Magic Quadrant for Identity Governance and Administration

Published 21 February 2018 - ID G00326925 - 73 min read

By Analysts Felix Gaehtgens, Kevin Kampman, Brian Iverson

While the market for IGA tools delivered as on-premises software is mature, intense vendor activity renders many new choices for IGA delivered as a service. Security and risk management leaders responsible for IAM should emphasize future requirements when planning to purchase an IGA solution.

Strategic Planning Assumptions

This document was revised on 29 March 2018. The document you are viewing is the corrected version. For more information, see the Corrections (http://www.gartner.com/technology/about/policies/current_corrections.jsp) page on gartner.com.

By 2021, IGA as a service becomes the dominant delivery model for new deployments, where 40% of new buyers will opt for cloud-architected IGA and 15% for cloud-hosted IGA software, up from 5% and less than 5%, respectively, in 2018.

Through 2021, customers using a cloud-architected IGA solution will save an average of 30% in initial integration costs and 40% in overall professional services over a three-year period, and accelerate time to value by an average of three months.

Market Definition/Description

Security and risk management leaders responsible for identity and access management (IAM) must ensure that only the right people get access to the right resources (e.g., applications and data) at the right times for the right reasons. Identity governance and administration (IGA) is a fundamental building block of an organization's IAM strategy — these tools manage digital identity and access rights across multiple systems and applications by providing the following functions:

- **Identity life cycle:** Maintaining digital identities, their relationships with the organization and their attributes during the entire process from creation to eventual archiving, using one or more identity life cycle patterns (see Note 1).
- **Entitlement management:** Maintaining the link between identities and access rights to be able to tell who has access to what and who is responsible for maintaining an account or access right. This includes maintaining and curating the entitlements catalog to describe the types of accounts, roles, group memberships and other entitlements.
- **Access requests:** Enabling users, or others acting on behalf of a user, to request access rights through a business-friendly user interface.
- **Workflow:** Orchestrating tasks to enable functions such as access approvals, notifications, escalations, manual fulfillment requests and integration with other business processes. For example, this allows managers or resource owners to approve or deny requests.
- **Policy and role management:** Maintaining rules that govern automatic assignment (and removal) of access rights; providing visibility of access rights for selection in access requests, approval processes, dependencies and incompatibilities between access rights; and so on. Roles are a common vehicle for policy management.
- **Access certification:** Requiring people like managers and resource owners to review and certify the access rights that users have on a periodic basis to ensure access continues to comply with policies. (This is sometimes called "attestation.")

- **Fulfillment:** Propagating changes initiated by the IGA tool to account repositories. Automatic fulfillment (often called "provisioning") connects with account repositories, while manual fulfillment utilizes a workflow or external process to complete actions.
- **Auditing:** Evaluating business rules and controls against the current state of identities and access rights, providing a means for alerting control owners of exceptions (such as changes made directly on target systems) and allowing for orderly remediation.
- **Reporting and analytics:** Providing a mechanism to report on and deliver deeper insights into data available to an IGA tool. Role mining is a typical analytics scenario used to design and optimize role definitions; however, analytics can also be applied to operational data to evaluate quality of service, adhere to service-level agreements and identify anomalous usage patterns.

Applicability and Delivery Mechanisms

Gartner's clients are mainly midsize to global enterprises, and the vendors are evaluated on their ability to deliver to typical client requirements for these companies. All vendors covered in this Magic Quadrant are able to cater to organizations with more basic requirements (however, the complexity of the solutions varies). Vendors whose products score highest in the product/service evaluation criterion will have more capabilities and be more flexible to adapt to requirements typically found in more complex and mature organizations.

IGA is a mature market in terms of tools delivered as on-premises software; however, adoption of IGA tools delivered as a service is picking up rapidly, although still a low percentage: Gartner has reviewed more proposals over the last year that feature this delivery model. The principal driver for adoption of IGA as a service is the desire to reduce time to value — especially from midsize clients with basic IGA requirements. Last year saw intense activity by many vendors to build out IGA-as-a-service capabilities. There are several different scenarios for IGA as a service. This requires careful analysis by clients to find the optimal choice, which, in some cases, is a combination of two choices to support a hybrid scenario:

- **Cloud-architected IGA** represents purpose-built offerings for delivering IGA services from the cloud using modern cloud application architecture.
- **Cloud-hosted IGA software** is a modified software offering hosted in the cloud for delivering IGA in a managed-service sourcing model.
- **Cloud access management with light IGA services** are purpose-built offerings for delivering access management and single sign-on (SSO) services in the cloud with a limited set of IGA capabilities, which are used mostly to manage accounts in other cloud services.

Please see the "On-Premises or as a Service?" segment in the Context section for guidance on how to select the optimal combination.

The pricing model for most IGA software is based primarily on the number of people being managed. However, some vendors also offer processor-based licensing that may be more economical for managing large user populations. Some vendors charge extra for connectors, although this practice is diminishing. Most vendors now offer both perpetual licenses (with annual maintenance charges) and subscription pricing, with median cost over three years (for both perpetual and subscription pricing) starting at approximately $100,000 for 1,000 users. Discounts increase as the number of users increase — for example, the median cost over three years for 10,000 users will be in the neighborhood of $300,000.

Organizations almost always require assistance from system integrators for deployment of IGA software — only the most mature and well-staffed IAM programs can deploy on their own. Based on the review of several statements of work for IGA integration services, [1] (#dv_1_based_on) Gartner estimates that the typical first-year deployment of IGA software usually costs 50% to 200% of the three-year software cost in professional services (not counting internal labor costs). Some software is easier to deploy than others, but organizational complexity will be the main driver of deployment costs. Organizations should expect to spend around 50% of what was spent in the first year in subsequent years on labor costs for upgrades, enhanced functionality and expanded coverage. For this reason, IGA tools are

"sticky," meaning that the decision processes to choose a vendor must be thorough, as it can be onerous to switch to another provider.

This Magic Quadrant covers all the common use cases for IGA. It includes vendors that offer the basic functions listed above and have at least 1% of Gartner's estimated market share or drive considerable interest by Gartner clients. Some vendors offer multiple distinct IGA solutions that overlap in functionality (for example, a well-established and highly mature software solution and a newer, less mature cloud-architected IGA service solution). In those cases, we considered all available solutions for all Magic Quadrant vision and execution evaluation criteria except for the product/service criterion. We scored the product/service criterion by evaluating only the most capable solution with all modules included that would be needed to fulfill all technical IGA inclusion criteria (see the Inclusion and Exclusion Criteria section below). We then listed what solution was evaluated for product/service in the respective vendor write-up.

Magic Quadrant

Figure 1. Magic Quadrant for Identity Governance and Administration

Source: Gartner (February 2018)

Vendor Strengths and Cautions

AlertEnterprise

U.S.-based AlertEnterprise offers its Enterprise Guardian suite of products. It has the ability to extend beyond traditional IAM for logical assets toward areas of physical security and operational technology (OT), including visitor management, physical access control systems (PACSs), card badging and interfaces to supervisory control and data acquisition (SCADA) industrial control systems. The platform also includes threat and risk behavioral analytics for risk scoring by combining identity information with user activity feeds. AlertEnterprise does not yet offer IGA as a service.

Innovations in the last year included a big data reconciliation module to rapidly cover data across multiple logical and physical systems. The AlertEnterprise platform has a range of vertical offerings aimed at financial services, oil and gas, utilities, chemicals, pharmaceuticals, and other regulated industries. These industries make up a large percentage of its customer base, followed by airports and government agencies. Most of its customers are in North America, followed by Europe and Asia.

Strengths

- A clear focus on critical infrastructure industries and the integration of IAM and OT continue to give AlertEnterprise unique standing among all vendors in the IGA market.
- Clients like the solution's integration features and say the vendor is easy to work with.
- AlertEnterprise provides multiple industry-specific content packs, consisting of workflows, policies, request categories, reports and dashboards, to aid deployment.
- The vendor spends considerable R&D funds on the development of features pertinent to specific industries and regulatory frameworks.

Cautions

- Buyers should take care to verify that their future IGA plans align with AlertEnterprise's roadmap, because the vendor is focused on IT/OT integration rather than more general IGA trends.
- While there have been improvements in support for contractor and business partner life cycle scenarios, several basic employee, delegated administration and self-registration scenarios require more effort than with other products.
- While customers have commented positively on the technical expertise of the vendor's professional services, they also mentioned a lack of business-focused deployment methodologies and project management. Potential buyers should consider supplementing AlertEnterprise's professional services with a skilled IAM consultancy focused on product-neutral, business-focused IAM delivery.

Atos (Evidian)

Atos, headquartered in France, offers Evidian Identity Governance and Administration and its new Evidian Analytics and Intelligence as software products. The current version, evolution 10, is a converged offering that combines technology from Evidian and the legacy DirX IGA solution that Atos acquired from Siemens years ago. A managed service offering is also available through Atos.

In the past year, Atos has introduced risk scoring analytics to support access certification and new functionality to facilitate and preview bulk changes due to corporate restructuring. The solution is particularly interesting for clients in EMEA that are looking for an integrated solution that combines IGA and access management. Manufacturing and natural resources; healthcare; and banking, securities and insurance make up the largest part of Atos' IGA customers, followed by government. Three-quarters of its customers are in Europe, followed by Japan and the U.S.

Strengths

- Evidian's IGA, access management (AM) and enterprise single sign-on (ESSO) products are more tightly integrated than any other IAM product suite in the market. This makes it a good choice for organizations looking for a combined solution.
- The latest Evidian product has built-in support for all four identity life cycle patterns with an organization model to support delegated administration, which can ease deployment.

- Atos provides additional out-of-the box features around self-registration, identity proofing and social media integration that make Evidian IGA well suited for managing customer identities.
- Atos has extended its product beyond traditional IGA uses to serve use cases for identity management of industrial connected objects and OT applications.

Cautions

- Core governance-related capabilities such as entitlements management, access requests and access certification are less mature than what is typically available in other IGA products in the market.
- While customers commented positively about the technical capabilities and helpfulness of the vendor's integration services, they also reported some inconsistencies around project management.
- Atos' brand awareness and marketing efforts outside of Europe are limited. It intends to leverage third parties such as ISPs to grow in regions such as North America, but this has not been realized.

CA Technologies

U.S.-based CA Technologies offers the CA Identity Suite, which includes the CA Identity Portal as a common user interface for two distinct products: CA Identity Manager (provisioning) and CA Identity Governance (governance). Some of CA's partners offer this solution as a managed service. In addition, CA also offers a separate cloud access management solution with light IGA services called CA Identity Service. Clients can complement the CA Identity Suite with CA Identity Service as part of a hybrid deployment model or use CA Identity Service in lieu of CA Identity Suite when IGA requirements are very simple. For evaluation of this Magic Quadrant's product/service score, we considered only the CA Identity Suite.

The solution will appeal to global-to-midsize enterprises that have medium-to-complex IGA requirements and appreciate an agile deployment approach. CA Technologies is a major vendor in the IGA space and offers an extensive suite of IAM and enterprise security products. Recent innovations include a rapid deployment model leveraging DevOps concepts and policy templates, and a governance-as-a-service option that includes event-based machine learning algorithms to identify risks and anomalies for reporting and alerting. Its customer base spans the globe in all major industries, with a particularly deep presence in banking, securities and insurance; government; and utilities.

Strengths

- Customers like the end-user interface and comment on good availability of technical resources and support.
- CA Technologies offers a virtual appliance quick deployment tool that uses a DevOps approach combined with a customer "marketplace" featuring preconfigured, pluggable scenario templates, which can accelerate deployments and help in rapidly evaluating the solution.
- CA Identity Manager is very scalable — the solution is used in large, consumer-facing deployments.

Cautions

- There is no central console for defining audit policies — even segregation of duties (SOD) policy definition is handled inconsistently. The concept of case management to resolve audit issues is not supported directly, so workflow and access certification must be used as alternatives.
- Customers comment on overall complexity of the solution, compounded with the challenges of working with a large and complex vendor. Some customers solved these issues by proactively building and managing a close relationship with the vendor to maximize the long-term success of the implementation.
- While the new version of its IGA solution is compelling for new customers, existing customers will face a challenging upgrade path from older versions.

Core Security

Core Security is headquartered in the U.S. and offers the Core Access Assurance Suite (AAS) as software. The solution will have a strong appeal to organizations with a heavy focus on security that are looking for synergies between IGA and real-time security intelligence.

After a period of significant disruption due to the acquisition of and merger with several companies in the security space (in terms of IGA, Courion and Bay31), Core Security has bounced back with a strong IGA offering that has a special focus on real-time security intelligence, detection and response. Major milestones last year were the launch of AAS 9.0 with a new end-user experience for access request management, Core Role Designer and API enablement of its IGA platform to ease integration with other systems.

The largest group of Core Security's IGA customers are in healthcare; banking, securities and insurance; and manufacturing and natural resources. More than two-thirds of its customers are in North America, followed by Europe, with a small percentage in the rest of the world.

Strengths

- Core Security has a strong focus on security analytics to provide actionable insight through real-time security intelligence. The company has a significant head start in this area over many other IGA vendors.
- Core Security has become much more aggressive with discounting over the last year, to the point where it is likely to be the low-cost provider in competitive evaluations.
- Customers are impressed with Core Security's new role design capabilities and advanced analytics.

Cautions

- Core Security continues its path of acquiring companies to grow and expand its market coverage. This creates significant opportunities but also disruptions.
- Gartner still hears mixed reports regarding Core Security's ability to support deployments, and it is too early to judge whether the company has turned a corner in terms of customer relationship practices. Clients are advised to build a strong relationship with their customer success manager and recruit the help of an experienced integration partner to help with their deployment.
- Core Security's rich role design capabilities are compromised by a below-average mechanism for policy management that makes managing access with roles more difficult overall.

Dell Technologies (RSA)

U.S.-based RSA, a Dell Technologies business, offers its IGA solution RSA Identity Governance and Lifecycle (IG&L) as software. The solution is also available as a cloud-hosted option called "My Access Live." Several partners of RSA also host the solution as a managed service. The solution consists of several modules that are licensed separately. It is a good fit for organizations with heavy governance requirements.

RSA is a major vendor in the IGA space and offers an extensive suite of IAM and enterprise security products. Within the past year, RSA has focused on improving the user experience through UI enhancements and ease of deployments via a set of end-to-end best practices. It also added telemetry capabilities for sending live operational metrics to RSA (assuming that the client has consented to this) that can help shorten support requests and potentially identify operational issues early. RSA has customers across all major industry verticals, primarily in North America followed by Europe.

Strengths

- First-time IGA buyers can make use of RSA's large collection of recommended practices, use-case blue prints and "Quick Start" standardized deployments to streamline deployments.
- Clients like the end-user interface and the high configurability of the solution, mentioning that it is easy to maintain.
- The product benefits from an efficient data model that pushes significant processing to the database tier, which makes it one of the highest-performing products.

- RSA's brand depth in security and its strong IGA offering, combined with RSA's position as a leader in several risk management markets with RSA Archer, create strong product synergies for organizations facing heavy regulatory compliance obligations.

Cautions

- Gartner still hears complaints about support and maintenance, and quality issues in updates. However, this may be improving, as we have noted significant efforts by RSA to improve support and maintenance since last year by restructuring internal processes and adding telemetry support.
- The product is difficult to customize. It works best when organizations can deploy the solution by adapting to the way it is designed, rather than trying to do extensive customizing.
- Dell's salesforce is still predominantly selling One Identity's IGA solution rather than RSA IG&L, causing existing Dell customers to potentially overlook the RSA offering.

Hitachi ID Systems

Canada-based Hitachi ID Systems offers its Hitachi ID Identity Manager as a software solution or hosted in the cloud. It is one of the most affordable IGA solutions for managing employees, contractors and business partners. The product is a good option for IT buyers who are looking for a flexible IGA solution that is simple to deploy and has strong support for policy-based administration.

Developments in the last 12 months include collaborative certifications. This is where multiple users can work on the same access certifications at the same time, and detection of account or group name changes on target systems. The largest customer vertical is banking, securities and insurance, which accounts for a quarter of the business, followed by manufacturing and natural resources, and education. The majority of its customers are in North America, with Europe being a distant second.

Strengths

- Hitachi ID Systems continues to be one of the lowest-cost providers of IGA software.
- New customers can profit from Hitachi ID Systems' preconfigured reference implementations for several common deployment scenarios to accelerate deployments and lower time to value.
- Clients comment positively on Hitachi ID Systems' support and maintenance and like the solution's compliance capabilities, especially around access certification.
- The product benefits from an efficient data model that pushes significant processing to the database tier, which makes it one of the highest-performing products.

Cautions

- The product provides a generous collection of built-in reports, but a report designer is not included. Custom reports are written as Python scripts, requiring special skills. Analytics, including role mining, are delivered via reports and are not interactive.
- The company is limited by its lack of marketing investment and subsequent recognition, which causes potential buyers to overlook it.
- Gartner has received some client complaints regarding inconsistency around the responsiveness of Hitachi ID Systems' sales and support process.

IBM

U.S.-based IBM offers the IBM Security Identity Governance and Intelligence (IGI) suite as software that consists of several modules that can be licensed separately. IBM also offers a separate cloud access management solution with light IGA called IBM Cloud Identity Service (CIS). Clients can complement IBM IGI with IBM Cloud Identity Service as

part of a hybrid IGA deployment model to gain more cloud provisioning capabilities. For evaluation of this Magic Quadrant's product/service score, we considered only IBM IGI.

IBM IGI is a good choice for large organizations with complex processes that need a flexible product with good automation and governance capabilities and organizations that are buying into the IBM Security Immune System vision. Milestones in the past year for IBM IGI include audit case management and added integration for data access governance with the IBM Security Guardium solution.

One-quarter of IBM's customers are in banking, securities and insurance, with the rest evenly distributed across all other industry verticals. IBM's IGA customers are widely spread across the globe.

Strengths

- IGI's business activity model uses application-specific content for linking business processes and controls with entitlements, which has become a valuable differentiator for customers looking for more application-specific risk intelligence than that provided by most other IGA solutions.
- IBM has become much more aggressive with discounting over the last year, making it likely to be one of the lowest-cost providers in competitive evaluations.
- IBM is dedicating efforts to build a deeper integration with native ServiceNow plug-ins that extend much of the access request and full audit trail functionality to ServiceNow. This goes beyond the API-based or HTML frame-based integration that other IGA vendors have.
- The vendor's large, global presence allows products to be sold and supported effectively virtually everywhere.

Cautions

- Customers complain about product complexity and the upgrade process.
- Customers' comments about the solution's user interface are negative.
- IGI relies on an inefficient data model that requires all processing to be performed in the application server. This imposes performance penalties that limit IGI's abilities to deliver advanced analytics when managing large user populations.
- IBM's product strategy is mostly focused on integration with other products and building out its cloud IGA offering, rather than improving the features and architecture of IGI — its flagship IGA product.

Micro Focus (NetIQ)

U.K.-based Micro Focus offers its Identity Manager and Identity Governance (formerly Access Review) software solutions with several optional modules. Some of the vendor's partners offer the solution as a managed service. At the time of this research, Micro Focus did not offer an IGA as a service, but the vendor said it plans to announce the availability of a SaaS-based offering. Micro Focus' products should especially appeal to organizations that are looking for a flexible solution that provides the ability to scale over time with strong automation and provisioning capabilities.

In September 2017, Micro Focus merged with Hewlett Packard Enterprise's (HPE's) software business. This led to a delay in planned enhancements to focus on a new longer-term roadmap that integrates the vendor's Vertica analytics engine into the offerings. At the same time its product strategy was impacted by the merger, Micro Focus added several execution improvements around its product and customer satisfaction. In relation to last year, Micro Focus shifted from the Visionaries quadrant to the Challengers quadrant.

Developments in the past year include role analysis and mining — a feature that was long outstanding — and analytics-based decision support and risk scoring using static identity data. It introduced crowdsourcing for enhancement requests in its user community. Customers are evenly distributed over multiple verticals, led by healthcare; banking, securities and insurance; and education. Micro Focus' customers are evenly spread across the globe.

Strengths

- The addition of integrated role mining fills an important gap in what was otherwise excellent support for policy and role management provided by the Identity Governance product.
- Customers comment positively about the product's flexibility and powerful provisioning features.
- Micro Focus has a well-developed, worldwide channel network that provides local experience and helps to sell its products globally.
- The vendor's focus on IAM analytics and its strategy of aligning and integrating its IGA offering with its portfolio of adjacent analytics products are promising for clients looking for a risk-aware IAM solution that reduces certification fatigue and enhances productivity.

Cautions

- A stated key initiative by the new Micro Focus management team has been an increased effort on customer relations. However, many customers have not experienced the benefits of this strategy yet and continue to express frustration over issues such as annual license audit practices and limited options for training.
- Customers also complain about a la carte pricing for connectors. Micro Focus' pricing for some provisioning connectors for NetIQ Identity Manager is unique in the market and can escalate costs rapidly for some deployment scenarios.
- Some functionality overlap still exists between Identity Manager and Identity Governance. Customers migrating from one to the other should clarify feature and data overlap and the associated roadmap for the upgrade.
- Micro Focus must now fulfill its promises and deliver several new features on the previous roadmap after delays due to the merger with HPE's software business.

Microsoft

U.S.-based Microsoft offers IGA capabilities through a software solution called Microsoft Identity Manager (MIM) and an optional module called BHOLD that adds role management, analytics and access certification. MIM and BHOLD can be acquired stand-alone or as part of a cloud access management solution called Azure Active Directory Premium (which is also included in Microsoft's Enterprise Mobility + Security [EMS]).

Microsoft is a newcomer to this Magic Quadrant. In previous years, Gartner had not found MIM to be a viable IGA solution due to a lack of investment in the product and an unclear roadmap. However, Microsoft has since started to reinvest in its IGA offering and build new cloud-architected IGA capabilities. While Microsoft is building out these new capabilities, it points to its strategic partnerships with Omada, SailPoint and Saviynt for clients looking for more mature IGA capabilities. For evaluation of this Magic Quadrant's product/service score, we considered MIM, including the BHOLD module, and the cloud fulfillment capabilities of the Azure Active Directory platform. After the research collection of this Magic Quadrant had concluded, Microsoft announced the deprecation of the BHOLD component (https://docs.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016-deprecated-features) .

MIM will appeal to clients with an investment in EMS or Azure Active Directory Premium that have basic-to-medium complex IGA requirements, are willing to follow Microsoft's cloud strategy and are willing to wait for Microsoft to deliver updated IGA capabilities corresponding to current industry norms in the medium future. Clients with in-house experience of MIM or its predecessor Forefront Identity Manager (FIM) may also benefit from leveraging their existing knowledge to deliver basic IGA capabilities.

Strengths

- Customers that have subscribed to EMS get IGA features in combination with a rich portfolio of adjacent IAM capabilities. This makes the solution appealing to customers with basic IGA requirements that view the vendor as a strategic partner and are willing to grow into more mature IGA capabilities as Microsoft delivers them over time.
- Microsoft has a well-developed, worldwide partner network that provides local experience for MIM.

- Microsoft is building a significant customer base that is currently licensed for IGA capabilities through sales of EMS and Azure Active Directory Premium. This provides Microsoft with an opportunity to shape the market for cloud-delivered IGA over the next three years.

Cautions

- There have been few enhancements to functionality in Microsoft Identity Manager since the final release of Forefront Identity Manager 2010 r.2 in 2012.
- Significant configuration and even customization are needed to achieve standard IGA use cases with Microsoft Identity Manager 2016. This has resulted in numerous abandoned deployments after IAM leaders chose to use MIM because it was included at no additional cost with Azure Active Directory Premium or EMS.
- Clients should exercise caution when using MIM. Most of its capabilities — aside from its metadirectory and provisioning features — are likely to be replaced by new functionality that will be delivered from the cloud on the Azure Active Directory platform.

Omada

Omada, headquartered in Denmark, offers the Omada Identity Suite (OIS) as software or hosted in the cloud. The solution has multiple editions with different sets of functionality. OIS should appeal to organizations that require a flexible solution with strong reporting capabilities.

In the last 12 months, Omada also created a software development kit (SDK) for creating custom provisioning connectors and collectors, and the customer identity and access governance module that provides self-service for B2B and B2C identities. One-third of Omada's customers are within banking, securities and insurance, and one-fifth are in healthcare. The rest of its customers are evenly split across the remaining verticals. Its customers are predominantly in Europe and North America.

Strengths

- Omada continues to be highly rated by customers for its products, support and maintenance. Customers are very positive about the end-user experience and the ease of maintenance of the highly configurable product.
- The vendor has created a strong best practices process framework that can help customers streamline the deployment of its solution.
- Despite a slight price increase for the second straight year, Omada remains one of the best-value IGA software vendors.

Cautions

- Despite ramping up its international presence, a lack of brand recognition still causes Omada to be overlooked by potential buyers outside Europe.
- Gartner received some customer complaints on limited availability of Omada's professional services and some inconsistency around quality of Omada's system integration partners. Potential buyers are advised to closely vet implementation partners, get hard commitments for qualified staff and ask for references.

One Identity

U.S.-based One Identity offers Identity Manager as software. Several of One Identity's partners such as Core IT and Tieto also offer the solution as a managed service. A new cloud-architected identity analytics solution called Starling Identity Analytics and Risk Intelligence can complement Identity Manager or other IGA solutions to provide risk-based analysis on identity, access and usage information. Identity Manager is a good fit for companies requiring strong governance and SAP integration.

The company has crossed into the Leaders quadrant this year, following a year that saw strong execution coupled with significant improvements to its level of innovation, and product and sales strategy. Other developments in the last 12 months include an Office 365 connected system module and an operations support web portal for the administration

of the solution. One Identity's customers are predominantly in Europe and the U.S., and can be found across all major industry verticals.

Strengths

- Customers comment that the product is easy to use and customize, powerful and fast.
- Identity Manager provides superior policy and role management features. It has a rich role framework that supports numerous types of roles and dynamic rules with sufficient flexibility to control the behavior of how users are added and removed from roles.
- Identity Manager provides deeper integration with complex applications than most other vendors through "connected system modules" that leverage forms and reports to include additional application-specific context.

Cautions

- Customers complain about the limited availability of vendor professional services in a timely manner and support taking longer than expected (although the quality of technical support has been highly rated). This indicates that One Identity needs to ramp up its availability in these areas.
- Although Identity Manager provides an elegant end-user interface, its interfaces for administration are fragmented and continue to rely on a Windows application for some configuration activities.

Oracle

U.S.-based Oracle offers its Oracle Identity Governance (OIG) suite as a software solution. In addition, Oracle offers a cloud access management solution with light IGA services called Oracle Identity Cloud Service (IDCS). OIG is especially suited for organizations with complex processes that require flexibility in the product. Clients can complement OIG with IDCS as part of a hybrid deployment model to gain more cloud provisioning capabilities or use IDCS in lieu of OIG when IGA requirements are simple. For evaluation of this Magic Quadrant's product/service score, we considered only OIG.

Within the last 12 months, Oracle released version 12c PS3 of OIG that added features to significantly simplify operational aspects such as installation, application onboarding and upgrading of the solution. Oracle has IGA customers well-distributed across industry verticals and widely spread across the globe, which are supported by channel partners worldwide.

Strengths

- Oracle customers say the solution is very powerful and flexible to adapt to any situation. Customers also like the API enablement within the product.
- Oracle's global presence and global channel partners allow clients to find local skills for its IGA worldwide.
- The product benefits from an efficient data model that pushes significant processing to the database tier, which makes it one of the highest-performing products.
- Unlike most competitors, Oracle has focused significant development effort on improving the efficiency of application onboarding, which is one of the most important and time-consuming activities for IAM teams after initial deployment.

Cautions

- Customers point out that OIG is complex to implement, exacerbated by the fact that finding, training and retaining experienced in-house talent for Oracle's IGA product is difficult, raising requirements for long-term professional services.
- Customers comment negatively on OIG's user interface.
- A shift in focus of internal resources to work on IDCS combined with recent staff churn has caused some complaints regarding inconsistency of ongoing support and maintenance of OIG.

SailPoint

U.S.-based SailPoint offers a software solution called IdentityIQ with several optional modules, and a separate, cloud-architected IGA solution called IdentityNow. IdentityIQ and/or IdentityNow should appeal to organizations with a strong governance focus, although IdentityNow is not at the same functional level as IdentityIQ. Several of SailPoint's partners also offer a managed service based on IdentityIQ. For evaluation of this Magic Quadrant's product/service score, we considered only SailPoint IdentityIQ.

SailPoint completed an IPO in November 2017. In the past year, SailPoint added functionality expanding the integration of IdentityIQ with its SecurityIQ data access governance product and with other vendors' privileged access management (PAM) solutions. The majority of its customers are in banking, securities and insurance. The rest are distributed evenly among other verticals. SailPoint's customers are spread across the globe, with North America and Europe leading in terms of deployments.

Strengths

- SailPoint clients consistently note that the business user experience is a particular strong point of the solution, and that the configurability of the product simplifies deployments.
- A large partner network gives SailPoint momentum to sell and deploy its products worldwide. However, customers report inconsistencies in the ability and level of knowledge of integration partners, so it is prudent to get firm resource commitments and check references when choosing a system integrator.
- A strong messaging focus on identity enablement and generally favorable customer references are responsible for the strong awareness and brand recognition, and make SailPoint a commonly evaluated vendor.
- Although SailPoint's market share is dwarfed by several larger competitors, SailPoint continues to grow faster than the market due to the vendor's dominance in the midsize-to-large enterprise market.

Cautions

- Compared with previous years and to current market trends, SailPoint's innovation on IdentityIQ has slowed and is mainly focused on integrating with other products.
- The product is difficult to customize. It works best when organizations can deploy the solution by adapting to the way it is designed rather than trying to do extensive customizing. Customers report a lack of flexibility and complexity of extending the product to do tasks for which it was not designed.
- IdentityIQ relies on an inefficient data model that requires all processing to be performed in the application server. This imposes performance penalties on actions such as large access certification and batch jobs on large datasets, which requires careful tuning and horizontal scaling.

SAP

Germany-based SAP offers an IGA software solution consisting of SAP Access Control and SAP Identity Management. A separate cloud-architected IGA solution is also available through a combination of SAP Cloud Identity Access Governance and SAP Cloud Platform Identity Provisioning. The cloud-architected IGA solution can be used in lieu of the on-premises solution for clients that have more basic IGA requirements and are primarily looking to target cloud applications. However, this is expected to change with the introduction of the new Cloud IAG Bridge to add support for on-premises applications.

SAP's products are an excellent fit for existing SAP customers that can take advantage of its extensive and unequaled SAP application integration. For evaluation of this Magic Quadrant's product/service score, we considered only the combination of SAP Identity Management and SAP Access Control.

Other developments in the last 12 months include a cloud-based role designer and integration with SAP SuccessFactors. SAP's customers are distributed across many verticals, with utilities making up one-fifth of its customer base, and manufacturing and natural resources making up one-fifth.

Strengths

- SAP has made big strides with its SAP Cloud Identity Access Governance tool. It provides an attractive alternative to organizations that are hesitant to purchase SAP Access Control.
- SAP Access Control offers rich access rights and event analytics, including "what-if" analytics to support decision making related to cleanup activities.
- Using the full-featured SOD controls monitoring capabilities included with SAP Access Control, clients can gain deeper insight into complex business applications than with most other products in the IGA market.
- SAP provides the most informative profile views for users in SAP Access Control and SAP Cloud Identity Access Governance, providing not only information about entitlements but also relevant statistics.

Cautions

- SAP Identity Management provides built-in integration with SAP's HR applications, Human Capital Management (HCM) and SuccessFactors, but offers little support beyond that for typical identity life cycle scenarios, which increases deployment complexity.
- SAP's pricing practices are opaque. Gartner has observed wide variations in pricing offered to clients, especially for SAP Access Control. Gartner clients are encouraged to contact us for pricing reviews.
- A multitude of IGA products and services with significant overlap in capabilities and a lack of clarity on SAP's on-premises roadmap make it challenging for customers to choose the right combination.
- Its IGA offering prioritizes integrations with other SAP products, making SAP Identity Management and SAP Access Control only suitable for organizations with investments in SAP solutions.

Saviynt

U.S.-based Saviynt offers Saviynt Security Manager as a cloud-architected IGA service solution that can alternatively be delivered as a virtual appliance. Several modules are available to support application, data or infrastructure access governance for specific applications or environments, such as Oracle, SAP, Epic, Amazon Web Services (AWS), Microsoft Azure, Salesforce, Office 365 and others. The solution is a compelling option for organizations that are looking beyond traditional IGA for an integrated risk-aware approach combining access governance for applications, data and infrastructure across multiple environments, including the cloud, and that are willing to adopt new technology from a small vendor.

Saviynt crossed into the Leaders quadrant this year from its position in the Challengers quadrant last year. We have seen improvements in the vendor's product, and the vendor has an ambitious roadmap with a good history of executing on it. We have also seen improvements to Saviynt's vertical strategy, developing a vertical industry team, outreach to leading industry providers and industry-specific solutions. This was counterbalanced with a slight decrease in customer satisfaction, which is the main reason for a somewhat lower position in the Ability to Execute axis compared with last year.

Developments in the last 12 months include a just-in-time access escalation model for privileged access scenarios and a new analytics engine based on Elasticsearch. Saviynt's clients are predominantly based in North America, followed by a significantly smaller amount of customers in Europe and Asia/Pacific. Clients are spread across multiple verticals, with banking, securities and insurance leading, followed by manufacturing and natural resources, healthcare, and utilities.

Strengths

- Saviynt has the most fully featured IGA solution delivered as a service of any vendor reviewed in this Magic Quadrant.
- The vendor leverages a powerful analytics base to combine IGA with elements of data access governance (DAG), SOD controls monitoring and a cloud access security broker (CASB) in a single platform.
- Saviynt consistently places at or near the top rating for all product use cases evaluated.

Cautions

- After a period of accelerated growth, there are inconsistencies in execution and ability to support deployments. Some clients report mixed experiences with integration services provided by Saviynt and its integration partners. Clients should consider recruiting the help of vendor-neutral, business-oriented IAM consultant services in addition to the integration services from Saviynt and/or its integration partners, ask for references and get firm commitments for availability of skilled staff for integration services.
- Saviynt must prove that its DevOps-style continuous integration methodology can scale to support separate code trains (release environments) for some individual customers to offer flexibility to clients that want to run a customized version — an approach that has been problematic for other vendors in terms of support consistency and scalability.
- Saviynt has ambitious plans to expand globally, but it needs to build out the respective country organizations and ramp up its delivery capability to serve regions outside of North America and Europe.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant 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

Hitachi ID Systems comes back into this year's Magic Quadrant after having been dropped last year due to missing the elevated minimum revenue inclusion criterion.

Microsoft has been added this year as a result of the vendor starting to build new cloud-based IGA capabilities.

Dropped

No vendors were dropped since last year.

Inclusion and Exclusion Criteria

To qualify for inclusion, vendor organizations must:

- Have booked a total revenue of at least $22 million for IGA products and subscriptions (inclusive of maintenance revenue) for any period of 12 consecutive months (fiscal year) between 1 January 2016 and 30 September 2017, or be mentioned as a considered vendor for evaluation in 15% of Gartner inquiries in this market between 1 October 2016 and 30 September 2017.
- Sell and support their own IGA product or service developed in-house, rather than offer it as a reseller or third-party provider.
- Have sold their IGA product or service to customers in different vertical industries (vendors who only sell their product within a particular industry or vertical are excluded).

To further qualify for inclusion in the 2018 Magic Quadrant for Identity Governance and Administration, the vendor's IGA product/solution must offer:

- An integrated identity repository that masters information about people for whom access to managed information systems must be administered, along with the ability to support multiple identity life cycles to manage this information including synchronization with authoritative sources (such as HR systems) as well as administrative workflows.
- Tools for application entitlement discovery, mining, management and enrichment, including the maintenance of an entitlements catalog.

- Functionality to manage the linkage of identities with accounts and entitlements, including the ability to tell who has access to what and who is responsible for maintaining an account or entitlement.
- Tools to manage the end-to-end process of requesting access through business-user-friendly user interfaces by end users with approval workflows.
- Support for role-based administration across multiple applications, including governance over role engineering and administration as well as integrated role mining and role analytics to allow for replacement of direct entitlement assignments for users with role assignments.
- Facilities for specifying and enforcing policies such as those that govern automatic assignment (and removal) of roles and entitlements; visibility of roles and entitlements for selection in access requests; dependencies and incompatibilities between roles and entitlements; and so on.
- Support for specification and execution of access certification campaigns covering identities and entitlement assignments involving specified actors (e.g., managers and resource/application owners).
- Tools to reconcile data from target systems with IGA data for multiple targeted technical environments (e.g., Windows, iSeries, Unix/Linux, multiple applications and SaaS).
- Tools and connectors to automatically propagate changes to target systems (e.g., direct fulfillment or "provisioning"), as well as indirect fulfillment where changes are made using workflows or external processes (such as service tickets submitted through ITSM tools).
- Analytics and reporting of identities, entitlement assignments and administrative actions.
- Underlying architecture for the above, including connector architecture for data collection and fulfillment actions.
- Products must be deployed for use with customer production environments for purposes consistent with objectives of IGA.

Changes in Inclusion Criteria From Last Year

With respect to the 2017 Magic Quadrant inclusion criteria, the following has changed:

- The minimum revenue was raised to focus this research on the segment of the market that is most relevant across Gartner's customers. This means that a vendor must have more than roughly 1% market share by revenue to be included in this research. Alternatively, a vendor could qualify by being mentioned as a considered vendor for evaluation in 15% of Gartner inquiries in this market from 1 October 2016 through 30 September 2017.

Honorable Mentions

IGA is a mature market, with Gartner being aware of at least 19 other vendors that fulfill a significant majority of *technical* inclusion criteria used in this Magic Quadrant. The following vendors have credible IGA offerings, but did not meet the inclusion criteria for this Magic Quadrant:

- AdNovum (https://www.nevis-security.ch/en/products/nevisIDM.html) (Switzerland)
- AutoSeg (http://www.autoseg.com/) (Brazil)
- Avatier (https://www.avatier.com/) (U.S.)
- Beta Systems Software (https://www.betasystems.com/en/) (Germany)
- Brainwave (https://www.brainwavegrc.com/) (France)
- Deep Identity (https://deepidentity.com/) (Singapore)
- EmpowerID (http://www.empowerid.com/) (U.S.)
- E-Trust (http://www.e-trustsecurity.com/) (Brazil)

- Fischer Identity (https://www.fischerinternational.com/) (U.S.)
- ForgeRock (https://www.forgerock.com/) (U.S.)
- FSP (http://www.fsp-gmbh.com/en/software/org-identity-governance-and-administration-suite/index.php) (Germany)
- Identity Automation (https://www.identityautomation.com/) (U.S.)
- Imprivata (https://www.imprivata.com/caradigm-identity-and-access-management) (U.S.)
- iSM Secu-Sys (http://www.secu-sys.de/en/) (Germany)
- OpenIAM (http://www.openiam.com/) (U.S.)
- ProofID (https://www.proofid.co.uk/) (U.K.)
- Soffid (http://www.soffid.com/) (Spain)
- Systancia (https://www.systancia.com/en/) (France)
- Tuebora (http://www.tuebora.com/) (U.S.)

Free Open-Source Software (FOSS) Alternatives

Two options are available for organizations that are looking for a free open-source alternative, and are willing to either support the deployment themselves or contract a third party for support (see "Options for Open-Source Identity and Access Management: 2017 Update"):

- midPoint (http://www.evolveum.com/midpoint) is the most capable FOSS option for IGA, as measured by availability of features. It is based on a provisioning system with synchronization and reconciliation and a UI for end users that implements a shopping cart paradigm. midPoint features role-based access control (RBAC) using a hierarchical role catalog with fine-grained access control and delegated administration over role management. Access certification and basic segregation of duties controls monitoring is also supported. midPoint is licensed under the Apache License, version 2.0, and several vendors provide commercial support.
- Apache Syncope (http://syncope.apache.org/) is an open-source provisioning system maintained by the Apache Software Foundation. It offers many functions around user administration and provisioning, and has auditing, certification and reporting capabilities. Syncope is licensed under the Apache License, version 2.0. It has an active international developer community with critical mass. Tirasa (http://syncope.tirasa.net/) provides commercial support for Syncope.

Alternative Tools to Cover Some IGA Needs

Some organizations are using alternative tools, like the following, to fulfill a partial set of common IGA requirements:

- **Active Directory focus:** Organizations with use cases that are centered on the Microsoft environment may be able to use Microsoft-centric resource administration tools in lieu of IGA tools to manage identities, accounts and permissions within this restricted scenario. The following is a nonexhaustive list of vendors and products that, at the time of this writing, offered specialized tools for Microsoft Active Directory delegated administration: CionSystems' Active Directory Manager Pro, Imanami's GroupID, ManageEngine's ADManager Plus, Micro Focus' Directory and Resource Administrator, Namescape's rDirectory, One Identity's Active Roles, Softerra's Adaxes, Thycotic Group Management Server, Varonis, Visual Click Software's DSRAZOR, and Zohno's Z-Hire and Z-Term.
- **SOD control monitoring tools:** These are products that provide organizations with the means to analyze and manage risks associated with SOD conflicts, sensitive access and other types of policy violations for specific applications with complex, role-based authorization models, such as those from Epic, Infor, Microsoft, Oracle and SAP. These tools are generally composed of six key features: risk analysis, compliant provisioning, emergency access management, role management, access certification and transaction management (see "Market Guide for

SOD Controls Monitoring Tools"). However, SOD control monitoring tools lack identity life cycle components and the ability to work with a broad range of applications and directory services used in most environments.

- **IT service management (ITSM) tools:** These offer service catalogs and support access request fulfillment by simplifying both the documentation of orderable IT service offerings and the creation of a portal that enables end users and business unit customers to easily submit IT service requests (see "Magic Quadrant for IT Service Management Tools"). This portal includes space for clear information on service pricing, service-level commitments and escalation-/exception-handling procedures, as well as how to request IT services. IT service catalog tools also provide a process workflow engine to automate, manage and track service request fulfillment. Some clients are using this technology to provide self-service access requests and automate fulfillment. However, unlike IGA tools, ITSM tools do not manage identity and entitlement life cycles nor implement governance capabilities.
- **Consumer-focused IAM:** While many vendors in this Magic Quadrant sell their IGA solutions to support consumer IAM use cases, a number of vendors deliver distinct products and services focused on managing consumer identities (see "Finding the Right Consumer IAM Products, 2016 Update").

Evaluation Criteria

Ability to Execute

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

- Identity life cycle
- Entitlement management
- Access requests
- Workflow
- Policy and role management
- Access certification
- Fulfillment
- Auditing
- Reporting and analytics
- Ease of deployment
- Scalability and performance

Overall Viability (i.e., business unit, financial, strategy and organization): Viability includes an assessment of the organization's overall financial health, as well as the financial and practical success of the business unit. It views 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. Factors include:

- Revenue growth and trends in revenue mix (e.g., license sales, maintenance, subscriptions and services)
- Customer acquisition and retention
- Importance of IGA product and business unit in overall organization

Sales Execution/Pricing: The organization'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. Factors include:

- Growth in license sales
- Value (i.e., price relative to product quality)

Market Responsiveness/Record: The 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 to changing market demands. Factors include:

- Meeting customer needs in different use cases
- General responsiveness within the past 24 months
- Responsiveness to market developments of other adjacent technologies

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This mind share can be driven by a combination of publicity, promotional, thought leadership, social media, referrals and sales activities. Factors include:

- Marketing activities and messaging
- Visibility
- Brand depth and equity
- Buyer understanding

Customer Experience: Products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions with technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups and service-level agreements, for example. We are specifically focused on those that add value to the client (rather than adding upsell capabilities to the vendor). Factors include:

- Customer relationships and services
- Customer satisfaction
- Reference customer feedback (if reference customers are provided)
- Other Gartner client feedback (including information gathered in inquiry and from customer interactions, customer surveys and other Gartner data sources [such as Peer Insights]).

Operations: The ability of the organization to meet goals and commitments. Factors considered are quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. Additional factors include:

- People
- Organizational changes
- Processes

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Product or Service	High

Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (February 2018)

Completeness of Vision

Market Understanding: The ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market listen to and understand customer demands, and can shape or enhance market changes with their added vision. Factors include:

- Understanding customer needs
- Identifying market trends and changes

Marketing Strategy: Clear, differentiated messaging consistently communicated internally and externalized through social media, advertising, customer programs and positioning statements. Factors include:

- Communications and brand awareness
- Use of media
- Marketing organization

Sales Strategy: A sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication. Partners should extend the scope and depth of the vendor's market reach, expertise, technologies, services and customer base. Factors include:

- Understanding buyers
- Sales organization (including use of partnerships, value-added resellers [VARs] and system integrators [SIs])
- Channel revenue

Offering (Product) Strategy: An approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements. Factors include:

- Meeting customers' selection criteria
- Meeting the needs created by the Nexus of Forces
- The vendor's development plans, participation in IGA and adjacent standards development

Business Model: The design, logic and execution of the organization's business proposition to achieve continued success.

Vertical/Industry Strategy: The strategy to direct resources (e.g., sales, product and development), skills and products to meet the specific needs of individual market segments, including vertical industries. Factors include:

- Applicability of offering to specific vertical industries or sizes of organizations
- Strategy

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes. Factors include:

- Foundational, distinguishing technical and nontechnical innovations made over the course of the product
- Recent technical and nontechnical innovations introduced since October 2015
- The vendor's roadmap over the next few years
- Culture
- Past innovations made 12 to 24 months ago

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its home or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market. Factors include:

- The presence of the vendor in international markets
- Trends that support the spread of the vendor's products and services into other geographies
- Strategies for expanding global reach
- Multilingual support and availability of support and services in distinct geographies

Table 2: Completeness of Vision Evaluation Criteria

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

Source: Gartner (February 2018)

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 services. 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 regarding 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 use 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

When people think about IAM, IGA tools are often one of the first things that come to mind. In fact, some clients still use the term "IAM tool" to actually refer to identity governance and administration. However, there are multiple distinct technologies to support an IAM program, out of which IGA is typically the most expensive as well as the most difficult to implement and get right. This is in part due to the intersection of many distinct identity life cycle processes and the resulting challenges to change established business process to streamline implementation of a tool to derive business value early and often. Another reason IGA tools tend to be associated with challenging deployments is because of the multitude of systems and applications that must be supported.

Careful Planning Is Essential to Successful IGA Adoption

IGA tools are expensive to adopt — not just because of acquiring the solution, but also due to the significant costs for internal work and professional services to deploy the tool. This makes IGA tools difficult to "rip and replace," requiring careful planning around tool selection.

IAM leaders often jump, or are pushed, into IGA tool acquisition without being fully aware of the organization's detailed requirements or how new tools fit within an overall IAM architecture. To ensure maximum success, use Gartner's recommended practices for choosing an IAM vendor described in "Buyer's Guide for Choosing an IAM Solution," and make IGA buying decisions only within the framework of a formal IAM program (see "Best Practices for IAM Program Management and Governance").

IGA tools require careful planning in terms of how and when distinct functional capabilities are deployed. A governance-first, automation-later strategy, as described in "IGA Best Practices: Governance First, Automated Provisioning Later," has been proven to realize business value early and often.

Selection Criteria

Organizations should consider IGA products from vendors in every quadrant of this Magic Quadrant based on their specific functional and operational requirements. Placement of a vendor in this Magic Quadrant does not directly indicate which vendors have the most mature products or which vendors receive the best customer feedback. In fact, some of the IGA tools that receive the highest product scores in the associated Critical Capabilities research come from vendors outside the Leaders quadrant.

Product selection decisions should be driven by several factors, including:

- Does the vendor sufficiently address my requirements in terms of the required technical capabilities? Use the associated Critical Capabilities research to evaluate how well vendors support specific functional capabilities that are most important to your organization. Using the interactive version of the Critical Capabilities to insert your own weightings can generate a customized snapshot that you can use to build an initial shortlist.
- What is the total cost related to deploying the tool? Keep in mind that the cost for deploying and integrating IGA tools is generally correlated with the purchase price — a general rule of thumb is to assume that the typical first-year deployment of IGA software usually costs 50% to 200% of the three-year software cost in professional services.
- What is the estimated length of time needed to deploy the tools? Most IGA deployments take at least a year before functions such as access requests with approval workflow and automated fulfillment are fully realized. However, it is possible to derive value earlier in other areas, such as identity life cycle management, reporting and access certification. See "Toolkit: IGA Deployment Planning Model" for guidance on how find the optimal sequence to roll out distinct capabilities.
- Does the vendor have an efficient, working partner network that can quickly deliver specialized services around the deployment and operation of the IGA products? Smaller or more specialized vendors will generally have fewer, but well-trained, resources available. Large vendors will have an extensive partner network. Fast-growing vendors will actively build out their partner delivery channel, however the quality of integration partners may be inconsistent.
- Is support available locally, in the language of your organization and during regular business hours within your geographies? Also keep in mind that product engineering operations may be centered in a different time zone, which may cause a delay of a day or more to get a response for more complicated questions or bugs.
- How easy is it to integrate this technology into your existing infrastructure? Ask prospective vendors about the availability of data collectors and connectors for existing applications and infrastructure. A recent trend has shifted the focus of most vendors to support generic connectors that need to be adapted (sometimes requiring software development skills), rather than supporting a specific application or infrastructure.
- Will your IT organization be able to support it? Apart from the business administration side of IGA, there is a technical administration overhead in running IGA tools. This overhead can be reduced, but not eliminated, by choosing IGA as a service. However, ensure that the technology underlying the IGA tool is in line with what your organization can support. For example, many IGA tools are built using a Java or .NET architecture, including their generic connector framework.
- Can the vendor provide a tool that will offer best practices for you to adopt, or must you have a tool that allows easy customization to match your special processes? In general, customizations tend to be costly to implement and support and, thus, should be avoided, although they may be necessary in some specific cases. Some vendors offer rapid deployment frameworks, or reference builds, which is generally called out in the specific Strengths section.
- Following up on the last point: Will you require many customizations? This may be the case for a small number of organizations with very complex internal processes. In this case, look for comprehensive APIs (specifically using REST-based protocols) available in the solution that allows you to create customizations outside the product that should survive product upgrades without too much trouble.
- What is the footprint of the solution (if delivered as on-premises software), and how will your usage profile affect the performance of the solution? Some solutions have a very efficient data model that pushes heavy data processing to the database layer. This allows bulk operations to execute in a fraction of time compared with other solutions that do all data processing in the application layer. We have called this out in the respective Strengths and Cautions sections for vendors affected by this.

- Does this vendor help your organization deliver compliance with security policies and regulations more effectively? While every vendor has experience with common national regulations frameworks that drive IGA adoption, some vendors have special features or guidance framework for industry-specific regulation or policies.
- Does this vendor align with your organization's future roadmap of adopting technology or changing business requirements? Large megavendors such as Microsoft, Oracle, IBM and SAP tend to have IGA solutions that fit into their respective technology stacks. But, does this align with your future needs?

On-Premises or as a Service?

IGA tools exist primarily to manage on-premises applications. However, this is changing as the popularity of SaaS, platform as a service (PaaS) and infrastructure as a service (IaaS) is rising rapidly. To cater to the growing appetite for cloud-delivered services, vendors are offering one or more service-based solutions that include IGA either as a full-blown IGA solution or by delivering a subset of basic IGA services bundled into an adjacent technology.

Here are the differences, advantages and disadvantages of different IGA service solutions:

- **Cloud-architected IGA** is compelling for organizations that require basic-to-medium complex IGA capabilities that are mostly focused on managing on-premises applications. The advantages of this solution are rapid deployment, seamless and continuous software upgrades, and rapid availability of new features (sometimes on a weekly or biweekly release cycle). Vendors such as SAP and SailPoint offer an on-premises software solution plus a distinct and overlapping cloud-architected SAP solution that is less mature (at the time of this writing) than on-premises solutions and allows for little (if any) customization. Other vendors such as Fischer Identity (not rated in this Magic Quadrant) and Saviynt offer a cloud-architected IGA solution that can alternatively be hosted on-premises.
- **Cloud-hosted IGA software** is compelling for organizations that require medium-to-advanced IGA capabilities that are mostly focused on managing on-premises applications. The advantage of this model is that it shifts management of the infrastructure and upgrades to a service provider (which may be the software vendor or another organization). Customizations may be supported when agreed upon with the service provider, or customizations can happen by leveraging supported external APIs built into the product. This way, the actual running software hosted by the provider is not "touched." However, new features will only be available during regular updates, which happen infrequently (typically once or twice a year). Updates can be disruptive, even when managed by the service provider, and will require planning.
- **Cloud access management with light IGA services** are purpose-built offerings for delivering access management and single sign-on (SSO) services in the cloud with a limited set of IGA capabilities, mostly to manage accounts in other cloud services. These offerings tend to be too simplistic for most organizations that are specifically looking for an IGA solution. However, they may be acceptable for organizations that are primarily interested in access management and have only very simple IGA requirements that will evolve slowly over time.

At this time, however, it is difficult to buy only one solution that will fully address IGA requirements for on-premises applications and cloud applications:

- Although there is some variation among vendors, IGA software in general has limited cloud provisioning capabilities. It does cover some basics in terms of cloud connectivity such as connectors for cloud applications like G Suite, Office 365 and Salesforce. Although most IGA tools provide flexible connectors that could be used to integrate with APIs provided by cloud applications, such connectors have proven difficult for customers to maintain.
- IGA software tends to have no, or very limited, visibility into entitlement models from cloud applications.
- Vendors that deliver strong cloud-based access management (AM) capabilities, such as Okta, Centrify, Microsoft, Ping Identity and OneLogin, also have IGA capabilities, but they are lightweight and provide limited or no legacy on-premises application support, have no governance features and limited approval workflow, and are extremely limited with regard to customizations.
- To complicate matters further, many SaaS applications do not even have APIs for managing users and access, which makes development of provisioning connectors for these applications challenging.

Organizations looking to address both requirements (on-premises applications and cloud applications) will often require a hybrid IGA solution that combines different products that may be on-premises software and/or cloud services. One common solution is adding cloud access management services such as Microsoft Azure AD Premium or Okta to extend existing fully featured IGA tools.

Buyers looking to replace an existing IGA tool that are considering a replacement delivered as a service should also consider leaving the current tool in place (for the time being) and supplement its functionality through an additional IGA-as-a-service option. For example, role mining, SOD controls monitoring for complex business applications, certification and analytics that can be run in combination with an existing tool are available as subscription services by several vendors. An example is One Identity's Starling Identity Analytics and Risk Intelligence, although other vendors have told us they plan to launch similar service options in early 2018.

Market Overview

In this Magic Quadrant, we focused on vendors that had at least around 1% of estimated market share and a global reach. In the research for last year's IGA Magic Quadrant, we noticed increasing focus from vendors to offer service-based IGA solutions. This intensified in 2017, and we expect this trend to continue and user adoption of IGA to ramp up significantly over the next four years. At that time, we expect IGA as a service to be the predominant delivery model, notwithstanding hybrid deployments where on-premises IGA is used in conjunction with other IGA capabilities delivered from the cloud.

IGA cloud strategies differ between vendors:

- Megavendors such as Microsoft, Oracle and SAP are positioning their IGA-as-a-service offering as the primary solution to manage the respective vendor's enterprise application and ecosystem. There is often significant overlap between a vendor's on-premises IGA tools and IGA tools offered as a service, with the latter rapidly gaining maturity. In some cases, IGA offered as a service is sold as part of a more comprehensive IAM-as-a-service option with additional IAM capabilities such as directory services and access management. Expect these vendors to exert pressure to adopt their cloud-based IAM solution, even if you already own an existing IGA tool from another vendor.
- Other vendors offer IGA by lifting existing on-premises IGA capabilities to the cloud or creating an entirely new offering in the cloud. In some cases, vendors are offering partial, modularized capabilities such as identity analytics or certification as a service that can be used in conjunction with an existing IGA tool (from another vendor).
- Managed services are also available, either through third parties offering to run (and optionally host) an on-premises solution in the cloud or inside an organization's data center. Some IGA vendors will also do this upon request. Gartner does not consider this business model stable, and we foresee that this will ultimately be supplanted by vendor-based IGA as a service.

As to who makes the purchase decision for IGA, we have detected a slight shift in the types of roles involved. In previous years, CISOs tended to be influencers in this decision, and the actual purchasing decision was taken by the CIO, IT operations, or compliance and risk teams. Several vendors are reporting an uptick in CISOs being the primary decision makers.

The main drivers for IGA adoption fall into three categories:

- **Governanceand risk management** is driven by the desire to gain insight into risk pertaining to access, and by regulation and internal policies that establish control objectives to govern access to systems, applications and data. Effectively, the requirement is to establish tight control over accounts and access, and ensure that access is granted only as needed (for example, by applying procedural controls such as approvals and automatic controls such as policies). Additionally, monitoring accounts and access ensures visibility into the level of access, why it was granted and whether it is still needed (for example, by using procedural controls such as certification or automatic controls involving analytics). Monitoring will also identify possible violations (for example, orphan accounts or rogue accounts that were created directly in target systems without passing through an approved process).
- **Efficiency** saves time and money by streamlining the granting and removal of access. Automatic fulfillment, also known as provisioning, will save time otherwise spent in manual processes. Self-service access requests allow users to ask for access and can save time of IT operations and help desk staff.

- **Business enablement** provides additional value from IGA solutions by facilitating a business to run faster or enable new business processes. One common example is digital transformation as enterprise systems and business processes are extended to business partners, which requires a focus on managing an increased risk surface. IGA tools can also enable supply chains by managing B2B identities and access, and enable Internet of Things (IoT) or enterprise mobility initiatives by managing the relationship between people, devices and things.

In the last year, we have noticed the following trends that have affected, or evolved, the classical drivers mentioned above:

- The use of **robotic process automation** (RPA). This is driving new requirements on IGA tools. Some vendors, such as SailPoint and Saviynt, have introduced special features to govern bot access to a variety of systems and applications, and manage the linkage and life cycle between a bot and human users responsible for them. In addition, some vendors such as Saviynt are using RPA to facilitate automatic fulfillment (provisioning) to applications and systems that do not offer a programmatic provisioning API. In addition, Oracle is developing a chatbot specifically designed to assist in IGA processes by providing an alternative way to interact with users (see "IGA, RPA, and Managing Software Robot Identities").

- Most vendors have done significant efforts to open up their IGA solution through **REST-based APIs** that can be leveraged to integrate IGA solutions with other technology without requiring proprietary integration. Examples of how these REST APIs are used include ITSM, PAM, and user and entity behavior analytics (UEBA) integration. This allows other applications to trigger IGA processes or calls external components from within the IGA tool to support specialized processes or workflows.

- An increased focus on **threat protection,** including insider threats, is driving IGA products to mature by providing more value to organizations wanting to improve their security posture. They accomplish this by providing better and faster security incident detection and response capabilities in addition to the classical IGA drivers of support for compliance and business enablement. In addition, continuing integration of IGA with **user and entity behavior analytics** capabilities allows for a more intelligent, real-time detection and response capacity. This trend has accelerated over the last year. Typically, use cases are the initiation of remedial actions in IGA tools (such as an instant lockdown of an account or an unscheduled recertification of a user) when certain events are triggered, and many vendors can already support these use cases. Vendors with multiple security products, such as Core Security, IBM and Oracle, have also staked out their identity-driven security vision that leverages the synergy between those products.

- The state of the art and adoption of **analytics** is continuing. A big problem is **certification fatigue,** where people tasked with access approval approve or certify many requests without paying much attention to what they are approving. Also known as "rubber stamping," this can cause a variant of the "watermelon problem," where dashboards look green because everything has been approved, but the situation is actually red because there can be no faith in the quality of the approval process. Access certification methods using procedural controls are labor-intensive, and the more burden this places on business users, the more error-prone they become. Applying analytics to help in defining policies to automatically grant common patterns of access is an evolution of role mining that reduces manual effort, saves time and has the potential to eliminate errors. Analytics can also help by adding support for advanced risk analysis, fine-grained SOD analysis across the spectrum of corporate business systems with complex authorization models (such as ERP, CRM and electronic health record [EHR] products), and decision support for procedural controls such as approvals and certifications.

- Following up on the issue of **certification fatigue,** Micro Focus has added functionality to its access certification mechanism recently to capture metrics such as time spent on reviewing access for a particular request to try to catch cases of rubber stamping.

- IGA solutions in general are complex to deploy because they integrate with many target systems, are susceptible to data quality issues and require a tight integration with an organization's processes (which, to start with, are very often focused on manual procedural controls that are not efficient to automate). Apart from offering cloud-based IGA services, several vendors are continuing to make efforts to **alleviate complex deployment** and upgrade processes with virtual-appliance-based models and now even container-based deployment scenarios (e.g., One Identity). Of particular interest are enhanced application onboarding frameworks that focus on features to rapidly

improve data quality and rapid connector frameworks. In addition, several vendors such as Omada and RSA have issued standard process guides to accelerate deployments and time to value.

- Similarly, a few vendors are providing **libraries of workflow templates** to better fit common business processes, thereby reducing startup cost/time and simplifying customization. Some of those vendors are taking it a step further and providing a set of **reference builds** that brings together workflow templates and user-experience elements to produce a specific configuration of their product that is more closely aligned with the needs of the customer.

- Due to **user experience** being an important selection criterion across a range of business use cases, most vendors have significantly re-engineered their IGA business user interfaces, while other vendors are still catching up. Virtually every vendor has called this UI re-engineering out as something they either did or are still doing.

- Similarly, many vendors now feature **mobile** apps or special mobile web interfaces to cater to targeted business requirements such as approval processes, access requests and certifications, continuing a trend that we noticed over the last two years.

- Most vendors have also integrated with **IT service management tools** (especially ServiceNow) in combination with an IGA product. The most common scenario is to use ITSM tools for manual fulfillment (when a change gets triggered by IGA as a service ticket). Some clients are also looking at using ITSM tools as the front end for access requests. Some vendors have invested in bidirectional integration with ITSM tools, as well as exposed internal IGA services via APIs to facilitate this integration. The latter type of integration is not without complications due to the lack of entitlement catalog context available to the ITSM tool for making access requests. An example of a vendor that has made strides there is IBM, a company that provides a plug-in that makes the entitlement catalog available from ServiceNow. For detailed guidance, see "Integrate IAM With ServiceNow or BMC for Streamlined Business Services."

- Governing access to **unstructured data** is driving interest in integration of IGA with **data access governance** products, such as those from STEALTHbits Technologies, for more mature organizations. Several vendors, such as SailPoint, Micro Focus, One Identity and Saviynt, already have DAG products; others are partnering with DAG vendors or are in discussions with potential partners. However, since last year, SailPoint has deprecated its integration module with STEALTHbits, and Gartner has received customer feedback indicating pressure from SailPoint to sell its own SecurityIQ product instead. IBM stands out for integrating not only with STEALTHbits, but also with its own Guardium product line to include structure data. Since DAG tools provide important context, their inclusion will be important for organizations looking to make use of security intelligence to improve their detection and response capabilities.

- The emergence of cloud identity stores and cloud directories **for consumer identitiesmanagement** use cases has put pressure on IGA vendors to keep their solutions competitive in terms of scalability, performance and pricing for those use cases. Consumer identity management is different from workforce-focused IGA — solutions focused on the latter, such as those covered in this Magic Quadrant, have many features and capabilities that are not needed for consumer IAM. Most IGA vendors are reacting to this pressure by aggressively discounting for external identities such as consumers, while others are offering special editions of their products for external identity management (see "Finding the Right Consumer IAM Products, 2016 Update"). Upcoming privacy regulation in the EU (General Data Protection Regulation [GDPR]) is driving vendors to offer specific guidance or new features to address new regulatory requirements. Some examples are Atos, which has added consent management and privacy-by-design features into its IGA product, and Omada, which recently released new "Customer Identity and Access Management" functionality.

- Virtually every IGA vendor now supports the **System for Cross-Domain Identity Management (SCIM)** standard for SaaS provisioning. Several vendors are using SCIM internally in the backbone of their connector framework or offering connector development kits that leverage SCIM. SailPoint and other IGA vendors are involved in a move to standardize a SCIM extension (https://tools.ietf.org/id/draft-grizzle-scim-pam-ext-00.html) for privileged access management.

- **Integration between IGA products and PAM products** is continuing rapidly. Virtually all IGA vendors covered in this Magic Quadrant support out-of-the-box integration with several popular PAM products. One Identity and SailPoint have created specific privileged account governance extensions; other vendors are leveraging existing functionality

to track administrative entitlements. Some vendors such as CA Technologies and Hitachi ID offer out-of-the-box integration with their own PAM solutions only.

Several vendors this year went through significant changes in and restructuring of their operations due to acquisitions, initial public offerings and investments. Examples include:

- "Imprivata Acquires Identity and Access Management Business of Caradigm" (https://www.imprivata.com/company/press/imprivata-acquires-identity-and-access-management-business-caradigm)
- "Hewlett Packard Enterprise Completes Spin-Off and Merger of Software Business With Micro Focus" (https://globenewswire.com/news-release/2017/09/01/1106512/0/en/Hewlett-Packard-Enterprise-Completes-Spin-Off-and-Merger-of-Software-Business-with-Micro-Focus.html)
- SailPoint completed its initial public offering and is now a publicly traded company (http://www.nasdaq.com/markets/ipos/company/sailpoint-technologies-holdings-inc-952413-85050)

In 2017, Gartner estimated the market size for IGA to be $1.75 billion, with an annual growth rate of 9.4% from 2016 to 2017 ($1.60 billion to $1.75 billion) (see "Forecast: Information Security, Worldwide, 2015-2021, 4Q17 Update"). The most important market trend this year has been an approximately 10% decrease in license costs as SailPoint's shift to a focus on growth has forced vendors to respond with more aggressive discounting to win competitive deals. Total cost of ownership (TCO) continues to be a focus for client scrutiny for the majority of clients seeking replacements for existing products. This suggests that TCO is a primary reason for making a switch.

Evidence

The following sources were used in the creation of this research:

- Gartner client interactions.
- A comprehensive vendor survey that aligned with the evaluation criteria.
- Phone interviews with, and online surveys completed by, vendor-provided references and customers of vendors identified by Gartner.
- Feedback from Gartner Peer Insights.
- Secondary research services to support the overall viability evaluation criterion.

[1] Based on the review of 24 statements of work and other proposal documents for IAM professional services between April 2016 and September 2017.

Note 1
Identity Life Cycles

IGA systems support several independent and distinct identity life cycles. The four most common patterns are:

- **Authoritative source:** This is the classic identity life cycle pattern where the IGA tool is integrated with an external system that encapsulates life cycle processes, such as HR, vendor management or student information systems.
- **Sponsorship and expiration:** These identity life cycles typically cover nonemployees (that is, those who are not covered by HR systems or external processes, like contractors or vendors). A sponsor requests temporary authorization (limited in time and subject to a maximum threshold, typically between 60 and 120 days), which can be extended upon request.
- **Delegated administration:** When there are vendors or customers where numerous individuals from those business partners will require access, authorized personnel from the business partner act as sponsors for the creation and maintenance of identity information for people who are working with the organization on behalf of the business

partner. As with the sponsorship-and-expiration pattern, either expiration dates or periodic recertification should be used to close the loop for this type of life cycle.

- **Self-registration:** When consumers need to interact with an organization's website in a way that requires personalization, they are generally required to create some kind of account. This identity life cycle pattern usually is reserved for access scenarios where there is no reason to remove access in the future, such as when there is no definite end to the relationship.

See "IGA Best Practices: Establish an Identity Perimeter With Identity Life Cycle Processes" for more information about these basic four identity life cycle patterns.

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 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.