

# Magic Quadrant for Identity Governance and Administration

30 December 2013 ID:G00253758

**Analyst(s):** Earl Perkins, Felix Gaehtgens, Brian Iverson

The identity and access management market has experienced significant upheaval along with its usual growth over the past two years. What began as two relatively distinct markets, user provisioning and access governance, have merged into a single category of identity governance and administration.

## Market Definition/Description

This document was revised on 31 December 2013. The document you are viewing is the corrected version. For more information, see the [Corrections page](#) on gartner.com.

Identity governance and administration (IGA) is a set of processes to manage identity and access information across systems. It includes management of the identity life cycle that creates, maintains and retires identities as needed, as well as governing the access request process, including approval, certification, risk scoring and segregation of duties (SOD) enforcement. Core functionality includes identity life cycle processes, automated provisioning of accounts among heterogeneous systems, access requests (including self-service) and governance over user access to critical systems via workflows for policy enforcement, as well as for access certification processes. Additional capabilities often included in IGA systems are role management, role and entitlements mining, identity analytics, and reporting.

For 2013, Gartner introduces this Magic Quadrant for Identity Governance and Administration, which consolidates two separate Magic Quadrants — "Magic Quadrant for User Administration and Provisioning" and "Magic Quadrant for Identity and Access Governance."

## Magic Quadrant

**Figure 1.** Magic Quadrant for Identity and Governance Administration



### STRATEGIC PLANNING ASSUMPTION

By year-end 2017, half of all identity governance and administration providers will be new to the IGA market.

### EVALUATION CRITERIA DEFINITIONS

#### Ability to Execute

**Product/Service:** Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

**Overall Viability:** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

**Market Responsiveness/Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

#### Completeness of Vision

**Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance



changes to support operations appear to have been favorably received by some customers.

- Extensive support for regulatory controls in the product has been known to increase the amount of work required during implementation when inputting and configuring controls. Enterprise Guardian deployments would benefit if better integration with IT governance, risk and compliance (GRC) tools were available in the product.

▲ [Return to Top](#)

## Atos

Atos, based in Bezons, France, is an IT consulting, system integration and managed services organization that purchased Siemens IT Solutions and Services group in 2011, including the DirX product line. Atos offers DirX Identity and DirX Audit as an IGA solution. As part of Atos' DirX suite, its offerings include Web access management and federation, directory services, and biometric authentication.

DirX products are software components developed with Java and .NET technologies and scripting, and can be flexibly deployed on Windows, Solarix or Linux platforms. DirX has its own directory, but can also support other vendor directories as the primary repository. Due to its metadirectory origins, even the product's system objects and configurations are stored in the directory, supporting flexibility in deployments. Log entries can be sent to DirX Audit, written to files or stored in a database (Oracle or Microsoft SQL Server). The component nature of DirX means that it can be deployed as a single software solution on one platform, or spread across a number of platforms to optimize performance and availability.

### Strengths

- DirX Identity provides a clean, business-oriented user interface that offers flexibility for users initiating requests.
- Atos has leveraged its managed services experience to package the DirX products as a hosted service.
- DirX allows for fine-grained delegation of governance tasks to managers, project sponsors, contract owners and business partners, and limits their scope to the identities and roles/entitlements/projects/contracts they are responsible for.

### Cautions

- Historically, Atos has focused primarily on the European market, although it does have some penetration in other geographies through its Siemens channel relationships.
- In some case, the DirX approval process can become confusing because the product splits requests for multiple roles and entitlements into separate requests for individual items, each with their own workflows.
- In contrast to a flexible individual reapproval of temporarily assigned roles/entitlements, the access certification campaign capability is rudimentary and limited to supporting only certifications by owners of individual privileges or roles.

## Avatier

Avatier, based in San Ramon, California, has focused exclusively on IAM since 2005. The Avatier Identity Management Software (AIMS) Suite is available modularly and includes any combination of the following products: Identity Enforcer, Password Station, Group Requester, Group Enforcer and Compliance Auditor. AIMS is a Web-based application that runs on .NET (32- or 64-bit), with components hosted on IIS application servers and every component called as a Web service. Identity information is stored in an LDAP directory, while policy and other runtime data are stored in a database repository. AIMS can use Oracle, Microsoft SQL Server, IBM DB2 and Teradata databases.

Avatier has focused on delivering a product that is easy to configure and deploy without the need for scripting or other customization, often promising a low deployment-to-license cost ratio of 1:3 to 1:2. Avatier was one of the first IGA vendors to deliver an access request interface using the shopping cart paradigm to improve the experience for end users. It was also among the first to offer mobile apps to allow access to identity data and functions from mobile devices.

### Strengths

- Avatier has expanded its appeal to clients across multiple industry pillars through effective, targeted marketing.
- Avatier's UIs, design principles and target delivery platforms (including mobile devices) appeal to new-generation IGA buyers.
- Avatier has a solid record of rapid implementation and customer satisfaction.

### Cautions

- Avatier is relatively new to the system integration market and only recently has begun to significantly leverage the channels.

- While active in North America and some Asia/Pacific markets, Avatier is still developing opportunities in other geographies.

## Beta Systems

Beta Systems, which is based in Berlin, has been selling its flagship Security Access Manager (SAM) product since 1994, making SAM one of the longest-running IGA solutions from a single vendor. SAM addresses the needs of the IGA market with its SAM Enterprise Identity Manager, SAM Business Process Workflow and SAM Garancy Access Intelligence Manager products. Garancy is a completely new element of the product line, providing access intelligence capabilities based on business intelligence (BI) technology to attract the business end user.

The SAM suite is cross-platform, and most of Beta System's customers have deployed it on Windows, Linux, and Unix. Enterprise Identity Manager's origins are in the mainframe market, so its support for managing mainframe security can be expected to be richer than that of competing products. With its mainframe heritage, customers can also run key components (Database, Master Courier, Reporting Server and Business Servers) on a mainframe (z/OS). Workflow and analytics components are installed on Windows servers. End-user functionality is delivered via a PHP Web application, while much administrative functionality is delivered via Java applets that can run on Windows workstations or can be downloaded via Web servers. The product repositories can use Oracle, Microsoft SQL Server or IBM DB2 databases.

Beta Systems is recovering from a difficult period in 2011, when license revenue declined sharply. Growth returned in 2012. In 2013, the company brought in a new CEO and other executives, and is investing in the product and the expansion of its sales channels, and in building an international presence.

### Strengths

- Garancy Access Intelligence Manager is pushing the envelope in terms of identity analytics and intelligence through the adoption of a BI approach.
- Beta Systems is using an OEM workflow engine, JobRouter, which is preconfigured to work with Beta's repositories and provisioning engine, instead of providing a purpose-built workflow system, as is often done with other products.
- Beta Systems has carved out a strong niche in the financial services industry, which accounts for 75% of its customers. More than 50% of its customers are in banking, particularly in German-speaking markets, where its knowledge of regulatory requirements are deep.

### Cautions

- Beta Systems still has a limited presence outside Europe and has just recently started to invest in increasing its presence in North America.
- SAM Enterprise Identity Manager has demonstrated rigidity in policy management capabilities, especially with respect to handling issues concerning segregation of duties.
- After facing hard times in 2011, Beta Systems has turned the corner and is growing again with a positive outlook, although license revenue has not yet returned to 2010 levels.

## Caradigm

Caradigm, based in Bellevue, Washington, was formed as a joint venture between GE Healthcare and Microsoft in 2013. Caradigm's entrant in the IGA market is Caradigm Provisioning, which is packaged as a complete solution aimed exclusively at healthcare providers. Caradigm Provisioning is a Java-based Web application that runs with the Jetty application server on a Windows platform. Its identity auditing, reporting and analytics functions are provided by SQL Server Reporting Services (SSRS) running with IIS on a Windows platform. The application uses Microsoft SQL Server as its repository.

Caradigm Provisioning is part of a portfolio of products intended to satisfy a full range of healthcare needs, including offerings for single sign-on and context management. A key distinguishing feature is its ability to provide detailed and product-specific role-based provisioning for clinical applications.

### Strengths

- Caradigm's intense specialization on providers in the healthcare industry positions it favorably in a market that is expected to grow significantly as a result of increased healthcare spending and consolidation.
- Partnerships have allowed Caradigm to penetrate overseas markets in EMEA, Australia and New Zealand.
- Caradigm Provisioning offers deep integration with Epic, the dominant application for patient management in the healthcare industry, utilizing Epic's Web services API. Epic integration usually is a significant pain point for healthcare customers working with other products.

### Cautions

- Despite Caradigm's focus on healthcare, it lags in governance features, especially key access certification, which has allowed competitors with a broader focus on the IGA market some room to maneuver and win deals.
- The user interface for Caradigm Provisioning is primitive compared with the offerings of other IGA vendors.
- Caradigm has a lot of ground to make up in order to restore goodwill among customers after shutting down the former technology that it had acquired.

▲ [Return to Top](#)

## CA Technologies

CA Technologies, based in Islandia, New York, is a major vendor in the IAM market that has made many acquisitions in this space over the years. Alongside CA's on-premises offerings, it has an ambitious, cloud-centric strategy and delivers cloud-based IAM services, including user administration, through its CA CloudMinder Identity Management product.

CA Technologies offers IGA services through its IdentityMinder and GovernanceMinder products. Until 2011, the product was called Role & Compliance Manager. GovernanceMinder uses the same workflow engine as IdentityMinder and has significant integration capabilities with other IAM portfolio products, such as Shared Account Manager (SAM), which is a part of CA's ControlMinder PAM suite. IdentityMinder and GovernanceMinder have been written in Java and run on WebSphere, JBoss or WebLogic application servers. The underlying synchronization and reconciliation engine is written in C++. Oracle or Microsoft SQL Server can be used for the identity warehouse.

### Strengths

- CA Technologies leverages its extensive suite of enterprise products and deep relationships with customers to provide visibility for its IAM products.
- CA Technologies is one of the most well-known companies in the IAM market, and marketing messages in the media are clear and high-quality, resulting in one of the highest market participation rates reported for IGA vendors in vendor selection exercises by its customers.
- GovernanceMinder has strong role-mining features, with real-time analytics that add information about role and entitlement usage, which can be made available during certifications and when viewing information about users.

### Cautions

- Despite a visionary focus on delivering parity between its on-premises and cloud IGA offerings, CA Technologies has had difficulty keeping up with the innovations of leaders in the market.
- CA Technologies has not made significant progress toward unifying its IGA suite, as IdentityMinder and GovernanceMinder still lack the integration that competitors have been able to achieve with their offerings. CA partners have demonstrated unified UI frameworks that can bridge both products and provide an enhanced user experience.
- Gartner continues to hear some negative customer feedback about product complexity and CA Technologies' support for IdentityMinder and GovernanceMinder, which may have had an impact on CA's inability to win deals.

## Courion

Courion, with headquarters in Westborough, Massachusetts, has been devoted to IAM since 1996. Courion offers two products for IGA: Access Assurance Suite (AAS), an on-premises solution, and CourionLive, a cloud-based offering. AAS is the more full-featured of the two solutions and the primary subject of analysis here. The AAS platform is composed of modules that can be purchased separately, and include AccountCourier, PasswordCourier, ProfileCourier, RoleCourier and ComplianceCourier. An additional module, Access Insight, offers robust identity analytics and intelligence capabilities.

Most Access Assurance Suite modules are delivered as .NET applications (C#, C++, ASPX and MVC) that run on Windows servers. The synchronization and reconciliation engine can be deployed as a Java application running with Tomcat or a .NET application running with IIS (both may be installed on a Windows server). For the repository, Courion can use the customer's preferred database. The most unique feature of Courion's product is that identity information does not coexist with policy and rule definitions in the repository; its Dynamic Link technology is used to fetch authoritative identity information from managed account repositories when it is needed for system operations.

### Strengths

- Although CourionLive does not offer parity with Access Assurance Suite in terms of overall functionality, it does provide a compelling deployment option for many customers at a lower price.
- Courion packages connectors, which are usually sold separately, to appeal to specific vertical markets such as healthcare, financial services, retail, energy and manufacturing.

- Access Assurance Suite provides one of the most business-friendly user interfaces in the IGA market for access requests, approvals and access certification.

#### Cautions

- Courion's IGA product line remains confusing to prospects because of the many potential combinations of modules and connectors. New offerings and methods of delivery exacerbate that confusion.
- Courion has experienced multiple reorganizations in recent years that have had a negative impact on partners and customers, which has affected sales, support and deployments/upgrades.
- Courion has a weak partner ecosystem and one of the lowest percentages of deployment projects that have participation from partners and system integrators.

#### CrossIdeas

CrossIdeas, which is based in Rome, was established in 2011, but traces its origins back to 2001 as a company called Engiweb Security. The company operates in the IGA market exclusively with its IDEAS (IDEntity and Access governance Solution) suite, which supports IGA functionality through three modules: IDEAS Access Governance Foundation, IDEAS Access Provisioning and IDEAS Access Analytics. IDEAS is a Java EE Web application that runs with multiple application server containers (JBoss, WebSphere and WebLogic) on Windows, AIX, Solaris and Linux platforms. It can use Oracle or PostgreSQL databases for its repository.

The IDEAS suite of modules provides the full range of IGA functionality, as well as externalized authorization enforcement for attribute-based access management. IDEAS offers a unique object-relational data model known as Access Warehouse that supports fine-grained management of entitlements and flexible modeling of roles, organization information and business activities. IDEAS has also been developed to include an inherent multitenancy architecture that promises easier transition to cloud-based hosting arrangements.

#### Strengths

- CrossIdeas has embarked on an aggressive push to expand its partners program, including a new cloud delivery (IGA as a service) with a white-box OEM program, allowing partners to deliver IDEAS solution components with their own branding, distinctive content, service levels and pricing models.
- CrossIdeas has cultivated a reputation as one of the most innovative companies in the IGA market in terms of product features and delivery/pricing models.
- CrossIdeas possess an unusually clean model for managing identities, attributes, accounts, roles and entitlements.
- IDEAS has anticipated the need to coexist with other IGA products by offering connectors to utilize some competitors' provisioning systems for fulfillment.

#### Cautions

- CrossIdeas has limited platform support for pure Microsoft-based infrastructures, including the lack of support for SQL Server and .NET.
- CrossIdeas has a small customer base and limited channels into international markets, which continues to be a challenge. Recent changes in its international sales and marketing strategy have yet to bear fruit.
- Despite a track record that demonstrates superior vision and innovation, CrossIdeas remains largely unknown outside Europe.

#### Deep Identity

Singapore-based Deep Identity had focused on access governance, beginning with its founding in 2009. The company's restructuring in 2013 resulted in changes to its focus and road map. Although small compared with other vendors in this market, Deep Identity remains the only IGA product vendor Gartner has identified that is headquartered in the Asia/Pacific region.

The relevant Deep Identity offerings for IGA are its Identity Audit & Compliance Manager (IACM) and Identity Manager (IM) products. The products are .NET Web applications that run with the IIS Web server on Windows 2008 servers, using Microsoft SQL Server as the repository. Beyond IGA functionality, Deep Identity has a file-server plugin called BigData Governance & Administration that allows governance to be extended to cover unstructured data as well.

#### Strengths

- Deep Identity architecture can be deployed in multitenant cloud-ready configurations where required.
- IACM and IM have out-of-the-box policy templates for performing user and role SOD compliance

checks, and include a basic risk-scoring methodology and some data access governance functionality.

- Deep Identity has very competitive pricing compared with other IGA vendors.

#### Cautions

- Deep Identity IACM is based predominantly on Microsoft infrastructure and development environments, though it does provide adapter support for other platform environments.
- Company recognition is primarily confined to markets in Asia/Pacific, including China, Indonesia, Vietnam and Australia.
- Deep Identity must continue to compete with bigger IGA vendors that attract larger Asia/Pacific customers. Moreover, the company lacks feature differentiation aside from some flexibility in its adapter architecture.

## Dell

Dell, which is based in Round Rock, Texas, offers IGA functionality with Quest One Identity Manager (Q1IM). The product, which will soon be rebranded Dell One Identity Manager, came to Dell through the acquisition of Quest Software in 2012. Q1IM expands Dell's IAM support significantly beyond the current Microsoft-centric audience, and provides an effective foundation for an identity data model as part of an IGA solution. Q1IM can also be deployed with Dell One Password Manager. Other options include the Dell One Quick Connect Sync Engine and the Dell One Quick Connect Virtual Directory Server. Q1IM is written for the .NET environment and runs on Windows or on Linux and Unix using the Mono .NET framework. It uses a service-oriented architecture that allows application components to run on separate systems. Oracle or Microsoft SQL Server can be used for its identity data warehouse.

The identity data and log model for Q1IM is known as the Unified Namespace. It is declarative and provides object-oriented database capabilities in an SQL environment. All manual and system-initiated actions in Q1IM are traced and stored. A proprietary analytics tool provides correlation and analysis. More than 40 standard reports are delivered out of the box by Q1IM's reporting tool, and a report designer is provided. Risk scoring of access during policy checking, mining and discovery is supported.

#### Strengths

- Dell offers an identity vision, strategy and portfolio that spans administration and governance without an undue focus on any single platform or software development environment.
- Dell can leverage a strong global presence throughout the world based on an extensive network of resellers, value-added resellers (VARs) and system integrators.
- Dell's support offering includes a user community where customers can interface with R&D.

#### Cautions

- Dell's pricing model favors smaller companies, but can be expensive for larger companies, especially with add-ons.
- Dell has not been successful with any distinctive marketing, as IAM products are not highlighted as part of Dell's enterprise software offerings.
- Dell's current restructuring plans create a level of uncertainty: All products in the IAM portfolio have experienced some upheavals over the past few years — first after being acquired by Quest Software and then following Quest's acquisition by Dell.

## EMC (RSA Aveksa)

Aveksa was acquired by EMC in July 2013, and is now part of RSA, The Security Division of EMC. RSA Aveksa's Identity and Access Management Platform consist of the core component Access Certification Manager with several additional optional modules (Access Request Manager, Access Fulfillment Express [AFX], Business Role Manager and Data Access Governance). RSA Aveksa, based in Waltham, Massachusetts, also offers MyAccessLive, a cloud-based SaaS version of its IGA offering, that includes single sign-on features via a OneLogin partnership.

Most components of the Access Management Platform are Java-based, running on Linux and Unix platforms within WebLogic, WebSphere or JBoss application servers, and using an Oracle Database as a primary identity repository. The business client interface is a Web browser. AFX employs an open-source enterprise service bus (ESB) that is composed of public message definitions, interaction patterns and adapters. It has now been extended to SaaS applications, such as salesforce.com and Google Apps.

RSA Aveksa's identity data and log model uses its Access Management Database called XMDB to combine identity information and log data in the same repository for report intelligence. Workflow, analytics, rule processing, administration and reporting are available. Mining and discovery tools scan

for key identity data in applications and systems to help populate the XMDB for use.

### Strengths

- EMC's acquisition of Aveksa embeds Aveksa's products into a viable IAM suite offering, and is expected to boost sales and geographical reach.
- A best-practice proof-of-concept process, aggressive pricing, improvements in scalability, high maintenance renewal rates and an expanding partner list are providing Aveksa with continued momentum in the IGA market.
- Aveksa's clean data model and architecture emphasize configuration instead of customization to achieve flexibility and adapt to customers' specific demands, as well as to simplify deployments and future upgrades.

### Cautions

- Aveksa's AFX module that offers provisioning and deprovisioning has yet to reach parity with the breadth and depth of features available with other, longer-established user administration and provisioning (UAP) products.
- Aveksa's channel sales strategy has lagged behind its main competitors, and will likely lag until the RSA channel ecosystem is engaged with the Aveksa solution.
- Aveksa is not invited to participate in RFI and/or RFP processes as often as some of its competitors, and needs to improve market awareness of its products in order to avoid being inadvertently overlooked.

## e-trust

Sao Paulo, Brazil-based e-trust offers an IGA product called Horacius. The product, which has been sold since 2006, evolved from e-trust's experience with professional services engagements within IAM projects. Horacius was developed with a focus on security and governance. This has led e-trust to develop many features out of the box. Horacius emphasizes configuration over customization.

Horacius provides access request workflow functionality and tools to create managerial approval, multiple data owner approval, incident management, and segregation of duties. Horacius supports multiple data feeds in order to cater to complex corporate structures with many HR systems, and provides connectors to automate provisioning on Microsoft AD, Microsoft Exchange, SAP, LDAP, Web Services and Oracle with optional password synchronization. Discovery tools are available on all connectors; mining tools are only available in conjunction with the Microsoft AD connector. Analytics tools aren't available; however, Horacius has integrated with security information and event management (SIEM) products to support automatic lockdown or flagging of accounts that have been linked to suspect activity.

### Strengths

- In order to comply with Brazilian federal regulations, Horacius supports privacy guards within the products. Access rights can be tagged to information classification levels.
- Horacius has the notion of "security events" that can be triggered from outside or by detecting patterns such as an SOD violation, or differences between effectively approved rights versus rights discovered on a target platform. These security events can then be handled according to configured actions.
- Of all products covered in this report, Horacius has one of the smallest footprints in terms of hardware required.

### Cautions

- The UI is functional but oriented more to an IT audience.
- E-trust is growing, but the company is small, and its customer base is still exclusively within Brazil. The company is expanding into other Latin American markets and has plans to enter the U.S. market.
- The product is developed to emphasize configuration, but customization requires code changes that can be carried out only by e-trust.

## Evidian

Evidian, based in Les Clayes-sous-Bois, France, was established in 2000 as a subsidiary of Groupe Bull. Most of its suite has been developed in-house, apart from the acquisition of Enatel, to supplement Evidian with an enterprise single sign-on (ESSO) product. Evidian approaches the IGA market through its Identity & Access Manager. Additional options include ID Synchronization, a built-in connectors package and configurations for high availability. The product is written in Java and runs within the Tomcat application server on Windows, Solaris, AIX or Linux. Oracle, SQL Server, MySQL or PostgreSQL can be used as the identity warehouse. The current solution has IGA features such as access policy management, a workflow-based access request manager, rule-based entitlement administration and a role-based identity data model.

## Strengths

- Evidian can leverage its two shareholders, Bull and NEC, to reach customers typically beyond the reach of a company of Evidian's size.
- Evidian has extended the role-based access control (RBAC) model with concepts such as organization and context. This provides enterprises with the opportunity to implement a powerful security policy while using a simple security policy model.

## Cautions

- While the company is growing at low double-digit rates, it still has most of its customer base in Europe. The number of customers in the U.S. is picking up, but at a slow rate, with a 12% increase expected for 2013.
- Evidian is still lacking some of the role mining, role life cycle and identity analytics features found in many other IGA products; however, these features are on the product road map.
- Evidian must build a stronger partner network, especially in the U.S., where a partnership with Quest Software (now part of Dell) has been limited by Dell being a direct competitor in the IAM space.

## Fischer International

Fischer International, based in Naples, Florida, offers Fischer Identity Suite for the IGA market with the following modules: Fischer Automated Role & Account Management, Fischer Password Manager, Fischer Identity Compliance and Fischer Identity Connectors. Fischer Identity Suite is a Java EE Web-based application that runs within Tomcat on Java-supported platforms such as Windows, Unix and Linux. Any Java Database Connectivity (JDBC)-compliant database can be used as the repository.

Fischer Identity Suite was built with inherent support for both cloud and on-premises delivery models, and the company-provided cloud-based hosting option includes the full-featured product with subscription pricing. The suite also provides privileged account access management as an option. Fischer designed the product with ease of deployment as a primary objective, so all product features are accessible and configurable through the administrative interface without requiring any coding or scripting.

## Strengths

- Fischer's solution is particularly appealing to smaller enterprises requiring IGA capabilities, enterprises with simpler governance-oriented requirements, and those that are cost-sensitive regarding deployment and maintenance.
- Fischer International was the first IGA vendor to offer a multitenant cloud-based product more than four years ago, and it has continued to mature the product while other vendors are just getting started.
- Fischer offers low base prices for both perpetual and subscription licenses, with flexible license options, especially for higher education and retail customers with large user populations (for example, students and store personnel) with relatively standardized provisioning needs.

## Cautions

- Governance-specific functionality such as access certification is limited, reflecting the product's heritage as a UAP tool.
- Fischer International is a small company with limited visibility and name recognition, and with the emergence of many identity-as-a-service providers, it risks being crowded out of its primary market.
- Despite making investments to broaden its network of partners for sales and system integration, Fischer International has not been able to generate momentum in this area, which could constrain growth in the future.

## Hitachi ID Systems

Hitachi ID Systems, based in Calgary, Alberta, Canada, offers the Hitachi ID Identity Management Suite, which consists of Hitachi ID Identity Manager and Hitachi ID Password Manager. All provisioning connectors are included at no additional cost. The software is written in C++ and SQL-stored procedures, and runs on Microsoft Windows 2008 R2 or Windows Server 2012 with IIS or Apache. Load balancing and replication across multiple, concurrently active servers are standard features of the product. The back end may be Microsoft SQL Server or Oracle Database. The products support technical standards as well as most features included in IGA solutions, including workflow for access certifications, entitlement mining and discovery, role engineering, a data repository, and connector architecture.

Hitachi ID policy engines support change approvals, SOD and RBAC. For access control within the product, relationships between identities can be defined, and access rights can then be attached to

those relationships. Users access the system via an HTML5 Web portal, which supports self-service and delegated administration, as well as analytics and certification. Risk classification can be calculated based on entitlements and identity attributes. Connectors are included, and almost all are bidirectional. The Hitachi ID data model is a normalized, relational database supporting users, accounts, groups, identity attributes, roles and more. Event logs include SQL (structured), text (debugging) and syslog integration (SIEM). Hitachi offers ID Identity Manager for one price for IGA based solely on the number of human users. Implementation services are provided by Hitachi on a fixed-price basis and by partners.

### Strengths

- Hitachi's product has organically grown through in-house development. It has a considerably smaller footprint than most competing products, scales well and consistently generates positive customer feedback.
- Hitachi's price model is simple and appeals to many potential buyers. Hitachi ID has a low deployment-to-license cost ratio and therefore a low TCO.
- The internal data model supports multiactor relationships to closely model existing structures in organizations for access control within the product. The SOD engine is one of the most advanced found in IGA products.

### Cautions

- Analytics are basic and accessed via reports, rather than through an interactive UI. There is no report editor to allow for creation of custom report formats, although individual reports can be filtered.
- Hitachi ID Systems' user interfaces are clean, usable and customizable; however, the interfaces trail a number of competitors in overall look-and-feel and usability.
- Hitachi ID Systems' growth in regions outside North America has been slow. Despite a credible product offering, Hitachi ID Systems is still overlooked by organizations during their RFI/RFP process.

## IBM

IBM's IGA solution is IBM Security Identity Manager (ISIM). Armonk, New York-based IBM acquired Q1 Labs in late 2011, adding Q1's foundational QRadar security intelligence technology for security analytics and use within IGA. Originally a user administration and provisioning product, IBM has opted to expand ISIM by developing access governance functionality in-house. The original access governance effort, known as Role and Policy Modeler (RaPM), is now fully incorporated as a module with ISIM as of the most recent version — 6.0.

ISIM is developed on a Java EE platform using WebSphere Application Server, and supports IBM DB2, Oracle Database and Microsoft SQL Server databases. ISIM provides many of the capabilities expected of an independent IGA product, including user request, access recertification, entitlement and role mining, role modeling, analytics, and compliance reporting. ISIM's connector architecture provides more than 50 out-of-the-box connectors and can be delivered agentless or agent-based. Entitlement and role mining, discovery and engineering are also supported. Analytics are enhanced by IBM's Cognos technology, and include common reporting modules.

### Strengths

- IBM's global reach and cross-industry customer base provide extensive opportunities for developing IGA best practices and business scenarios.
- IBM's ISIM suite is relatively comprehensive and includes all connectors for a single price, along with governance modules (certification, access requests and separation of duties).
- IBM has a long-standing presence in IGA, is found in many IGA product evaluations, and is still recognized as a major solution despite the rebranding that removed "Tivoli" from the name.

### Cautions

- ISIM's license is competitively priced; however, it is known to have a deployment to license cost ratio of 2.5:1 or higher, which needs to be considered when calculating TCO.
- Gartner continues to hear complaints from IBM customers related to ISIM about product complexity and technical support.
- Although IBM has provided updates to the ISIM user interface through its service center UI, as well as enhancements to improve identity administration, the product still presents an IT-oriented user experience and trails the leaders in access certification features.

## iSM Secu-Sys

iSM Secu-Sys, based in Rostock, Germany, offers IGA functionality through its bi-Cube IAM suite. The product was first released in 2000 and builds on more than a decade of experience and close customer contact. The bi-Cube suite is built according to a modular architecture that consists of an

intelligent middleware, which links administration tools with interfaces to different systems and platforms. In addition to providing IGA features, iSM Secu-Sys offers other modules for SSO, secure authentication, password management, public-key infrastructure (PKI), license management, IT asset management and physical access control.

All of iSM Secu-Sys customers are based in Europe, mostly in Austria, Germany and Switzerland. The software runs on Windows Server 2003 and above, and is written in C# and Delphi. The platform has been consistently structured using a service-oriented architecture (SOA).

### Strengths

- Most bi-Cube deals are priced as a package deal, and come out at a lower cost when compared with competitors.
- bi-Cube has a well-designed modular architecture and a flexible, process-driven, business-centric data model that allows a good fit into existing business processes.
- iSM Secu-Sys offers fixed-price rapid implementation projects with a clearly specified scope, such as "IAM in 30 days" in some situations.

### Cautions

- iSM Secu-Sys is a relatively small player with a focus on the German-speaking markets. Thus, it is not well known elsewhere and easily overlooked.
- iSM Secu-Sys has a price list composed of an unusually high number of line items. Even though the intention is to allow for a custom-made composition of the solution, in practice it is virtually impossible to navigate the price list without the help and guidance of a product specialist.
- The company's relatively small presence can cause technical resources to become stretched during periods of high activity, such as before new product releases, and customers have indicated longer response times for support during those situations.

## NetIQ

NetIQ, with headquarters in Houston, Texas, entered the IAM market with The Attachmate Group's acquisition of Novell in 2011. NetIQ addresses IGA via a combination of NetIQ Identity Manager (available in Standard and Advanced editions) integrated with the NetIQ Access Governance Suite, which is a white-labeled version of SailPoint's products that is sold and supported by NetIQ under an OEM agreement. NetIQ also sells an additional component, NetIQ Identity Tracking, which enables identity intelligence for user activity monitoring. IAM is a central element of NetIQ's security-centric operations business strategy, which offers a vision of identity-enabled security innovation in the form of tight integration with SIEM, as well as solutions for cloud, mobility, "bring your own device" (BYOD) and social identity.

NetIQ Identity Manager is a Java Web application that runs with JBoss, WebSphere or WebLogic application servers on Windows, Linux, AIX and Solaris servers. Many connectors (called drivers) are developed in C and .NET, depending on interfaces exposed by targets for integration. Identity information is stored in an integrated eDirectory repository, while Oracle, Microsoft SQL Server or PostgreSQL databases can be used for the storage of other objects. The Access Governance Suite, based on OEM technology from SailPoint, shares some similar technical architecture in terms of platform support.

### Strengths

- NetIQ continues to benefit from the IAM assets it acquired from Novell. The company has continued to evolve its solutions and is benefiting from the fact that many prospects have shown renewed interest in doing business with NetIQ.
- NetIQ Identity Manager remains popular, and the company is enjoying good brand recognition, as illustrated by the number of times that NetIQ is asked to participate in enterprises' RFI/RFP processes.
- NetIQ continues to foster a strong partner ecosystem of resellers, VARs and system integrators that address a diverse customer base, from sales through deployment.

### Cautions

- Any major acquisition and alliance moves by SailPoint could adversely affect NetIQ.
- There is some overlap between features in NetIQ Identity Manager and Access Governance Suite, especially in the area of access requests and workflow, which can cause confusion for customers.
- NetIQ's Identity Manager core is based on a fairly old metadirectory approach coupled with forms and workflow, and will eventually need a refresh to keep up with competitive products.

## Omada

Omada, with headquarters in Copenhagen, Denmark, offers IGA via its Omada Identity Suite (OIS).

OIS builds on a foundational Omada Base Server with additional modules: Omada Password Manager, Omada Business Process Engine, Omada Role & Policy Engine, Omada Attestation Engine, Omada IAG Data Warehouse (with compliance reporting and analytics) and the Omada Connectivity Framework.

Omada has a strategic partnership with Microsoft, and OIS uses Microsoft's Forefront Identity Manager (FIM) 2010 Sync engine for fulfillment and ILM 2007 Sync as middleware for provisioning users to target applications. Alternatively, for fulfillment, OIS can integrate with any other UAP product that supports message bus architecture. OIS has also had significant integration with several SAP products for several years, including SAP BusinessObjects Governance, Risk and Compliance (GRC).

OIS is written in Microsoft .NET C# and uses Microsoft SQL Server. The OIS identity data and log model is extensible and incorporates identities, resources, access, user behavior and other data elements. Role and entitlement discovery, mining, and engineering are supported, as well as controls modeling and risk scoring. An Omada Compliance Reporting Center supports user-driven dashboards, SOD compliance and other reports. The Omada Attestation survey engine supports various types of data governance and recertifications — enabling continuous compliance and high-data quality. The Omada product supports various collaborative processes/workflows out of the box, such as a process for onboarding of applications into a governance model.

### Strengths

- Omada has a flexible and adaptable data model compared to other competitors. This gives Omada a unique advantage in modeling complex organizational structures and relationships in a natural way that fits like a glove.
- Omada provides significant integration and support for IGA with SAP applications.
- Omada has introduced rapid data enhancement to accelerate deployments in which organizational data of less-than-perfect quality can be enhanced quickly through well-defined collaborative processes that use streamlined organizational involvement.

### Cautions

- Omada could use more diversity than using Microsoft Forefront Identity Manager (FIM) Sync for fulfillment, as Microsoft is shifting its focus from the on-premises FIM product line toward cloud-based alternatives in Azure over the long term.
- While Omada is selling new licenses, the company's revenue derived from professional services is as high as the license revenue. Omada is profitable, but growth in license sales has been slow.
- While functional and business-focused, Omada's user interface would benefit from receiving enhancements.

## Oracle

Oracle Identity Governance (OIG) Suite consists of the following modules: Oracle Identity Manager (OIM), Oracle Identity Analytics (OIA) and Oracle Privileged Account Manager (OPAM). The first two, OIM and OIA, work together to deliver comprehensive IGA capabilities.

OIM and OIA are Java enterprise applications capable of running on any compatible application server. They use an Oracle SQL database as an identity warehouse. The business client interface is a Web browser. Workflow is based on Oracle's Business Process Execution Language (BPEL) engine, while the reporting and analytics make use of Oracle's BI architecture. The product supports the breadth of features and technical standards for IGA, and is part of Oracle's extensive IAM product portfolio.

OIM came to Oracle through its acquisitions of Thor Technologies in 2005. OIA was initially a product called RBACx from the company Vaau that was acquired by Sun Microsystems in 2007, and came into Oracle's IAM stack through Oracle's acquisition of Sun in 2010. Both products originally were loosely coupled with different user interfaces and some duplicated functionality. Oracle has spent considerable effort bringing both products together in an integrated manner.

Version 11g R2 represents an inflection point that provides a unified business user interface and tears down the traditional borders between both products. As part of Oracle's Fusion Applications architecture road map, it is part of the broader Oracle IAM suite, which includes IGA, Web access management, ESSO, privileged account activity management, federation, directory and virtual directory, fraud prevention, authentication, and externalized authorization management.

### Strengths

- The release of Oracle Identity Management 11g R2 is a competitive differentiator for Oracle, because it offers a truly integrated IAM platform that is based on internally developed and externally acquired software.
- OIG is a cornerstone of Oracle's Fusion Middleware and one of the most popular IAM products in the world.

- Oracle's pricing structure has been changed to include fixed processor-based pricing for some scenarios, addressing previous concerns from large customers regarding the pricing of those scenarios. On the other end of the spectrum, Oracle is working with hosted service providers to offer entry-level solutions based on Oracle Identity Management to smaller enterprises.

#### Cautions

- On average, Oracle's OIG deployment and customization costs can be higher than many Oracle competitors.
- Oracle has dedicated significant time and effort into the integration of its suite into release 11g R2. While some of Oracle's competitors have used the past few years to continuously drive innovation, this "inner focus" by Oracle has caused OIG to lag behind in functionality and flexibility.
- OIG has a large footprint and requires significant resources compared with some competitors, which partially neutralizes the benefits of the fixed CPU pricing model.

### SailPoint

Austin, Texas-based SailPoint's IdentityIQ is Java software that can run on Windows, Unix and Linux platforms. Its identity warehouse has flexible database deployment options, with support for Oracle, IBM DB2, Microsoft and MySQL. The business client interface is a Web browser. The product supports the breadth of features and technical standards normally required with IGA.

IdentityIQ's data and log model (known as Identity Cube) combines identity information and log data in the same repository for report intelligence. The adapter architecture aggregates required data, and can be expanded at no additional charge to provide fulfillment capabilities for enterprise and cloud applications. SailPoint offers IdentityIQ Compliance Manager to access certifications and policy management, and IdentityIQ Lifecycle Manager for self-service access requests, password management and automated life cycle events. IdentityIQ's Governance Platform delivers workflow functionality, policy and role modeling, and risk scoring where applicable.

Workflow, analytics, administration and reporting are available. Mining and discovery tools build detailed application as well as entitlement catalogs, and provide intelligence regarding patterns of behavior to inform policy, rule and role development.

#### Strengths

- Consistent marketing, an expanding partner network and rapid innovation lead to SailPoint's evaluation in many competitive bids, and has validated its perception as a market leader in IGA.
- Recent expansion and technology acquisition have positioned SailPoint well for supporting SaaS applications through its newly released IdentityNow service.
- In 2012, SailPoint grew its sales team by more than 50% across the U.S. and Europe, including specialists with experience in the healthcare and government verticals, and it is partnering with other verticals.

#### Cautions

- Customers have reported that SailPoint's IGA solution can be complex to deploy when used beyond identity and access governance — often requiring significant customization for scenarios involving access request and management of identities.
- The skill sets of SailPoint's partners beyond typical configuration and deployment are limited. This puts a strain on SailPoint's own resources, which are in short supply due to high demand.
- Although SailPoint has made some improvements in version 6.1, its capabilities in provisioning have not reached parity with the maturity and depth of features available with other, longer-established UAP products.
- The acquisition of BMC's Control-SA assets was driven more by new customer opportunities, rather than by the use of the Control-SA technology, which has created some unease with some Control-SA customers who have concerns regarding migration to SailPoint.

### SAP

SAP's IGA offering consists of three products that work together: SAP NetWeaver Identity Management, SAP Access Control and SAP Identity Analytics. As a global leader in business management software, SAP enjoys strong name recognition, and its technology offering is deployed widely in many of the world's largest organizations. SAP NetWeaver Identity Management is its current UAP offering for managing identities. SAP Access Control can run together with NetWeaver or on its own, and consists of four modules for supporting access governance scenarios: Access Risk Analysis, Business Role Management, Emergency Access Management and User Provisioning. SAP Identity Analytics is a native SAP Hana cloud application that can extend SAP's IGA solution beyond on-premises applications using in-memory technology to process high volumes of data.

SAP, which is based in Walldorf, Germany, does not charge customers for NetWeaver Identity Management as long as this module is used only within the SAP environment or if read-only connectors are used elsewhere. NetWeaver Identity Management is optimally designed for providing IGA services to SAP-centric enterprises, but also supports non-SAP application and infrastructure environments. For connecting other target systems, additional license costs apply. NetWeaver Identity Management and Access Control provide significant IGA features for role-based administration and auditing for SAP applications incorporated into UAP.

Improvements were made in the UI environment and integration with various SAP applications, such as Access Control and Business Warehouse for analytics improvements. SAP also has an SSO product that has been updated to support federation. In August 2012, SAP released a "rapid deployment solution" of preconfigured product templates and professional services packaged into the license cost to improve implementation time, leveraging IGA features to speed deployment of the product. Implementation projects at customer premises can be led by SAP consultants or a selection of solution integrators.

### Strengths

- SAP can leverage its footprint and experience within its large customer base to sell its IGA technology.
- SAP's Hana in-memory database technology provides a solid technology for analysis of user, role, organization and activity data.
- Gartner expects SAP to be able to leverage its ecosystem for a business-process-centric identity workflow and life cycle to unify data managed within the SAP environment.

### Cautions

- Clients have expressed concern about a perceived limited bandwidth of the SAP NetWeaver development team in developing new features and delivering timely updates.
- Customer feedback indicates that SAP has lost several deals because of perceived high pricing.
- SAP's role mining functionalities are basic at best.
- The fact that SAP's NetWeaver and Access Control have overlapping features, with both running stand-alone to deliver basic IGA functionality or together to deliver a wider set of IGA features, can be confusing to potential customers.

## Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

### Added

Because this is the inaugural Magic Quadrant for Identity Governance and Administration, technically all vendors are additions. However, vendors included here that were not rated in the predecessors to this Magic Quadrant (the "Magic Quadrant for User Administration and Provisioning" and the "Magic Quadrant for Identity and Access Governance") are:

- Caradigm
- e-trust
- iSM Secu-Sys

### Dropped

Vendors dropped from this Magic Quadrant that had been rated in the "Magic Quadrant for User Administration and Provisioning" and the "Magic Quadrant for Identity and Access Governance" are:

- Brainwave
- Efecte (formerly RM5 Software)
- Ilex
- Microsoft

## Other Changes

One vendor that was included in the "Magic Quadrant for Identity and Access Governance" has had a change of ownership:

- Aveksa, which was acquired by EMC, is now a division of RSA, The Security Division of EMC, and is known as RSA Aveksa.

## Vendors to Watch

Gartner reviewed many vendors that had significant IGA functionality, but did not meet the criteria for inclusion. Gartner clients should closely read the Inclusion and Exclusion Criteria as a key point of reference for this research.

### Bay31

Zug, Switzerland-based Bay31 (with software development in Italy) remains a vendor to watch in the IGA market. It offers a set of analytics and design tools for role mining and engineering, as well as reporting for audit and remediation in IGA. Bay31 continues to expand its support of SAP, primarily through its Role Designer for SAP tool, particularly in projects involving SAP GRC Access Control, where Role Designer can supplement (and, in some simpler cases, replace) SAP's solution. The Bay31 Analytics tool allows for analysis and visualization of entitlement assignment activity, and has a configurable reporting capability. The products are offered in different editions, and can be delivered in both on-premises and cloud-based configurations. The products are Java-based with Web-based user interfaces, and are compatible with standard SQL databases from Oracle, SQL Server and others. The adapter architecture is relatively simple, as is role data import and export.

For enterprises that seek to expand their design, analytics and intelligence functionality, Bay31's solutions are a possibility.

### Brainwave

Asniers-sur-Seine, France-based Brainwave was included in the "Magic Quadrant for Identity and Access Governance" in 2012 due to its capabilities in identity analytics, reporting and intelligence. Its Identity GRC solution is written in Java and SQL and uses a standard SQL database server (such as Oracle, Microsoft or PostgreSQL) for identity repository information (known as the Identity Entitlements Ledger). Identity GRC provides entitlement ledger, data feed and reconciliation, data analysis, reporting, and Web portal functionality. Brainwave introduced a workflow engine and preconfigured agentless connectors in 2012. The Web portal module is used as the UI for search, browsing and reporting. The product also supports discovery, mining, and engineering of roles and entitlements.

Brainwave is suitable for delivery as identity and access intelligence (IAI) as a service or as an enterprise product. The convergence of identity administration and governance capabilities highlights the fact that Brainwave's functions are more effective as a supplement to IGA solutions to enable more effective identity analytics and intelligence from those solutions.

### Efecte

Espoo, Finland-based Efecte, a Nordic service and contract management solution provider, acquired RM5 Software in early 2013. RM5 Software was included in the "Magic Quadrant for Identity and Access Governance" in 2012 with its RM5 IdM. The product is a series of Java-based modules to address repository, access, programming, audit, synchronization and other capabilities. A central data repository uses SQL (supports Oracle, DB2 SQL and MySQL), not only for database, but also for synchronization, logging and some reporting. Agentless connector architecture is read/write, and import/export supports many formats. The Web-based UI is used by business users and administrators, and is dynamically customizable. A wizard framework provides additional customization capability for self-service and delegated administration. Policy management is particularly robust and provides extensive definition ability. Efecte's IdM has a minimal discovery and mining capability. It does not have the user administration found in most UAP tools, though some workflow and user interface modules can be configured to perform certain administrative functions. Proprietary workflow is provided for IAG process automation. A simple analytics tool provides for basic permissions and role reporting. Detection and enforcement of SOD are also supported. While Efecte provides some of the features and supports the technical standards expected of an IAG solution, it works best when combined with an established UAP solution.

### ForgeRock

San Francisco-based ForgeRock was founded by former Sun Microsystem engineers that left the company after it had been acquired by Oracle. Sun had at that time offered the OpenSSO access manager and the OpenDS directory server as open source with a CDDL license: a community version that was unsupported and free to use, and an enterprise version that was officially supported with SLA-based support agreements and a rigid release plan. In 2010, ForgeRock created the latest branch of the community versions of OpenSSO and OpenDS, naming them OpenAM and OpenDJ. ForgeRock was boosted by acquiring many ex-Sun Microsystems customers who were using the

original products and switched over to the ForgeRock brand for a continuation of the product line. The company also began a project to build its own identity management and provisioning system, called OpenIDM. Salesforce.com announced Identity Connect in 2013, which is built on ForgeRock's identity stack components OpenIDM and OpenAM.

The product is still at an early maturity level, although ForgeRock has several midsize customers that are running the product. OpenIDM is part of ForgeRock's Open Identity Stack, is written in Java, and runs on the included Apache Felix OSGi service and Jetty container. For the identity warehouse, OrientDB is included for development; production repositories supported are MySQL and Microsoft SQL Server. The ForgeRock identity stack has a common REST API across all products. OpenIDM supports REST for all CRUD (create, read, update, delete), provisioning, UI and user administration functions. As of late 2013, ForgeRock has increased its number of employees to more than 100, including several previous key executives from Sun Microsystems who recently joined the company.

## **FSP**

FSP was founded 2002 in Cologne, Germany. The company offers its product Organization and Resource Guards (ORG) to provide some IGA functionality and externalized authorization management. The ORG server runs on z/OS, Unix and Windows. It is able to centrally manage complex rule sets, allow modeling of corporate structure, and add extensions called "competencies" to the traditional data model of roles and users in order to render fine-grained attribute-based access control (ABAC), as well as RBAC.

Apart from provisioning, ORG has authorization capabilities using an XACML-based policy decision point (PDP). The provisioning engine has connectors to several target systems, including SAP R/3, RACF, Interflex, LDAP Directory servers including Active Directory, and systems supporting SPML. Authorization APIs are available for Java, Windows in C, as well as z/OS (COBOL, PL/1 and C).

## **Microsoft**

Microsoft, based in Redmond, Washington, made its entry into the IGA market by folding certain assets of Bhold, a Dutch-based solution it acquired in 2011, into its Forefront Identity Manager (FIM) product. With Bhold, FIM is capable of offering some basic access governance features, and uses FIM connectors for synchronization. The solution provides mining and discovery tools to scan for key identity data in applications and systems to help populate the identity database, which combines static and historical log data about identities for identity and access intelligence reporting. With the help of skilled integrators, customers can use Microsoft FIM to deliver many aspects of an IGA product.

As of late 2013, Microsoft is in the process of restructuring its identity and access management portfolio to reflect the importance of hybrid (that is, on-premises and cloud) identity scenarios, especially with respect to Windows Azure Active Directory. Microsoft's work with Azure Active Directory and related systems, combined with continued investments in on-premises assets, represents a significant shift in its approach to a number of IAM services, managing identity across systems to provide SSO and federation to cloud services and for B2B. It is due to these evolving changes that Microsoft is not included in the 2013 Magic Quadrant for Identity Governance and Administration.

## **OpenIAM**

OpenIAM is a small Cortlandt Manor, New York-based firm that provides an open-source based framework for some IGA functions, including user provisioning, password management, auditing and delegated administration. Its IGA product, Identity Manager, has undergone a major transition in version 3 with a new business user and administrator UI. Open-source JBoss and Tomcat are part of the delivery, which also includes the Activiti workflow engine, and BIRT Report designer and scripting language. Policy management provides for the creation of rules based on attributes, or written in the Groovy scripting language. Reconciliation event configuration and mapping are available, and there is some role management functionality based on resource, policy or group mapping. The product supports SOAP and RESTful services, as well as some analytics functionality and event correlation.

OpenIAM has a following that includes some notable clients. While Identity Manager v2.3 was more suited as a developer's kit, it has evolved significantly with v3.0. In the hands of the right integrator or skilled internal staff, OpenIAM can provide a starting point for effective IGA.

## **Security Compliance Corp. (SCC)**

Orinda, California-based SCC provides access review, certification, reporting, alerting and SOD capabilities with its Access Auditor product. It also delivers a workflow tool and its Identity Mapper to link people with appropriate accounts and role modeling functionality to help define enterprise roles. Automation for entitlement review and remediation is available, as are automatic alerts to changes and real-time views of who has access to which application. Basic analytics functionality is also available, and an access request module serves as an IAG foundation. The most recent release includes support to combine Splunk log/event data with its own identity stores, providing context-based alerting where needed.

SCC has enjoyed increased sales — driven by federal regulations — and has had success in several industries, including healthcare. Access Auditor is particularly appealing to smaller enterprises (5,000

to 25,000 users) that do not seek comprehensive IGA, but prefer something simple to use and deploy. Pricing for the product is also a differentiator for SCC, particularly in the small and midsize business (SMB) space with IGA needs.

## Securonix

Before starting Los Angeles based-Securonix in 2009, CEO Sachin Nayyar already had a background in the IGA market as founder and CEO of Vaau. Securonix Identity and Access Intelligence builds on this experience by combining advanced governance capabilities with identity-aware security monitoring to provide customers with greater insight into threats within their environments. The goal of Securonix is to bridge the gap between identity management and security monitoring by applying behavior risk analysis, identity correlation and access risk context to the dominant security monitoring approaches. As an access intelligence and analytics tool, the product lacks provisioning and access management capabilities that are considered parts of complete IGA solutions. As such, Securonix Identity Intelligence usually is considered complementary to IGA platforms.

## Tuebora

Tuebora, which is based in Santa Clara, California, was founded in 2011 with the goal of applying continuous compliance principles to IGA in a scalable yet lightweight and easy-to-deploy package. Its iGovernance 360 product was designed with a multitenancy architecture so it could be offered as a governance-as-a-service solution with deployment and pricing models that customers expect of cloud-based offerings. Beyond the standard features typically provided by IGA solutions, iGovernance 360 provides advanced analytics that can be used independently or to provide better contextual information during access certifications. Tuebora has also launched a white-label program where managed service providers can offer iGovernance 360 as their own cloud service.

## Whitebox Security

Tel Aviv, Israel-based Whitebox Security, which offers its WhiteOPS intelligent access governance solution, has shown considerable growth in the past year, both in its feature offerings and customer base. While primarily characterized as an IAI solution, Whitebox has expanded its capabilities to include access certification and request automation, as well as enhancing its access policy engine. WhiteOPS is one of the few products in this area that also has a distinct data access governance capability, with data classification and usage profiling among some of its features. The monitoring and analytics functions collect activity and event information about application and data access, and allow that collected information to be used in real time to report on the identity and access policy violations defined in the solution.

Although designed more for an analytics team, WhiteOPS does provide an effective UI for reporting and good input into role engineering and forensic activities. It is one of the more complete products Gartner has seen in this area, and, with its road map for feature expansion, Whitebox Security will likely be in the 2014 edition of this Magic Quadrant.

# Inclusion and Exclusion Criteria

## Inclusion Criteria

While there are IAM products that deliver some of the functionality listed below, the IGA study covers vendors that contain all of these features in a product specifically tailored and sold to manage access request life cycles. These core features consist of:

- User interface configuration for multiple user profiles
- Comprehensive workflow for the identity and access request administration life cycle
- Tools for application entitlement discovery, mining and management
- Tools for role discovery and engineering (that is, the identity data model)
- Tools for user or application role and entitlement administration, and management
- Tools for defining and enforcing identity and access policies, as well as remediation of violations
- Configurable logging for identity and access activities and actions
- Analytics and reporting of identity and access activities and actions
- The underlying architecture for the all of the abovementioned features, including connector architecture for data collection and fulfillment actions

Products must be deployed in customer production environments, and customer references must be available.

IGA vendors included in this Magic Quadrant meet one or more of the following conditions:

- The IGA solution combines identity and access governance functionality and user administration and provisioning functionality into a single offering, effectively charging one time for functionality found in both (such as user interface, workflow, reporting and connectors).
-

The IGA solution must be able to provide the ability to create and use an entitlement catalog for granular access assignments within the governance process.

- The IGA solution provides enough provisioning and deprovisioning functionality to compete effectively with stand-alone UAP competitors, or has an integrated OEM relationship packaged with its governance solution and offered as *one* solution.
- The vendor must be able to demonstrate that at least five verifiable clients within the past six months are using the product for IGA purposes.

## Exclusion Criteria

IGA vendors that are not included in this Magic Quadrant have been excluded for one or more of these reasons:

- They do not meet at least half of the inclusion criteria.
- They supply IGA capabilities for only one specific/targeted technical environment, such as Windows, iSeries or Unix/Linux.
- Vendors have minimal or negligible market share, or have no shipping products.
- They sell only UAP-related or IAG-related products, but don't have an IGA product of their own.
- They are external service providers (ESPs) that provide managed services, such as data center operations outsourcing.
- They offer a distinctive IGA product, IGA feature set or IGA solution offering that has not been available on the market for at least six months (measured from January 2013).
- There is insufficient market penetration as measured by the number of clients, scale of deployment, revenue generated from a specific IGA product, or revenue generated from a UAP deployment, as used by the client.
- Product packaging, use practices, marketing and sales approaches are not IGA-specific and, instead, focus on identity administration for IT administrators or access governance only.

## Evaluation Criteria

Gartner analysts evaluate technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation. Ultimately, technology providers are judged on their ability and success in capitalizing on their vision.

Each Magic Quadrant has two evaluation categories: Ability to Execute and Completeness of Vision. Each is described below, with subcriteria and weightings provided.

## Ability to Execute

### Product or Service

Core goods and services offered by the IGA provider that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria. Specific subcriteria are:

- User interface configuration for multiple user profiles
- Password management
- User account management
- Comprehensive workflow for the access request administration life cycle
- Application entitlement discovery, and mining
- Application entitlement administration and management
- Role discovery and engineering (that is, the identity data model)
- Role life cycle management
- Configurable logging for identity and access activities and actions
- Analytics and reporting of identity and access activities and actions
- Identity and access policy administration, enforcement and remediation of violations
- Role modeling and simulation
- Resource access administration
- Underlying architecture to support all the subcriteria listed above, including connector architecture for data collection and fulfillment actions

## Overall Viability

Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue to invest in its IGA product, continue offering the product and continue advancing the state of the art within the organization's portfolio of IGA products. Specific subcriteria are:

- History of investment in identity and access management product development and management
- Contribution of IGA to revenue growth

### Sales Execution/Pricing

The IGA providers' capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. Specific subcriteria are:

- Pricing
- Market share
- Additional purchases (for example, relational database management system [RDBMS], application server, Web server, and so on)

### Market Responsiveness/Record

Ability to respond, change direction, be flexible and achieve competitive success in the IGA market as opportunities develop, competitors act, customer needs evolve, and market dynamics change. This criterion also considers the IGA provider's history of responsiveness. Specific subcriteria are:

- Product release cycle
- Timing
- Take-aways

### Marketing Execution

The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the IGA market, promote the brand and business, increase awareness of its IGA products and establish a positive identification with the product/brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities. Specific subcriteria are:

- Integrated communications execution
- Customer perception measurement

### Customer Experience

Relationships, products and services/programs that enable clients to be successful with the IGA products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, and so on. Specific subcriteria are:

- Customer support programs
- Service-level agreements

### Operations

The ability of the organization to meet its goals and commitments regarding its IGA product. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis. Specific subcriteria are:

- Training and recruitment
- Number of major reorganizations in past 12 months

**Table 1. Ability to Execute Evaluation Criteria**

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High

Market Responsiveness/Record	High
Marketing Execution	High
Customer Experience	High
Operations	Medium

Source: Gartner (December 2013)

## Completeness of Vision

### Market Understanding

Ability of the IGA provider to understand buyers' needs and translate these needs into products and services. IGA vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those wants with their added vision. Specific subcriteria are:

- Market research delivery
- Product development
- Agility to market change

### Marketing Strategy

A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements regarding the IGA products. Specific subcriteria are:

- Integrated communications planning
- Advertising planning

### Sales Strategy

The strategy for selling IGA products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base. Specific subcriteria are:

- Business development
- Partnerships with system integrators
- Channel execution

### Offering (Product) Strategy

An IGA provider's approach to product development and delivery that emphasizes differentiation, functionality, methodology, and feature set as they map to current and future requirements. Specific subcriteria are:

- Product themes
- Foundational or platform differentiation

### Business Model

The soundness and logic of the IGA provider's underlying business proposition. Specific subcriteria are:

- Track record of growth
- Consistency with other product lines

### Vertical/Industry Strategy

The IGA provider's strategy to direct resources, skills, and offerings to meet the specific needs of individual market segments, including verticals. Subcriteria are:

- SMB support
- Industry-specific support

### Innovation

The IGA vendor's direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes. Specific subcriteria are:

- Distinctive differentiation in feature or service (such as IT service management [ITSM], FIM and

facilities)

- Synergy from multiple acquisitions or focused investment
- Attribute-based access support
- BI support
- Business process management (BPM) support
- Effective role and attribute-based access capability and support
- Support for identity and access management as a service (IDaaS)
- Support for mobile identities
- Support for data access governance, particularly for unstructured and semi-structured data access
- Support for consumer-oriented identity architectures

### Geographic Strategy

The IGA provider's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market. Specific subcriteria are:

- Home market
- International distribution

**Table 2. Completeness of Vision Evaluation Criteria**

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	High
Sales Strategy	High
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (December 2013)

## Quadrant Descriptions

### Leaders

IGA Leaders deliver a comprehensive toolset for governance and administration of identity and access. These vendors have successfully built a significant installed customer base and revenue stream, and have high viability ratings and robust revenue growth. Leaders also show evidence of superior vision and execution for anticipated requirements related to technology, methodology or means of delivery. Leaders typically demonstrate customer satisfaction with IGA capabilities and/or related service and support.

### Challengers

IGA Challengers deliver a relatively strong set of governance and administration features for identity and access. Some have major clients using their IGA solution. Challengers also show strong execution, and most have significant sales and brand presence. However, Challengers have not yet demonstrated the feature completeness, scale of deployment or vision for IGA that Leaders have. Rather, their vision and execution for technology, methodology and/or means of delivery tend to be more focused or restricted to specific platforms, geographies or service. Clients of Challengers are relatively satisfied but ask for additional IGA features as they mature.

### Visionaries

Vendors in the Visionaries quadrant provide products that meet many IGA client requirements, but may not have the means (such as budget, personnel, geographic presence, visibility and so on) to

execute as Leaders do. Due to smaller size, there may be initial concerns among some potential buyers of long-term viability. Visionaries are noted for their innovative approach to IGA technology, methodology and/or means of delivery. They often may have unique features, and may be focused on a specific industry or specific set of use cases, more so than others. Visionaries are often the technology leaders in evolving markets such as IGA, and enterprises that seek the latest solutions often look to Visionaries.

## Niche Players

Niche Players provide IGA technology that is a good match for specific IGA uses, cases or methodology. They may focus on specific industries and can actually outperform many competitors. They may focus their IGA features primarily on a specific vendor's applications, data and/or infrastructure. Vendors in this quadrant often have a small installed base, a limited investment in IGA, a geographically limited footprint, or other factors that inhibit providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant, however, does not reflect negatively on the vendor's value in the more narrowly focused service spectrum. Niche solutions can be very effective in their area of focus.

## Context

All vendors included in the 2013 Magic Quadrant for Identity Governance and Administration have customers that are successfully using their products and services; however, this is not an exhaustive list. Some IGA vendors did not meet our inclusion criteria, chose not to participate in the study, or chose not to present products for evaluation. This Magic Quadrant encompasses a wide cross-section of vendors, including those that offer different delivery models (such as on-premises, hosted and SaaS), differing levels of functional breadth and sophistication, and different regional and/or vertical industry specializations. Regardless of the provider under consideration, we suggest clients ask the following questions:

- Will this vendor help my organization satisfy our business requirements for simplifying and automating processes for managing users' access?
- Does this vendor help my organization deliver compliance with security policies and regulations more effectively?

Your organization should look beyond a vendor's suite of product offerings and evaluate the ecosystem of providers that provide important functions and capabilities the considered vendor on the Magic Quadrant may not offer.

Gartner clients should consider:

- The variance in professional services' effort required to integrate IGA products in technology environments
- The degree to which some vendors are more process-centric and business-focused than other vendors that focus more on IT-specific concepts and the RBAC model
- The extent to which IGA vendors view IGA as a strategic initiative requiring major changes in IT infrastructure versus which view IGA as a series of targeted, short-term improvements — or both
- The role that clients believe IGA should play in their broader security and risk strategy, particularly with GRC and intelligence initiatives, and how well IGA vendors fare in doing so
- The accelerating changes that are in occurring in the IGA market that can affect decisions related to methods of delivery and cost, such as cloud-based options and changing price models

Use this Magic Quadrant as a reference for evaluations, but explore the market further to qualify the capacity of each vendor to address your unique business problems and technical concerns. Depending on the complexity and scale of your requirements, your shortlist will be unique. The Magic Quadrant for IGA is not designed to be the sole tool for creating a vendor shortlist. Use it as part of your due diligence, and in conjunction with discussions with Gartner analysts.

Magic Quadrants are snapshots in time. To be fair and complete in the analysis, we cease data collection efforts at a consistent time.

## Market Overview

Gartner believes that the IGA market is in a volatile and rapid growth period that will last for the next five years with a stream of new entrants with innovative product features and delivery methods. For 15 years, the IGA market was dominated first by directory administration and then user provisioning products. In the past five years, identity and access governance solutions usurped the lead role. Going forward, a hybrid market will unify user provisioning and identity and access governance as

solutions converge toward a focus on the end-user experience, process automation and easier integration.

In 2013, IGA has been the fastest-growing sector of identity and access management (IAM). Gartner estimates combined 2012 UAP and IAG product sales at \$1.8 billion — with estimated sales in 2013 exceeding \$2.2 billion. Growth rates for IGA products and services are estimated to be more than 10% for the next five years. Sales for the consulting and system integration service for IGA in 2013 are believed to be between two to three times the estimated product sales for the year.

In 2013, UAP and IAG have merged in offerings from several IGA vendors. IGA features for have improved, particularly in data modeling, analytics, logging and reporting. Integration with security products such as SIEM and data loss prevention (DLP) has been bolstered by strong interest in security intelligence. Tighter integration with privileged account management (PAM) and PAM capabilities within some IGA products have occurred. New IGA delivery methods via SaaS have been introduced. Similarly, new access modes for IGA tools and services via mobile devices are being explored. In 2014 and 2015, data access governance will be a trend for IGA as new features begin to allow governance of access to unstructured and semistructured data. Gartner expects IGA market consolidation via acquisition during this five-year period of volatility.

---

---