Magic Quadrant for IT Vendor Risk Management

Published: 28 April 2016

Analyst(s): Christopher Ambrose, Joanne Spencer, Edward Arthur Weinstein

The market for IT VRM software exists to enable the assessment, monitoring and remediation of risks arising from the use of IT vendors and IT service providers. Gartner’s Magic Quadrant on this small but growing market evaluates 12 vendors to help you in your vendor evaluation process.

Strategic Planning Assumption

By 2019, the need for transparency into operational and security activities within a vendor’s value network (including subcontractors) will drive demand for vendor security, as well as risk management solutions and services, by 30%.

Market Definition/Description

IT vendor risk management (VRM) is the process of ensuring that the use of external IT service providers and other IT vendors (third parties) does not create unacceptable potential for business disruption or negative impact on business performance. IT VRM solutions support enterprises that have to assess, monitor and manage their exposure to risks arising from their use of third parties, which provide IT products and services or have access to enterprises' client information. Many solutions' capabilities now extend to identifying, assessing and tracking a vendor’s subcontractors (or fourth-party relationships), a feature that is increasingly important to enterprises.

High-profile failures of IT service providers, increasing rollouts of enterprise risk management programs and third-party access to regulated information are contributing to the demand for IT VRM solutions. Still, however, the biggest driver of VRM is regulatory requirements to address vendor risks, vendor performance, and mandates for the risk monitoring of third parties that can access personal data (such as payment card and protected health information). These mandates include U.S. state-level data breach notification laws, the Payment Card Industry (PCI) standard, privacy and data protection regulations worldwide, and industry-specific regulations in the banking, financial services, healthcare and telecom sectors.

The basic concept of IT VRM is the same as that of supplier risk management (SRM). The difference is that, in the case of IT VRM, the risks are associated principally with the "logical" or information supply chain rather than the "physical" supply chain, which is associated with tangible
commodities, supply chain services or manufactured goods. Naturally, there is some overlap in the
types and classes of data needed for IT VRM and SRM — for example, data on the financial
strength of vendors and geopolitical (or country) risks is common to both — but there are also many
differences. SRM must address the risks associated with companies that provide or manage
physical goods and physical infrastructure, while IT VRM must address the risks associated with
third parties that access, provide, or manage information assets and IT infrastructure. There are, of
course, physical assets within IT infrastructure, and, conversely, there is often controlled information
associated with the physical supply chain. However, in general, IT VRM focuses more on the risks
associated with logical assets, information governance and IT controls than the risks associated
with physical supply chain assets.

Although this Magic Quadrant focuses only on the featured vendors’ IT VRM capabilities, many of
these vendors — like others in this market — also have solutions for broader vendor and third-party
risk management.

IT VRM solutions often include abilities in the following areas, which we considered when evaluating
the vendors:

**Access and user controls:** This area concerns the ability to provide roles for personalized access
to an IT VRM application, and to assign relationships between job roles and individuals, and risks
and controls.

**Assessment (vendor risks):** This area concerns the ability to categorize vendors and/or their
services and contracts into different tiers of risk. It includes customizable capabilities to support
methodologies for the detailed assessment of risks associated with services and contracts; the
ability to assess the impact of vendor risks against compliance obligations; and qualitative and
quantitative analytical tools to assess and prioritize risk, as well as discover relationships and
patterns. Also included are templates and frameworks designed to support specific mandates (such
as those of the PCI and the Gramm-Leach-Bliley Act) and any shared content, including a database
of vendor risk assessments or scores that can be used by multiple customers. Additionally, this area
embraces the ability to create a risk register that includes a description of risks and their metrics
(from a business perspective) and maps them to controls, owners, remediation actions, vendors,
business entities, performance metrics and others.

**Collaboration:** This area concerns support for users to work together, communicate and share
information on vendor risks and remediation. Included are email integration, document sharing and
the ability to have multiple team members work on documents together.

**Contract management:** This area concerns the ability to support the development of contracts and
the ongoing monitoring of delivery against them. Although full contract life cycle management
functionality is not required, an IT VRM solution does need to have, at a minimum, an ability to
collect and track key contract data and services associated with a vendor, as well as the ability to
assess the risks and controls associated with each contract and service.

**Control assessment and monitoring:** This area concerns the ability to assess the effectiveness of
controls and carry out ongoing monitoring of vendor risks. It also includes process management
that, at a minimum, supports the workflow for the IT VRM solution’s other functions, such as
exception management and reporting. Advanced abilities include modeling and simulation, the creation of executable processes for data collection, and the development of rules for risk monitoring and control enforcement.

**Exception management:** This area concerns the ability to manage vendor risk exceptions in relation to control requirements, the compensating controls to mitigate risks, and periodic reviews of whether exceptions are still required.

**History:** This area covers the ability to see the IT VRM status of an earlier time, such as a past quarter or year.

**Remediation management:** This area concerns the recording of action plans to identify control failures and other IT VRM deficiencies, and to track those plans to fulfillment.

**Third-party content delivery:** This area concerns such examples as news feeds, ownership structures, liens, safety violations, financial performance, risk-related alerts and risk ratings.

**Vendor performance management:** This area includes the ability to collect performance data and assess it against expected service levels and deliverables.

**Vendor profile management:** This area includes the ability to import vendor and related contract (engagement) data from other systems, or to input them manually; the ability to collect and organize intelligence about vendors; the ability to manage vendor documentation and other content; and vendor self-service capabilities that enable vendors to maintain and update information themselves.
Magic Quadrant

Figure 1. Magic Quadrant for IT Vendor Risk Management

Vendor Strengths and Cautions

Allgress

Allgress, a governance, risk and compliance (GRC) solution vendor founded in 2008, is based in Livermore, California. Its solution is based on its broader GRC platform, which includes IT VRM
capabilities. It can be delivered as SaaS or on the customer’s premises. Allgress' primary industries are healthcare, financial services and retail in North America. It sells primarily to information security, compliance and risk management departments.

**Strengths**

- Allgress’ risk assessment and monitoring capabilities can be quickly deployed, often with minimal configuration or customizations.
- Allgress has a simplified module-based pricing model, or pricing based on customer size, which scales adequately for its targeted market of large enterprises.
- Allgress' size, agility, pricing model and rapid deployment make it a good option for midsize enterprises.

**Cautions**

- Allgress' solution, while adequate when performing the fundamental functions clients expect, is not as extensive as some of its competitors’ solutions.
- Allgress lacks the prebuilt connections to common third-party content providers (for example, Dun & Bradstreet, LexisNexis and so on), and, while this is not a critical issue, an increasing number of enterprises are looking for third-party content feeds.

**Brinqa**

Brinqa is an Austin, Texas-based risk management vendor that was founded in 2008. Its product strategy is to deliver a broad risk management and analytics platform, of which the Vendor Risk Management application is a component. Brinqa's Vendor Risk Management offering is available as a SaaS subscription — either directly or resold through partner companies and solution providers — and is primarily in use in the financial services, retail and healthcare industries.

**Strengths**

- Brinqa has a simple pricing model based on named users, with discounting applied for multiple-year contracts, as opposed to other module-based or assessed-vendor-based pricing. In addition, Brinqa supports role-based access and budgeting.
- Brinqa provides a lower-cost option relative to its competitors, which makes it an attractive offering for midsize enterprises that are challenged to fund point solutions.
- Prebuilt integrations and connectors, and support for third-party content providers and standards (SIG, OCIL), allow for assessment and scoring based on internally collected surveys and externally accessed vendor information.
Cautions

- Setup and administration of the Brinqa solution has been relatively complex; however, Brinqa has added new features to reduce configuration efforts, and allows "superusers" to develop their own content.
- Client references were limited in the number of active implementations, with 75% of Brinqa's references in development versus in production (however, Brinqa did indicate that approximately 75% of its IT VRM customer base is in production).
- Although Brinqa is growing, it is still one of the smaller vendors evaluated, and its scalability to larger environments is unproven.

EMC (RSA)

RSA, The Security Division of EMC (which is based in Hopkinton, Massachusetts), offers RSA Archer Vendor Management. Its broad GRC platform includes IT VRM capabilities. Clients can maintain IT VRM, contract and vendor profile data, as well as performance management, remediation and assessment data. RSA Archer Vendor Management is targeted to large enterprises.

Strengths

- RSA Archer remains the largest and one of the most comprehensive IT VRM solutions in the market, and has the ability to scale for large clients that have significant numbers of vendors to assess and monitor.
- RSA Archer's tool is relatively mature in a fairly new but growing and dynamic market. Many of its customers have been using the IT VRM module for a number of years, which is affording Archer insight into changing customer and market needs.
- RSA Archer holds a number of client conferences and events throughout the year, which affords it the ability to closely track and respond to the requirements of its customer base.

Cautions

- Some customers are looking for more transparency in pricing models. At the end of 2015, RSA Archer released new Use Case-based pricing models that are designed to improve clients' ability to select the right solution sets, and, therefore, better align their pricing models to the maturity and specific IT VRM needs of their customers.
- Some references still view RSA Archer's workflows and user interface (UI) to be complex and nonintuitive to the casual or infrequent business user, and those users who regularly utilize the tool need a deeper knowledge of its processes and workflows in order for it to be effective. However, RSA Archer v.6.0 was released in 4Q15, after research for this Magic Quadrant was concluded, and one of its intentions is to improve usability.
- EMC, RSA Archer's parent company, is currently in talks to be acquired by Dell. Prospects and customers should monitor market intelligence that may point to Dell's acquisition strategy and plans for EMC's security businesses.
LockPath

LockPath is a GRC solution vendor headquartered in Overland Park, Kansas. In 2010, it launched its Keylight platform, which addresses VRM specifically with Compliance Manager, Risk Manager, Vendor Manager and the Advanced Analytics Add-on. These applications may be used in conjunction with the entire Keylight suite or on a stand-alone basis. LockPath predominantly offers solutions via the cloud, but also offers on-premises, hybrid and third-party-hosted models. LockPath targets clients based in North America and EMEA, and primarily in the healthcare and finance sectors. It serves organizations ranging from small and midsize companies to large enterprises in more than 15 industries.

Strengths

- LockPath's applications are configurable, with minimal customization reported by references, and have an easy-to-use UI.
- LockPath's application strongly supports the most common requirements in automating assessments, monitoring and tracking risks, and risk tiering and rating, and therefore is viewed as easier to use than some of its larger competitors.
- LockPath prices Keylight at one price across all modules, and offers prospective customers the option to try the solution without a financial commitment. These pricing and contracting models make Keylight an attractive option for midsize enterprises that may be challenged to get funding for point solutions.

Cautions

- Customers have often brought their own custom assessments, but LockPath has expanded its library of assessment questionnaires.
- LockPath remains one of the smaller GRC providers in this market, but is growing at a pace that requires continued investment in sales and operations. This will require rapid scaling and product enhancements to support growth.
- LockPath currently remains 100% focused on North America; however, it intends to slowly expand into EMEA in the near future.

MetricStream

MetricStream, founded in 1999, is a GRC solution vendor based in Palo Alto, California. Its IT VRM solution is built on its GRC platform and can be acquired with other GRC modules or separately. MetricStream's predominant delivery model is hosted SaaS, and it targets highly regulated industries. MetricStream's main geographic market is North America, but it also has some customers in Europe and the Middle East, and it plans to expand into Asia/Pacific.
Strengths

- MetricStream received a very high overall customer satisfaction rating across the largest number of references in this study, and was above the average score when the functionality of its solution was evaluated.
- MetricStream has a relatively mature offering, and is one of the largest providers with some of the longest IT VRM experience in this study, which has resulted in a range of capabilities and an intuitive UI.
- MetricStream continues to add functionality that expands its overall offering to help support clients across the life cycles of their vendor relationships, which include contract and performance management features.

Cautions

- While MetricStream improved from 2014, some references rated its professional services below the overall average; however, the vendor has increased its “FastTrack” implementation methodology to expedite implementations and reduce customizations.
- MetricStream’s application, while moving toward more “out of the box” deployments, is often customized (as is common in VRM applications). This creates some additional complexity, which can impact upgrades.

Modulo

Modulo is a global provider of GRC solutions that focuses on risk management. It is based in Brazil — with offices in Brazil, the U.S., the U.K. and India — and operates globally through a network of partners. Its solutions focus on industries such as the government sector, defense, energy and finance, where the monitoring and management of information security and the supply chain are important. IT VRM features are available as an add-on to the Modulo GRC platform, which is usually procured as a SaaS solution.

Strengths

- Modulo’s integrated customer support — which connects sales, consultants and support resources — was viewed by a number of its references as a key differentiator, and is attributed to Modulo’s heritage as a consulting and service vendor.
- Modulo has a complete set of capabilities in VRM, and also has a client base that is the most global of all the vendors in this Magic Quadrant.
- Modulo scored relatively high when references evaluated the overall ease of installation and problem-free upgrades, even with customizations.
Cautions

- Modulo’s heritage is as a consultant in the government sector, primarily in Brazil, and the Brazilian government remains its single largest vertical industry (although that percentage has been decreasing over the past two years). Modulo has expanded its presence in specifically North America, EMEA and Asia/Pacific, where IT VRM is its fastest-growing use case.
- Modulo had the highest percentage of customizations among the Magic Quadrant vendors, which likely led to the longer learning curves expressed by some references.
- While delivering adequate functionality, Modulo doesn’t innovate with new VRM solutions and services as well as some of its competitors do.

Prevalent

Prevalent, a privately owned vendor based in Warren, New Jersey, and founded in 2004, focuses on cybersecurity, risk and compliance. It launched its IT VRM solution in 2011 to help organizations reduce the risk of third-party data loss. Prevalent’s Vendor Risk Manager and Vendor Threat Monitor can be delivered as cloud-based SaaS, or installed on the customer’s premises for a monthly subscription fee based on the number of vendors managed and monitored. Prevalent sells through resellers and OEMs, primarily to midsize and large enterprise clients in industries with high data security needs (that is, financial services, healthcare and retail).

Strengths

- The combination of Vendor Risk Manager with Vendor Threat Monitor is a value-added enhancement, because more organizations are seeking solutions and services that provide an automation of assessment, as well as ongoing monitoring of specific risk and security issues within their vendor portfolios.
- Prevalent has a strong vision for the future requirements in the dynamic and regulatory-driven VRM market, and continues to add new solutions and services to accommodate the need for greater transparency into vendor risks.
- A number of references viewed Prevalent’s solutions as easier to configure, implement and use compared with other platforms.

Cautions

- Some clients have experienced workflow inconsistencies due to Prevalent’s heavy emphasis on and experience in financial services; however, Prevalent has been quick to resolve these inconsistencies.
- Prevalent is still building up and deploying its customer support capabilities, because it’s been heavily focused on R&D and new capability deployment.
- Some references viewed Prevalent as weaker than competitors in its analytics and reporting capabilities, despite its intuitive UI.
Quantivate

Quantivate, which was founded in 2005, is a GRC solution vendor based in Woodinville, Washington. Its IT VRM solution is built on its broader GRC platform, and can be acquired with other GRC modules or separately. Its predominant delivery model is hosted SaaS. Principally, it targets small and midsize banks and credit unions, and secondarily targets organizations in other highly regulated industries. Quantivate competes only in the U.S. Its IT VRM solution features a suite of capabilities, including vendor risk assessment, monitoring and mitigation.

Strengths

- Quantivate’s software is configurable and has limited customizations, and is generally viewed as intuitive and easy to use by business users with minimal training.
- Quantivate offers a simplified fixed-pricing model based on company size or assets, which makes pricing more transparent.
- Quantivate is responsive to customer needs and wants, and its recent VRM upgrade was based mostly on its review and integration of customer requests.

Cautions

- The Quantivate solution offers a basic set of capabilities, and Quantivate’s limited number of references provided mixed reviews of its solution’s capabilities.
- The solution is lacking in the areas of reporting and prebuilt connectors and integrations to common enterprise applications.
- Quantivate currently delivers its solution only to U.S.-based customers, and has no near-term plans to expand to other geographies.

RecoveryPlanner

RecoveryPlanner is a business continuity service provider that was founded in 1999. Based in Trumbull, Connecticut, and with a network of international resellers, it offers a GRC suite called RPX that provides business continuity management (BCM)/disaster recovery (DR), incident management, risk management and vendor management functionalities. Primarily targeted to industries with strong regulatory requirements and supply chain concerns (that is, financial, healthcare, insurance and manufacturing), RPX is available as a SaaS application, or sold via site license to customers seeking an on-premises solution.

Strengths

- RPX licensing is offered on an unlimited concurrent usage model, allowing internal, external and vendor resources to use the system as needed without increasing the cost or creating a complicated licensure/entitlement structure.
- The SaaS option for the RPX product is aggressively priced, making this a potentially attractive option for midsize enterprises that are challenged to fund point solutions.
RecoveryPlanner scored very high customer satisfaction ratings, and was well above the average of all the vendors evaluated in this Magic Quadrant.

Cautions

- RecoveryPlanner is focused heavily on BCM and DR, and the VRM solution is much less flexible and feature-rich outside of operational considerations.
- While there are APIs available to configure RPX and integrate it with other systems, the out-of-the-box options are limited.
- RecoveryPlanner is one of the smaller vendors in this study. If the market grows rapidly, this could impact its ability to scale up to meet future demands.

RiskVision (Formerly Agiliance)

RiskVision is a privately owned GRC vendor, based in Sunnyvale, California, that has offered commercial solutions since 2007. Its current GRC solution is the RiskVision 8.0 platform (released in March 2016), in which VRM is one of seven available modules. The platform can be delivered as a cloud-based service, or it can be installed on the customer’s premises for an annual subscription fee, or for an upfront payment for a perpetual license. It is used in a number of industries — such as global banking and insurance, federal public sector, healthcare and life sciences, retail and consumer, new media and entertainment, and energy and utilities — and is aimed at midsize to large enterprise deployments.

Strengths

- References reported strong support services and consulting support during the implementation stage.
- RiskVision has increased capabilities to support the life cycle of a vendor relationship, thereby allowing clients to leverage RiskVision across organizational boundaries and to create shortlists of risk-qualified vendors.
- RiskVision initiates automated assessments of existing vendors based on inputs from other systems in which it has built connectors, thereby reducing the level of manual intervention in tracking assessments.
- Most IT VRM solutions are predominantly delivered to North America-based customers; however, RiskVision has an EMEA presence, which increases its likelihood for expansion into global markets.

Cautions

- The RiskVision UI is not as user-friendly as some competitors’ UIs, but is expected to improve with future releases.
While its VRM tools are not contract management suites or performance management tools, RiskVision could benefit from enhanced integration into existing contract and performance management suites.

Rsam

Rsam is a Secaucus, New Jersey-based GRC vendor that was founded in 2002. It has offered a VRM module as part of its broader Rsam platform since 2010. The Rsam platform is cloud-based, but VRM is also offered as an on-premises hybrid architecture. Rsam targets large companies in highly regulated industries, and the upper end of the midsize enterprise market. Historically, it has focused primarily on North America, but is now seeking to expand its EMEA presence and move into Asia in 2016.

Strengths

- While not as large as several competitors, Rsam has a relatively mature offering with capabilities for issue tracking and alerts, assessment, reporting, and remediation plans and management.
- The application is viewed as easy to implement, and intuitive workflows make it relatively easy for business users to operate.
- Rsam is viewed as a very customer-centric vendor, and its size allows it to operate with flexibility, which drove relatively high customer satisfaction ratings (on average) from its references.

Cautions

- Data ingestion is available and API options exist, but customers are looking for more prebuilt connectors and integrations with other systems.
- Several references commented that the UI was in need of updating. In February 2016, this was done with the release of v.9.0.
- Some references provided mixed feedback on Rsam’s professional services when they were engaged.

SAI Global

SAI Global is a risk management service and solution provider based in Sydney, with more than 50% of its business in Australia. It delivers its IT VRM capabilities from its acquisition of Compliance 360 in 2012, and its IT VRM solution is Third Party Risk Management. SAI Global offers its IT VRM solution only as a SaaS solution.

Strengths

- Overall client reference experiences rated relatively high compared with the Magic Quadrant’s overall average, with strengths in functional capability and price and pricing model.
SAI Global is a client-service-focused vendor with strong technical support resources and capabilities.

SAI Global is a large, publicly traded company relative to most of its competitors, which gives it scale to grow the Compliance 360 offerings across geographies and industries.

Cautions

SAI Global’s solution, while adequate when performing the fundamental functions clients expect, is not as extensive compared with some of its competitors’ solutions, but it is well-suited to midsize and small organizations.

Some references found the workflows and functional processes to be complex; however, SAI Global has enhanced the workflow and is releasing an upgrade to Third Party Risk Management later in 2016.

The only deployment option available is SaaS delivery. This could restrict SAI Global’s ability in the near term to sell to large banks, many of which prefer on-premises or hybrid solutions.

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

We added two vendors to this year’s Magic Quadrant:

- RecoveryPlanner
- SAI Global

Dropped

No vendors were dropped from this year’s Magic Quadrant.

Inclusion and Exclusion Criteria

A broad range of vendors offer IT VRM products, but not all could be included in this Magic Quadrant. Vendors that are included in this Magic Quadrant had to show that they provide one or more IT VRM products, and meet other criteria.

Qualifying vendors were then evaluated in more detail using quantitative and qualitative criteria.
Inclusion Criteria

We use quantitative criteria to determine which vendors will qualify for this Magic Quadrant. We want to ensure that each vendor has experience delivering IT VRM solutions, and is currently generating revenue from its IT VRM module(s). To that end, each vendor had to have:

- Annual revenue of $1 million or more from IT VRM solutions, independent of consulting or implementation revenue
- A minimum of 15 IT VRM customer implementations, and a strong likelihood of customer growth over the next three years

We also use qualitative criteria to determine which vendors will qualify for this Magic Quadrant. We want to ensure that each vendor has a defined offering for IT VRM, that existing and prospective customers are considering this offering, and that each vendor has a defined product roadmap for IT VRM solutions that supports vendor risk identification and assessment, risk monitoring, and risk remediation. To that end, each vendor had to have:

- Overall market interest and vendor visibility, as determined by serious consideration for selection by enterprise clients
- Breadth of capability and technical/solution-related expertise, in combination with domain and process knowledge in the field of IT VRM

Exclusion Criteria

We excluded vendors that focus only on non-IT third-party risk management, or that provide support solely for the due diligence phase (not ongoing monitoring). We also excluded vendors that provide primarily VRM services (consulting or implementation) or VRM content, as opposed to VRM software solutions.

Evaluation Criteria

Ability to Execute

Vendors were evaluated on the quality and efficacy of the processes, systems, methods and procedures that enable their performance to be competitive, efficient and effective, and that positively impact their revenue, customer retention and reputation. Vendors were also judged on their ability to capitalize on their vision.

**Product or Service:** The IT VRM use case focuses on the process of ensuring that the use of third-party service providers and IT suppliers does not create an unacceptable potential for business disruption, or a negative impact on business performance. IT VRM solutions support enterprises that must assess, monitor and manage their risk exposure from third parties that provide IT products and services, or that have access to enterprise information. In general, IT VRM solutions focus on the risks associated with logical assets, information governance and IT controls, rather than the risks associated with physical supply chain assets.
Overall Viability: This criterion includes an assessment of a vendor’s overall financial health, the financial and practical success of the relevant business unit, and the likelihood that the business unit will continue to invest in the software, offer the software and advance the state of the art within the organization’s portfolio of products. Evidence of ongoing investment in IT VRM, overall company revenue, and revenue from the IT VRM platform determines a vendor’s score for this criterion.

Sales Execution/Pricing: This criterion concerns a 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. A key metric is sales performance in the past year. For pricing, the key metrics are the transparency and ease of calculation of the pricing model.

Market Responsiveness/Record: This criterion concerns a vendor’s ability to respond and adapt to changing competitive forces as opportunities develop, competitors act, customers’ needs evolve and market dynamics change. It also considers a vendor’s history of responsiveness and its ability to quickly address changing requirements. A key metric is the growth of a vendor’s IT VRM customer base over the past three years.

Customer Experience: This criterion covers a vendor’s relationships, products and services/programs that enable customers to be successful with the products evaluated. Customers were asked questions to determine their experience with their vendor and its IT VRM solution, including whether the product met, exceeded or fell short of their expectations; areas in which they think the vendor needs to improve; and their overall satisfaction with the vendor. Key metrics include overall satisfaction, value for money, and positive and negative comments from reference customers.

Operations: This criterion considers an organization’s ability to meet its goals and commitments. Factors include the quality of the organizational structure — including skills, experiences, programs, systems and other factors that enable the organization to operate effectively and efficiently on an ongoing basis. Key metrics are customer satisfaction with support and ongoing upgrades, customer satisfaction with professional education and training programs, and the availability of user conferences and other means by which customers can improve their skills.
Table 1. Ability to Execute Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product or Service</td>
<td>High</td>
</tr>
<tr>
<td>Overall Viability</td>
<td>Medium</td>
</tr>
<tr>
<td>Sales Execution/Pricing</td>
<td>Low</td>
</tr>
<tr>
<td>Market Responsiveness/Record</td>
<td>Medium</td>
</tr>
<tr>
<td>Marketing Execution</td>
<td>Not Rated</td>
</tr>
<tr>
<td>Customer Experience</td>
<td>High</td>
</tr>
<tr>
<td>Operations</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Source: Gartner (April 2016)

Completeness of Vision

Vendors were evaluated on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs and competitive forces. Vendors were also rated on their understanding of how market forces can be exploited to create opportunities for themselves and their clients.

**Market Understanding:** This criterion considers a vendor’s ability to understand buyers’ needs and translate them into products and services. Vendors with the most vision listen to and understand buyers’ wants and needs, and they can shape or enhance those wants and needs. Vendors need to understand the business and regulatory drivers for IT VRM in the short term, as well as the market’s long-term requirements.

**Sales Strategy:** This criterion considers a vendor’s strategy for selling IT VRM solutions. We looked for use of an appropriate network of direct and indirect sales resources, partner networks and alliance relationships to extend a vendor’s market reach to existing and prospective customers.

**Offering (Product) Strategy:** This criterion considers a vendor’s approach to product development and delivery, with an emphasis on differentiation, functionality, methodology and features as they map to current and future requirements. Vendors are evaluated on their roadmaps to advance current capabilities and deliver new ones.

**Vertical/Industry Strategy:** This criterion considers a vendor’s strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including industries. Ideally, vendors should have differentiated strategies for the financial services, healthcare and life science sectors, and offer value to customers in less regulated industries.

**Innovation:** This criterion concerns a vendor’s direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive
purposes. This criterion also evaluates the percentage of revenue dedicated to R&D and clearly innovative offerings that shape the market.

**Geographic Strategy:** This criterion concerns a vendor’s strategy to direct resources, skills and offerings to meet the needs of geographies (as appropriate) outside its native geographic area, either directly or through partners, channels and subsidiaries. The primary metrics are direct sales and support presence in multiple geographies, and reseller and service partner support.

### Table 2. Completeness of Vision Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Understanding</td>
<td>High</td>
</tr>
<tr>
<td>Marketing Strategy</td>
<td>Not Rated</td>
</tr>
<tr>
<td>Sales Strategy</td>
<td>Low</td>
</tr>
<tr>
<td>Offering (Product) Strategy</td>
<td>Medium</td>
</tr>
<tr>
<td>Business Model</td>
<td>Not Rated</td>
</tr>
<tr>
<td>Vertical/Industry Strategy</td>
<td>Medium</td>
</tr>
<tr>
<td>Innovation</td>
<td>Medium</td>
</tr>
<tr>
<td>Geographic Strategy</td>
<td>Low</td>
</tr>
</tbody>
</table>

Source: Gartner (April 2016)

### Quadrant Descriptions

**Leaders**

Leaders have a clear understanding of the IT VRM market’s needs and deliver solutions that are functionally robust, use emerging technologies and delivery models, and receive high marks from customers. Leaders also are able to deliver IT VRM solutions that integrate with broader GRC platforms and other security, risk, and vendor management applications.

**Challengers**

Challengers have proved their viability, and demonstrated market performance and the ability to exceed customers’ expectations for technical functionality. However, Challengers will need to focus on their product roadmaps — as well as their sales, marketing, geographical and industry strategies — if they are to become Leaders.
Visionaries

Visionaries have a solid understanding of the market, as demonstrated by domain expertise and responsiveness to customers’ expectations. They are actively executing against an aggressive product roadmap that extends support to additional regulatory and nonregulatory compliance and risk management needs, including support for the integration of IT VRM with GRC.

Niche Players

Niche Players often have a unique approach to the market, but may need to improve their core platform’s functions and their market execution. Niche Players also may target a specific industry or the needs of particular professionals. All Niche Players are successful in the market with competitive solutions.

Context

This Magic Quadrant presents Gartner's assessment of 12 GRC and vendor management software and solution providers that should be considered by enterprises seeking a technology solution for the identification, assessment and monitoring of risks relating to their use of IT service providers and IT vendors — that is, companies that typically have access to, or even control over, information assets that may be critical to an enterprise’s success and viability.

The placement of vendors in this Magic Quadrant, and the associated analyses, are based on multiple sources of information. The details of customers’ perceptions of vendors’ strengths and weaknesses are derived from clients’ IT VRM-related inquiries with Gartner, as well as from an automated survey of vendors’ reference customers conducted from December 2015 to February 2016. The evaluations also draw on vendor briefings, a vendor-completed questionnaire about IT VRM strategy and operations, product demonstrations by vendors, and other financial, product and vendor information that is publicly available and proprietary.

Most of the vendors in this Magic Quadrant are relatively small, given that the market is fairly new. When evaluating vendors, focus on the specific use case and risks you are addressing. Don’t restrict your evaluations to the Leaders, because vendors in other quadrants may be more suitable to your needs. Also, consider other vendors that are not evaluated in this Magic Quadrant, since it cannot include all vendors in this market.

On that subject, recognize that this Magic Quadrant does not cover the entire market for IT VRM solutions. A number of vendors were not evaluated either because their offerings are more aligned to SRM or third-party risk management (as defined earlier in this research), or because they did not meet one or more of the inclusion criteria. Prospective buyers may want to include the following vendors in future evaluations:

- Aravo
- CMO Software
- Evantix
Market Overview

The IT VRM market emerged primarily to support the requirements for regulatory compliance and information security that arose from enterprises' increased use of, and reliance on, third-party IT service providers and IT vendors. Enterprises' past failures to identify, monitor and mitigate the risks posed by such third parties have been recognized as factors leading to data breaches, operational failures and business disruptions. Consequently, organizations in highly regulated industries are now often mandated to have a VRM program with adequate controls for BCM, vendor performance, vendor viability and data protection. Failure to comply with these mandates can have significant audit-related repercussions that can undermine shareholder value and corporate viability.

Solutions in this market have capabilities ranging from risk assessment to risk monitoring and risk rating. Many of the leading IT VRM solution providers have backgrounds in GRC, and their IT VRM solutions are often modules or applications within a broader GRC platform. (Additionally, the market for BCM planning software includes vendors with some VRM capabilities, such as those for risk tiering and aligning risk with business processes.) While some organizations look for broad GRC platforms that include IT VRM capabilities, others are more interested in using IT VRM software to resolve a risk-related or regulation-related challenge in the short term. However, the latter group may end up buying a broader set of capabilities for IT risk management, operational risk management and BCM, among other things, to meet broader enterprise risk needs.

The IT VRM market is young and relatively small, but it is growing, and its vendors expect higher growth in the coming years. Many indicate that their IT VRM solutions are the fastest-growing of their GRC modules.

All the offerings considered in this Magic Quadrant are available as SaaS or have on-premises deployment options. However, the trend for many vendors is to offer SaaS, and, for some, this is the default method of delivery. Many of these vendors have roadmaps for expanded mobility services, access to real-time data from external sources, advanced analytics, and integration with a wider set of applications.

All the vendors in this Magic Quadrant allow the purchase of IT VRM as a stand-alone application, but the functionality is often built on a GRC platform, which frequently requires the purchase of foundational applications and modules.

IT VRM functionality is primarily directed toward the following customer requirements:

- Initial and ongoing assessments of IT service providers and other IT vendors in the areas of information security, adherence to regulatory standards, and compliance
- Collection of IT VRM data, and the ongoing monitoring of, and remediation planning for, vendor risks
Vendor profile creation, data collection and vendor profile management
Contract data collection — most clients want to track risk at a vendor level and a contract level
Collection and maintenance of security data and audit reports

Key Trends Affecting the IT VRM Market

IT VRM offerings are evolving due to the following trends:

- Customer demands for solutions that span the entirety of a sourcing life cycle, from the early identification and vetting of vendors, through the contracting stage, into onboarding and transitioning, management and monitoring, and termination and disposition.
- Increased reliance on external services and external sources for IT and business services. On average, more than 55% of an enterprise's IT budget is now spent externally.
- Pressure on corporate boards for better visibility into, and oversight of, their enterprises' exposure to third-party risks and third-party performance.
- The need for greater visibility into the information supply chain, including vendors' subcontractors.
- The intersection of IT and operational technology: the Internet of Things.
- Digital and bimodal sourcing demands in the business, where vendor speed and agility are favored over governance and risk.
- Increased demands placed on internal audit organizations as they cope with growing regulatory VRM oversight requirements and demands for more audits of business performance.
- Increasing regulatory focus on third-party risks, and expansion into performance management and performance tracking.
- Growing interest in VRM to support regulators' transparency objectives and business leaders' decision making.
- Increasing interest in predictive risk analytics to support the forecasting of risk events and impacts.

As we've noted, the market for IT VRM solutions is still relatively young, and offerings are often part of larger GRC or third-party risk management platforms that incorporate SRM, anti-bribery, anti-corruption and conflict minerals, and track-and-trace solutions.

This market is driven primarily by regulatory forces. Its solutions, therefore, are often tailored to unique regulatory requirements relating to certain industries, data types and processes.

Over the past three years, vendors have increased their revenue and number of customers in this market. Given their expectations, all indications point to continued growth.
Gartner Recommended Reading

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

"How Markets and Vendors Are Evaluated in Gartner Magic Quadrants"

"Toolkit: How to Scope a Supply Risk Program and Solution"

"2014 Strategic Road Map for Supply Risk Solution Deployment"

"Best Practices in Automating Supplier Relationship Management"

Evidence

- The Strengths and Cautions in this Magic Quadrant cover the evaluation criteria in which a vendor is above average or below average. We do not provide commentary for every evaluation criterion, or for criteria in which an individual vendor's capability did not stand out from the others. Where no commentary is provided, it should be assumed that the capability is adequate for most organizations' needs.

- As part of the vendor survey conducted for this Magic Quadrant, we asked each vendor to identify five reference customers. These customers' comments come from more than 56 IT VRM surveys and reference reviews that were completed between November 2015 and February 2016. Vendors' placement in the Magic Quadrant was also influenced by our IT VRM discussions with Gartner clients and non-Gartner clients.

- All 12 vendors in this Magic Quadrant completed a survey in which they provided information about their business and operational strategies, an overview of their capabilities and how they align with the inclusion and evaluation criteria, and their most important financial, sales and operational data.

Vendors were evaluated as if they were responding to an RFP, and ranked on their ability to document and qualify their strengths and features. It is important to remember that a Magic Quadrant does not solely rate product quality or capabilities and features; rather, it also indicates Gartner's view of a vendor's overall position in a specific market. Although product portfolio was an important consideration in our assessment, a vendor's ability to acquire customers and expand its presence in the market also was deemed important, as was its ability to increase its product revenue. A vendor that offers a strong, technically elegant product, but is unable or unwilling to devote funding and attention to marketing and sales in order to increase revenue and improve profitability, will find itself unable to invest in future product development.

- In addition, each vendor conducted a detailed briefing about, and a demonstration of, its IT VRM solution. Each vendor also was rated on its ability to conduct an effective briefing and demonstration, based on the provided use case and evaluation criteria for IT VRM.
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.