. This process may sound straightforward, but consider how complex it can be if the IGA tools don't track entitlements in the same way in their data models, or don't have out-of-box functionality and reporting that can accurately and automatically track the identification and subsequent removal of an inappropriate entitlement.
- **Manual control of the timing of activities instead of real-time updates in both areas of functionality.** Again, this is all part of the remediation of inappropriate access. If an out-of-box integration isn't available, then it's extremely important that access review and remediation activities be kept very carefully in sync during the recertification campaign so that the data can be tracked effectively. This need to keep data in sync during the remediation work results in the need to create artificial "freeze" periods for access request management so that these activities do not cloud the data and counts that compliance managers rely upon to certify access. These "freeze" periods can cause day-to-day disruptions in needed, business-as-usual management of access.

Just as buyers typically start their investigation with a preference for either provisioning or governance, some IGA tool providers also developed their products with more focus on one or the other. In some cases, this means that an "integrated" tool actually comprises one or more acquired products. In other cases, it means that the sophistication of the "weaker" side continually lags behind, since it's a lower, or at least later, priority in terms of development effort. While buyers can accomplish their due diligence with regard to this issue by following the steps outlined in the "Converged Audit Reporting and Governance" section of this document, emphasis on this item is provided to ensure that it is not overlooked.

The effectiveness of any IGA tool will be the result of how well the tool performs in multiple dimensions, such as workflow, ease-of-use, connectivity, and performance, rather than how it stacks up in any single area. The key business needs of an IGA tool are summarized below, followed by sections specific to each area:

- **Speed/Ease of Deployment** – Customers must be able to quickly deploy IGA capabilities, supported by out-of-box functionalities that are configurations rather than customizations.

- **Ease-of-Use** – Getting ROI out of an IGA solution requires that the provisioning process become less an IT administrator task and more of a business task performed in a self-service mode by employees and their line managers. The functionality must therefore be accessible and understandable to end users.
- **Customization, Integration, and Extensibility** – While the majority of functions should be supported through out-of-box configuration options, the nature of the IGA business problem is such that there will *always* be a need to customize *some* aspects of an IGA tool to meet the unique business needs of any given customer. It is therefore critical that the tool offer a standards-based framework for tailoring.
- **Converged Audit Reporting and Governance** – The provisioning side of an IGA tool is only one dimension of the product. Businesses should have access to a comprehensive reporting suite that enables efficient and intelligent actions to continually verify compliance, report to auditors, and receive proactive notification of items needing investigation and remediation.
- **Standards-Based Architecture and Vendor Viability** – IGA systems will become part of the long-term, strategic IT landscape. Long-term supportability is therefore critical. It is imperative that the tool vendor demonstrate long-term viability, and that the product itself be built upon technologies that are open and standards-based so that an organization can effectively support, enhance, and maintain it over the long term.
- **Performance and Scalability** – IGA systems must store and process a great deal of information about each user. Consider the example of a large, regulated enterprise that depends on the IGA system to efficiently automate the provisioning process, and also serve as the source of record for internal and external auditors. As described later in this document, the amount of data that must be tracked and processed by an IGA tool in order to provide comprehensive functionality can easily translate to millions of records for just a few systems. Therefore, the scalability and performance of *all* components are absolute requirements when choosing a tool.

3. Ease of deployment and maintenance

ROI from an IGA tool is expected to increase as the number of integrated systems rises, and as the *depth* of the integrations increases. For example, ROI can be derived simply from using the IGA tool to manage the "front-end" parts of provisioning, such as the request-approval workflow and basic record-keeping of "who has access to what." A level of ROI is achievable even if the "last mile" provisioning remains an admin-performed task.

However, consider how much *more* value is added whenever that last mile can be automated as well. High volumes of access requests can be off-loaded from admin or helpdesk staff, access can be granted or revoked at the speed of the network, accuracy of the process increases markedly, and avenues for out-of-band access can be greatly reduced. This "last mile" value is further compounded when management can quickly and easily report, audit, notify, and resolve issues related to compliance and regulations.

The ability to get to this deep, end-to-end set of capabilities depends upon four factors:

- Modular architecture facilitates flexibility by allowing every component to be deployed with an enterprise standard approach. This includes an enterprise-class database, application server, and workflow engine, and their associated backup, recovery, and maintenance attributes.
- A robust, out-of-box connector library with pre-built hooks to enterprise resource planning (ERP), leading line-of-business applications, productivity and collaboration tools, and infrastructure such as email systems, directories based on LDAP (Lightweight Directory Access Protocol), and Active Directory
- A framework that provides pre-built hooks, or enables standards-based connectors to be developed for cloud services.
- A framework that enables standards-based, custom connectors to be developed for one-off or homegrown system integration.

Buyers should evaluate all of the factors in order to understand the effort required to achieve the depth of integration needed.

3.1. Evaluation criteria

1. Evaluate the vendor's list of available, out-of-box connectors against the list of internal applications that are targeted for integration.
2. Select an example application for which an out-of-box connector is available, but where there is also a moderately complex set of workflow, audit, or other requirements associated with the provisioning process. Work with the vendor to understand exactly how those requirements can be met through configuration.
3. Select an example application for which no out-of-box connector is available and work with the vendor to understand exactly how integration will be achieved.
4. Analyze the product documentation and identify how the application is internally tiered with regard to the database type/structure, application server type, workflow engine capabilities, and user interface (UI) builder and rendering technology.
5. For each of the tiers above, compare the underlying components to existing internal skillsets and ability to incorporate them into existing backup, recovery, and maintenance facilities and processes.

4. Ease-of-use

As mentioned previously, ROI increases when an IGA tool enables business users to perform provisioning through web-based request-approval workflows rather than via submission of tickets that ultimately require system administrators to perform manual provisioning tasks. This means that the IGA UI must be clear and simple so that end users can immediately use the tool with a minimum of training. It is also important that the IGA tool provides ease-of-use for the compliance-related functionalities necessary for internal and external audit staff.

Given that a key consideration with an IGA solution is ease-of-use, the out-of-box UI is important. However, buyers must keep in mind that tailoring or customization will always be required in the UI to meet unique branding and functionality needs. This means that a sound UI evaluation must include consideration of how difficult or easy the customization tasks will be. In particular, the following should be taken into consideration:

- Out-of-box UI components should be easily configurable using technologies familiar to web developers, and should conform to the standards that users expect of a web-based application.
- The tool's UI framework must be architected so that the UI *performs* well, and offer hooks for customization that can be performed *by web development professionals*, both from a front-end and logic perspective.

4.1. Evaluation criteria

1. Create a matrix of internal staff skillsets and/or outside firms who have responsibilities for UI development in the organization. Have representatives from this group conduct a walk-through implementing a single-example web page or multi-page workflow with customary branding elements and the addition of a small number of custom fields or default overrides.
2. If the organization offers IGA as a shared service, consider whether or not different consumer groups will need different branding. If this scenario is likely, walk through an example of how to achieve different branding for a given page set.

5. Customization, integration, and extensibility

Just as the UI components should provide buyers with the ability to add unique elements to the out-of-box capabilities, no IGA tool provider will be able to meet all of the unique requirements that a buyer will have within the application and database layers. Buyers should therefore carefully evaluate the capabilities that the tool offers for custom extension and integration with systems for which no out-of-box integration is available. In other words, extensibility should be thought of not only in terms of adding a custom process to a solution, but also the constant, natural need for extension of the solution as requirements evolve over time.

Key extensibility factors to consider are:

- Connectivity to target systems, meaning the ability to leverage application programming interfaces (APIs) to integrate with systems which do not have an out-of-box connector
- In larger enterprises, connectivity and integration with help-desk or service-tracking applications to maintain capabilities for metrics reporting, auditing, and troubleshooting
- The ability to customize request/approval workflows to meet unique approval and audit requirements
- An open and transparent database schema that allows for extension to keep unique fields and entities modeled, but also tracked using the built-in audit and reporting features

5.1. Evaluation criteria

1. Request the standard documentation set provided with the product to evaluate visibility and accessibility of the database schema.
2. Request a walkthrough or proof of concept (POC) on connecting to the database schema via standard query tools or provided API set.
3. Request a walkthrough or POC of extending tables, adding custom procedures, etc.

6. Converged audit, reporting, and governance

Converged identity lifecycle management, governance, and privileged access management ensures that there is no disconnect (or loose coupling) between the three processes. IGA buyers should pursue the combination of last-mile provisioning, access governance, and privileged access management. In other words, provisioning processes and policy evaluations should be integrated in a way that leverages alert notifications, workflow initiations, and closed-loop remediation in a continual, business-as-usual fashion.

From the reporting perspective, an IGA tool must provide users with an identity warehouse that can consolidate and correlate identity data such as users, roles, entitlements, their relationships, policies, and authentication/ authorization events into a single, unified repository. All enterprises will have some unique requirements when it comes to how they model data relationships, so it is critical that the IGA tool's internal data structures can accommodate these one-off situations.

Effective compliance and governance *action* will arise from a constantly available, holistic view of the identity data. This means that the IGA tool must help users to analyze identity data via key performance indicators (KPIs) and trend analysis—ideally with the ability to alert management to potential issues requiring investigation and resolution, such as out-of-band granting of access, potential regulatory violations, aging certifications, and other situations that may be outside of policy.

A key enabling factor in all of the above is the use of a unified database that can model the complexity of the underlying data and relationships in a proven, enterprise-class, database engine. Strong IGA tools cannot rely upon a disconnected-file or pointer-oriented data model without introducing inconsistencies, errors, and performance problems in both the provisioning and reporting functions of the tool.

Finally, an often-overlooked aspect of governance is the importance of the tool's ability to proactively mitigate risk every step of the way—during account provisioning, user login, application access, privilege assignments, policy changes, etc. The presence of a fine-grained security model underneath an IGA tool not only ensures privacy for the sensitive data—it also reduces the risk and manual overhead of auditing the routing of access requests to the right approver, ensures proper routing and handling of certifications, and limits end-users' requests and obtainment of inappropriate privileges.

6.1. Evaluation criteria

1. Request a standard documentation set provided with the product to evaluate visibility and accessibility of the database schema.

2. Select a connected system that has complex data modeling requirements and perform an analysis to determine how the data would be modeled in the solution.

3. Request a POC demonstration to evaluate out-of-box, canned reports as well as out-of-box capabilities for constructing ad-hoc reports.

4. Ensure that internal compliance and audit groups evaluate the out-of-box auditing capabilities by modeling an existing audit/compliance report in the IGA tool.

5. If possible, load the tool with the highest-volume and highest-churn identity data and evaluate performance of the reporting components.

6. Request a POC demonstration to perform an access/ entitlement review of an identity requiring a revocation of privilege. Evaluate the tool's capability to perform a closed-loop remediation.

7. Standards-based architecture and vendor viability

IGA development is an ongoing responsibility and is typically characterized by cycles of heavy development intermixed with periods of relative quiet. Some development demands will necessarily require specific skills with the IGA tool internals, but a significant proportion of the demand is related to standard application development tasks. Buyers should leverage outside partners to meet the staff ramp-up/ramp-down requirements associated with the latter need, so it is important that those aspects of the IGA tool be built upon standards-based architecture that is understandable by web and app developers that are available in the marketplace. To the extent that a solution is closed or proprietary, it becomes more difficult to manage the ongoing maintenance and development of the system.

The same is true of the data layer of the IGA product. Every business will have some unique characteristics that influence how they model entitlements and roles, as well as the basic data that they need to track and audit as part of their operations and compliance needs. Some access types lend themselves to roles, some only to entitlements, and some to a mix of the two. It is critical that businesses model their access requirements as flexibly as possible in the database and logic tiers of the solution via standards-based programming and database tools. In other words, the database schema and data-access layers must be as open and transparent as possible.

Finally, vendor viability is an important consideration under this heading, as an IGA tool will become a key, long-term component of the buyer's portfolio of technologies. Long-term maintenance difficulties and/or tool replacement due to a vendor exiting the market can be complex and costly.

7.1. Evaluation criteria

1. In order to develop a shortlist, leverage market research available to get a current-state understanding of the competitive positions of all major IGA vendors.

2. Request a walkthrough or POC where an existing tutorial or example workflow is created out-of-box, and then add a custom field, branching logic, or other customization to the UI, application layer, and database table. Compare the tools and methods required to the standards and skillsets in the buyer organization.

3. Obtain standard product documentation covering API integration capabilities with Java, .Net, Web Services, etc.

8. Performance and scalability

Even if the initial IGA deployment is small, enterprises naturally expand their use of the IGA tool over the long term to maximize ROI and increase operational efficiencies. In addition to basic entitlement management, most enterprises start to utilize roles and take advantage of governance capabilities to continually evaluate the appropriateness of access on a per-user basis. Indeed, leveraging these capabilities is key to the ROI proposition of IGA tools.

As use of the tool expands, the underlying data volumes and relationships among the stored entitlements will grow exponentially. For example, consider a scenario in which the IGA tool is managing 10 systems with 10 permissions per system with 1,000 users, for a total of 100,000 (10*10*1,000 = 100,000) records. This volume of records will regularly be evaluated and accessed by the reconciliation engine, the UI, the reporting engine, and all other key system components.

While that does not initially appear to be a large volume, consider that a typical organization will have 35 to 50 separate applications that require management and auditing for regulatory purposes. Data volumes in this scenario will range from 350,000 to 500,000 records across multiple tables if the number of entitlements is kept at 10 per system and there is no growth in user population. IGA tools are also increasingly used to track the provisioning of mobile device entitlements, with the average employee having a minimum of two devices and dozens of apps. But the volume of the entitlement data is just one aspect to consider. Tracking and reporting on the auditable *events* associated with all of these entitlements is a key requirement of IGA tools, and there are usually multiple events associated with any one entitlement. Audit records will therefore grow at an even greater rate than the entitlement data itself.

In addition to these internal scalability requirements, IGA tools must also scale to support business-to-business-oriented or business-to-consumer-oriented volume requirements. The scale requirements here are limited only by the size of an enterprise's customer and partner user base, and can easily reach user volumes measured in tens of thousands, hundreds of thousands, or even millions. For users who will extend their IGA capabilities externally, IGA solutions should be evaluated at the level of original design principles, and by how those principles meet the scalability needs of the extended enterprise.

Ultimately, as the number of users, systems, and entitlements grows, the number of database records that must be evaluated and accessed by the tool grows at an ever-increasing rate, and the potential impact on system performance hits increases as well. Buyers should keep in mind that scaling is not just a function of the scale of end-user population and concurrent connections, but extends deeply into the tool in terms of available processing threads, job queues, workflow touch points, bulk reconciliation data, historical snapshots of data, etc. If any of the tiers of the tool have bottlenecks, the other tiers will be blocked.

Finally, buyers should understand that the performance of the IGA tool itself is not the only scaling consideration. Reconciliation operations require real-time comparison of the IGA repository to the user entitlement repositories of all the connected systems, many of which are mission-critical applications that can't tolerate performance hits caused by an inefficient reconciliation engine. It is of paramount importance that the IGA tool manage that data in a scalable manner with good real-time performance. Any evaluation of products in this space *must* test the product's ability to scale.

8.1. Evaluation criteria

1. Determine the highest-volume identity sources and targets to be integrated with the initial IGA implementation. Request a walkthrough or POC of the following types of operations using typical data volumes in the environment:

    a. Initial reconciliation of user identities to populate the IGA repository

    b. Moderate to heavy update of attributes within IGA repository which will require an outward synchronization back to the source(s) or target(s). Perform the target reconciliation to push updates.

    c. Target reconciliation to identify rogue entitlements.

    d. If password reset or synchronization is a significant capability being pursued, perform a typical daily volume of these activities.

    e. Entitlement Management

        i. Entitlement Lifecycle Management (Join, Transfer, Leave of Absence (LOA)/Return LOA, Termination, etc.)

    f. Evaluation of a moderate number of lifecycle management tasks performed in bulk for specific, high-volume entitlement types in the buyer environment. (Join, Transfer, LOA/Return LOA, Termination, etc.):

        i. Entitlement Lifecycle Management

        ii. Role Lifecycle Management

        iii. Role Content Certification

    g. If the IGA solution will need to authenticate to a distributed directory system or SSO (single sign-on) system, evaluate performance under typical loads and scenarios.

    h. Evaluate the performance of the reporting engine by identifying report types that are critical in the environment and running them with typical scopes in place. In particular, if the buyer environment is subject to industry regulations or other mandates, look at reports that are significant for compliance and audit purposes. Key report types will generally include the following:

        i. Orphaned/Unmatched Accounts Report

        ii. Managed System: Accounts Report

        iii. Search/Value User Report

        iv. Entitlements Aggregation Report by users and groups

        v. Historical entitlements by individual with approver detail

        vi. Users/Groups having specific entitlements or roles

        vii. Custom reporting via out-of-box interface

        viii. Custom reporting with database query tools

9. Strategic roadmap considerations

The criteria outlined above provide guidelines for evaluating core IGA tool functionality. They form the basis of a solid IGA capability and are must-have capabilities.

Strategic, market-leading IGA vendors differentiate themselves by expanding the breadth and depth of their offerings, and by bringing more identity and access management functions under the same governance "umbrella" in order to achieve greater leverage from the IGA investment. One area that is of particular interest in this context is privileged access management (PAM). These solutions typically comprise a password "vault" for highly-privileged administrative accounts, and allow firms to lock these passwords in the vault and securely check them in and out as needed via auditable workflow.

PAM has traditionally been addressed with standalone tools, but now, PAM lends itself to the same kinds of ongoing technology, management, and governance requirements as traditional provisioning and certification of entitlements. PAM solutions should provide the following features, similar to those of a "traditional" IGA tool:

- An extensible framework for the development of UI components via configuration
- An open-standards-based framework for the configuration of connectors to the target systems managed by the PAM solution
- Support for custom workflows for the assignment and ongoing management of access to the privileged credentials
- Detailed, auditable event reporting about users with highly privileged accounts (HPA) access and the ongoing use of that access in real time
- Recertification of access to HPA credentials

Given the similarity of requirements, the incorporation of PAM as out-of-box functionality in an IGA tool will allow firms to achieve the same level of consistency and capability out of a single investment.

Another area of strategic differentiation is the integration of mobile and cloud technologies within the IGA tool. Although the integration of mobile and cloud with IGA is currently in its early stages, truly strategic vendors are looking in this direction, given the growing importance of these technologies. While mobile and cloud apps allow companies access to features and functions without the requirement of building the infrastructure themselves, the management of identity and access within those services is just as critical. Uncontrolled access to the data and functions exposes businesses to the same risks that are present in home-hosted applications. If the level of risk from traditional, self-hosted applications makes IGA tools a worthwhile investment, then the IGA investment makes even more sense when applied to data and functionality that is hosted and provided outside of the walls of the enterprise. The need to provision entitlements, manage them, and report and recertify are exactly the same. Strategic IGA tool vendors will have greater depth of features in the mobile and cloud realms, and will have pre-built hooks to the industry-leading apps and services so that integration is a configuration exercise, rather than a customization exercise.

10. Conclusion

When researching and choosing an IGA solution for an enterprise, many factors come into play. It's important to approach the challenge of finding just the right solution with an understanding of how various options solve business problems and offer significant, ongoing ROI.

One of the most important features to look for in a solution is tight integration of identity provisioning, identity governance and compliance, and privileged access management. This can be a challenge to find because often developers focus on either provisioning, governance, or privileged access—not all three—resulting in one area being weaker than the other three. When the three are designed to work together, businesses avoid an array of costly and time-consuming tasks that must be undertaken during either initial implementation or updates. Moreover, the IGA will not only demand far fewer customizations, but also have the capacity to grow with the enterprise over time.

It's to an enterprise's advantage to keep particular business needs in mind when choosing an IGA. Speed of deployment, for example, often depends on out-of-box functionalities. It's also crucial to have a solution that provides ease-of-use for end-users (often managers and auditors) who do not have IT expertise. Then, because it's inevitable that some customization will be required, it's important that the system be built on a standards-based framework. Converged audit reporting and governance ensure that provisioning processes and policy evaluations are integrated; when those are well-designed, loops remain secure and closed, and good management is well-supported. Choosing a reliable, well-established vendor that has a track record with the product that is standards-based keeps maintenance costs down.

Finally, a good IGA solution should perform well and be scalable. It should be designed to accommodate the volume of entitlement and event data that a company generates not just at the time of purchase, but that increases over time and as the business grows.

Investigating IGA solutions for an enterprise requires a keen understanding of how the IGA will support business needs now and for years down the line, as well as an understanding of just how much ROI is affected by the right choice.

11. Global Success Stories

Consistently recognized as a global leader in information security, PwC has performed security assessments or implementations at 78 percent of the Fortune 500 and more than 200 Oracle Identity Access Management/IGA implementations in the United States. Recognized by market influencers as a leader in security and identity and access management solutions, we have developed proven tools and methodologies that we deliver on every engagement.

Examples of the leading-edge IGA implementation work that PwC has provided to its clients include the following:

Global Pharmaceutical Firm - Divestiture

PwC assisted a global biopharmaceutical company in a multi-year divestiture initiative to separate its IT infrastructure from the parent company. As part of the separation, the divested company needed to develop a comprehensive security investment plan and operating model to proactively identify and mitigate information security risks and protect the new organization's intellectual property, trade secrets, and business intelligence.

- Faced with the reality of quickly losing the parent company's IT support, the company also had to contend with cost and schedule pressures to stand up new capabilities.
- PwC developed an actionable identity and access management (IAM) strategy, and assisted the client with an ahead-of-schedule delivery of a foundational deployment of Oracle Identity Manager 11g R2 for identity management.
- After working with the client on additional integrations to the initial deployment, the divested entity now has a globally simplified and consistent identity management process, enabling secure collaboration with a broad range of partners and vendors.
- End-users now have a seamless transition and on-boarding experience, with automated provisioning of access and IDs. Productivity has increased significantly since contractors and users don't have to wait for access to critical applications, and improved lifecycle management of access and roles has significantly reduced inappropriate access, enabling the company to protect its intellectual property, reduce the cost, and bring more agility in its business operations.

Global Financial Firm – IGA Re-architecture

PwC's client had been investing in IGA tools for several years. However, due to limitations and support complexity with their previous implementations, in 2012 the client decided to develop a new target state architecture and implementation roadmap to meet the following business objectives:

- Provide a common framework for enabling IAM related processes.
- Provide a service-oriented focus based on industry standards.
- Enable efficient and cost effective integration of the heterogeneous components with the client's IT environment.
- Leverage out-of-the-box functionality to limit customizations and associated support overhead.
- Allow for application on-boarding and functionality at an increased pace.

PwC helped the client to successfully enable the following technology components of their chosen provider: Access Management, Identity Management, Federation, Virtual Directory, and Adaptive Access Management (for fraud prevention). This implementation was sized to serve in excess of five million users and the management of entitlements throughout the organization.

Global Pharmaceutical Firm – Technology Refresh

A leading pharmaceutical and life sciences company had a mature, existing implementation of Sun Identity Manager (SIM) as its identity and access management platform. The client needed assistance in order to define a strategy and plan an approach for replacing the SIM platform. As with most Sun clients, the company had customized the core SIM platform extensively, resulting in a very robust but highly customized SIM implementation with vast business complexity built into it.

As the company planned its strategy for migrating to a new platform, it sought to develop a future-proof architecture that could serve as a platform for ensuing use cases such as cloud provisioning and enabling mobility. In addition to developing an advanced platform to handle future use cases, the company also sought to accomplish the following goals:

- Reduce the complexity in its highly customized environment over all aspects of Identity Management, including recertification and governance
- Simplify business processes around access requests and identity management provisioning
- Drastically reduce the level of support that the solution required for day-to-day maintenance

The client engaged PwC to perform a strategy and road mapping exercise. After a detailed analysis of the company's existing system, PwC gained a strong understanding of the business drivers, technical drivers, and the functionality the company would require in the future state, and developed a strategy and roadmap to move the client in a phased approach to Oracle Identity Manager 11g R2.

The client agreed with our recommendation of a parallel upgrade approach, and after taking the implementation project to RFP and evaluating bids from other organizations, it selected PwC to perform the migration. The company chose PwC based on the depth of our Sun to Oracle migration experience (including access to our targeted investments in process, tools, and accelerators), and our strong global IAM capabilities and Oracle-specific expertise. Not only do we have the world's largest information security consulting practice, but we are also the clear leader in strategy, implementation, and integrations of Oracle Identity Governance.

Our delivery approach leveraged staff working across our global ecosystem, led and coordinated by a strong onsite team and supported by our off-shore resources, bringing the right skills and experience to the project in an extremely cost-effective model.

Leveraging our deep industry knowledge and expertise in business consulting, we help our clients address the financial, human capital, operational, technical, and compliance challenges that our clients face when undertaking significant IGA upgrades or new implementations.