Magic Quadrant for IT Vendor Risk Management Tools

Published 24 August 2020 - ID G00465546 - 56 min read

IT vendor risk management software provides solutions to manage and automate the vendor risk management life cycle, address third-party risk and meet regulatory compliance. Gartner’s Magic Quadrant helps sourcing, procurement and vendor management leaders evaluate this growing and dynamic market.

Market Definition/Description

IT vendor risk management (IT VRM) is the discipline of addressing the residual risk that businesses and governments face when working with external service providers, IT vendors and related third parties. IT VRM solutions provide capabilities to automate and support the identification, assessment, analysis, remediation and monitoring of the information and operational risks arising from an organization’s use of third parties. These third parties include any external entity that can access, provide or manage sensitive data, and those entities that connect to a customer’s systems or networks, or support critical business processes. The market for IT VRM solutions continues to evolve in response to increased regulations, as well as increased appreciation for third-party risk. The vendors providing these solutions continue to change with new competition, merger and acquisition activity, and the addition of new capabilities. These capabilities can include:

* Software or a SaaS solution that automates the processes and workflows to manage vendor risks
* “Out-tasking” or outsourcing of the IT VRM workflows and processes
* The acquisition, analysis and reporting of vendor risk data sourced from public and private sources

The IT VRM solutions we evaluate in this report are principally associated with the “logical” or information supply chain risk, rather than the “physical” supply chain. There is some overlap in the types and classes of data needed for IT VRM and supplier risk management (SRM) — for example, data on the financial strength of vendors and geopolitical risk is common to both. However, there are also many differences. While SRM generally is focused on quality, timeliness and availability, IT VRM is generally focused on regulatory compliance, information and cybersecurity controls, and data privacy and protection. SRM addresses risks associated with companies that provide or manage physical goods and physical infrastructure, while IT VRM addresses risks associated with third parties that access, provide or manage information assets and IT infrastructure, applications, and some business processes. These solutions are increasingly focused on helping to identify, assess, analyze, monitor and remediate/mitigate cybersecurity and information security (infosec) risks. Therefore, in general, IT VRM focuses on information governance and IT to manage residual vendor risks.

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

* Assessment: This includes the ability to categorize vendors and/or their solutions and services into tiers of risk. As assessment approaches can vary, they need to be adaptable to support various methodologies and standards. This also involves the ability to assess the impact of vendor risks against compliance obligations, and qualitative and quantitative analytic tools to assess and prioritize risk. Templates and frameworks are designed to support specific mandates and regulatory requirements. Use cases that include shared content may include a database of vendor risk assessments or scores that can be accessed 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. It maps them to controls, owners, remediation actions, vendors, business entities, performance metrics and so on.
* Workflows and collaboration: This includes the ease of creating and editing workflows, workflow-level limitations, approval and escalation options, notification capability, rule engines for automated decision making and escalation, calendar population, to-do lists, and project management schedules. This also involves 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.
* Assess, validate and monitor controls: This includes the ability to assess the validity and effectiveness of controls; process management that, at a minimum, supports the workflow for the application; and other functions, such as exception management and reporting. Advanced abilities include modeling and simulation, creation of executable processes for data collection, and the development of rules for risk monitoring and control enforcement. Increasingly, regulators and customers are looking for more than static assessment; they’re requiring ongoing monitoring and continuous validation of controls.
* Exception management: The ability to manage vendor risk exceptions in relation to control requirements, compensating controls to mitigate risks and periodic reviews of whether exceptions are still required.
* Dashboards and reporting: The ability to collect and analyze vendor risk data to evaluate historical trends, improve planning for risk assessment and mitigation, and/or provide predictive capabilities around potential risk events. This also includes the ability to provide out-of-the-box or easily configurable reporting of tactical and strategic vendor risk data.
* Connectors and integrations: Prebuilt integrations into common software applications, services or content feeds required to perform vendor risk management. They offer application integration methods, specific applications and content sources supported, data association mapping on import, and data validation on import.
* Configurability: This involves configurations and the ease at which they can be accomplished, including code-free changes, look-and-feel configuration, template configuration, label/term changes, database object creation and management, page/screen updating support, and organizational hierarchy management support.
* History: The ability to see the assessment status and vendor risks of an earlier time, such as a past quarter or year.
* Access and user controls: 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.
* Remediation management: The recording of action plans to identify control failures and other IT VRM deficiencies, and to track those plans to fulfillment.
* User interface and navigation: The usability and ease of use of the workflows and screens. Workflows are somewhat intuitive, do not require an extensive learning curve, and are accessible and usable across multiple organizational roles, as well as through vendor self-service.
* Vendor profile management: The ability to import vendor and related contract (engagement) data from other systems, or to input it manually. This also includes the ability to collect and organize intelligence about vendors, and to manage vendor documentation and other content. It also covers vendor self-service capabilities that enable vendors to maintain and update information themselves.

Magic Quadrant

Figure 1. Magic Quadrant for IT Vendor Risk Management Tools

Source: Gartner (August 2020)



Vendor Strengths and Cautions

Allgress

Allgress is a Challenger in this Magic Quadrant.

Its solution is focused on vendor reviews and risk assessment, with functionality for both client and vendor, and supports additional governance, risk and compliance (GRC) modules, such as compliance management and incident response. Its operations are mostly focused in North America and its clients are spread across financial services, healthcare, technology and government.

Strengths

* Product or Service — With an updated UI, navigation is simplified, and screens and workflows are easy to use. Its table-based approach to selecting vendor risk templates and actions means it’s an intuitive model for managing vendor risk assessments.
* Sales Execution/Pricing Strategy — Pricing is defined on company annual revenue, with no user seat or functional pricing, meaning that the solution can be scaled without additional cost.
* Market Understanding — Allgress’ preconfigured workflows support over 300 regulations and standards, with automation capabilities that include reducing the cost of Federal Risk and Authorization Management Program (FedRAMP), Cybersecurity Maturity Model Certification (CMMC) and other reporting.

Cautions

* Offering (Product) Strategy — Some prebuilt integrations into some common applications and external content providers are in place. However, unlike many of its competitors, Allgress currently lacks alliances and integrations into the most commonly used security rating services.
* Geographic Strategy — Clients with requirements that span multiple geographies should know that the vendor’s operations are predominantly in North America.
* Product or Service — Global reports that focus on vendor risk posture and management are provided for an enterprise or business. However, additional information can only be incorporated from the various other modules when acquired by the customer.

Aravo

Aravo, a new entrant, is a Challenger in this Magic Quadrant.

Aravo for Third Party Management is a highly configurable solution that acts as a central repository for all vendor information and automates risk management and mitigation processes. Operations are based in North America and EMEA. Aravo targets midsize and large enterprises with a focus on financial services, life sciences and IT/cloud services.

Strengths

* Offering (Product) Strategy — Aravo provides a highly configurable solution that allows for the creation of workflows to support existing vendor risk processes. The Third Party Management Express solution allows for out-of-the-box assessments and practices when users do not have defined processes in place.
* Market Understanding — Aravo’s solution provides additional capabilities in contract and performance management, a requirement that more customers are looking for. The solution covers multiple related risk domains (infosec, data privacy and protection, business continuity, and disaster recovery) as well as ancillary risk domains (bribery and corruption, health and safety, environmental, and quality).
* Sales Execution/Pricing Strategy — Pricing is defined on revenue size, with unlimited users and an unlimited number of assessments. This includes unlimited data and file storage. The IT VRM application is available as a stand-alone solution.

Cautions

* Customer Experience — While Aravo’s configurability is a strength, it can also result in a good deal of modification and data integration during implementation, depending on customer requirements.
* Product or Service — Security rating services (SRS) integration is available; however, licenses with those SRS providers are required to access ratings.
* Innovation — Aravo’s broad coverage across multiple risk compliance domains supports a comprehensive third-party risk management strategy, but may result in a reduced focus on innovation for IT VRM exclusively.

CyberGRX

CyberGRX is a Niche Player in this Magic Quadrant.

CyberGRX offers a centralized risk assessment exchange platform and service that collects and validates vendor risk data through its cloud-based services. The solution allows users to apply analytics across a standardized set of data so they can shift their focus from assessment chasing to risk reduction. Its focus is primarily on North America. However, it is expanding into EMEA and Asia/Pacific (APAC).

Strengths

* Market Understanding — CyberGRX provides an alternative approach that doesn’t require implementation, customization or configuration of a solution. This platform provides access to vendor risk assessments; alternatively, a vendor risk assessment validation can be provided by its own analytics, its assessment team or its consulting partners.
* Market Responsiveness — CyberGRX has more than 70,000 vendors on its platform, and its approach can reduce resource needs and improve assessment cycle time, especially where a vendor risk assessment already exists. Its tool can be implemented quickly through its SaaS platform.
* Customer Experience — The CyberGRX offering is based on a framework for risk assessments with standardized processes, workflows and datasets. This allows users to share and exchange information efficiently and facilitates the use of analytics to inform decision making.

Cautions

* Offering (Product) Strategy — The CyberGRX platform does not allow customers to modify or customize the risk assessment process. Its “one to many” model has been established to drive a repeatable and scalable approach by using one assessment that produces a standardized dataset. CyberGRX Assessments are roughly based on NIST 800-53 and ISO 27001, and CyberGRX will map controls to industry standards or a customer’s proprietary standards.
* Offering (Product) Strategy — Despite having 70,000 vendors on CyberGRX, it does not have 70,000 assessments. If an assessment is ordered that is not already in the CyberGRX Exchange, CyberGRX has built up a process and dedicated team that is focused on bringing these new vendors on board. However, this activity will take additional time and effort.
* Product or Service — While the tool does provide online storage of vendor risk assessments, some clients will likely need to integrate (via APIs) with other solutions. To allow for full life cycle management, some clients may choose to use another tool as a system of record.

Fusion Risk Management

Fusion Risk Management, a new entrant, is a Niche Player in this Magic Quadrant.

The Fusion Framework System is a SaaS-based GRC solution hosted on the Salesforce Lightning Platform. It includes IT VRM, business continuity, disaster recovery, crisis/incident management, and operational and enterprise risk management. Fusion currently targets North America and EMEA customers across all industry verticals, with its highest concentration of customers in the financial services industry.

Strengths

* Offering (Product) Strategy — As the Fusion Framework System is a GRC solution, the IT VRM component integrates nicely with business continuity management (BCM) and operational risk management, making it a scalable solution, if needed.
* Sales Execution/Pricing Strategy — There is no limit to the number of vendors that can be managed in the system, unlike competitors that rely on “number of vendors” to estimate subscription fees.
* Innovation — The Fusion Framework System is built on cloud-based technology that is easy to configure, enhance and add functionality to where needed.

Cautions

* Product or Service — Third-party management was launched in February 2019 and has a small number of customers and implementations. This limited experience is reflective of the newness of the solution.
* Overall Viability — Fusion Risk Management was acquired by Vista Equity Partners in September 2019; it is too early to say if the acquisition will impact the company strategy for IT VRM. Therefore, be aware that the offering/product strategy may change.
* Sales Execution/Pricing — The pricing strategy is relatively simple. However, for those prospects who are looking purely for IT VRM, be aware that the core system includes all its operational resilience capabilities. Therefore, you may be paying for more than you need.

Galvanize

Galvanize is a Leader in this Magic Quadrant.

The Galvanize GRC platform incorporates the IT VRM life cycle management solution ThirdPartyBond (onboarding, classifications, assessment). Galvanize targets large companies in highly regulated industries (financial services, healthcare, public sector) and is geographically diversified. A SaaS platform HighBond IT VRM solution is also available for midmarket clients as part of the Galvanize GRC platform.

Strengths

* Product or Service — ThirdPartyBond is a mature offering and integrates with several external content providers, including security rating providers, as part of its offering. The solution is highly configurable, with intuitive workflows. It is considered by Galvanize’s customers to be relatively quick and easy to implement.
* Customer Experience — Galvanize has a global 24/7 support team, with support offices in Vancouver, London, Paris, Munich, Singapore and Japan. It offers a native language support network through partners.
* Geographic Strategy — Implementations are balanced across multiple geographies, with expanding support capability in Australia, specifically, and it is not overly focused in any one industry.

Cautions

* Innovation — Galvanize continues to work on a scalable SaaS delivery model for 2020, and while R&D is funded, it is not exclusively for IT VRM.
* Offering (Product) Strategy — Some customers who are on legacy products now have a dedicated API data bridge between the old and the new, which allows users to utilize the full IT VRM capability. However, Galvanize is still migrating customers to its new HighBond offering, and this may take some time.
* Sales Execution/Pricing Strategy — Galvanize’s pricing model is rather complex, with multiple packages across products and use cases available. Consider all options across the use cases before purchasing.

IBM

IBM, a new entrant, is a Challenger in this Magic Quadrant.

The IBM OpenPages with Watson offering is a GRC solution that includes IT VRM capabilities. It is available as SaaS-based or on-premises. IBM has customers throughout all global regions, and is represented in the following industries: financial services, energy/utility/telecom, manufacturing, retail and healthcare.

In 2020, IBM continues to infuse Watson capabilities within OpenPages in support of the GRC platform.

Strengths

* Vertical/Industry Strategy — IBM OpenPages has a web-based service called Assessment for IT VRM. This entry-level product is an out-of-the box solution targeted for smaller, less-mature organizations, and allows approximately 500 vendors and 40 concurrent business users to understand their third-party risk exposures through the vendor relationship.
* Sales Execution/Pricing Strategy — A simple new cloud subscription pricing model is in place with three different bundles. On-premises licensing is also available and can be bundled into Enterprise License agreements.
* Geographic Strategy — IBM has a wide geographical presence, with operations in 170 countries and a global network of system integrators and integration partners.

Cautions

* Offering (Product) Strategy — The OpenPages IT VRM capability is firmly embedded within the GRC platform. Therefore, the full GRC platform is required to use the IT VRM capability.
* Product or Service — IBM OpenPages currently lacks alliances and out-of-the box integrations into the most commonly used security rating services, although it does have API connectivity.
* Market Understanding — IBM OpenPages is based on a comprehensive modular structure, with a focus on GRC. Buyers for IT VRM-only solutions need to be aware of the investment that may be required to achieve the intended capability and insight.

LogicGate

LogicGate, a new entrant, is a Niche Player in this Magic Quadrant.

LogicGate’s third-party risk management component sits within the LogicGate Risk Cloud GRC offering. Delivered as a SaaS-only product, out-of-the-box assessments are aligned to either ISO 27001 or SIG Lite, with custom frameworks/questionnaires also an option. Primarily focused on the North American market, LogicGate targets regulated industries, such as financial services and healthcare.

Strengths

* Customer Experience — Implementation is via a consultative approach, with a focus on digital user groups, online communities for sharing best practices, communication and virtual training, and certification.
* Sales Strategy — LogicGate targets risk professionals. It has both direct and indirect sales channels, including resellers and affiliates, and a team of dedicated relationship managers.
* Market Understanding — As a GRC solution, LogicGate’s vision is to understand the risk exposure of the vendor portfolio. The configurability and workflows of the product support this vision.

Cautions

* Market Responsiveness — As a relatively new entrant to the market (2015), LogicGate’s IT VRM solution is still developing functionality and growing its customer base.
* Geographic Strategy — With a strong focus on North America, LogicGate does not yet have a complete global capability.
* Sales Execution/Pricing — As with many GRC solutions, the third-party risk management component can be sold as an individual application. However, the customer must purchase the GRC platform to access many of the key features (such as reporting, workflow builder and API integration).

LogicManager

LogicManager is a Challenger in this Magic Quadrant.

LogicManager provides an IT VRM solution for automating the IT VRM life cycle and is offered exclusively as a SaaS platform. Its operations are centered in North America, and it has a focus on the financial services industry.

Strengths

* Product or Service — LogicManager has migrated to its modern interface, Horizon. Its highly configurable and intuitive UI, workflows and processes make Horizon very easy to use.
* Market Responsiveness — LogicManager runs usability sessions with a select group of customers for new product features. Due to the single codebase and standard product deployment, these product updates are then transferable across all users.
* Customer Experience — LogicManager offers one of the more cost-effective and quicker-to-deploy solutions among vendors in this research. It is a good choice for midsize enterprises wanting rapid implementation and a tool suited to business users.

Cautions

* Vertical/Industry — LogicManager primarily serves and targets the financial services vertical, so organizations in other verticals should carefully assess its suitability.
* Sales Execution/Pricing Strategy — LogicManager provides a named user pricing model, which is broken down into users, industry and organization size. Although there is no additional cost for unlimited vendors, buyers need to work through which pricing pack would best suit their requirements.
* Geographic Strategy — LogicManager has a presence in multiple geographies but is primarily focused in North America. Organizations with a global footprint must validate the availability of support in specific regions.

MetricStream

MetricStream is a Leader in this Magic Quadrant.

MetricStream’s IT VRM solution is built on its M7 GRC platform, and can be acquired with other GRC modules or separately. MetricStream’s predominant delivery model is SaaS, and it targets highly regulated industries such as banking and financial services, and healthcare and life sciences. MetricStream’s focus is on North America, but it also has customers across Latin America, EMEA and APAC.

Strengths

* Geographic Strategy — While most other IT VRM solutions are heavily focused in North America, MetricStream has been successful in expanding its global presence. This geographic diversification also extends to vertical industries where MetricStream is not overly dependent on a single industry or regulatory drivers.
* Product or Service — Version M7 is more intuitive and has a more modern UI than previous versions. MetricStream has moved quickly to increase the percentage of new customers that are choosing a SaaS model as opposed to an on-premises delivery model.
* Vertical/Industry Strategy — MetricStream targets highly regulated industries as its priority and creates specific solutions for those target verticals, including prepackaged content (such as industry standards and regulations).

Cautions

* Customer Experience — Postimplementation configurations and customizations are highly dependent on support from MetricStream. While implementations can be achieved quickly, the follow-up support can delay the ability to access full functionality as intended. MetricStream has recognized that this is an issue and is enabling self-administration of configurations during implementation and ongoing support.
* Sales Execution/Pricing Strategy — While MetricStream has a very clear pricing strategy, based on user bands and market size, and many alternatives for large and midsize organizations, it offers little room for maneuvering for small organizations. However, the recently launched simple pricing approach may be valuable for smaller organizations with multiple users.
* Offering (Product) Strategy — MetricStream’s IT VRM solution is closely tied to the GRC strategy and focuses on operational and cyber risks. Although useful to some customers, those looking purely for an IT VRM solution may find this connection too much for their needs.

NAVEX Global

NAVEX Global is a Leader in this Magic Quadrant.

NAVEX Global delivers its IT VRM platform through its Lockpath editions, which provide users with IT VRM and broader IRM functionality. NAVEX Global (Lockpath) targets clients based in North America and EMEA, and primarily in the financial services, manufacturing and healthcare sectors.

Strengths

* Vertical/Industry Strategy — NAVEX Global (Lockpath) serves several verticals and can incorporate any regulatory content. It creates “content packs” for various industries, which include policy templates and assessment-specific content.
* Sales Execution/Pricing — The third-party risk management solution is sold separately, with an option to scale to full GRC if needed. Pricing models reflect small, midsize and large organizations.
* Sales Strategy — NAVEX Global (Lockpath) has expanded its sales and services teams and developed a network of key sales partners internationally to grow its presence outside of North America.

Cautions

* Offering (Product) Strategy — Lockpath is now offered exclusively as a SaaS solution. However, NAVEX Global still supports legacy on-premises Lockpath implementations. Existing customers seeking to move to a SaaS solution will have options, but those who may have been considering NAVEX Global (Lockpath) as an on-premises solution no longer have that option.
* Customer Experience — Technical support is currently limited to Monday to Friday, 7 a.m. to 7 p.m., U.S. Central Standard Time. Although emergency support is available, customers that require 24/7 support will need to consider other options.
* Geographic Strategy — While NAVEX Global (Lockpath) has a few international customers, most of its customer base is in North America — and this is reflected in the support it offers. Outside of North America, NAVEX Global (Lockpath) partners with resellers and advisory firms.

Ncontracts

Ncontracts is a Challenger in this Magic Quadrant.

Ncontracts’ Nvendor product is mainly focused on inherent risk assessments, onboarding and monitoring negative news, cybersecurity issues and compliance issues. Ncontracts’ target market is currently nearly 100% focused on financial services companies in the U.S. However, it has a small number of customers in the healthcare market.

In January 2020, Ncontracts was acquired by private equity firm Gryphon Investors.

Strengths

* Sales Execution/Pricing Strategy — Ncontracts has several sales executives across the U.S., and has a simple pricing structure based on the size of the organization and number of vendors under management. All models allow for unlimited users and unlimited storage of vendor information.
* Customer Experience — Ncontracts provides technical support Monday to Friday 7 a.m. to 7 p.m., U.S. Central Standard Time, which is beneficial for its U.S. customer base. Due to the geographic and vertical strategy, regional user conferences are well-attended and primarily share best practices and training.
* Market Understanding — Ncontracts has a strong knowledge set of industry skills, and a deep understanding of regulatory requirements and trends in financial services. This means Ncontracts is well-positioned to meet the specialized requirements of the financial services market.

Cautions

* Geographic Strategy — Ncontracts lacks geographic diversification, as it is heavily focused on the North American market, making competitiveness with larger global customers a challenge.
* Vertical/Industry Strategy — Ncontracts is nearly 100% focused on financial services and is heavily aligned to regulatory requirements. Outside of this vertical, Ncontracts offers little to no support. It is still too early to understand the impact of its acquisition by Gryphon Investors on the product/geography or vertical strategy.
* Product or Service — While clients indicate that the Nvendor tool is intuitive, the UI could use a refresh compared to some of the other IT VRM products in this research.

OneTrust

OneTrust is a Leader in this Magic Quadrant.

OneTrust’s Vendorpedia offering focuses on process and workflow automation for onboarding, due diligence, monitoring and offboarding. Its primary market is financial services and technology, across North America and EMEA.

In April 2020, OneTrust launched Athena, an AI and robotic automation and machine learning engine that listens to security and financial scores.

Strengths

* Market Responsiveness — Vendorpedia roadmap items are validated by customers, with over 85% of product development driven by collaboration. Successful joint collaborations have included the Vendorpedia Exchange and Chasing Services.
* Geographic Strategy — OneTrust continues to expand beyond its primary geographies of North America and EMEA into APAC and Latin America. It also supports a large number of languages out of the box, including right-to-left text.
* Customer Experience — OneTrust has highly collaborative and responsive support teams based in Atlanta, London, Melbourne and Bangalore, with global time zone coverage. It hosts user group events across the world and has executive management that clients praise for proactive and responsive client involvement.

Cautions

* Sales Strategy — OneTrust has built a direct sales model globally. However, its reseller model and direct sales support are limited outside of Europe and North America.
* Product or Service — Vendor data can be at a general level, and Vendorpedia is still growing (currently at more than 60,000 vendor profiles). The tool is useful for information about whether a vendor is compliant, but may not be detailed enough for some customers.
* Offering (Product) Strategy — While OneTrust has several product releases to support its expansion in IT VRM, some clients cannot quickly adopt those changes.

Prevalent

Prevalent is a Leader in this Magic Quadrant.

Prevalent’s third-party risk management platform is delivered as SaaS. It also provides managed support services through its Risk Operations Centers (ROC), where teams of third-party risk management experts collect and review evidence, perform red-flag analysis and provide remediation guidance. Its operations are primarily in North America and Western Europe, and its primary markets are financial services, healthcare and retail.

Strengths

* Product or Service — The new Prevalent third-party risk management (TPRM) platform incorporates an improved UI, ease of use and intuitive workflows. The more rigid approach to leveraging the full standardized assessments has been modified and allows vendors to complete shorter multiple-choice questionnaires.
* Vertical/Industry Strategy — Prevalent targets highly regulated industries, and tailors assessments and content for the financial services market and associated regulations.
* Offering (Product) Strategy — The ROC managed service approach is an advantage for some customers, as internal customer resource constraints make out-tasking or outsourcing some parts of the IT VRM process increasingly attractive.

Cautions

* Sales Strategy — Although IT VRM is the primary use case, Prevalent also targets three distinct organizational groups: security/incident, compliance/audit/privacy and procurement. Given the breadth of the GRC platform, buyers should be very specific in their requirements.
* Geographic Strategy — For those customers seeking solutions and vendors with a global presence, note that Prevalent targets North America and Western Europe, with sales and support teams working in those geographies.
* Sales Execution/Pricing Strategy — The Prevalent pricing strategy can be complex, with platform-only options, jump-start packages and service options. Additional licenses may also be required for optional modules.

ProcessUnity

ProcessUnity is a Leader in this Magic Quadrant.

ProcessUnity Vendor Risk Management is a SaaS application that supports vendor onboarding, assessment, performance reviews and SLAs. ProcessUnity targets highly regulated industries, with an emphasis on midsize and large enterprises in financial services, and is delivered primarily in North America and EMEA.

Strengths

* Customer Experience — ProcessUnity’s solution is highly responsive, quick to deploy, configurable and flexible. It can be adapted to customer demand and requirements and clients continually praise the ability to quickly configure workflows to their business processes.
* Sales Execution/Pricing — ProcessUnity has very transparent and simple pricing models, and makes its use-based IT VRM pricing available on its website.
* Offering (Product) Strategy — ProcessUnity goes beyond traditional IT VRM by offering built-in capabilities in performance management, contract management and procurement process.

Cautions

* Geographic Strategy — ProcessUnity has limited customer experience in larger nonfinancial services enterprises outside of North America. This could make it a less compelling offering for those in other geographies.
* Vertical/Industry Strategy — ProcessUnity’s key market is financial services, but it does not have any prebuilt special financial services capabilities. It is branching out into other highly regulated industries, such as high tech and pharmaceuticals — although those client numbers are currently low.
* Offering (Product) Strategy — Clients that forgo ProcessUnity’s out-of-the-box program in favor of a completely configured option must have well-defined processes before implementation. With no standard user manual for custom configured deployments, ProcessUnity could become harder to learn and require longer training times.

Quantivate

Quantivate is a Challenger in this Magic Quadrant.

Quantivate’s IT VRM solution features a suite of capabilities, including vendor risk assessment, monitoring and mitigation. It is built on its broader GRC platform and can be acquired either with other GRC modules or separately. Its predominant delivery model is hosted SaaS. It primarily targets midsize and large banks and credit unions, and only competes in the U.S.

Strengths

* Sales Strategy — Quantivate has a new partnership with the Credit Union National Association (CUNA) for its Compliance Management Module, whereby members receive a basic version, and it builds on upselling opportunities to deliver a more feature-heavy version. Both the member benefit version and the advanced paid version tightly integrate with Quantivate’s other GRC modules, including VRM.
* Product or Service — Improvements to the UI, the intuitiveness of screens and the solution’s linear processing workflows have improved the usability since the last version of this Magic Quadrant research.
* Customer Experience — Quantivate’s technical and business support consultants are made available to customers Monday to Friday, 6 a.m. to 6 p.m., Pacific Standard Time, with emergency support available 24/7. The support team is viewed as a valuable resource for its U.S. customer base for implementation support, training and ongoing product consulting.

Cautions

* Offering (Product) Strategy — Unlike most of the other GRC and IT VRM solutions in this Magic Quadrant, Quantivate does not have an integration with SRS.
* Vertical/Industry Strategy — Quantivate targets a limited number of verticals, and target content relates back to specific regulations, particularly in relation to financial services. IT VRM buyers should diligently assess content to ensure it reflects their specific requirements and regulations.
* Geographic Strategy — The solution is currently only sold and available in the U.S., and primarily serves the financial services industry. This limits Quantivate’s ability to scale up for global companies looking for a single enterprise solution.

Riskonnect

Riskonnect, a new entrant, is a Niche Player in this Magic Quadrant.

Riskonnect’s Third-Party Risk Management tool is part of its integrated risk management (IRM) solution. It focuses on tracking and monitoring of third parties and is delivered exclusively via SaaS. It offers its product set in North America, EMEA and APAC. It supports a broad range of vertical industries — such as manufacturing, retail and financial services.

Strengths

* Geographic Strategy — Riskonnect targets North America, EMEA and APAC due to their regulatory environments. Local sales, support teams and implementation partners are available across these geographies, and consulting firms are available to deliver legal and regulatory advisory support.
* Sales Execution/Pricing — Riskonnect built a geographically diverse direct sales and support team, covering the core and emerging geographies.
* Vertical/Industry Strategy — Riskonnect provides many API connectors for enhancing different user experiences in various use cases and industry-specific workflows. It also has direct integration with the Unified Compliance Framework.

Cautions

* Product/Service — Riskonnect does not have an integration with SRS.
* Offering (Product) Strategy — The VRM solution is sold as a stand-alone module. However, the IRM platform is the foundation that includes data infrastructure, analytics and base number of users, and many enhancements are IRM-focused. Additional data subscriptions and APIs may also be needed, depending on the package chosen.
* Customer Experience — IT VRM buyers should ask explicitly for IT risk management customer references, given that Riskonnect is relatively new to the IT VRM market.

RSA

RSA is a Leader in this Magic Quadrant.

RSA offers its RSA Archer Third Party Governance solution as part of its IRM platform, where clients can maintain IT VRM, contract and vendor profile data, performance management, remediation and assessment data. The solution is targeted to large enterprises with more mature IT VRM programs. RSA customers primarily come from the financial services, healthcare, and the public sector and government.

RSA was sold to a consortium led by Symphony Technology Group in February 2020. Although it is too early to understand the strategic impact, the deal allows RSA to focus on holistically managing digital risk.

Strengths

* Verticals/Industry Strategy — RSA targets financial, healthcare and public-sector verticals with individual user groups, and industry-focused days at RSA events. RSA also provides industry-targeted content throughout its releases.
* Product or Service — RSA continues to focus on improving configurability, usability and maintenance, with further improvements to reporting and UI made in 2020.
* Geographic Strategy — RSA provides its solution primarily in North America and EMEA. It has a global strategy and a growing customer base in APAC. It has support staff located in all three geographies.

Cautions

* Offering (Product) Strategy — RSA Archer may be a complex platform for some large organizations, as they may need dedicated resources to configure, enhance and maintain it.
* Sales Execution/Pricing — RSA’s pricing strategy is complex and is tied to the foundational concept of an IRM solution. Multiple factors may impact the final price including license type, maturity, deployment choices and base options.
* Innovation — Much of RSA’s innovation is tied to enabling IRM. Although IRM may be beneficial to IT VRM buyers, IRM may not always be relevant for the IT VRM market.

SAI Global

SAI Global is a Leader in this Magic Quadrant.

SAI Global’s IT VRM solution uses the SAI360 platform, out-of-the-box templates and an automated vendor portal. It delivers its solution in all geographies, and covers four core industries: healthcare, financial services, retail and manufacturing. SAI Global offers its IT VRM solution primarily as a SaaS solution, but will also deliver it as an on-premises solution.

Strengths

* Geographical Strategy — SAI Global’s global strategy is diverse, and is linked to regulation and legislation in each territory. It differentiates from other providers by offering primary presence and support in Southern Europe, the Nordics, DACH, the Middle East, Africa, Southeast Asia and Australia/New Zealand. These areas are not directly supported by most vendors in the market.
* Sales Strategy — SAI Global has a large direct sales and support team split between the Americas and the rest of the world. Each team then supports key segments (either industry- or country-driven). It also has several global and regional partnerships, including resellers, to complement the sales strategy.
* Market Responsiveness — SAI Global has several mechanisms to collect customer feedback and enhancement suggestions, including advisory boards, groups, ideas portal, user conferences and client steering committees.

Cautions

* Product or Service — Reporting capabilities available out of the box have historically been quite clunky, especially when importing reports. The use of Microsoft Power BI and the option to create PDF reports have improved this capability.
* Innovation — Many of SAI Global’s innovations tie back to a wider IRM solution, rather than IT VRM specifically, covering an integrated approach across risk. Although these capabilities may be beneficial to IT VRM buyers, they are not specifically tailored for the IT VRM market.
* Vertical/Industry Strategy — SAI Global targets a limited number of verticals, and target content relates back to specific regulations, including, for example, U.S. healthcare content. IT VRM buyers should diligently assess content to ensure that it reflects their specific requirements and regulations.

ServiceNow

ServiceNow is a Leader in this Magic Quadrant.

ServiceNow VRM is a key application within its IRM solution suite, and automates assessing, managing and mitigating vendor risk. ServiceNow has business in multiple geographies, but with the majority of IT VRM sales in North America. For IT VRM, ServiceNow targets its installed base, promoting the integration of vendor data with an enterprise’s, as well as with other organizations’ assets across a range of industries.

Strengths

* Sales Strategy — Much of the IT VRM solution growth has been achieved through adoption by ServiceNow’s existing client base. The ability to integrate across ServiceNow applications creates a unique value proposition for existing customers.
* Offering (Product) Strategy — The IT VRM solution is built on the Now Platform and integrates seamlessly with other ServiceNow IRM applications. This is particularly important for organizations looking to incorporate additional vendor management activities (such as performance and contract management).
* Vertical/Industry Strategy — Highly regulated industries, such as financial services and telecommunications, are the focus of ServiceNow’s IT VRM industry strategy. These industries are supported by targeted sales teams and industry-specific regulatory content (such as ORX integration for banking customers). In 2020, partnership ecosystems were launched with Deloitte and Accenture to target industry solutions. Online apps are searchable by industry.

Cautions

* Sales Execution/Pricing — With a price per vendor assessed annually, the initial entry costs can be relatively low, but increase rapidly as a client scales up ServiceNow’s program.
* Customer Experience — As a tool designed for large enterprises and their complex vendor risk management requirements, IT VRM requires a good amount of use-case configuration to be effectively deployed with business users.
* Product/Service — IT VRM can be purchased as a stand-alone product, with core capabilities for assessment, monitoring and managing vendor risk. However, security rating services are an optional extra, and much of the GRC functionality (policy, compliance, risk, audit management) requires an additional purchase.

SureCloud

SureCloud is a Challenger in this Magic Quadrant.

SureCloud’s third-party risk management solution focuses on vendor evaluation and assessment. It is a SaaS-only delivery model. It primarily targets the retail, healthcare and financial services sectors, and its operations are mostly focused in EMEA and North America.

Strengths

* Offering (Product) Strategy — SureCloud provides a flexible functional offering with rule-based recommendations, integrations to BitSight and RiskRecon, and GRC product integrations (such as vulnerability data). The cost of automation of the vendor risk assessment process is affordable for midsize or small companies.
* Product or Service — The UI is user-friendly and intuitive, with the ability to scale and build customized assessment surveys and manage contracts and vendors within a centralized register.
* Customer Experience — SureCloud is highly responsive to customer needs, and provides very good technical and business support over the life cycle of an engagement. It has recently introduced formal user communities; this, combined with any insights gained from future end-user conferences, is expected to improve product development over time.

Cautions

* Sales Execution/Pricing — SureCloud’s third-party risk management offering is part of its larger GRC solution, yet is available as a stand-alone module. While pricing options are simple, the platform and use-case strategy mean additional cost is likely — especially if SureCloud Accelerate (the implementation service to get the solution up and running) and Assist (administration) services are added.
* Sales Strategy — SureCloud has built direct sales teams in its core geographies and relies on a number of implementation partners. Currently, there are limited resellers, particularly in the U.S. market.
* Geographic Strategy — Unlike other players in this market, SureCloud’s heritage was delivering its solutions and services to European customers, but its North American presence is growing.

ThirdPartyTrust

ThirdPartyTrust, a new entrant, is a Niche Player in this Magic Quadrant.

ThirdPartyTrust was launched in 2015 and is headquartered in Chicago. The ThirdPartyTrust enterprise risk platform automates security questionnaires, collects information and evidence from attestations and reports such as SOC, and provides a unified view of the life cycle of risk assessment. As a startup, ThirdPartyTrust has initially focused on the North American market.

Strengths

* Product or Service — ThirdPartyTrust has built integrations with several SRS providers and is continuing to develop this network to provide a holistic vendor risk management view.
* Vertical/Industry Strategy — Vendors can update their profiles, and customers have direct access to vendor profiles via a permission-based connection.
* Customer Experience — As ThirdPartyTrust focuses on the North American market, local support is available for customers from 6 a.m. to 6 p.m., U.S. Central Standard Time. It runs several customer forums and online communities where best practices, tips, white papers and success stories can be shared.

Cautions

* Offering (Product) Strategy — ThirdPartyTrust is a pure-play IT VRM solution focused exclusively on vendor and third-party data/information security/privacy analysis. Buyers looking for more than an information security/privacy IT VRM solution will need to consider alternatives.
* Geographic Strategy — ThirdPartyTrust primarily focuses on the North American market, which limits those clients who are geographically diverse. With a North American focus, there are limited support hours for the rest of the world.
* Sales Strategy — The ThirdPartyTrust assessment platform is only available through managed security service provider (MSSP) partners or integration partners linked to an existing solution; it is not available to purchase directly.

Venminder

Venminder is a Challenger in this Magic Quadrant.

Venminder is an IT VRM solution and service provider focusing on vendor oversight, risk assessment, contract management and questionnaires. Its operations are exclusively focused in North America, and its clients tend to be financial services organizations.

Strengths

* Product or Service — Venminder offers a highly configurable and cost-effective solution for its target market, as well as a deep managed service assessment offering.
* Customer Experience — Implementation can be achieved relatively quickly, and if support is needed, a dedicated support team is available 8 a.m. to 8 p.m., U.S. Eastern Standard Time to reflect the North American customer base. Training can be provided virtually or on-site, and Venminder has an active community network.
* Market Responsiveness — Potential product enhancements from clients are evaluated on a quarterly basis and, if successful, are then released onto the platform. Recent requests include security rating services dashboard integration, advanced questionnaire and assessments, and business unit permissions.

Cautions

* Vertical/Industry Strategy — Venminder has strong knowledge and skills in the financial services industry, the regulatory climate and the requirements to meet these specialized needs. However, it has limited experience and expertise in other industries.
* Offering (Product) Strategy — Its managed services offering can be a differentiator. However, it may not be consistent with customers’ internal framework and processes for assessment and validation of data and controls.
* Geographic Strategy — Most of Venminder’s IT VRM business is still within financial services, and 99% is within the U.S. The lack of diversification could hinder competitiveness when compared to global IRM and IT VRM competitors. This is a challenge that Venminder is addressing as it looks to expand with global enterprises.

Whistic

Whistic, a new entrant, is a Niche Player in this Magic Quadrant.

Whistic’s Vendor Security offering is a SaaS-based platform built around security questionnaires and corresponding workflows. This allows customers to maintain a vendor catalog containing profile and security information. Whistic targets information security teams, with an emphasis on technology companies and the midmarket, and is primarily operating in North America.

Strengths

* Market Understanding — Whistic is proactively targeting new markets and verticals, with an emphasis on all organization types and sizes, from startups to multinationals. Currently, IT security teams are the main consumers of the Vendor Security product.
* Product or Service — Users who find their vendors are already in the Whistic Trust Catalog may be able to ramp up relatively quickly. Platform configuration is relatively quick and easy, with assessments in place within days or weeks.
* Customer Experience — Whistic has a robust training plan in place with one-on-one training during the implementation process. Accessible user guides and product updates are delivered via the Whistic Help Center.

Cautions

* Offering (Product) Strategy — Vendor profiles need to be completed and published by the vendor in Whistic Trust Catalog. Users may find that information is generic and out of date, as responsibility lies with the vendor to keep the data current.
* Vertical/Industry Strategy — Most of Whistic’s business is within the technology vertical, with as-yet-limited exposure to or experience with other verticals.
* Geographic Strategy — Whistic’s primary focus is on North America, with support for Latin-based languages. This is limiting for those clients who are geographically diverse; and with a North American focus, there are limited support hours for the rest of the world.

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

* Aravo
* Fusion Risk Manager
* IBM
* LogicGate
* Riskonnect
* ThirdPartyTrust
* Whistic

Dropped

No vendors were dropped from the 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 had to show that they provide one or more IT VRM products, and that they 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 $1.5 million or more from IT VRM solutions, independent of consulting or implementation revenue
* A minimum of 20 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
* Existing and prospective customers that are considering this offering
* 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

This Magic Quadrant does not cover the entire market for VRM solutions. 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: This criterion focuses on the core goods and services that compete in and/or serve the IT VRM market. This includes current product and service capabilities, quality, feature sets and skills. This can be offered natively or through OEM agreements/partnerships, as defined in the Market Definition/Description section and detailed in the subcriteria.

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, and the financial and practical success of the relevant business unit. Factors include 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 determine 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.

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 activities, thought leadership, social media, referrals and sales activities.

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. These included whether the product met, exceeded or fell short of their expectations; areas where 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

Enlarge Table

| Evaluation Criteria | Weighting |
| --- | --- |
| Product or Service | High |
| Overall Viability | Medium |
| Sales Execution/Pricing | Low |
| Market Responsiveness/Record | Medium |
| Marketing Execution | Low |
| Customer Experience | High |
| Operations | Medium |

Source: Gartner (August 2020)

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 to translate those needs into products and services. Vendors with the most vision listen to and understand buyers’ wants and needs, and can shape or enhance those wants and needs. Vendors need to understand the business and regulatory drivers for IT VRM in the short term, and the market’s long-term requirements.

Sales Strategy: This criterion considers a vendor’s strategy for selling IT VRM solutions. We look for the use of an appropriate network of direct and indirect sales resources, partner networks and alliance relationships to extend a vendor’s market reach to both 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 IT VRM 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 preemptive purposes. The criterion also evaluates the percentage of revenue dedicated to both R&D and the 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 outside its native geographic area, either directly or through partners, channels and subsidiaries, as appropriate for that area and market. The primary metrics are a direct sales and support presence in multiple geographies, as well as reseller and service partner support.

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

| Evaluation Criteria | Weighting |
| --- | --- |
| Market Understanding | High |
| Marketing Strategy | Not Rated |
| Sales Strategy | Low |
| Offering (Product) Strategy | High |
| Business Model | Not Rated |
| Vertical/Industry Strategy | Medium |
| Innovation | Medium |
| Geographic Strategy | Low |

Source: Gartner (August 2020)

Quadrant Descriptions

Leaders

Leaders have a clear understanding of the IT VRM market’s needs. They deliver solutions that are functionally robust, use emerging technologies and delivery models, and receive high marks from customers. Leaders are also able to deliver IT VRM solutions that integrate with broader IRM 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 and can affect the course of technological developments in the market, but are still building out their execution skills. They are actively progressing 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 IRM.

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 and have competitive solutions.

Context

This Magic Quadrant presents Gartner’s assessment of 23 vendors providing software and solutions that should be considered by enterprises seeking technology solutions for the identification, assessment and monitoring of risks relating to their use of service providers and IT vendors. They are 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 evaluations draw on vendor briefings; a vendor-completed questionnaire about IT VRM strategies and operations; product demonstrations by vendors; and other financial, product and vendor information that is publicly available, as well as proprietary information. Additionally, we collect client opinions directly from Gartner Peer Insights reviews in the IT vendor risk management market.

Many of the vendors in this Magic Quadrant are small; some are relatively new to the VRM market; and several are larger, publicly traded technology and service providers. 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.

Market Overview

The IT VRM market emerged to support requirements for regulatory compliance and infosec, arising from enterprises’ increased use of, and reliance on, third-party IT service providers and other vendors that have access to sensitive data or customer systems and networks. 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 an IT VRM program with adequate controls for business continuity management, vendor performance, vendor viability and data protection. The challenge for many is that the functional responsibilities for VRM are often siloed within different parts of the organizations. IT VRM should be looked at within the context of a broader, integrated approach to risk and VRM. 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 such as risk assessment, risk monitoring and risk rating. Many of the leading IT VRM solution providers have broader offerings in IRM, and their IT VRM solutions are often modules or applications within a broader platform (see Note 1). 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 IRM solution 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 continues to expand, and new entrants are seen regularly in a highly fragmented marketplace. This can make it difficult to understand and differentiate the variety of services and solutions available to support the vendor risk management life cycle.

All the offerings considered in this Magic Quadrant are available as SaaS or have on-premises deployment options. However, the trend continues for many vendors to only offer their solution as SaaS as 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 an IRM platform, which frequently requires the purchase of foundational applications and modules. All have some amount of prebuilt integrations to common software applications (for example, ERP and contract management). Many are integrated with external content providers (for example, BitSight, Dun & Bradstreet and SecurityScorecard).

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 infosec, 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:

* The COVID-19 pandemic has hit the entire world in 2020, and the VRM market has responded with free assessments, monitoring tools and tracking capabilities. Most discussions have tied back to business continuity management and planning.
* Customers demand 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.
* Increasing labor demands and costs associated with collecting and validating vendor and third-party assessment data are driving growth in security rating services, VRM managed services and assessment information exchanges.
* Reliance on external services and external sources for IT and business services is increasing. On average, more than 60% of an enterprise’s IT budget is spent on products and external services.
* Corporate boards are under pressure to provide better visibility into and oversight of their enterprises’ exposure to third-party risks and third-party performance.
* Increasing emphasis is put on fourth-party relationships, which are not clearly visible in all third-party relationships, partly due to increased use of cloud and SaaS solutions.
* Information and operational technologies (Internet of Things [IoT]) are driving the growth and interconnectedness of technology.
* Digital business growth, and the needs of IT and sourcing to support a bimodal IT operating environment require agile and faster processes for evaluating and bringing new vendors on board.
* Increased demands are placed on internal audit organizations as they cope with growing regulatory VRM oversight requirements and demands for more audits of business performance.
* Third-party risks and expansion into performance management and performance tracking are subject to increased regulatory focus.
* Demand is growing for predictive risk analytics to support the forecasting of risk events and impacts.

Third-party risks continue to affect businesses through, for example, failures, outages, strategy and operational changes, data losses, data breaches, and brand/reputation risk. Enterprises need continuous monitoring of these vendor risks.

Evidence

* The vendor 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 enterprises’ needs.
* Vendors’ placement in the Magic Quadrant was also influenced by our IT VRM discussions with Gartner clients and non-Gartner clients.
* All 23 vendors in this Magic Quadrant completed a survey in which they provided information about:
  + Their business and operational strategies
  + Their capabilities and how they align with the inclusion and evaluation criteria
  + Their most important financial, sales and operational data
* Vendors were evaluated as if they were responding to an RFP, and 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; 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 was also 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 to increase revenue and improve profitability, will find itself unable to invest in future product development.
* Each vendor conducted a detailed briefing and IT VRM solution demonstration. Each vendor was also rated on its ability to conduct an effective briefing and demonstration, based on the provided use case and evaluation criteria for IT VRM.

Note 1Definition of Integrated Risk Management (IRM) Solutions

Gartner defines IRM as a set of practices and processes, supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. Consequently, Gartner recommends IT VRM as an element of a broader IRM approach to build and sustain successful IT risk management programs.

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.