Gartner

Licensed for Distribution

Magic Quadrant for IT Risk Management

Published 3 July 2019 - ID G00383242 - 35 min read

By Analysts Khushbu Pratap, Brian Reed

Demand for ITRM solutions continues to increase as digital ecosystems evolve. Security and risk management leaders managing cybersecurity initiatives, board risk oversight and digital compliance should use this research to evaluate the opportunities and challenges in automating IT risk workflows.

Strategic Planning Assumptions

By 2025, 60% of global IT risk management (ITRM) buyers will depend on risk management solutions to aggregate digital risks in their business ecosystem, up from 15% in 2019.

Through 2025, 50% of ITRM solutions will evolve to support digital risk management capabilities, including cloud, operational technology (OT), Internet of Things (IoT) and the social media environments of digital businesses, up from less than 30% in 2019.

Market Definition/Description

Gartner defines the ITRM solution market as software and services that operationalize the risk management life cycle related to IT and security activities. Scenarios originating in or attributed to the digital infrastructure, applications, systems, processes and teams are the subject of analysis and reporting in such solutions. Core functions include:

- Facilitation of risk workflows to implement chosen risk management practices, methods and principles. Preconfigured workflows usually address risk identification, ownership, analysis, scoring, controls assessment, remediation and reporting.
- Aggregation of risk-related data from IT operations and security operations, business applications, and analysis and reporting tools in a central repository where it can be aggregated, normalized, parsed and correlated.
- Creation of risk and control repositories in relation to asset inventory, business process definitions and third-party engagement.
- Provision of off-the-shelf, mapped regulatory content and compliance mandates from multiple authorities and standards-authoring bodies.

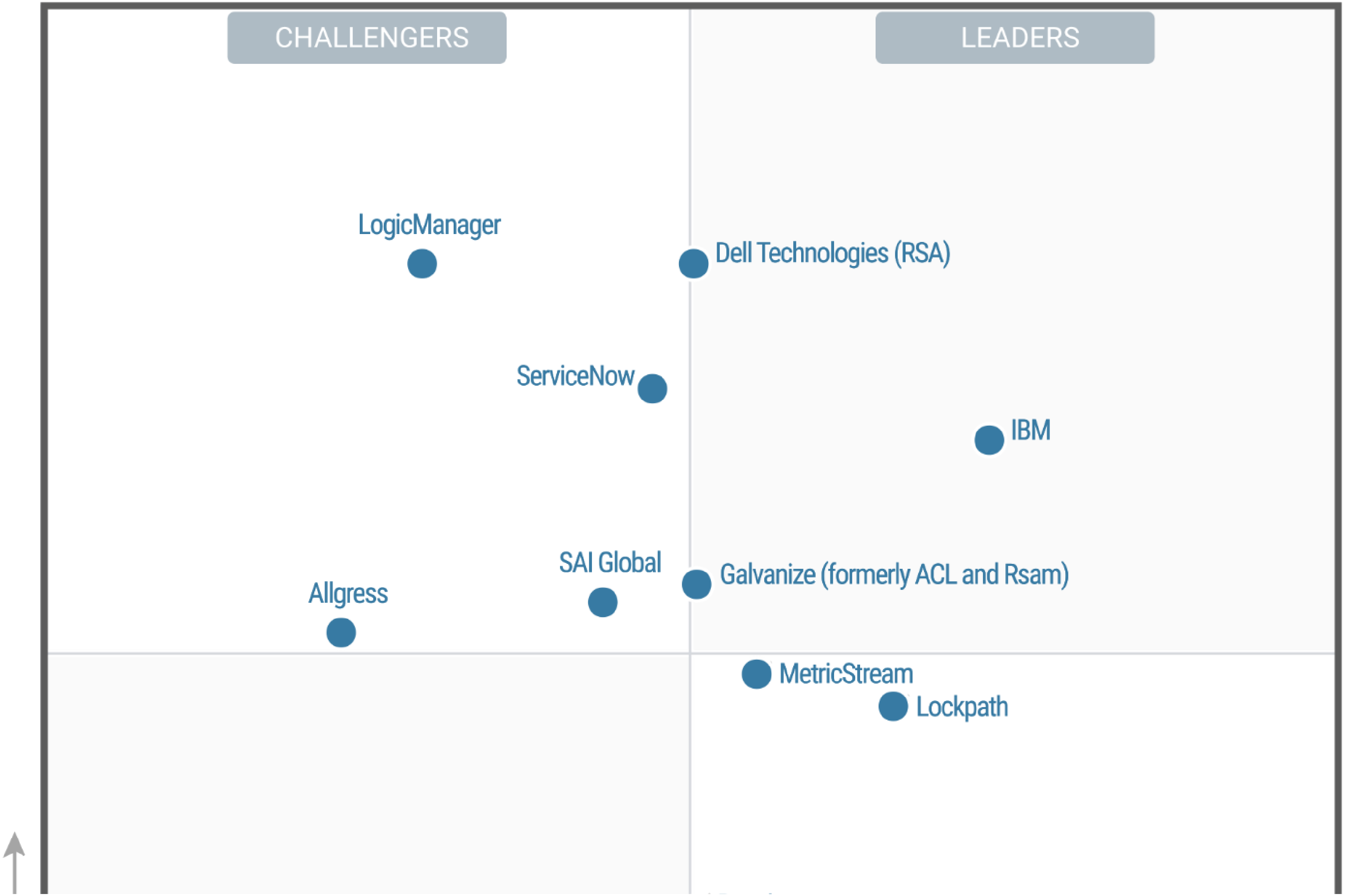
ITRM solutions are typically deployed to:

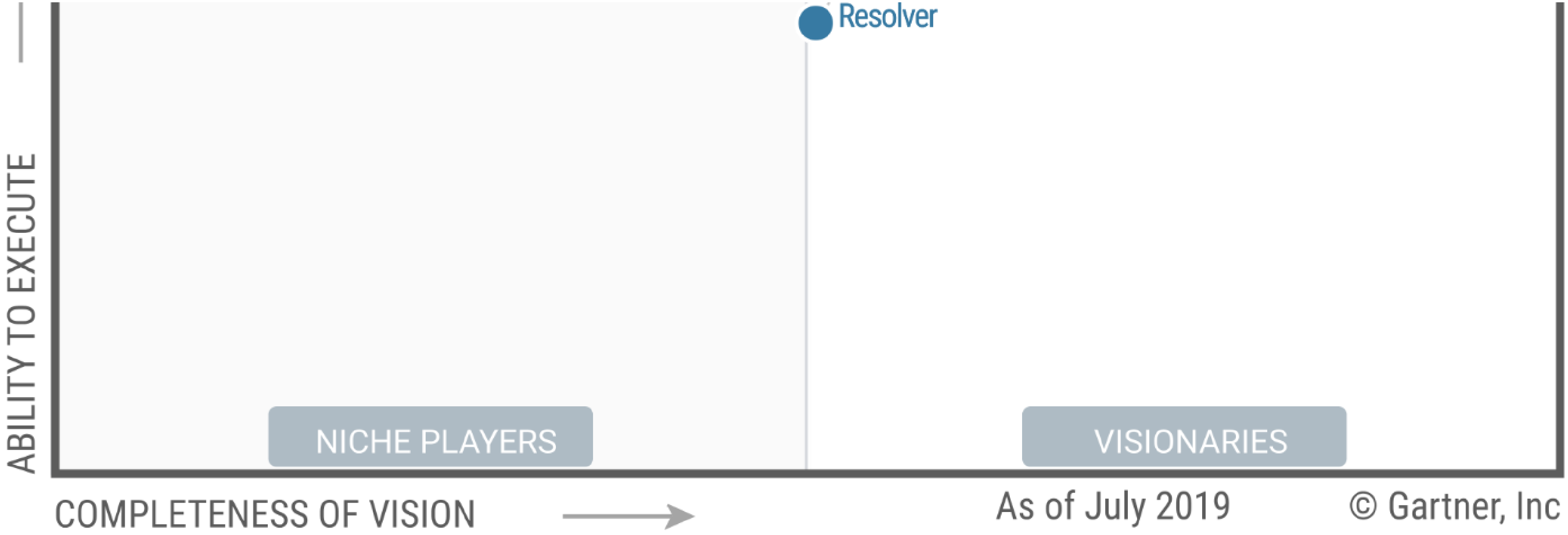
- Establish a consistent mechanism to analyze, score and report risks and related controls.
- Facilitate an automated risk remediation activity and link remediation to incident response and closure of audit findings of internal/external reviews.
- Provide IT- and security-related compliance reporting against standards, such as ISO 27001 (and others in the ISO 27000 family of standards), PCI DSS, SOX, HIPAA, NIST CSF, NIST 800-53, and a variety of state-level, national, global and industry-specific cybersecurity- and privacy-related guidance that overlaps with information security guidance.
- Leverage analytics and reporting capabilities to report on chosen key performance and risk indicators for the second line of defense (risk, security and compliance professionals) and first line of defense (risk owners) roles.
- Leverage reporting templates and customizable reporting capability to present to C-suite, board members and external stakeholders.

Emerging trends we observe in this market are indicative of how ITRM needs will evolve for advanced risk management and cybersecurity use cases.

Magic Quadrant

Figure 1. Magic Quadrant for IT Risk Management





Source: Gartner (July 2019)

Vendor Strengths and Cautions

Allgress

Headquartered in Livermore, California, Allgress (https://allgress.com/) is a privately held company and an established provider of ITRM solutions meeting the needs of both first-time and existing ITRM buyers. The vendor's Insight Risk Management Suite version 7 was evaluated for this research. Allgress offers on-premises, SaaS and hosted delivery options. The majority of its customers opt for the SaaS model. The offering is differentiated in the market by its affordability, simple-to-understand pricing model, basic integrations and time to implement the solution. Small to midsize organizations or larger organizations that are setting up their ITRM function, and transitioning from spreadsheets, should consider Allgress in their shortlists. Support is offered from Livermore, California 8/5 (included) or 24/7 (for an added fee). Allgress continues to offer its compliance assessment and regulatory content mapping capabilities in Amazon Web Services for customers leveraging this environment.

Strengths

- Market Understanding: Allgress offers compliance content mapping to include 350-plus instances of regulatory and standards content. Standards Mapping Explorer shows coverage for all standards mapped to the selected one. Harmonizing requirements through this capability has saved risk owners, assessors and auditors time among their customer base, and has given compliance coverage visibility.

- Product Strategy: API support and strides in product development are customer-focused for risk and control self-assessments. Allgress has proven its focus on near-real-time risk reporting and having consistency in on-premises and cloud environments, as well as consuming data from a large set of IT and non-IT data sources.

Cautions

- Geographic Strategy: Buyers implementing ITRM in multiple geographies or in EMEA and the Asia/Pacific region should know that the vendor’s operations are primarily in North America. There are partnerships with AT&T and NTT to offer deployment and customization in EMEA, the Asia/Pacific region and Latin America. The solution currently supports English and Spanish.

- Advanced Risk Management and Governance: Three areas commonly observed in advanced IT risk requirements are not fully evident in customer implementations. These are interconnected and layered risk management workflows, federated organization structures, and loss projection (going beyond human input). ITRM buyers should validate specific requirements through a proof of concept.

Dell Technologies (RSA)

Headquartered in Bedford, Massachusetts, RSA (https://www.rsa.com/) , a Dell Technologies business, offers its RSA Archer Suite, version 6.5 (made available in February 2019) across multiple use cases and domains. The suite consists of multiple solutions, from the integrated RSA Archer offering, including Audit Management, Business Resiliency, Third-Party Governance and others. RSA Archer deployment options include on-premises, hosted and third-party hosted, with approximately a current 3:1 ratio of on-premises versus cloud-hosted. Implementation services are available through RSA professional services and its partners. System integration and value-added reseller services are offered worldwide, while professional services and consulting are focused in the Americas, EMEA, and the Asia/Pacific region and Japan. Customers for the products and services exist across industries such as financial services, healthcare, public sector/government, professional services, transportation, telecommunications, retail, energy and technology.

Strengths

- Geographic and Language Parity: Market understanding comes through local consulting service providers, system integrators and value-added resellers in EMEA, the Asia/Pacific region and Japan, and the vendor has continued to provide positive customer experiences in those regions. The solution supports Chinese, French, German, Italian, Portuguese, Japanese and Spanish, in addition to English. This illustrates RSA Archer's ability to support multinational organizations that may or may not have a presence in North America.

- Delivery Model and Viability: While buyers are increasingly gravitating toward the SaaS model, RSA Archer continues to be the preferred solution for on-premises-only implementations, especially among public-sector and financial organizations. In 2018, it had the maximum year-over-year increase in on-premises implementations in the market. Recurring revenue combined with new accounts added to its viability.

Cautions

- Customer Experience for Deployment Time and User Interface: Specific customer needs, enterprise size, cost and level of consulting, and project-management-related challenges can significantly influence deployment time. RSA Archer has made efforts to minimize deployment times, but some customers with complex implementations continue to report nine- to 12-month deployments or more. The average time in the market is three to six months. The 2018 and 2019 releases were aimed at improvements to facilitate shorter deployments. Releases planned for 2019 were slated to improve user interface and navigation. Expected changes will be evidenced in 2019 and 2020.

- Solution Architecture and Total Cost of Ownership: While not new, RSA Archer's on-premises instances continue to constitute multiple components that require orchestration and maintenance by dedicated full-time personnel after deployment. This has been a critical decision-making factor for small and midsize organizations in estimating total cost of ownership. For large and extra-large organizations, requisitions are made in budget planning for hiring or training personnel.

Galvanize (formerly ACL and Rsam)

In May 2019, ACL and Rsam announced that they have rebranded as Galvanize (https://www.wegalvanize.com/) .

ACL is headquartered in Vancouver, British Columbia, and is privately held. On 4 February 2019, ACL completed the acquisition of Rsam. The combined entity has been rebranded as Galvanize. For the purposes of this research, ACL and Rsam are being evaluated in a combined fashion, as the acquisition was completed just before this research began.

Formerly headquartered in Vancouver, British Columbia, ACL's legacy software solutions are focused on audit, compliance, risk management, IT governance and data analytics. Its ITRM solution for evaluation includes the HighBond (previously known as ACL GRC) cloud platform — offering SaaS continuous delivery — and ACL Robotics (previously known as ACL Analytics). The solution set is deployed exclusively via SaaS. ACL supports clients in North America, EMEA, Latin America and the Caribbean, and Asia. Clients are primarily within the general commercial, public-sector, manufacturing, professional services, financial services, insurance and healthcare industries. Technical support is provided in each region, with Latin America and the Caribbean supported out of North America.

Rsam was formerly headquartered in Secaucus, New Jersey. Its legacy software solutions are focused on ITRM, security incident response, cybersecurity, third-party and vendor risk, policy, and business continuity. Rsam's legacy product can be deployed via on-premises, privately hosted or SaaS models. Targeted clients are in North America, Europe, the Middle East and the Asia/Pacific region, and in healthcare, financial services, government, retail, education and energy. Rsam has a global 24/7 support team with support offices in New Jersey and Bangalore, India.

Strengths

- Geographic Strategy: The combined entity has a wide geographical presence. Existing customer implementations and support availability in multiple regions facilitate multinational ITRM projects.
- Product capabilities: ACL's out-of-the-box reports for senior management and board reporting deliver easy-to-understand narratives, and configurable workflows make it easier to stay aligned to changes in business processes. When combined with Rsam's basic and advanced integrations for IT and security OT and reliability for processing large volumes of data, the overall product capabilities meet a variety of ITRM buyer requirements.

Cautions

- Product Roadmap: The roadmap for joining two sets of products introduces complexity and uncertainty, due to the required integrations and investments with Rsam. Integrating ACL and Rsam will require multiple releases. However, data exchange for the purposes of integration is already available in production and was demonstrated during this research.
- Customer Experience: Rsam's customers reported moderate to low satisfaction levels in their experiences with Rsam, especially in quality and availability of end-user training and ease of integration using standard application interfaces and tools. The integration with ACL will result in

revised training material in the future. It is recommended to communicate expectations for end-user training material at the contracting stage.

IBM

IBM (https://www.ibm.com/) , publicly traded and headquartered in Armonk, New York, targets a broad set of buyers across the enterprise, including governance, risk management and internal audit professionals. IBM OpenPages Version 8, reviewed for this research, is offered as an on-premises, privately hosted or SaaS solution. Targeted buyers for OpenPages include risk and security leaders at global organizations whose short- or long-term goal is enterprisewide integrated risk management (IRM). OpenPages' clients are located in all global regions. Approximately 50% of OpenPages' clients are in the financial services sector, with the remaining spread across energy, utilities, healthcare, telecommunications and government. IBM provides OpenPages support via nine help center facilities, with locations in the U.S. and Canada, as well as in six other countries around the world.

Strengths

- Market Understanding: IBM has incorporated customer feedback to focus on improved usability, sharper analytics and use of machine learning algorithms to allow data classification and control mapping recommendations. End-user dashboards and onboarding guidance for risk owners facilitate inclusive risk decision making. Embedded Cognos Analytics and Watson AI (if enabled and licensed) address data-driven risk analysis. The product strategy reflects evolved ITRM customer journeys as compared to previous years, which in turn evidences a better understanding of the target market.

- Product Strategy: IBM has an expansive offering to leverage complementary solutions such as Cognos Analytics, Watson, i2 Enterprise Insight Analysis and QRadar SIEM. ITRM buyers attempting to design an IRM function are at an advantage to roll up risk information from different sources of IT-related risk information. Promontory Financial Group, an IBM Company (offering regulatory compliance consulting as a service) and IBM Regulatory Compliance Analytics are being leveraged by a few customers.

Cautions

- Pricing: IBM offers a user-based licensing model to accommodate organization-specific pricing needs. Changes made to the pricing model have not yet translated into expected flexibility in contract negotiations for many customers. Total cost of ownership in 2018 continues to be higher-than-average spend for ITRM buyers because IBM OpenPages is usually procured by multiple buying centers, including enterprise risk use cases.

- Sales Strategy and Marketing Execution: IBM’s sales and marketing efforts appeal to IRM buyers. Marketing efforts are more relevant to advanced risk and compliance management use cases. Buyers seeking basic risk and security assessment and cybersecurity risk management should fully understand the level of integration with non-IBM applications, the required investment and the consulting effort that might be required to achieve the intended level of maturity.

Lockpath

Lockpath (https://www.lockpath.com/) , privately held and headquartered in Overland Park, Kansas, offers the Keylight platform as its ITRM solution. It targets the following buyers: chief information security officers (CISOs), compliance teams and chief risk officers (CROs). Keylight Enterprise, demonstrated for this research, can be deployed via SaaS, as well as in an on-premises model. The majority of Lockpath’s customers (over 70%) are on the SaaS model. Customers in healthcare, financial services and technology make up over 50% of its current installed base. Most of Lockpath’s customers are located in North America, with a few spread across South America, Europe and Asia. Lockpath offers support out of its headquarters in Kansas. Implementation services are delivered by the vendor’s professional services team and a network of global partners. In 2018, Lockpath introduced Blacklight to complement existing offerings. Backlight provides automated configuration and control testing, as well as host and application asset discovery capabilities.

Strengths

- Market Understanding: Lockpath has focused on customer challenges around compliance tracking, posture assessment and budgeting for cybersecurity. In 2018 and 2019, customers provided positive reviews for workflow design, risk analysis, remediation and compliance content mapping capabilities that improve risk oversight. Recognizing the challenges of lean customer teams, Lockpath offers a managed service where customers outsource routine program administration in vendor and incident management.

- Implementation Services: In a market where buyers’ ITRM maturity is low to moderate, customers provided positive feedback on ease of deployment and configuration in 2018. Customers like that implementation time is typically three months or less. Deployment is amenable to a global workforce. Lockpath supports languages listed in ISO 639, and has deployed French, German, Portuguese, Italian, Spanish and German among its customer base.

Cautions

- Product Performance: In 2019, customers report expecting better board and senior executive reporting. Reporting requirements often remain ambiguous during procurement; it is recommended to identify what stakeholders are looking for before relying on off-the-shelf reporting capabilities.

- Support: Technical support is currently limited to Monday through Friday, 7 a.m. to 7 p.m., U.S. Central Standard Time. Lockpath has plans to expand support coverage in the future; enterprises that require 24/7 support will need to consider other options.

LogicManager

LogicManager (https://www.logicmanager.com/) is headquartered in Boston and privately held. LogicManager's legacy software solutions have been focused on enterprise risk management for midsize enterprises. Its target buyers are chief risk, compliance, information security and audit officers, as well as their direct reports. LogicManager's IRM solution set demonstrated for evaluation is offered exclusively as a SaaS platform with continuous delivery of release updates. LogicManager supports clients in North America, Asia, the U.K. and Western Europe. Banking, credit unions and other financial services combine to make up about half of LogicManager's client base. Healthcare, insurance, manufacturing, education, energy, and civic and social organizations each encompass between 5% and 20% of the client base. Technical support is provided from the Boston headquarters and from Europe satellite offices.

Strengths

- Clarity of Pricing and Total Cost of Ownership: The simple-to-understand pricing strategy and no professional fees for implementation, configuration, data retrofitting, training, reporting, content, and templates are highly valued by customers. Customers can consult LogicManager's advisory analysts without time restrictions; this is an added benefit, but might be tough to scale with account growth.

- Customer Experience: Customers provide consistent positive feedback on risk analysis, issue remediation and incident management. The majority of customers find themselves in a better position to report to senior management and facilitate controls mapping across standards. The biggest driver for procurement is moving away from spreadsheets, where LogicManager exceeds expectations.

Cautions

- Geographic Strategy: LogicManager has a presence in multiple geographies in 2018 and 2019, but is primarily focused in North America. Multinational organizations or federated enterprises with a global footprint must validate the availability of support in specific regions.

- Advanced Risk and Cybersecurity Use Cases: The majority of customers are in the initial stages of ITRM implementations. Advanced risk management and cybersecurity tracking are not observed widely in the market. For extremely complex or advanced implementations, buyers should validate use-case definition and support for integration with security operational technology.

MetricStream

MetricStream (https://www.metricstream.com/) , privately held and headquartered in Palo Alto, California, offers its M7 Release across three updates per year at this time. For example, as of this writing, the current release is the February 2019 one. The vendor uses a continuous integration/continuous delivery (CI/CD) model for those releases. The applications making up MetricStream's suite are Enterprise Risk Management, Operational Risk Management, Internal Audit Management, Compliance Management, SOX Compliance, and Policy and Document Management. MetricStream's M7 platform can be deployed via SaaS or a privately hosted, hybrid or on-premises model. MetricStream's suite targets a wide range of buyers, including all primary C-suite executives, plus buyers such as CISOs, vendor risk management (VRM) executives and quality management executives. Approximately 80% of MetricStream's revenue comes from SaaS-delivered services. Financial services, healthcare and manufacturing are top-priority verticals, with 45% of the vendor's revenue coming from the financial services sector. MetricStream has support staff worldwide and primary support centers in the U.S., U.K. and India, with secondary support services in Europe, the UAE and the Philippines.

Strengths

- Product Performance: Customer feedback indicates above-average performance of individual capabilities. Workflow design, risk analysis and near-real-time assessments, in particular, exceed customer expectations.

- Customer Understanding: M7 provides a front-end, user-driven rule engine that offers the capability to orchestrate prioritization rules based on vulnerability context and the business context of the underlying assets and processes. These rules are used to determine the current remediation template, target system, incident priority and incident ownership in a scalable manner, without regular user intervention.

Cautions

- Implementation Services: For most ITRM implementations in the market, satisfactory service is dependent on the definition of success criteria. Previous years illustrate reasonable customer satisfaction. In 2019, select customers reported less-than-satisfactory experiences with implementation services due to success criteria definition. It is recommended to confirm output, deliverables and success criteria of implementation services before contract negotiation and deployment.

- Customer Experience: Through 2017 and 2018, MetricStream invested effort to minimize customer customization requests and offer more off-the-shelf capabilities. M7 has had numerous deployments, but deployment concerns persist as reported by end users, including response time, quality of technical support and customization in some cases. When considering M7, ITRM buyers should articulate sample output requirements during the proof-of-concept stage.

Resolver

Resolver (https://www.resolver.com/) , headquartered in Toronto, Ontario, is privately held. Resolver Core was demonstrated for this research. The RiskVision part of Core is offered via SaaS and on-premises deployment. Almost half of Resolver's customers are in financial services and insurance, with the remainder in education, software publishing and other businesses. Resolver targets clients located predominantly in North America (70%) and the U.K., with more international expansion planned. The vendor has 24/7 emergency support coverage and scheduled support from offices in London; Toronto; Charleston, West Virginia; Edmonton, Alberta; Sunnyvale, California; Christchurch, New Zealand; and Hyderabad, India.

Strengths

- Product Offering: Customers attribute product functionality, performance and roadmap as key reasons for selecting RiskVision. Specifically, customers report above-average satisfaction for risk analysis, near-real-time assessments, integrations and workflow design.

- Innovation: RiskVision continues to evolve previously introduced concepts such as always-on assessments and threat-linked risk objects. R&D efforts focus on vertical-specific incident and risk category prioritization and tracking anonymized loss analysis.

Cautions

- Product Offering: Resolver relies on partners to facilitate digital asset discovery through integration with CMDB and scanning tools. The majority of the vendors in the market offer digital asset discovery through partners and customers have not raised this as a concern yet. However, ITRM buyers should validate the weighting of digital asset discovery capabilities against their implementation vision, and ensure their team's comfort level regarding reliance on partners to deliver these seamlessly.

- Price Influencers: ITRM buyers will find it difficult to estimate cost if there is lack of consensus on number of users, assets, vendors and data sources. ITRM teams evaluating RiskVision should have agreement on user (practitioner) count, number of assets and vendor entities (if applicable), and required data connectors for their ITRM implementation.

SAI Global

On 11 February 2019, SAI Global (https://www.saiglobal.com/) announced its intention to acquire the Nasdaq BWise product line. This acquisition was completed on 1 April 2019. However, for this research, SAI Global is evaluated preacquisition; BWise is not included in this research iteration. The impact of changes is likely to be seen in 2020.

SAI Global, headquartered in Chicago, offers its SAI360 platform to target ITRM use cases. SAI360 Digital Risk, demonstrated for this research, is delivered primarily via privately hosted or SaaS environments. This solution focuses on sectors such as financial services, healthcare, life sciences, retail, manufacturing, energy and utilities. Its client base is distributed across Europe, the U.K./Ireland, Middle East/Africa, North America and the Asia/Pacific region. Customer support is offered in the U.K., Germany, Middle East, Asia, Australia and the U.S.

Strengths

- Clarity of Pricing: SAI Global has a simple and easy-to-understand pricing model, and lower price points than other vendors.
- Overall Customer Experience: Overall, customers speak well of SAI Global, citing knowledge of ITRM, a complete life cycle for risk management, control mapping, and ease of use and configuration as positives.

Cautions

- Customer Understanding and Product Function: SAI Global is executing on its vision to help customers operationalize IRM solutions without the need for extensive customization. As such, the vendor might not be an ideal option in extremely complex ITRM environments.
- Innovation: SAI Global’s initiatives are typically ideas or delivery mechanisms (such as chatbots) that are focused on vendor onboarding. The vendor will need to continue innovating in its IT and digital risk portfolio to stay competitive.

ServiceNow

ServiceNow (https://www.servicenow.com/) , a public company headquartered in Santa Clara, California, built ServiceNow governance, risk and compliance on the ServiceNow platform. The ITRM solution targets buyers such as IT security teams, risk management directors and internal audit teams. ServiceNow GRC, version Madrid, was demonstrated for this research. It is almost exclusively deployed via a SaaS model, although on-premises is available upon request by customers. ServiceNow primarily targets North America, Europe, the Asia/Pacific region and Australia/New Zealand, but also has a limited presence in the Middle East and Latin/South America. The vendor has solution consultants and industry marketing teams dedicated to financial services, healthcare, education, life sciences and government. Support centers are located in Santa Clara, California; San Diego, California; Amsterdam, Netherlands; Staines, U.K.; and Sydney, Australia.

Strengths

- Product Strategy: Product performance and the roadmap in 2017, 2018 and early 2019 demonstrate delivery of commitments and goals set for ITRM offerings. ServiceNow is among the few vendors in this market to promptly align upcoming releases with immediate customer needs and to execute future releases as planned. ServiceNow has also added risk management professionals to its team. While some of the effort planned and executed in previous years can be equated to playing catch-up with more-experienced ITRM vendors, ServiceNow GRC implementations reviewed in 2019 demonstrate high levels of customer satisfaction and new customer interest.

- Customer Experience: It is challenging to strike a balance between features/functions and user experience for administrators in the ITRM space. For greater impact, instead of focusing on the administrator's user experience, ServiceNow adopted an end-user-centric focus, facilitating risk analysis, risk mitigation such as patching based on performance indicators, and incident response for the first line of defense, or risk owners. For administrators evaluating upgrades, ServiceNow offers to-the-point release notes to validate purpose and checklists for facilitating smooth upgrades. 2019 and 2020 will add more perspective as new customers upgrade the versions purchased in late 2018 and early 2019.

Cautions

- Target Buyers: Although we have started to notice a change in the number of new customers for ServiceNow GRC in 2019, the majority of targeted buyers are existing ServiceNow customers with a need to add ITRM capabilities. ITRM buyers that are not already customers should ensure the compatibility of their existing technology portfolio with ServiceNow connectors.

- Delivery Model: Buyers with an on-premises preference must know ServiceNow supports on-premises implementations, but these are rare; however, its private cloud infrastructure aims to provide flexibility and support akin to on-premises implementations.

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

- Rsam rebranded to Galvanize

Dropped

- Nasdaq

Inclusion and Exclusion Criteria

Inclusion Criteria

For inclusion in the 2019 Magic Quadrant for ITRM solutions, Gartner focuses on vendors that offer not only ITRM applications, but also professional services and hand-holding support to end users in a market increasingly influenced by digital risks not included in traditional IT risk assessments.

ITRM solution products must:

- Include functionality for all critical capabilities
- Be sold individually and be actively marketed by its vendor
- Be evaluated and the version of the product that is generally available (GA) must have been in production as of 1 March 2019

- Have annualized revenue from ITRM solutions (not combined with other risk and compliance solutions) at or above $4 million, have at least 25 paying customers, and have at least 25,000 seats/end users deployed
- Must compete in at least two of the four major regional markets (Americas, Europe, Asia/Pacific and the Middle East/Africa)

Vendors that do not meet the criteria above may be included if Gartner analysts consider that aspects of the company’s product, execution or vision are particularly noteworthy.

Exclusion Criteria

Vendors will be excluded if product design and capability align with only one industry (for example, only government or only healthcare or only higher education).

Vendors with minimal or negligible apparent market share among Gartner clients, or with no current GA services, may be excluded from the evaluation.

Notable Mentions

- TechDemocracy
- Acuity Risk Management
- SDG (TruOps)
- EGERIE
- Maclear
- Energent

Evaluation Criteria

Ability to Execute

Product or Service: A well-executed product/solution strategy for ITRM solutions delivers risk and compliance management outcomes as designed in the “problem statement” for the various risk, compliance, security, privacy and business stakeholders. ITRM solutions meet or exceed buyer expectations when they “own the delivery of the solution.” meaning not just deploy the solution, but also stay invested in project milestones for the term of the contract. Ease of navigation, time to retrieve and reference information, ease of integrating data external to the solution, control mapping, incident response, and storyboarding capabilities will be weighted. Additionally, customer experience in managing product updates and syncing with customer’s digital environment are given importance.

Overall Viability: Overall viability refers to sustained funding sources (venture capital or otherwise), including positive year-over-year growth in customers, seats and revenue. There should be evidence of continual investment in product development and sales.

Sales Execution/Pricing: This criterion includes pricing that places few restrictions on which modules can be used. Use cases and pricing lists should be simple to interpret. Prospects should be offered different packages with full disclosure on reasons why a certain package was aligned. Vendors should be able to successfully compete in deals that displace incumbents because of better value and customer use-case alignment with effective sales, presales and marketing teams, and to win in highly competitive shortlists.

Market Responsiveness/Record: This includes creating alliances/partnerships and integrations with niche IT/security/legal/finance/business applications, improving usability and introducing storyboarding faster than competitors. Addressing evolving risk assessment needs of IT risk managers, CISOs and CIOs quickly will be weighted.

Marketing Execution: This criterion includes evidencing well-defined use cases, target buyers and personas, and articulation with examples or case studies and testimonials of the claimed differentiators.

Customer Experience: This criterion includes quality interactions with technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc.

Operations: This criterion was not evaluated in this research.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	Low
Customer Experience	High
Operations	Not Rated

Source: Gartner (July 2019)

Completeness of Vision

Market Understanding: This refers to a blend of risk visibility, workflow design, user experience, control mapping and storyboarding capabilities that meet or exceed the requirements of ITRM and business stakeholders. Innovation, forecasting customer requirements and being ahead of competitors on new features are also considered, as well as integration with IT operations, security operations, threat intelligence, analytics, and robotic process automation products and services.

Marketing Strategy: An understanding of and commitment to the ITRM space, the prevailing challenges in risk management, reporting on cybersecurity and, more specifically, bringing different stakeholders the disparity or similarity in their risk view are evaluated. Avoidance of nondifferentiating terms (such as “robust,” “easy to use,” “single pane of glass,” etc.) is also considered. Marketing messages must align with actual product and service deliverables.

Sales Strategy: This criterion includes a recognition that not all buyers of ITRM solutions have dedicated teams using the solution. Pricing and packaging options suitable for ITRM team size, maturity of processes and intended outcomes for prospects will be weighted. Immediate after-sales assistance with deployment is weighted. Periodic follow-up contact with existing customers must be evident, along with a capable channel program that enables consistency and high-quality access to the product or service to organizations in all available geographies.

Offering (Product) Strategy: Well-regarded solutions deliver comprehensive risk and compliance workflows in IT or digital environments, and are easy to change based on user environment change, business process changes or change in maturity level. In addition, solutions offer building blocks to create narratives that go beyond operational reports. Preconfigured indicators of measurements are available in the solution for novice users or stakeholders new in their roles within ITRM. At the same time, advanced users have options to simulate output from the use of different risk assessment models/approaches. Off-the-shelf versions supporting a combination of qualitative and quantitative risk assessment approaches are weighted.

Business Model: The process and success rate for developing new features and innovation through investments in research and development are evaluated. This includes a demonstrated understanding of the particular challenges associated with integrating multiple cloud applications and third-party noncloud providers, or partnering with solution providers and a track record of translating that understanding into a competitive go-to-market strategy. Applications and providers can be in a variety of areas (for example, analytics, data visualization, regulatory content mapping, security operations, analysis, reporting, threat intelligence and incident management).

Vertical/Industry Strategy: This criterion includes evidence of customers spread across industries. Hiring subject matter experts, supporting regulations and directives for specific industries, or supporting business models of prospects/customers in chosen industries are weighted. Partnerships or alliances with industry associations or special forums and working groups, resulting in added value to the ITRM reports, are weighted.

Innovation: This criterion includes evidence of continued research and development with quality differentiators, such as performance, management interface and clarity of reporting. Features should be aligned with the realities of the distributed nature of risk assessments and complexity of business workflows. Included are a roadmap showing a risk decision-making focus, continued support for more integrations relevant to digital environments, and strategies for addressing evolving risks and risk assessment models.

Geographic Strategy: The vendor should have an effective channel that delivers consistent messaging and support in every available geography. Third-party attestations relevant to regions in which the product is sold and an ability to help customers meet regional compliance requirements are weighted. Language support, presence of support teams and/or reseller-provided support are also weighted.

Table 2: Completeness of Vision Evaluation Criteria

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

Source: Gartner (July 2019)

Quadrant Descriptions

Leaders

The Leaders in the ITRM market show up most often on the shortlists of larger and more complex organizations with more aggressive customization and integration requirements. Leaders are noted for their ability to innovate and forecast future needs of enterprises across a range of industries and geographies, while being able to support large, complex deployments.

Challengers

The Challengers in this market execute well with simple requirements, but they have a less well-defined view of the market's direction compared to Leaders. Challengers are capable of being future leaders as long as they continue to focus on execution and bolstering their focus on innovation and the future needs of clients.

Visionaries

Visionaries articulate important market trends and directions. They have an ability to identify the longer-term needs of the market and may have advanced capabilities in one or two critical capabilities. However, they may not be in a position to fully deliver and consistently execute on that vision. They may need to improve their service delivery.

Niche Players

Niche Players often have a unique approach to the market. They focus on a particular segment of the market, such as smaller organizations with more modest requirements, or on one key capability. Their Ability to Execute is limited to the narrower areas of focus, and is assessed accordingly. Their ability to innovate may be affected by their narrow focus.

Context

This Magic Quadrant for ITRM solutions is intended to provide insight into ITRM buyers' needs and experiences in the context of available vendor options in this market. ITRM buyers should consider the following recommendations:

- **Define IT risk processes and workflows before contacting vendors.** Leverage existing information workflows and processes that directly impact business objectives and commitments to define IT risk workflow. Align risk workflows to business processes. While refinements can be expected by migrating to an ITRM solution, the definition and agreement regarding it should be obtained before contacting ITRM vendors.

- **Start scouting early.** Typically, it's best to begin nine to 12 months before the contract award date. Internal buy-ins and agreement on requirement specifications, and business case approval, can take one to six months. Vendors take anywhere between two and four weeks to respond to proposal requirements, depending on complexity of needs. Proof-of-concept sessions and detailed briefings can take one to two weeks. Final vendor evaluation and contract negotiation can take anywhere from one to four weeks.

- **Focus on must-have risk outcomes.** Have a top five must-have list of outcomes and a top five wish list of outcomes. Get agreement from all stakeholders about the difference between the two lists.

- **Ask customer references about their IT risk journey.** Don't just ask about ITRM software and support experience; also request to know their IT risk requirements, team size, and expectations from their IT risk function and dashboard.

- **Obtain stakeholder buy-in.** Communicate with sponsors of IT, security, digital and risk initiatives within the organization before carving out an RFP. These sponsors should have representation from the business.

- **Align ITRM goals with IRM solutions.** All IRM goals can be roughly categorized under simplification, automation and integration. ITRM buyers need to:

  - **Identify their top four to five granular requirements.** These include risk analysis, mitigation and follow-up, which can be objectively compared across vendors.

  - **Identify "to-be processes" as a visual or write-up.** These outline how existing manual or partially automated activities will change by translating existing processes into an ITRM solution. This will help to evaluate vendors in the proof-of-concept stage. Leverage existing cross-functional flow charts, if any.

  - **Identify whether the current requirement aligns to a point solution that is focused on ITRM capabilities or to a platform solution** that may address more than ITRM capabilities. The key determination in going down the integration path is to understand if all needed applications have the same or a similar level of maturity in order to leverage the benefits of an integrated platform.

Market Overview

The ITRM market's maturity level continues at early mainstream, with a market penetration of 20% to 50%; it is not projected to plateau for another two to five years. A heightened focus on cybersecurity initiatives has led to continued interest in the capabilities of ITRM solutions. These solutions support management of IT-related risk, and facilitate reporting on cybersecurity-related initiatives. Specifically of recent interest are IT risk assessment, security incident response, and security orchestration, analytics and reporting (SOAR) capabilities. Interest in ITRM initiatives will persist due to cybersecurity and privacy mandates.

According to inquiries in 2018 and 2019, bringing efficiencies in compliance tracking for IT-related risks and cybersecurity activity tracking are the primary drivers for evaluating ITRM solutions. We also continue to see more interest among buyers trying to answer inquiries from their boards or customers about ITRM's close link to cybersecurity initiatives and risk quantification requirements. This is especially true in North America and Europe; however, the Middle East, Brazil and India are also showing signs of increased interest in ITRM solutions' capabilities.

As part of our customer reference study in March/April 2019 for this Magic Quadrant, we surveyed 59 customers provided by participating vendors for their ITRM implementations. Based on their responses, we observed a preference for deployment model, and low levels of readiness in implementing ITRM solutions:

- Deployment model — Deployment preference is entirely dependent on the buyer organization's priorities and regulatory obligations. We have observed a slow, yet steady, shift to the SaaS model. In 2019, 39% of deployments were on-premises (54% in 2016), 56% are SaaS (31% in 2016), and 5% are off-premises and hosted by the vendor or a third party (15% in 2016).
- Readiness to implement ITRM solutions — Most ITRM buyers do not have defined and mutually agreed-on risk processes. This has led to the emergence of many second-time buyers in the market. ITRM solutions are bought with the hope that processes will be defined with the help of the solution. Standard workflows in ITRM solutions help ITRM teams kick-start the process definitions. However, if these workflows are not aligned to the organization's business processes, and/or buy-in from stakeholders (e.g., business, IT, security, compliance, legal and risk teams) is missing, these teams will be back in the market hoping to solve these issues with another ITRM solution. Of ITRM buyers, 34% confirmed they bought ITRM solutions in the hope that their IT risk processes will mature with the procurement. Fifty-three percent of the buyers confirmed that their primary goal was to make it easier to track and monitor compliance obligations, followed by 43% looking to automate risk remediation workflows.

Evidence

The following Gartner resources were consulted in the writing of this research:

- Primary research facilitated by the Magic Quadrant customer reference survey
- ITRM Magic Quadrant and Critical Capabilities vendor survey facilitated by project manager
- Gartner client interactions at conferences in 2018 and 2019
- Gartner client inquiries and document reviews
- Gartner Peer Insights
- 2018 and 2019 Gartner Security and Risk Management Survey
- 2019 Gartner CIO Survey

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.

About Careers Newsroom Policies Site Index IT Glossary Gartner Blog Network Contact Send Feedback