G00235195

Magic Quadrant for Identity and Access Governance

Published: 17 December 2012

Analyst(s): Earl Perkins

Identity and access governance is replacing user administration and provisioning as the new center of gravity for identity and access management.

Strategic Planning Assumption

By 2016, identity and access governance will replace user administration and provisioning as the most frequently purchased solution for managing identities.

Market Definition/Description

Identity and access governance (IAG) is defined as (1) the process of requesting, approving, certifying and auditing access to applications, data and other IT services; and (2) the process of delivering security and business intelligence (BI) on how identities are created, managed and used for access. Software tools and services that provide support for most or all of this process are known as IAG products.

The IAG market (also referred to in vendor marketing as "identity governance," "access governance" and "role management") is not new. While first appearing as part of user administration and provisioning (UAP) in the late 1990s, distinctive IAG tools appeared between 2004 and 2006 as a response to concerns by clients about regulatory compliance involving access to critical IT resources. Concerns were also raised about the inability of UAP tools to be usable by the non-IT professional in addressing compliance requirements. Although UAP provided a user interface (UI) and reporting that could be leveraged by IT administrators, the ability to request, approve and certify specific access to applications, data and IT services — and then have that process audited — was not addressed adequately by UAP. A business-friendly UI and reporting capability that emphasized response to compliance needs and provided visibility into the identity change management process evolved first as a separate feature set, then later as a product.

Today, IAG is the fastest-growing sector of identity and access management (IAM). Gartner estimates that 2011 IAG product sales alone ranged from $200 million to $300 million, with estimated growth rates in 2012 continuing to exceed 35% to 40% for most IAG vendors. Consulting and system integration service sales for IAG are believed to be at least twice that. Gartner believes

that the demand for IAG is just beginning, with a peak period for this functionality still four to six years in the future. Thus, most IAG vendors (and vendors with products that have IAG features) are enjoying increased sales — some more than others. The market can best be characterized by the quote "a rising tide lifts all boats," meaning even vendors with mediocre IAG capability are having some success. Although some early indicators show that market consolidation via acquisition may begin in 2013, the numerous vendors in and entering the IAG market will ensure much choice for buyers over the next two years. The disaggregation of IAG functions may also bring vendors into the IAM market that were not previously seen or thought of as IAM vendors.

Features of IAG products are still evolving, as is the relationship of IAG to other IAM and security products. New methods of delivering IAG, including software as a service (SaaS), are being tested. New methods of accessing IAG tools and services via mobile devices are also being explored. Although IAG tools and services are starting to mature, an architectural trend within the industry is reshaping the feature set. The UAP vendors that first introduced IAG features are redesigning their solutions to deliver "super IAG" functionality — that is, IAG with UAP fulfillment and synchronization capabilities. This means that user provisioning interfaces are being redesigned for business use, and the provisioning workflow is expanding to include access requests, approval and certification functions, and other steps to update UAP with IAG functionality. IAG vendors are doing the opposite — incorporating UAP connector architecture and fulfillment functions to existing IAG features. This is essentially redefining the IAG market to include UAP.

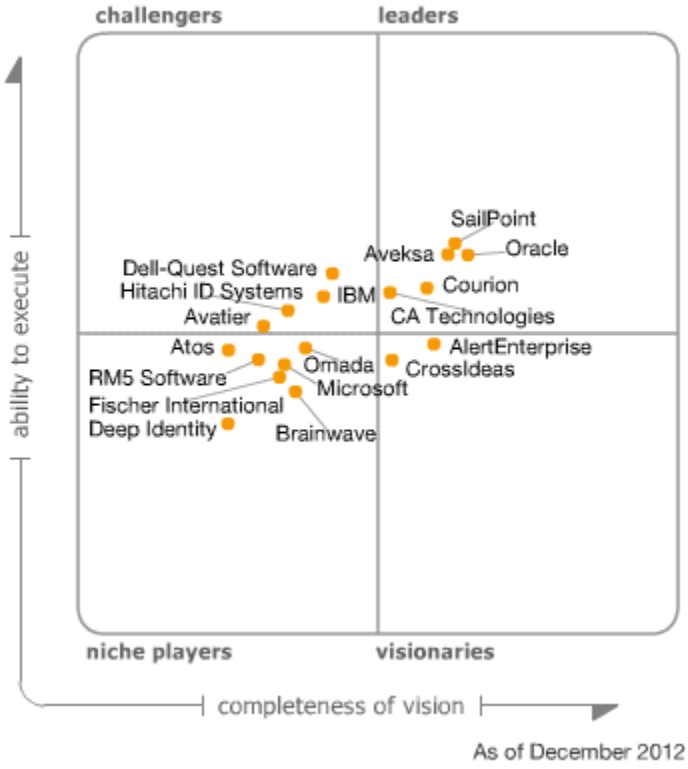
A market is also evolving for more advanced IAG tools that provide design, modeling, analytics and reporting functions for identity and access alone, without the approval, certification, and general administration and fulfillment components. These same tools initiate the creation of a formal identity data and log model for defining the data ecosystem to be most effective for all IAM tools, including IAG. Gartner believes this will give rise to a revised view of IAG to mean "identity governance and administration" of access. Products will divide between those focused on day-to-day administration activities for access request, approval and certification, and those devoted to mining, discovery, modeling, analytics and forensics capabilities — that is, identity and access intelligence (IAI). Advanced analytics is one of several criteria particularly important to a vendor's road map and vision.

IAI products deliver advanced data model design, pattern analysis, forensics, and other advanced analytics and reporting capabilities that are not generally found in today's products. The identity and access data collection, correlation and analysis have expanded to include input from security information and event management (SIEM), data loss prevention (DLP), and other IT security and system tools. For SIEM and DLP, it also means that IAG data can be used in its own collection, correlation and analysis. A renewed focus on access governance for data by incorporating new features (and acquiring other vendors) to govern access to unstructured and semistructured data will be a trend for 2013 and 2014. Improved integration with privileged-account activity management (PAAM) will also occur.

Because of the convergence of administration and governance products for IAM, the Gartner user administration and provisioning Magic Quadrant and the IAG Magic Quadrant will be combined into a single Magic Quadrant in 2013, tentatively labeled the identity governance and administration Magic Quadrant.

Magic Quadrant

Figure 1. Magic Quadrant for Identity and Access Governance



Source: Gartner (December 2012)

Vendor Strengths and Cautions

AlertEnterprise

AlertEnterprise's Identity and Access Governance (v.3.5, May 2012) is Java, HTML5 and Flex-based business logic running on a number of Linux and Unix enterprise server platforms and using a number of SQL-based databases for identity information and logging. The business client interface is a Web browser. The product supports many of the functions and technical standards normally required in an IAG system.

AlertEnterprise uses an "identity warehouse" concept for its identity data and log model, and emphasizes the inclusion of physical security and OT (that is, industrial control) security in its data collection. The workflow system (AlertCertify) automates the review and approval process for that expanded enterprise view. Although AlertEnterprise does have a baseline analytics tool, it leverages other analytics system output for intelligence reporting. The OEM software provided is used for reporting and report design. AlertEnterprise delivers Industry Content Packs with predefined rules,

regulatory content and workflow specific to various industries, such as utilities, oil and gas, and transportation.

Workflow, analytics, rule processing, administration and reporting are available. Mining and discovery tools scan for key identity data in applications and systems to build the identity warehouse.

Strengths

- AlertEnterprise targets a superset of IAG, covering physical security and operational technology (OT) security systems as well as traditional IT systems. This introduces a layer on the Security Convergence platform that includes compliance automation and incident management and response.
- The overlay-style architecture of AlertCertify and other IAG products from AlertEnterprise provide regulatory compliance capabilities, such as mitigating control management, policy enforcement and risk visualization.
- Specific industry focus in energy and utilities, transportation, and other industries with OT security requirements have provided AlertEnterprise with early momentum in the market.

Cautions

- A complex role architecture and a large number of different products in AlertEnterprise's portfolio can be confusing to the user for selection and development purposes.
- As a relatively recent entrant in the IAG market, traditional IAG adapters for data collection are not as comprehensive as competitive products; however, adapters for major physical access systems (such as cameras, sensors and industrial control) are available.
- Improvements in the product's advanced entitlements database and engine are still needed for scalability and performance, and pricing for some adapters is high.

Atos

France-based Atos delivers an IAM suite known as DirX. IAG functionality is offered as part of its UAP software known as DirX Identity (v.8.2B, November 2011). The software is written in Java, C++ and script languages (Tcl and JavaScript) and is supported on Microsoft Windows, SUSE and Red Hat Linux, and Solaris systems. DirX Identity IAG uses workflow, analytics and reporting functions that are already part of UAP features (for example, DirX Audit). The identity repository is primarily hierarchical (based on DirX Directory and LDAPv3). Two different Web UIs provide administrative and business user access. DirX Identity's connector architecture is primarily bidirectional and uses an Integration Framework for batch-oriented workflows.

DirX Identity's data and log model are distinct. The data model is based on LDAPv3, and the log model is based on XML formats. Basic discovery for roles and entitlements is supported, as is role engineering. The DirX Audit module provides key performance indicators, trend analysis, metrics and statistics based on online analytical processing (OLAP) methods. It can use dashboards for

delivery. Access certification campaigns are supported, and reports from it are accessed by managers via the Web Center module.

In July 2011, Atos acquired DirX as part of Siemens IT Solutions and Services. Although primarily focused on UAP, it provides several IAG features as part of that solution, such as role and entitlement administration, access review and certification, and role-based reporting.

Strengths

- As a large IT service provider, Atos provides broad European access for DirX Identity, and has established visibility and presence in the IAM market. Consulting and integration support are also available for DirX from Atos.
- IAG features are integrated into the UAP solution, have robust role-based access control (RBAC) support and come in a number of editions based on specific business scenarios.
- DirX Identity provides extensive SAP integration capability.

Cautions

- DirX Identity is a single package of UAP and IAG. It is not particularly suited for enterprises that already have UAP and want to add IAG.
- Although Atos has a strong presence in Europe, availability outside of that region is small.
- DirX Identity lacks some IAG features, such as mining roles and entitlements, risk scoring, and remediation of entitlements, roles and rules.

Avatier

Avatier has three software components as an IAG solution: Compliance Auditor, Group Enforcer and Identity Analyzer. These components are complementary to Avatier's UAP solution Identity Enforcer (v.9.x, June 2012). Avatier IAG components are written in C#, require Microsoft's Internet Information Services (IIS) for delivery and uses Microsoft SQL Server as the back-end repository. The connector architecture is leveraged across the entire Avatier suite, and uses standard APIs and Web services. The solution provides core analytics functions and a large set of prepackaged reports at installation. Patented (No. 7950049) workflow provides support for IAG automation.

Avatier uses a project model for access reviews. Projects are created through a simple wizard interface. In addition to basic project information (such as ownership, start/stop date and certification rules), Avatier exposes business attributes that allow fine-grained governance reviews. Avatier user provisioning customers benefit from integrated access removal, automatic workflow and inherited project/resource ownership. The unified HTML5 UI is designed for mobile and desktop browsers, and reflects a consumer-oriented and simpler approach.

Avatier's primary focus is UAP, but it is expanding its IAG features to be more competitive in the broader IAM market.

Strengths

- Avatier's access governance project-based approach enables business users to create or conduct audits with minimal training.
- Avatier's Group Enforcer provides a holistic approach to IAG by leveraging rules to enforce access, which results in access assurance and streamlined audits.
- Avatier's IAG solutions provide a quick time to value with high operational efficiency.

Cautions

- Avatier is not yet recognized in the IAG market as a significant player by potential buyers.
- It is dependent on Microsoft's IIS and Windows Server platforms for delivery, which may be limiting to some customers.
- Avatier's products can appear to be more expensive than those of other vendors; however, total cost of ownership amounts may be equivalent to competitors.

Aveksa

Aveksa's Access Governance Software Suite v.5.5 (v.6.0, September 2012) is Java-based business logic running on a number of Linux and Unix enterprise server platforms and using Oracle Database as its primary identity repository for identity information and logging. The business client interface is a Web browser. The product supports the breadth of functions and technical standards normally required in an IAG system.

Aveksa's identity data and log model use its Access Management Database (XMDB) to combine identity information and log data in the same repository for report intelligence. Adapter architecture (Access Fulfillment Express) aggregates the required data as part of a security integration fabric and is now extending to SaaS applications, such as salesforce.com and Google Apps.

Workflow, analytics, rules 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

- Aveksa's architectural changes in v.6 include broader support for adapters, improved integration with SIEM and DLP products, and rule process and workflow improvements.
- 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 IAG market.
- Integration with HP ArcSight SIEM allows expanded and richer intelligence for privileged accounts, remediation and insider threat tracking.

Cautions

- Increasingly aggressive large competitors, such as Oracle and CA Technologies, leverage their size and reach against Aveksa as competitors' technology improves to get to the client first.
- Aveksa's cloud and mobility strategy are still evolving and will face stiffening competition from new and existing cloud players in IAM as a service (such as identity as a service [IDaaS]).
- As a leader in IAG, inclusion and support of data from third-party security and identity sources (such as DLP and SIEM) could be expanded.

Brainwave

France-based Brainwave is a newcomer to the IAG market, with a solution known as Identity GRC (latest release in November 2011). The software is written in Java and SQL, and uses a standard SQL database server (such as Oracle, Microsoft or Postgres) for identity repository information (known as the Identity Ledger). Identity GRC uses a series of software modules to deliver functions, including entitlement ledger, data feed and reconciliation, data analysis, reporting, and Web portal. The product does not have a workflow module, focusing specifically on audit functions instead. It does not have connector architecture and relies on flat-file data extracts. The Web portal module is used as the UI for search, browsing and reporting.

Identity GRC's identity data and log model is multidimensional and supports repository and logging results in one store. The UI is composed of two components. Brainwave Portal is used by business users to access identity data through reports and analyses. Brainwave Analytics is used by security analysts for data collection and correlation, analyses and report configuration, and role and entitlement discovery. The product also supports discovery, mining, and engineering of roles and entitlements.

Brainwave is suitable for delivery as IAI as a service or as an enterprise product.

Strengths

- Brainwave offers a dual licensing model and offers Identity GRC with standard license pricing or as SaaS.
- Brainwave's approach to analytics and reporting leverages its approach to the data model that delivers rich identity intelligence for business users and IAM specialists.
- Focusing specifically on identity collection, correlation, visualization and analysis allows Identity GRC to be integrated into enterprises that already have core IAM systems.

Cautions

- Because of its small size, Brainwave is focused on the European market.
- Brainwave's philosophy of controls and audit is comparable more to SIEM products than IAG products.

- As an IAG solution, Identity GRC lacks more traditional features such as a workflow engine, connector architecture, and managing exceptions via role creation, to name a few.

CA Technologies

As of September 2012, CA GovernanceMinder v.12.6 became available. It replaced Role & Compliance Manager v.12.5 in July 2011. GovernanceMinder delivers a new and improved business-facing UI, customizable reporting, and integration with CA's privileged identity management offering, ControlMinder. An optional CA User Activity Reporting Module can be integrated with GovernanceMinder for reporting. The software is written in Java and Client Tools C++ and can run on a number of Microsoft Windows and Linux platforms. GovernanceMinder is part of an IAM product portfolio from CA Technologies, and supports technical standards and features expected of an IAG system.

The identity data model for GovernanceMinder delivers a namespace called "Universe," which is supported via Microsoft SQL or Oracle. GovernanceMinder uses the same workflow engine as CA IdentityMinder and has significant integration capabilities with other IAM portfolio products. A Web portal provides the business UI for IAG functions, and OEM workflow provides the required automation. GovernanceMinder shares the same connectors with IdentityMinder. It has a proprietary analytics engine, and has dashboard delivery functions that include compliance and risk, as well as role coverage. Support for risk scoring of access during policy checking, mining and discovery is included.

CA Technologies remains committed to an aggressive (and progressive) cloud computing strategy across most of its IAM solutions, including IAG.

Strengths

- CA Technologies is a longtime provider of IAM solutions in the market, has a significant international customer base, and has an extensive consulting and system integrator partner set.
- GovernanceMinder brings together functionality from several enterprise products to deliver a hybrid (cloud and enterprise) IAG offering.
- CA Technologies' deployment practices have shown improvement and are leveraging knowledge gained by integration partners and addressing different IAG business scenarios.

Cautions

- GovernanceMinder is essentially a rebranding of Role & Compliance Manager, except for UI and reporting changes.
- CA Technologies' aggressive strategy to support hybrid cloud and enterprise environments for IAG is a fundamental shift for most enterprises and will require time to be realized.
- GovernanceMinder's connector architecture still needs additional integration with Microsoft SharePoint and CA products, such as CA Advanced Authentication (formerly Arcot).

Courion

Courion has two basic offerings in IAG: the Access Assurance Suite (AAS v.8.1, July 2012) and its SaaS-based Access Risk Management Suite (or CourionLive v.1.0, May 2012). AAS is written in C#, C++ and JavaScript, and is a Microsoft Windows-based offering. Support for any SQL or file data repository with account data is supported. Logging of activities and events is written to flat files and Windows event logs. Account data stays in target systems, and is used and updated as needed. The solution supports the features and technical standards expected of IAG.

AAS is a suite consisting of AccountCourier, RoleCourier, ComplianceCourier, PasswordCourier, ProfileCourier and Access Insight. Access Insight is Courion's new analytics tool to provide data correlation, analysis and identity intelligence for IT and business. CourionLive is an IDaaS offering providing functionality in identity administration and provisioning.

Courion has developed an implementation methodology that uses a structured process. The IAG solution can integrate with other vendors' administration, analytics, workflow and reporting tools where competitor implementations already exist.

Strengths

- Courion's redesigned connector architecture and implementation methodology have significantly reduced installation times and costs for its clients.
- The cloud strategy of Courion provides potential clients with robust IAG features, as in different deployment options.
- Courion's Access Insight offers more analytics and reporting options for clients, allowing a more real-time and proactive approach to access governance.

Cautions

- Courion's IAG product line remains confusing to first-time IAG users. New offerings and methods of delivery exacerbate that confusion.
- More IAG vendors with equivalent features sets and greater reach and scale threaten Courion's plans to deliver to first-time IAG customers.
- Courion's identity and data log model depends primarily on repository and target system performance and data quality.

CrossIdeas

CrossIdeas is a European company that delivers an IAG and UAP solution known as Ideas IAG Suite (v.4.1, July 2012). Ideas is based on Java EE and is supported on most Java-capable platforms. The Ideas object-relational identity data model (known as Access Warehouse) supports fine-grained entitlement management and an access controls set that supports multiple controls modeling methods based on role, organizational information and business activities. Ideas'

multitenancy architecture delivers preventive/detective access controls, segregation of duties (SOD) management, role mining and comprehensive risk analytics capabilities.

Proprietary read/write-capable connectors support common platforms and protocols, and can interoperate with competitor UAP solutions. Specific support for NetIQ Identity Manager is available, and other UAP vendor support is planned. Applications can leverage Ideas' external authorization management capabilities, allowing real-time authorization management and access risk control.

CrossIdeas has made market progress since its inclusion in the 2011 Magic Quadrant, and continues to leverage its identity intelligence capabilities for the European market.

Strengths

- CrossIdeas' identity data model provides a business-driven modeling method for access controls and provisioning.
- CrossIdeas has significant integration capability with the SAP environment for access provisioning and compliance controls.
- CrossIdeas combines external authorization management and IAG capabilities within the same platform.

Cautions

- CrossIdeas has limited platform support for pure Microsoft-based infrastructures, including the lack of support of SQL Server and .NET.
- The Italian-based company has a small customer base and limited channels into international markets. This is changing via expanded venture capital and technology partnerships.
- The business UI needs further simplification for the nontechnical user. Release 4.1 provides some improvements.

Deep Identity

Singapore-based Deep Identity delivers an IAG solution known as Identity Audit and Compliance Manager (IACM). The architecture is multitenant and cloud-ready. A UAP product known as Identity Manager is also produced. The software is entirely Microsoft .NET-based and uses Active Directory for authentication and SQL Server as the identity repository. Simple connector architecture is used for building agentless connectors for deployment. Additionally, file server plug-ins are also available for governance of shared resources on the file servers. A lightweight workflow system is also developed in .NET and used in IACM and Identity Manager with out-of-box policy templates. The business and administrative UI is Web-based and uses Windows Web Server for delivery.

IACM's identity data and log model is delivered via Microsoft infrastructure and provides a basic foundation for role design and entitlement management. Role and entitlement discovery is also supported. IACM provides several layers of certification and recertification functions, including self-

service by manager/group/department and by endpoint systems. SOD, user, password and group compliance are also supported, as is risk scoring. A simple analytics and reporting function is also provided.

Deep Identity, which is based in the Asia/Pacific region, is an IAM provider that delivers many of the features and standards in support of IAG.

Strengths

- Deep Identity provides regional awareness in its product features and configurations.
- IACM provides many of the IAG features desired by Microsoft-centric enterprises that do not want to deploy complex alternatives.
- Deep Identity also provides UAP as another product to deliver fulfillment functionality and provide a minisuite solution, obviating the need for a UAP tool.

Cautions

- Deep Identity IACM is based predominantly on Microsoft infrastructure and development environments. It possesses a small — although growing — customer base.
- The company is focused primarily on regional markets in the near Asia/Pacific region, including China, Indonesia, Vietnam and Australia, as well as others.
- IACM is a good starting point for enterprises seeking basic IAG functionality, but more analytics and reporting features are needed for more complex environments.

Dell-Quest Software

Quest Software (now a part of Dell as of 2012) has incorporated IAG functionality into its Quest One Identity Manager (Q1IM v.5.1, March 2012). Q1IM's three-tiered architecture consists of a data tier running on SQL Server or Oracle Database, a service tier implemented in C# on .NET (Windows) or Mono (Linux), and a UI tier that provides both Web-based and thick-client access. Dell-Quest Software offers different editions of Q1IM: Data Governance, Active Directory, Adaptive Authorization, Privileged Accounts and Cloud Identity.

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 actions in Q1IM, including both manual activities and systems initiated, 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. Support for risk scoring of access during policy checking, mining and discovery is supported.

Q1IM has some integration capability with existing Dell-Quest identity and access solutions. Unlike many of its competitors, the integration does not create dependencies on other Dell-Quest Software IAM products to function.

Strengths

- Dell-Quest Software's history of delivering administration and management tools and providing integration to Microsoft infrastructure can be leveraged to introduce Q1IM to a large customer audience.
- Q1IM has a robust, enterprise-class identity data and log model to define policy, roles, accounts and other identity information for use within IAG.
- Q1IM's portal for business UI design is configurable by end users and relatively simple to use compared to other solutions based on the original UAP platform.

Cautions

- Quest Software is undergoing restructuring as part of the new software division of Dell, and the transition may mean changes for Quest Software's road map and organization.
- Q1IM is known more to enterprises as a UAP tool, rather than an IAG solution.
- Q1IM does not yet support pattern and behavior analysis of role and entitlement use as part of analytics at this time, although it is on the future road map.

Fischer International

Fischer International uses the same architecture to deliver an on-premises solution known as the Fischer Identity Suite (v.5.0, April 2011) and a SaaS solution known as Fischer Identity as a Service. The software architecture is based on a series of modules by function, and the software module provided for IAG is called Fischer Identity Compliance (v.5.0, November 2011). Although a stand-alone offering, the solution should be used with other modules, such as Fischer's Automated Role & Account Management, to be competitive with other IAG solutions. Identity Compliance is written in Java and is supported on Java-capable platforms.

The IAG solution uses an identity data and log model that supports event-based, request-driven or scheduled input, and stores both in a database. Workflow and analytics tools are proprietary. The connector architecture for IAG is shared by all other Fischer IAM software modules. Although role and entitlement discovery are supported, mining is not available. Identity Compliance does have a robust controls modeler for SOD and other controls.

Fischer Identity Compliance provides many of the capabilities and supports the technical standards used in IAG solutions.

Strengths

- Fischer's architecture for IAM allows for the sharing of different software modules among the products and is cloud-ready as written. No scripting is required for Identity Compliance.
- Pricing (including fixed-price options) is based on services or software, and is competitive.

- Fischer's solution is particularly appealing to smaller enterprises requiring IAG or enterprises with minimal IAG requirements, as well as those that are cost-constrained. Fischer is focusing on the higher education market to gain visibility.

Cautions

- As with many IAG vendors, Fischer's out-of-the-box connector library still needs expansion (although connector development is good). The product lacks some IAG features, such as role and entitlement mining, and pattern analysis.
- Fischer is a small company with limited visibility, particularly in the IAG market. Consulting services for regulatory compliance require a Fischer partner.
- As additional IAG companies enter the market with cloud-ready solutions, Fischer will face increasing competition and must innovate further to differentiate.

Hitachi ID Systems

Hitachi ID Systems delivers Hitachi ID Identity Manager (v.8.1, October 2012) and Access Certifier for IAG. Access Certifier is a component of Identity Manager, included at no additional cost. The software is written in C++ and SQL-stored procedures, runs on Microsoft Windows 2008/R2, and supports load balancing and replication across multiple, concurrently active servers. The back end may be Microsoft SQL Server or Oracle Database. The products support technical standards and most features of IAG 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, RBAC and relationship-based access control. 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 ID Systems Identity Manager offers one price for identity administration and entitlement governance, 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 IAG capability is integrated with identity administration, entitlement provisioning and credential management, rather than a loosely coupled bolt-on.
- The one price model is simple and appeals to many potential buyers.
- An SOD engine decomposes roles and access controls linked to relationships, rather than just roles.

Cautions

- Analytics are basic and accessed via reports, rather than an interactive UI.
- Access certification workflows could be more flexible.
- The current version does not generate graphical dashboards.

IBM

IBM's IAG solution consists of IBM Security Identity Manager (ISIM v.5.1, October 2011) and an incorporated software module known as Role and Policy Modeler (RaPM). IBM's recent acquisition of Q1 Labs in late 2011 also contributes foundational QRadar Security Intelligence technology for security analytics and intelligence for future use within IAG. For the purposes of this report, ISIM represents IBM's present IAG offering. IBM has released a new version (v.6.0) of ISIM in October 2012, and fully incorporates RaPM into ISIM. 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 IAG product, including user request, access recertification, entitlement and role mining, role modeling, analytics, and compliance reporting.

The identity data and log model used by ISIM is supplemented by RaPM schema to incorporate metadata into ISIM's operational role management model. Although integrated with ISIM, RaPM is a separate modeling environment, imports access and identity information using comma-separated values formats, and exports it into an XML format. ISIM's UI is Web-based and uses a Java applet form designer for development. 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 is enhanced with IBM's Cognos technology and includes common reporting modules.

IBM's strategy for IAG emphasizes policy and role modeling, coupled with access certification and identity intelligence.

Strengths

- IBM's global reach and cross-industry customer base provide extensive opportunity for developing IAG best practices and business scenarios.
- ISIM is a mature and comprehensive foundation for delivering IAG features as part of UAP.
- IBM's recent acquisition of Q1 Labs and use of rich analytics and reporting provide clients with choices when delivering enterprise identity intelligence.

Cautions

- IBM has completely restructured its IAM practice, rebranded its IAM products and reorganized with new leadership, potentially introducing some disruptive change for a short period.

- ISIM as an IAG platform is unlikely to be suitable for enterprises that seek to supplement a UAP solution with IAG.
- IBM's strategy for providing IAG in hybrid enterprise/cloud environments is evolving.

Microsoft

Microsoft completed a purchase of certain Bhold technology assets in 2011. That technology has been integrated into Forefront Identity Manager (FIM 2012 R2, June 2012), and provides basic access governance that leverages Microsoft SQL Server, .NET C# and Microsoft Silverlight scripting. The IAG features use an SQL Server database as identity repository for identity information and logging. The client interface is presented in SharePoint or Exchange/Outlook. The product supports LDAP and ODBC standards for provisioning brokers, and it relies exclusively on FIM for synchronization connectivity.

Microsoft's IAG identity data and log model allows for the combination of identity information and log data in the same repository for identity intelligence reporting. Data collection, processing and storage occur in a master database. This data model combines static and historical log data about identities as a single entity for processing and use. The connector architecture is read-only to aggregate required data. Workflow is provided via FIM, and analytics, administration and reporting are available — supported by underlying Microsoft FIM and Windows infrastructure. Mining and discovery tools are provided to scan for key identity data in applications and systems to help populate the identity database.

Microsoft's IAG is part of FIM 2010 R2 and is not a separate product that a customer can purchase. It is not marketed separately and is provided as part of FIM's purchase.

Strengths

- Adding IAG to FIM provides Microsoft clients with more choice when it comes to defining identities and potentially limits multiple vendors for IAM in the enterprise.
- Microsoft's global and pervasive presence in all enterprise sizes and types, as well as its extensive partner ecosystem, increases opportunities for developing best practices for IAG.
- Microsoft's IAG capabilities can be extended to support the company's evolving cloud strategy using Azure Active Directory as requirements dictate.

Cautions

- FIM's IAG capabilities are targeted at clients with significant Microsoft infrastructure and application investment. Support for non-Microsoft environments, although available, is less extensive than competitors. Integrators can develop additional connectors as needed.
- The addition of IAG is marketed more as a technology addition for UAP than as a requirement for business-centric access governance.

- FIM lacks features such as additional self-service and group management capabilities, as well as broader IAM support for SharePoint.

Omada

Omada delivers its IAG features via its Omada Identity Suite (OIS v.9.0, June 2012). The module within Identity Suite is known as Identity and Access Governance (v.3.0, June 2012). OIS is written in Microsoft .NET. The suite is built on the Microsoft Business Intelligence platform and leverages OLAP, SQL Server Integration Services (SSIS) and hypercube multithreading. Connector architecture consists of data collectors for enterprise and SaaS-based systems, and are provided by SSIS. Identity repository features are also provided by Microsoft Business Intelligence. A proprietary OIS workflow and policy engine supports business process modeling for key IAG functions. The UI is available in both "native Web" and SharePoint-based options. Analytics and reporting are provided by Microsoft's SQL Server Reporting Services (SSRS).

The OIS identity data and log model is extensible and incorporates identities, resources, access, user behavior and other data elements. The OIS Data Warehouse is based on SQL Server and includes audit and log data. 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. Omada Identity Suite also provides fulfillment features through its UAP capabilities.

Omada OIS provides most of the features and supports the technical standards expected of an IAG solution.

Strengths

- Omada leverages well-known Microsoft infrastructure and collaboration applications to deliver IAG functionality.
- Omada provides significant integration with SAP applications.
- The global reach of Microsoft and the scale of deployment of Microsoft applications ensure consulting and system integration services support for Omada customization.

Cautions

- OIS is heavily dependent on several Microsoft services for delivering IAG features. Microsoft's strategy for IAG will significantly impact Omada IAG decisions.
- Omada's size has limited its expansion primarily to European clients, although progress has been made in the North American market.
- OIS could use additional management agents for target systems and more industry-specific process templates.

Oracle

Oracle Identity Analytics (OIA v.11.1.2, August 2012) is a Java enterprise application capable of running on any compatible application server. It uses an SQL database as an identity warehouse. The business client interface is a Web browser. OIA's 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 IAG, and is part of Oracle's extensive IAM product portfolio.

OIA's identity and data log model combines identity information and log data in the same repository. Oracle's Identity Connector Framework (ICF) provides the data collection. Mining and discovery tools build application entitlement catalogs and inform patterns of behavior for role and rule definition, and role management capabilities manage the role life cycles after definition.

As part of Oracle's Fusion Applications architecture road map, OIA provides the compliance management and entitlement administration required for IAG, including support for continuous audit policy monitoring and closed-loop remediation. Release 11G R2 represents an inflection point for OIA in terms of further integration with other Oracle identity management products, including Oracle Identity Manager (OIM).

Strengths

- OIA is part of a broad and comprehensive set of Oracle IAM products and services, providing advanced functionality with Oracle enterprise applications and Oracle infrastructure.
- OIA's improved UI significantly reduces development time for workflow and can improve business customer user experience with IAG functions.
- Oracle's pricing structure has been changed to include fixed processor-based pricing for some scenarios, addressing previous concerns regarding the pricing of those scenarios.

Cautions

- Oracle's size and partner model still favor larger enterprises with more complex and comprehensive requirements, although pricing changes are the first step in becoming more attractive to smaller enterprises.
- Increasingly aggressive competitors with a similar reach and market presence offer similar functionality and competitive pricing.
- The "long tail" of earlier Oracle releases will need to upgrade to v.11.1.2 to realize many of the more attractive features that enable Oracle to compete with innovative, smaller competitors.

RM5 Software

Finland-based RM5 Software delivers an IAG solution with RM5 IdM (v.4.5, September 2012). 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 wizards framework provides additional customization capability for self-service and delegated administration. Policy management is particularly robust and provides extensive definition ability. RM5 IdM does not have a discovery or mining capability, however.

RM5 Software's identity data and log model is multidimensional and multitenant within shared services. The central repository depends on the connector architecture to import/export required data via RM5's synchronization engine. Modeling IT controls is done via RM5 Business Rules. 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.

RM5 Software provides some of the features and supports the technical standards expected of an IAG solution.

Strengths

- RM5 IdM's architecture is suitable for SaaS and enterprise-based delivery.
- Its synchronization capability enables RM5 IdM to provide some UAP functionality, along with IAG.
- RM5 IdM's policy management features are extensive and can address specific business scenarios, such as power of attorney and corporate service agreements.

Cautions

- Because of its small size, RM5 Software is focused on the European market.
- RM5 IdM third-party application support is limited, including more connectivity with major providers, such as SAP.
- As an IAG solution, RM5 IdM lacks more traditional features, such as discovery, mining, advanced analytics or risk scoring.

SailPoint

SailPoint's IdentityIQ (v.5.5) is Java software that can run on various Windows, Unix and Linux platforms. Its identity warehouse uses relational data schema from Oracle, IBM DB2, Microsoft or MySQL. The business client interface is a Web browser. The product supports the breadth of features and technical standards normally required in IAG (see "Identity and Access Governance: Definition and Market"), and incorporates identity administration and provisioning as well.

IdentityIQ's data and log model (known as Identity Cubes) combines identity information and log data in the same repository for report intelligence. Adapter architecture aggregates required data and can be expanded via the Provisioning Engine application to provide fulfillment capabilities.

IdentityIQ's Business Process Engineer delivers workflow functionality, and its policy management system allows for risk scoring where applicable.

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

Strengths

- SailPoint's features and support have yielded a growing and loyal customer base, as well as a partnership program that leverages reach and visibility.
- Recent expansion and technology acquisition have positioned SailPoint well for supporting SaaS applications in a hybrid environment and delivering SailPoint as a service.
- SailPoint has a growing international market, and IdentityIQ clients report general satisfaction with design and deployment experiences.

Cautions

- Mobile applications for approvals, access requests, alerts and notifications are not yet available, but are planned.
- SailPoint's embracing of UAP as part of a single IAG architecture requires additional adapter support, including cloud adapters for hybrid enterprise/cloud support.
- An increasingly capable and expanding competitor market — particularly in scale and performance — is challenging SailPoint's leadership.

Vendors Added or 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 appearing 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. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Added

The following vendors were added to the ratings portion of the report because of the evolving changes of IAG architecture:

- AlertEnterprise
- Atos
- Avatier

- Brainwave
- Deep Identity
- Dell-Quest Software
- Fischer International
- Hitachi ID Systems
- IBM
- Omada
- RM5 Software

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

Classifying whether a vendor is an IAG vendor is challenging. For 2012, Gartner has expanded the vendors that will be included in the Magic Quadrant ratings by using the following exclusion and inclusion criteria, in addition to the standard criteria for client base size, revenue and features.

Vendors are included if:

- IAG is marketed as a distinct product providing the following product feature sets:
  - Administrator and business UIs
  - A workflow system for automating IAG processes
  - An identity repository or warehouse for IAG-specific information
  - A connector architecture or service bus architecture for linking the IAG product with required resources
  - Mining, discovery and engineering tools that permit the construction of identity repository components, such as entitlement catalogs for applications
  - Comprehensive analytics tools for modeling, simulation and forensics activities with IAG information
  - A complete audit and reporting capability as part of the systems above or as a stand-alone capability
- The vendor can provide a majority of these features as part of UAP.
- The vendor can provide detailed IAI from advanced analytics and reporting specifically targeted to IAM clients as a distinctive product for IAM.

- The product is specifically positioned to address business user requirements for IAG by the vendor and the client in their implementation.
- The vendor must be able to demonstrate that at least five clients within the past six months are using the product for IAG and not UAP only.

Vendors are excluded if:

- A distinctive IAG product or IAG feature set within UAP has not been available on the market for at least six months (measured from January 2012).
- The vendor depends *entirely* on another vendor's distinctive IAG product to deliver any of the feature sets listed above.
- Analytics functionality does not extend beyond simple operational support requirements, such as performance or capacity management.
- There is insufficient market penetration as measured by the number of clients, scale of deployment or distinctiveness from a UAP deployment, as used by the client.
- Product packaging, use practices, marketing and sales approaches are not IAG-specific and, instead, focus on identity administration for IT administrators or related areas.

The research used in producing the Magic Quadrant for IAG uses vendor information regarding product capabilities, existing partnerships and the vendor's customer base as of May 2012, when the data collection process from vendors and clients completed. Product releases, new partnerships and new customer information after that date are not included in this study. This reflects a publishing schedule requirement, as well as a desire to provide clients with research from a production IAG environment. Although changes after May 2012 are noted in the study, they do not affect the ratings of the vendors.

IAG functionality appears throughout other products in the IAM market, and vendors that possess significant IAG function within their products are recognized in this study, as well as in "Identity and Access Governance: Definition and Market."

Evaluation Criteria

Ability to Execute

IAG vendors are evaluated on their Ability to Execute based on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider and business user performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation. Ultimately, vendors are judged on their ability and success in capitalizing on their vision:

- **Product/Service:** Core goods and services offered by the IAG vendor that competes in/serves 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.

- **Overall Viability (Business Unit, Financial, Strategy, Organization):** An assessment of the overall vendor's financial health, the financial and practical success of the IAG business unit (if multiple product types are sold), and the likelihood of the IAG vendor to continue investing in the product, offering the product and advancing the state of the art within the vendor's product portfolio.
- **Sales Execution/Pricing:** The IAG 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 and Track 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 IAG vendor's history of responsiveness where applicable.
- **Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the vendor's IAG message in order 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, thought leadership, word-of-mouth and sales activities. Marketing execution is critical in this early stage of IAG market development.
- **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 and SLAs. Retaining customers is also critical in an early market.
- **Operations:** The ability of the IAG vendor 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 vendor to operate effectively and efficiently on an ongoing basis.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	High
Market Responsiveness and Track Record	High
Marketing Execution	High
Customer Experience	High
Operations	Standard

Source: Gartner (December 2012)

Completeness of Vision

In the Completeness of Vision analysis, IAG vendors are evaluated on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs, and competitive forces and how well they map to the Gartner position. Ultimately, vendors are rated on their understanding of how IAM and IAG market forces can be exploited to create opportunity for the vendor:

- **Market Understanding:** Ability of the IAG vendor to understand buyers' needs and translate these needs 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 those wants with the vendor's added vision. It also means understanding the concept of market timing and having the ability to deliver viable solutions, both for vendor profit and for customer success.
- **Marketing Strategy:** A clear, differentiated set of IAG messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.
- **Sales Strategy:** The strategy for selling IAG product 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. This is particularly important in an early market to maximize customer acquisition.
- **Offering (Product) Strategy:** An IAG vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology, and feature set as they map to current and future requirements. IAG functionality is particularly important due to the capability of the business end user to make effective use of the solution.

- **Business Model:** The soundness and logic of an IAG vendor's underlying business proposition, and its alignment with a potential customer's business model and overall strategy in IAM.
- **Vertical/Industry Strategy:** The IAG vendor's strategy to direct resources, skills, and offerings to meet the specific needs of individual market segments, including verticals. This is at an early maturity stage at this point, while IAG feature sets are consolidated and confirmed by use.
- **Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.
- **Geographic Strategy:** The IAG vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography directly or through partners, channels and subsidiaries, as appropriate for that geography and market.

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	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Standard

Source: Gartner (December 2012)

Quadrant Descriptions

Leaders

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

Challengers

IAG Challengers have shown significant progress in delivering IAG feature sets. Some have major clients using their IAG features. Challengers have good execution capabilities, and most have a significant sales and brand presence. However, Challengers have not yet demonstrated the feature completeness or scale of deployment that Leaders have. Their vision and execution for technology and methodology, and/or their means of delivery, tend to be more focused on operational or management concerns, rather than governance. Clients of Challengers are somewhat satisfied but ask for additional IAG features, particularly in connectors or reporting.

Visionaries

Vendors in the Visionaries quadrant provide products that meet many IAG client requirements, but have a lower Ability to Execute rating than Leaders. This may be because of a smaller presence in the IAG market than the Leaders, as measured by installed base, revenue size or growth, or by smaller overall company size or general viability. Visionaries are noted for their innovative approach to IAG technology, methodology and/or means of delivery. They may often have unique features, and may be focused on a specific industry or specific set of use cases, more so than other competitors.

Niche Players

Niche Players provide IAG technology that is a good match to specific IAG uses, cases or methodology. They may focus on specific industries and can actually outperform many competitors. They may focus their IAG features on a specific vendor's applications, data and/or infrastructure. Vendors in this quadrant often have a small installed base or are limited according to investment in IAG, a geographically limited footprint, or other inhibitors to 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

IAG technology provides:

- Access policy management
- Administration of access entitlements (known also as user permissions, rights or authorizations)
- Role management (as one function of entitlement administration)
- Access request
- Access certification

IAG technology provides these functions with the following:

- Administrator and business UIs
- A workflow system for automating IAG processes
- An identity repository or warehouse for IAG-specific information (could be more than one repository)
- A connector architecture or service bus architecture for linking the IAG product with required resources
- Mining and discovery tools that permit the construction of identity repository components, such as roles and entitlement catalogs for applications
- Comprehensive analytics tools for modeling, simulation and forensics activities with IAG information
- A complete audit and reporting capability as part of the systems above or stand-alone

IAG deployments are often funded for one or more of the following reasons:

- Compliance reporting and control driven by regulation
- Accountability and transparency of access to critical business resources in an attempt to better manage business risks and protect privacy
- Streamlining an intensely manual process for access request, certification, and reporting for efficiency and cost savings

Enterprises should consider IAG products from vendors in every quadrant of this Magic Quadrant based on their specific functional and operational requirements. Product selection decisions should be driven by organization-specific requirements in areas such as:

- The relative importance of access request and certification
- The scale of the deployment
- IAG product deployment and support complexity
- The IT organization's project deployment and technology support capabilities, maturity and experience
- IAG requirements
- Integration with other established IAM systems

IT managers considering IAG deployments should first define and/or determine their requirements for the governance of identity and access functions. The requirements definition effort should include capabilities that will be needed for subsequent deployment phases to establish organizational structure and for training. The project will benefit from the input of other IT groups, including audit/compliance, IT operations and application owners, and security administration. A formal assessment of existing capabilities to address these requirements will then lead to a gap analysis and feature list required to fill that gap. Enterprises should describe their IAM deployment topology so that prospective IAG vendors can propose solutions to company-specific deployment

scenarios. The requirements definition effort should include later-phase deployments beyond the initial use case, because this is an ongoing process, not a one-time effort. This Magic Quadrant evaluates technology providers with respect to the most common technology selection scenario — an IAG project that is funded to satisfy access request and certification needs for compliance through accountability and transparency of access.

In summary, enterprises should:

- Use IAG products to establish an identity data model and data warehouse for governing the identity life cycle, particularly for access.
- Choose IAG products that provide a business-friendly user experience and that best address your enterprise process for access request, certification and audit reporting.
- Leverage the data created by your established identity administration and access management tools to provide IAI to IAG and to serve as fulfillment mechanisms for IAG.

Market Overview

The new IAG market is reflecting industry changes brought about by the Nexus of Forces — cloud, mobile, social and information. With cloud computing, IAG vendors are providing versions of their tools that can be run as SaaS applications in private and public cloud environments. Those same vendors are also providing changes to incorporate SaaS applications with enterprise applications under one access governance umbrella — providing capabilities for each. With mobile, IAG is extending support of the UI to include tablet computer and smartphone formats, allowing some administrative tasks (such as approvals and certifications) to be done no matter what access platform type is used. Social media forces are changing the nature of the identity itself and calling into question the role of the enterprise in defining, securing and providing identities versus the convenience of self-defined identities from social media. Providing a means to secure and audit social identities will be an added task for IAG. Information has the most significant impact on IAG in that it enables the practical expansion of IAG to new value propositions for the enterprise. IAI will become increasingly important to business decision making, and the IAI-to-BI bridge will be built on information.

IAG as a discipline within enterprises continues to evolve. The new IAG tool market will consist of vendors with

- Distinct IAG products
- Identity administration and governance combined (IAG plus UAP)
- Data modeling, design, analytics and forensics for identity and access, or for IAI

There will be cloud-based service variations of any and all of the vendor types above, but in an early and minimal state, meaning a reduced feature set or coverage.

Analysis and Findings

Gartner 2012 research of IAG has revealed the following:

- Addressing compliance remains the primary driver for IAG, but the contribution of IAI output to business decision making is expanding visibility and use of IAG into other areas of human resources and risk management support.
- IAG has incorporated UAP into a new superset of features: "identity administration and governance."
- Access governance for unstructured and semistructured data is growing in importance to IAG users and will be incorporated into IAG features.
- Providing IAG functionality to, from and for the cloud will significantly impact the market, with cloud versions of existing IAG tools and new IAG cloud-based vendors appearing on the market.
- Mobile endpoint options that support access to IAG approval, certification and analysis functions will be made available by existing and new IAG vendors.
- Formalizing the approach of modeling identity data and log output through organizational consolidation and skills updating is critical to establishing an effective identity repository for long-term data quality and accuracy.
- Next-generation IAG tools will provide advanced entitlement and role discovery and mining for data and applications; role engineering; modeling; simulation; analytics; and dashboard and reporting capabilities as mature additions to the IAG toolset.

IAG Changes, 2011-2012

This will be the last year Gartner produces an IAG Magic Quadrant study. As stated earlier, there is a restructuring of the IAG market occurring to incorporate UAP features and to form a more sophisticated analytics function. In 2013, IAG and UAP Magic Quadrants will be combined into a new and broader report focused on this new superset of functions.

In 2012, Gartner opened the IAG study to those vendors providing subsets of IAG features, whether as part of UAP solutions or as stand-alone vendors. The report also allowed for the inclusion of smaller vendors providing advanced identity and access design, and analytics tools, without IAG administration functionality. The lack of a complete feature set affects the ranking of many new entrants in the study.

The Leaders Quadrant

The 2012 IAG Leaders are Aveksa, CA Technologies, Courion, Oracle and SailPoint.

In the Leaders Quadrant, SailPoint, Oracle and Aveksa continue to show leadership in the Ability to Execute in the market. SailPoint's new-customer and feature momentum remains above the industry average. Aveksa continues to excel in proof-of-concept competitions and has shown

progress in developing its identity data and log model. Oracle's release of version 11G R2 has expanded its vision of IAG's role in its IAM suite and potentially redefines the pricing discussion.

Courion continues to show progress in connector architecture and cloud delivery capabilities. CA Technologies has moved clearly into the Leader Quadrant via its execution within its customer base and by making progress in its cloud vision for IAG.

The Challengers Quadrant

The 2012 IAG Challengers are Avatier, Dell-Quest Software, Hitachi ID Systems and IBM.

All the vendors listed in the Challengers quadrant are newcomers to the rated portion of the study. Quest Software (recently acquired by Dell) has shown considerable progress since 2011 in delivering Quest One Identity as an IAG solution, expanding its customer base and acquiring key new IAG customers. IBM enters the rated study with its improvements via role and policy modeling to its UAP product Security Identity Manager and resetting its overall security intelligence vision to incorporate IAG. Hitachi ID Systems has also shown progress in developing an identity and data log model that serves existing Hitachi ID Sync clients and has made progress in analytics and reporting. Avatier's innovative UI and mobile support have gained attention from existing Avatier clients, and its expanded presence is attracting the attention of others.

The Visionaries Quadrant

The 2012 IAG Visionaries are AlertEnterprise and CrossIdeas.

CrossIdeas continues to show improvement in the Visionaries quadrant through its acquisition of strategic and large-scale clients, its detailed data model and configurability. A new entrant into the quadrant is AlertEnterprise, with its broader view of IAG as a function of logical and physical security and its noted presence in the critical infrastructure industry.

The Niche Players Quadrant

The 2012 IAG Niche Players are Atos, Brainwave, Deep Identity, Fischer International, Microsoft, Omada and RM5 Software.

Niche Players do not get the credit they deserve because of the mistaken impression given by the quadrant's name. Many of these vendors are new to the Magic Quadrant and are rated here because of their focus on particular industries or function or because of their feature set completeness. Atos is a new entrant (formerly Siemens DirX) and provides a UAP-based version of IAG that has been in the market for years. Fischer International is one of the first true cloud IAM vendors, and enters the IAG market via a feature set offered as part of its UAP solution. Fischer has focused on the higher education market and has experienced some initial success. Microsoft's acquisition of Dutch-based Bhold in 2011 put it on the IAG map with features that are sold at no additional cost as part of its Forefront Identity Manager offering. Omada has demonstrated a good IAG feature set also built on Microsoft's Forefront and has notable analytics and reporting capabilities. RM5 Software is a Finland-based IAG provider with the ability to offer enterprise

software or SaaS services and a business-oriented reporting system. Brainwave is a French IAG company that provides advanced analytics and reporting capability in its offering. Deep Identity is a Singapore-based IAG provider with a flexible enterprise/SaaS design, a regional focus reflected in its configuration, and support for Microsoft-centric environments.

Vendors to Watch

IAM vendors with notable IAG functionality — both large and small — are listed below, but are *not* rated in the Magic Quadrant itself because of the criteria listed in the Inclusion and Exclusion Criteria section. Many customers that already possess these solutions in their enterprises use them as a basis for building IAG functionality by expanding capability through customization or by providing an IAG product as an overlay to their primary function of fulfillment.

Bay31: Role Designer

An Italian-based firm, Bay31's Role Designer focuses on the critical functions of role discovery and mining, which are key to constructing effective identity data models for IAG. Role Designer is available in enterprise, SAP and analyst editions, which include audit, remediation and reporting functions. Bay31's SAP relationship enables it to deliver visualization and analysis of SAP roles and to compete with in-house SAP tools that do the same. Collaboration with Atos and partnership with Trusteq in Finland are evidence of Bay31's European market intentions. Role Designer is also available in cloud-based and enterprise versions.

Beta Systems Software: SAM Enterprise Identity Manager

Like other European IAM vendors, Germany-based Beta Systems Software has many of the access request and certification features included as part of its user-provisioning offering. SAM Enterprise Identity Manager is notable for its business-process-centric approach to implementing workflow for IAG processes, and has IAG reporting and intelligent analysis functionality. A recent partnership with Microsoft leverages the company's BI capabilities with Beta Systems' identity data warehouse, and the company is poised to enter the IAG market in 2013. SAM Enterprise Identity Manager is being updated to include integrated discovery and analytics functionality for constructing an identity data and log model, and the company is on track to be considered an identity administration and governance provider in 2013.

The Dot Net Factory: EmpowerID

U.S.-based The Dot Net Factory delivers EmpowerID as a multitiered architecture hosted on Microsoft's IIS and SQL Server, and provides capabilities in access control, identity administration and directory services. The solution provides support for IAG visual workflow construction, a role- and attributed-based access modeling capability, good audit and compliance features, and a number of monitoring and logging features for access reviews, approvals, certifications and reporting. EmpowerID has significant customization capabilities to build many IAG features and interfaces, and it has good support for the Microsoft server platform environment.

e-trust: Horacius Identity Management System

E-trust is a Brazilian company that provides managed security services and project managers for information security. It also has a product known as Horacius, which provides access request workflow functionality and tools to create managerial approval, multiple data owner approval, incident management and segregation of duties. Access request and access granting can be automated by applying user-defined business rules on HR database records. Horacius 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 and mining tools are available on Microsoft AD connector. Analytics tools aren't available in this edition. E-trust has a small customer base in South American markets, ranging from small or midsize businesses (SMBs) to Fortune 500 firms, and has acquired new customers in 2012.

Evidian: Identity and Access Manager

France-based Evidian is known for its access management capability. It has expanded its user administration functionality in provisioning to include IAG features. Evidian designers believe IAG to be an integrated part of a core IAM platform. The current solution has IAG features such as access policy management, a workflow-based access request manager, rule-based entitlement administration and a role-based identity data model. Discovery, mining and analytics tools aren't available in this edition. Evidian has made progress in visibility and the availability of IAG features in 2012.

NetIQ: Access Governance Suite

NetIQ continues development, marketing and support of the access-governance-related assets that it received from its parent organization's acquisition of Novell in 2010. In that same year, NetIQ entered into an OEM relationship with SailPoint. The result is the NetIQ Access Governance Suite. NetIQ provides its own support for the suite and provides access to a partner network that enables Access Governance Suite to be an international offering. NetIQ's OEM solution has the same characteristics and capabilities as SailPoint's IdentityIQ. The company provides integration for customers that use NetIQ's Identity Manager to provide cross-product management of resources and entitlements, and leverages the provisioning and certification processes from the Access Governance Suite. The combination of Access Governance Suite and Identity Manager enables NetIQ to be competitive in the IAG market.

SAP: Access Control

SAP delivers SAP Access Control (v.10.0, June 2011) as a solution for access governance and certification processes integrated with core business processes. SAP Access Control's identity data and log model is heavily influenced by SAP's strategic authorization concept for SAP's application portfolio, and is an integrated user and role repository. SAP Access Control may be used as a stand-alone IAG solution and has UAP provided via integration to SAP NetWeaver Identity Management and other third-party IdM systems. Analytics capabilities include SOD, transaction and critical access risk analysis reporting, SLA provisioning, user and role analysis, and access rule

reports, to name a few. SAP Access Control offers integration with the SAP Risk Management application for enterprise risk scoring and analysis, and the SAP Process Control application for enterprise policy management and controls automation.

Security Compliance Corp. (SCC): Access Auditor

California-based SCC's Access Auditor provides access review, certification, reporting, alerting and SOD capabilities. It delivers a workflow tool and an "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 is 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 was added in 2012. SCC has enjoyed increased sales — driven by federal regulation — and has had success in several industries, including healthcare. Simplicity in use and deployment, as well as pricing, remain differentiators, particularly in the SMB space with IAG needs.

Securonix Solutions: Securonix Identity Matcher, Securonix Behavior Profile, and Securonix Event and Risk Analyzer

Securonix, which is based in Los Angeles, California, is more accurately described as an IAI provider that uses behavior and outlier analytics to risk-rank users, activity, access and resources (for certifications, access requests and monitoring). It has some capabilities in IAG through its use of tools for building an identity data model and warehouse that is optimized for scalability and analytics. Securonix's leadership originated in the IAG industry.

Tuebora: Governance 360

Tuebora, which was founded in 2011, is based in the U.S. and has a development team in India. Its experienced IAG staff believe that continuous compliance principles should be applied to IAG, and that access governance is a collaborative activity requiring metrics and analytics to provide the appropriate level of intelligence for decision making. Its Governance 360 offering comes in basic, standard and enterprise editions — depending on the client's requirements and size — and provides access request life cycle and detailed analytics capabilities.

Varonis: Data Governance Suite

Varonis is a New York-based company that offers a series of products known as DatAdvantage for different platform and directory environments. The products capture data regarding usage patterns, aggregate the data, and apply mathematical analysis to model behavior and map it back to business usage patterns. This allows an element of visibility into data access control. The company is also viewed as a possible complementary technology for tracking access control patterns and combining the results with DLP output. Varonis can be considered a part of the IAG product market by virtue of its data collection, analytics and reporting function.

Whitebox Security: WhiteOPS, Identity Monitoring and Activity Monitoring

An Israeli-based firm, Whitebox Security is best characterized as an IAI solution. It has monitoring and analytics capability that collects activity and event information about application and data access, and allows 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, it does provide an effective UI for reporting and good input into role engineering and forensic activities.

IAG Futures

The Magic Quadrant report divides those products that fit the detailed criteria of the IAG definition from those features in other IAM products that can perform some IAG functions. Future IAG Magic Quadrant reports will be absorbed into a broader governance-focused IAM product architecture. Basic IAM administration and intelligence features will be absorbed into future and more advanced IAG products. Gartner believes that, from 2013 through 2014, a bifurcation of the IAG feature set will occur. Basic IAG administration functionality will become part of more advanced identity administration (that is, expanded user provisioning), while more advanced IAG features (for example, mining, discovery, analytics and intelligence) will remain a distinctive IAG product offering. The market will see familiar IAM vendors repurpose identity administration tools into IAG tools, as well as new market entrants from the governance, analytics and BI markets. By 2016, many customer requirements for IAG analytics and intelligence will be serviced by existing data management, IT analytics and BI vendors.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Identity and Access Governance: Definition and Market"

"Cool Vendors in Security: Identity and Access Management, 2012"

"Oracle's Strategy for Identity and Access Management"

"IBM's Strategy for Identity and Access Management"

"Hype Cycle for Identity and Access Management Technologies, 2012"

"Identity and Access Intelligence: Making IAM Relevant to the Business"

Evidence

The Magic Quadrant for IAG was developed by incorporating IAG customer feedback (both from vendor-recommended customers and from direct client contacts) with Gartner research, as well as

through analysis of feedback from detailed IAG vendor surveys. This was supplemented by vendor briefings, strategic advisory day sessions with the vendors and clients, market statistics from the vendor, and extrapolated market data from private IAG companies and their partners. Care was taken to obtain more than one source for statistical or metrics information used in the study.

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): 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 and Track 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, SLAs 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 and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling 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.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor'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.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp