Gartner.

Magic Quadrant for Integrated Risk Management

Published 16 July 2018 - ID G00323128 - 42 min read

By Analysts John A. Wheeler, Jie Zhang, Earl Perkins

Integrated risk management enables simplification, automation and integration of strategic, operational and IT risk management processes and data. Security and risk management leaders should use Gartner's Magic Quadrant to identify solutions that support an integrated approach to risk management.

Market Definition/Description

Integrated risk management (IRM) solutions combine technology, processes and data that fulfill the objective of enabling the simplification, automation and integration of strategic, operational and IT risk management across an organization (see "Definition: Integrated Risk Management Solutions").

To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. As a result, new technology solutions are emerging to increase the collaborative nature of risk management, both within and external to an organization.

IRM Use Cases

There are a growing number of IRM vendors that automate various workflows in support of cross-organization collaboration for risk management. Through common functions, such as an asset repository, regulatory mapping, survey capabilities, workflow functions and data import, IRM vendors provide capabilities across the following six use cases:

Digital Risk Management (DRM)

DRM technology integrates the management of risks of digital business components, such as cloud, mobile, social and big data, and third-party technologies like artificial intelligence and machine learning, operational technology (OT), and the Internet of Things (IoT).

Vendor Risk Management (VRM)

Vendor risk management programs help organizations manage the risks of third parties with adequate controls for business continuity management, performance, viability, security and data protection. Failure to comply with these mandates can have significant customer- and service-related, audit-related, and, for some industries, regulatory repercussions that can undermine shareholder value and corporate viability. The VRM use case addresses risks to

regulatory compliance, information security and vendor performance arising from enterprises' increased use of, and reliance on, service providers and IT vendors. Solutions geared toward this use case have capabilities such as risk assessment, risk monitoring and/or risk rating.

Business Continuity Management (BCM)

Business continuity management is the practice of coordinating, facilitating and executing activities to identify risks of business disruptions, implement disaster recovery solutions and recovery plans, respond to disruptive events and recover mission-critical business operations. BCM software automates processes such as risk assessment, business impact analysis (BIA), and recovery plan development, exercising and invocation. Critical and enhanced capabilities that address BCM help organizations to initiate BCM programs and improve overall continuity capability.

Audit Management (AM)

Auditors independently and objectively evaluate, analyze and assess the effectiveness of an organization's system of internal control, governance processes and risk management capability. The auditors provide assurance, insight and recommendations on operational improvements to the board of directors, senior management and business process owners. Auditors do this through both auditing and consulting activities. The audit management solution market automates internal audit operations, such as audit planning, scheduling, work paper management, time and expense management, reporting, and issue management.

Corporate Compliance and Oversight (CCO)

As the compliance management program scope increases, regulatory compliance and change management becomes more complicated. An increase in focus on commercial compliance (increasingly required by business partners) and organizational compliance requirements (such as ethics and corporate social responsibility) makes compliance managers' roles challenging. Corporate compliance and oversight software supports the goals and activities of compliance leaders. CCO provides automated policy development and management, compliance risk assessment, control rationalization, assessment and attestation, regulatory change management and investigative case management.

Enterprise Legal Management (ELM)

Enterprise legal management software applications are focused on supporting legal and compliance departments, corporate secretaries, boards of directors and senior management. ELM provides better documentation, spend management, information availability and collaboration via an integrated set of applications. These applications include matter management, e-billing, financial/spend management, legal document management and business process management.

IRM Critical Capabilities

In support of these six use cases, the IRM critical capabilities provide business leaders with effective means of assessing risk and control effectiveness, identifying risk events, managing remediation efforts, and quantifying the associated risk exposure across the organization. What follows is an overview of the five critical capabilities evaluated in this report, as well as a description of their primary functions/features.

- **Risk and Control Documentation/Assessment**

  Risk statements and the related controls required to mitigate them to an acceptable level must be documented sufficiently to satisfy a number of key internal and external stakeholders — including regulators, external auditors, business partners/associates, suppliers, senior executives and board members. Statements and controls must also provide the basis for performing a comprehensive risk assessment at a strategic, operational and technological level. Features within this capability include:

  - Risk-related content, including a risk framework, taxonomy/library, key risk indicator (KRI) catalog, and legal, regulatory and organizational compliance requirements

  - Risk assessment methodology and calculation capabilities (for example, bow tie risk assessment)

  - Policy documentation and control mapping

  - Documentation workflow including authoring, versioning and approval

  - Business impact analysis/recovery plan documentation

  - Audit work paper and testing management

  - Third-party control evaluation

  - Contract management

- **Incident Management**

  Proactive management of risk incidents can lead to a reduction in business impact and inform future risk mitigation efforts. A record of incidents can be used to inform the risk assessment process and facilitate the identification of event causes. In addition, IRM solutions can integrate with external systems to identify potential risk events related to third-party risk profiles and known incidents. Features within this capability include:

  - Incident data capture

  - Incident management workflow and reporting

  - Root cause analysis

- Crisis management

- Emergency mass notification

- Investigative case management

- Legal matter management

- **Risk Mitigation Action Planning**

  When risks are assessed to be beyond defined risk tolerance levels, action plans must be developed to ensure that the appropriate mitigation steps are taken to meet the risk appetite set by the board of directors or other governance body. IRM solutions can provide support to risk professionals and business leaders in managing and testing the associated risk mitigation efforts. Features within this capability include:

  - Project management capabilities to track progress on risk-related initiatives, audits or investigations

  - Risk control testing capabilities, such as continuous control monitoring

  - Control mapping to risks, business processes and technology assets

  - Control mapping to legal requirements and compliance mandates

- **KRI Monitoring/Reporting**

  To effectively monitor risks across the organization, companies can utilize IRM solutions to aggregate and report a wide array of risk levels using key risk indicators (KRIs). Features within this capability include:

  - Risk scorecard/dashboard capabilities

  - External data integration (for example, information security vulnerability assessment data)

  - The ability to link KRIs to performance metrics

- **Risk Quantification and Analytics**

  Beyond the exercise of assessing risk from a qualitative perspective, companies in many industries (including banking, insurance and securities) seek to measure risk on a quantitative basis. Some of the quantitative analysis is used to support capital calculation requirements driven by regulatory mandates, such as Basel III and Solvency II. Other quantitative analysis methods are used to develop more precise predictive models to determine the potential for

certain operational risk events, such as fraud or theft. As such, the features within this capability include:

- "What if" risk scenario analysis capabilities

- Statistical modeling capabilities (for example, Monte Carlo simulation, value at risk, and Bayesian statistical inference)

- Predictive analytics

- Capital allocation/calculation

- Fraud detection capabilities

Magic Quadrant

Figure 1. Magic Quadrant for Integrated Risk Management

Source: Gartner (July 2018)

Vendor Strengths and Cautions

ACL

ACL is headquartered in Vancouver, British Columbia, and is privately held with a minority interest held by Norwest Venture Partners. ACL's legacy software solutions are focused on internal audit and data analytics. As such, the target buyer historically has been chief audit executive, but now has broadened to compliance, IT and risk management leaders. Its IRM solution set demonstrated for evaluation includes ACL GRC cloud platform — SaaS continuous delivery, ACL Analytics AX v.13 and ACL AN v.13. 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.

Strengths

- Geographic Strategy: ACL has invested in a wide range of geographical support and is highly rated by its references on global support coverage.

- Sales Execution: ACL's attention and focus to customer demand from sales teams have resulted in a smoother customer experience, as indicated by its references.

- Offering Strategy: ACL's rich out-of-box regulatory content combined with configurable workflows can deliver a wide range of risk data integration and reporting capabilities.

Cautions

- Product Roadmap: ACL presently has no planned focus on its roadmap to target digital business risk management and enterprise legal management capabilities.

- Market Segmentation: ACL stated a limited focus in segmenting its marketing strategy for each distinct market segment within IRM. This will be reflected in ability to support all IRM use cases.

- Industry Strategy: ACL started its industry-specific support effort in 2017, but it has teams only for government and financial services sectors.

CURA Software

CURA Software is the group name of the CURA governance, risk and compliance (GRC) product and related companies. CURA Singapore is the holding company for the group (CURA USA, CURA SA and CURA Australia), and CURA Technologies was the public traded company. In 2017, a structural change was made to go private by selling the Singapore holding to White Orchids. Software development for its CURA Platform remains based within India. CURA's main target buyers are chief risk officers (CROs) and chief compliance officers. The demonstrated solution, CURA Platform version 4.0, can be deployed through on-premises, private hosted and SaaS models. CURA's top generating verticals are government, manufacturing, banking, financial services and insurance. Primary support is provided out of respective local teams, and critical issues/development is handled by the India team. The majority (about 80%) of its customer base is in South Africa and Australia. CURA Software also has clients in the U.S., Malaysia, South America, U.K., Singapore and the Middle East.

Strengths

- Marketing Strategy: Within the critical capabilities that CURA Software supports today, the vendor presented a clearly stated view of the current market demand, as well as its evolution, and articulated a plan for how it would support such market development.

- Sales Satisfaction: Customer references' ratings on sales engagement and support are on the higher side of the score range.

Cautions

- Overall Viability: CURA Software's recent business ownership change is a risk factor for its business stability. However, CURA provided clarification that the structural change is not material for its execution; the holding company and stepdown entities continue to work independently of the structural change.

- Financial Viability: CURA's revenue has not grown in the last few years. CURA provided the explanation that with the current restructuring, the company is poised for growth.

- Geographic Distribution: Although having started in building out a global sales and support force in recent years, CURA Software's customer base is dominating in only two countries.

Dell Technologies (RSA)

RSA, a Dell Technologies business headquartered in Bedford, Massachusetts, offers its RSA Archer Suite to a broad set of roles, and supports a spectrum of IRM use cases. RSA Archer release 6.3, demonstrated for this research, has a set of use-case-based solutions that can be purchased independently. RSA's software can be deployed either on-premises or in a multitenant, private hosted environment. Implementation services are available through RSA professional services and its partners. RSA's clients are found in North America, EMEA, Asia/Pacific, Japan and Latin America across industries such as financial services, healthcare, public sector/government, professional services, transportation, telecommunications, retail, energy and technology. Four support centers are located in the U.S., the U.K., India and Australia.

Strengths

- Vertical Strategy: RSA sells to and supports a wide client base across industry sectors.

- Sales Strategy: RSA uses a maturity-based approach to segment targeted buyers. This approach can help customers to identify IRM implementation steps and RSA to align its sales and support experts with customer requirements.

- Geographic Strategy: RSA offers a fuller coverage for global users and continues to invest in supporting new IRM users outside North America. This makes the RSA Archer product a well-suited candidate for large and globally distributed business operations.

Cautions

- Time to Value: Some of RSA's references rated it less favorably in terms of deployment length, especially when implementing the RSA Archer Platform on-premises at a global scale.

- Product/Service: The RSA Archer Platform currently does not offer native capabilities to support enterprise legal management.

- Product/Service: The RSA Archer Platform scope of capabilities and features can be too complex for some small and medium clients.

IBM

IBM, 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's OpenPages Version 7.3, reviewed for this research, is offered as an on-premises, privately hosted or SaaS solution. Target buyers for OpenPages include risk and security leaders at global organizations whose short- or long-term goal is enterprisewide integrated risk management. 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

- Marketing Strategy: IBM has designed its marketing to appeal to all types of buyers both in user size and industry focus.

- Assessment and Documentation: OpenPages demonstrates effective risk assessment methodology and calculation capabilities, policy documentation and control mapping.

- Geographic Distribution: IBM's geographic support rating ranks as one of the highest in customer references.

Cautions

- Sales Satisfaction: Some references reported low satisfaction due to lengthy sales cycles and sales execution due to IBM, resulting in longer implementation times and frequent customization changes.

- Industry Focus: IBM supports all industries, but as its main customer base involves financial services, implementation and support expertise are directed by and at the financial services sector.

- Time to Value: IBM falls to the low end of the customer references' ratings on this category included in this study, including pricing.

Ideagen

Headquartered in Nottingham, U.K., Ideagen is a publicly traded company quoted on the Alternative Investment Market (AIM) of the London Stock Exchange and is a leading supplier of information management software to highly regulated industries. Ideagen's legacy solutions are focused on quality and safety management, but its newer solutions have been extended to address use cases across the IRM spectrum. Its primary solutions demonstrated for evaluation include Coruson for enterprise cloud safety and operational risk management and Pentana for audit and performance management. Ideagen solutions can be deployed in on-premises, privately hosted or SaaS environments. Ideagen's clients are located in EMEA, North America and Asia/Pacific. Its solutions are delivered across a range of industries including healthcare,

transport, aerospace and defense, life sciences, manufacturing and financial services. Support is offered primarily out of the U.K. with additional offices in Dubai and Kuala Lumpur.

Strengths

- Financial Viability: According to public financial data, Ideagen reported positive revenue growth, healthy customer base expansion, and several acquisitions.

- Product/Service: Ideagen's stated focus and R&D investment are primarily on the Coruson product, which has a product roadmap to support for an array of project scales.

- Vertical Industry Strategy: Ideagen has the heritage and expertise in supporting for safety in aviation and rail transportation and quality management in manufacturing among the evaluated vendors in this study.

Cautions

- Sales Strategy: Ideagen has only been leveraging direct sales and currently has limited support for North America, which hinders its market reach.

- Offering Strategy: Ideagen's IRM capabilities today include basic analytics, and advanced risk data analyses require implementations via Ideagen's APIs.

- Marketing Strategy: Ideagen has a broad statement on future market requirements without specifics on business continuity management or full support for digital risk management.

Lockpath

Lockpath, privately held and headquartered in Overland Park, Kansas, offers the Keylight platform as its IRM solution. It targets the following buyers: chief information security officers (CISOs), compliance teams and CROs. Keylight 4.8, 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 Overland Park, Kansas. Implementation services are delivered by Lockpath's professional services team and a network of global partners.

Strengths

- Marketing Strategy: Lockpath has wide market presence in company size and industry sector.

- Time to Value: References have consistently reported positive results on time to value with their Lockpath IRM implementation projects, attributed primarily to Lockpath's QuickStart program.

- Product Capabilities: Lockpath's Keylight platform has a full range of function across all desired IRM critical capabilities.

Cautions

- Vertical/Industry Strategy: Lockpath does not currently provide a path to support all features for legal-risk use cases.

- Sales Strategy: Despite Lockpath's leverage on joint sale and upsale opportunities, its sales force and channel are limited in one region — North America.

LogicManager

LogicManager is headquartered in Boston, Massachusetts, 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% the client base. Technical support is provided from the Boston, Massachusetts, headquarters and from Europe satellite offices.

Strengths

- Time to Value: References frequently reported rapid deployment as a characteristic of their LogicManager projects, and a higher number of project length is reported as three or fewer months.

- Offering Strategy: LogicManager has a stated product roadmap emphasizing simplicity and usability. It advocates designing functionalities to attract higher end-user engagement or self-service.

- Market Understanding: Among the evaluated vendors in this study and ranked by customer references, LogicManager received the highest rating for this measure.

Cautions

- Industry Coverage: Due to its customer concentration in financial services, some customers had negative feedback on LogicManager's expertise outside its main customer base.

- Product/Service: Though LogicManager has large-enterprise customers, the company's service structure is currently optimized to support midsize enterprises.

- Geographic Distribution: LogicManager's primary support is based in Boston, Massachusetts, a risk factor for globally distributed risk teams.

MetricStream

MetricStream, privately held and headquartered in Palo Alto, California, targets a wide range of buyers, including all primary C-suite executives, plus buyers such as CISOs, VRM executives and quality management executives. MetricStream's M7 platform, demonstrated for this research, can be deployed via SaaS or a privately hosted, hybrid or on-premises model. Over 45% of its revenue comes from the financial services sector. About 45% of its customer base is outside the U.S. Support is provided from centers in Palo Alto, California; New York; London; Milan; Dubai; and Bangalore, India.

Strengths

- Financial Viability: MetricStream has dozens of investors, including Goldman Sachs among other venture capitalists. The company's risk is rated low with a healthy financial performance by D&B Hoovers.

- Marketing Strategy: MetricStream has a stated marketing strategy that appeals to new IRM buyers and projects designed to modernize risk management practices.

- Market Responsiveness and Track Record: References reported higher satisfaction in their experience with MetricStream's sales and support.

Cautions

- Product/Service: Some early MetricStream M7 platform adopters reported performance issues and lack of customization support for advanced reporting features.

- Sales Execution/Pricing: For global distributed risk teams or large-scale projects, MetricStream's contracting and pricing can be complex.

- Offering Strategy: MetricStream's M7 platform released April 2017 has aimed to serve pent-up demand for a faster and simpler IRM solution, but early reports from upgrade customers are mixed.

Mitratech

Mitratech is a privately owned company headquartered in Austin, Texas. Its portfolio of enterprise legal and risk management solutions serves the needs of corporations throughout their legal departments, compliance and risk functions, and executive leadership teams. The IRM solution set demonstrated for evaluation includes TeamConnect 5.1, Compliance Manager 15.02 and PolicyHub 5.0.1. Mitratech's solution set can be deployed in both SaaS and privately hosted environments or on-premises. Clients are located in the Americas, EMEA and Asia/Pacific. Industries represented across Mitratech's client base include financial services, manufacturing, energy/utilities and professional services. Primary support is based in Mitratech's headquarters in Austin, Texas, with additional support teams in Houston, Texas; Blue Bell, Pennsylvania; Slough, U.K.; Swansea, U.K.; and Melbourne, Australia.

Strengths

- Market Responsiveness and Track Record: Mitratech gained the highest rating from customer references for this category among all the evaluated vendors in this study.

- Marketing Strategy: Mitratech has a stated strategy that appeals to a wide range of enterprise buyers involved in risk management, including enterprise legal management, compliance management, and environmental, health and safety.

- Geographic Strategy: Due to its established expertise in supporting a wide range of legal and compliance teams that typically represent multiple jurisdictions and complex legal operation requirements, Mitratech has a fuller support for all regions.

Cautions

- Offering Strategy: While the evaluated products have shared IRM elements to connect them, customers need to buy multiple products from Mitratech to support their IRM capabilities.

- Product/Service: Mitratech currently has no support for vendor risk, digital risk and business continuity management.

- Operations: Mitratech went through a phase of high merger and acquisition activity for technology assets, especially in 2015. Product integration, support and innovation focus across multiple products are risk factors.

Nasdaq

Headquartered in New York City, New York, Nasdaq's primary IRM platform, BWise, targets the following buyers: all C-suite-level executives, including corporate controllers and chief audit executives. BWise is part of a broader offering of board and governance software solutions and services. Version 5.0.1, demonstrated for this research, can be deployed in a single-tenant, private hosted environment or on-premises. BWise has customer distribution in all regions, with primary focus in North America, Europe, Asia/Pacific and Australia/New Zealand. Approximately 40% of its revenue is from the financial services sector. Support is provided across the globe but centralized in New York, the Netherlands and Portugal.

Strengths

- Geographic Strategy: Thirty percent of Nasdaq's client base is in the U.S., 40% is in Europe, and the remainder is spread across the globe. The strategy reflects the parent company's reach.

- Sales Execution: A simple subscription-based or perpetual-license model (hosted/SaaS or stand-alone) along with enterprise and midtier options provides flexible spending choices for customers.

- Overall Viability: As part of a global enterprise with extensive international experience in financial and corporate services and service partners to provide strategic information, Nasdaq is well-positioned for IRM clients.

Cautions

- Overall Viability: While gradually diversifying across IRM use cases, over 70% of deployments are focused on IT (digital) risk management, corporate compliance and audit.

- User Experience — Reference customers noted some concerns in postdeployment customer support.

- Product/Service: The business continuity management workflow process is limited primarily to documentation steps.

Resolver

Resolver is headquartered in Toronto, Ontario, and is privately held. Almost half of Resolver customers are in financial services and manufacturing, with the remainder in education, healthcare and other businesses. Resolver Core was demonstrated for this research. Core is a "cloud first" application deployed on Amazon Web Services (AWS). Resolver targets clients located predominantly in North America (70%) and the U.K., although more international expansion is planned. The company has 24/7 emergency support coverage and scheduled support from offices in London, U.K.; Toronto, Ontario; Charleston, West Virginia; Edmonton, Alberta; Sunnyvale, California; Christchurch, New Zealand; and Hyderabad, India.

Strengths

- Overall Viability: Though initially backed with venture funding for acquisitions, Resolver does not require investment to operate.

- Product/Service: Data visualization capabilities in incident management and risk mapping are useful to nontechnical audiences at simplifying complex relationships.

- Sales Execution and Pricing: As a cloud-based service, Core's pricing model is simple, based on a fixed annual fee for integrated use cases plus a platform fee for a "full user" — one with access across use cases.

Cautions

- Overall Viability: Resolver is one of the later entrants to the IRM market and possesses a limited number of IRM customers at this stage. The principal geographic focus remains North America, although some international expansion is beginning.

- Vertical Industry: Resolver does not yet have a vertical-industry market focus, with half of client revenue from financial services or manufacturing.

Riskonnect

Riskonnect is a privately held company headquartered in Kennesaw, Georgia, with offices in Atlanta, Chicago and London, and software development teams based in Mangalore and

Ahmedabad, India. In June 2017, Riskonnect was purchased by Thoma Bravo, a U.S.-based private equity investment firm. Riskonnect acquired GRC provider Aruvio in late 2017.

Target buyers include executives who want a consolidated view of risk (for example, the CIO, CISO, CFO and other C-level buyers). Riskonnect is a pure SaaS provider and demonstrated its IRM product version 2017 release 2 for this research. Riskonnect offers its product in North America, EMEA and Asia/Pacific with particular focus in manufacturing, retail and consumer goods, healthcare, construction and engineering, energy and utility, mining and natural resources, telecom and IT, transportation and logistics, financial services, and insurance.

Strengths

- Product/Service: Riskonnect operates on the Salesforce Lightning platform and is designed as a SaaS application delivery method. This aids in rapid deployment scenarios.

- Vertical Industry: Riskonnect has a relatively even distribution across at least four verticals (retail, manufacturing, transportation and insurance) with growth in others and provides approximately 600 APIs to support those verticals.

- Innovation: Almost one-third of Riskonnect's research and development is devoted to mobile capability enhancements and portal growth for simpler customer experience.

Cautions

- Deployment/Integration: While flexible, Riskonnect's use of Salesforce Lightning as a delivery platform may influence consideration by non-Salesforce clients.

- Innovation: Research and development spending as a percentage of annual revenue is slightly lower than many of Riskonnect's competitors.

- Product/Service: Riskonnect does not provide significant legal management functionality or statistical modeling capabilities.

Rsam

Rsam is headquartered in Secaucus, New Jersey, and is privately held. Target buyers include boards and executives who want a consolidated view of risk and CIOs who prefer to work with a handful of vendors/partners rather than siloed applications. Rsam version 9.2 Update 3, demonstrated for this research, can be deployed in on-premises, privately hosted or SaaS environments. Rsam targets clients located in North America, Europe, the Middle East and Asia/Pacific, as well as clients in healthcare, financial services, government, retail, education and energy. Rsam has a global 24/7 support team with support offices in New Jersey, U.S., and Bangalore, India.

Strengths

- Innovation: Rsam possesses an innovative approach to building relationships between any defined "object" (person, process, technology or data) as a foundation for its IRM management,

analysis and reporting approach.

- Product/Service: Rsam architecture permits scaling the databases used and external sources linked to manage large and complex IRM deployments. Content templates across these verticals, along with vertical information service partners, also provide options for clients in many verticals.

- Vertical Industry Strategy: Rsam has balanced distribution of customers across multiple verticals, including healthcare, financial services, government, retail and others.

Cautions

- Customer Experience: Although innovative in architecture and design, Rsam's object-oriented approach is not immediately intuitive to nontechnical users and requires training for many customers.

- Product/Service: Rsam does not possess functionality for legal risk management or emergency mass notifications, although some external integration to partner offerings is possible.

SAI Global

SAI Global, headquartered in Chicago, offers its Digital Manager 360 and Compliance 360 platform to the following buyers: compliance teams, risk managers and CROs, CIOs and CISOs. Digital Manager 360 version 2017.2 and Compliance 360, demonstrated for this research, are delivered primarily via privately hosted or SaaS environments. This solution focuses on sectors such as healthcare, life sciences, retail, financial services, manufacturing, energy and utilities. The client base is distributed across Europe, U.K./Ireland, Middle East/Africa, North America and Asia/Pacific. Customer support is offered in the U.K., Germany, Middle East, Asia, Australia and the U.S.

Strengths

- Customer Effectiveness: Clients continue to report high levels of satisfaction with presales and postsales support, including pricing, implementation, customization and ease of use.

- Geographical strategy: Changes in resource commitments have improved SAI Global's international coverage.

- Product/Service: SAI Global possesses robust incident management capability, support for privacy compliance and General Data Protection Regulation and effective third-party connectivity for monitoring and reporting functions.

Cautions

- Product/Service: SAI Global capabilities do not include significant legal matter management, scenario analysis or statistical modeling capabilities for calculating risks.

- Overall Viability: While SAI Global has significant deployments, growth in new clients has slowed slightly as competition stiffens and the market shifts to IRM.

ServiceNow

ServiceNow, a public company based in Santa Clara, California, built ServiceNow governance, risk and compliance on the ServiceNow platform (platform as a service) offering. The IRM solution targets buyers such as IT security teams, risk management directors and internal audit teams. ServiceNow GRC, version Jakarta, 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, Asia/Pacific and Australia/New Zealand, but also has limited presence in the Middle East and Latin/South America. ServiceNow 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/Service: ServiceNow possesses strong IT risk capabilities, particularly in risk and control documentation and in incident management.

- Customer Experience: Technical support is 24/7, and ServiceNow has service centers globally and well-attended conferences and forums.

- Geographic Strategy: ServiceNow possesses a significant global footprint and matching partner model, particularly in consulting and system integration partnerships.

Cautions

- Sales Execution/Pricing: Pricing due to bundling and subscription complexity can be challenging for clients, and customers have noted that some implementations can be more time-consuming than expected.

- Product/Service: ServiceNow does not yet possess significant scenario planning and statistical modeling functionality for risk calculation.

Thomson Reuters

Thomson Reuters, headquartered in New York City, New York, offers a spectrum of risk-and-compliance-related technologies and services. Its IRM software and services target the following buyers: CROs and managers of enterprise compliance and risk teams. Thomson Reuters' Connected Risk v.17.2, demonstrated for this research, can be deployed via on-premises, hosted and SaaS models. However, the majority of its customers are deployed on-premises. Thomson Reuters' customer base is widely distributed across financial industry sectors and major geographical regions. Primary product support is delivered by service centers in the U.S., U.K., and Philippines.

Strengths

- Product/Service: The Connected Risk platform provides a toolkit-style approach for developing customer portal screens and effective integration with third-party sources of information required for monitoring, analysis and reporting.

- Sales/Geographic Strategy: Thomson Reuters is a global company with a matching support organization. Connected Risk is also one of the lowest-cost offerings in IRM for capabilities offered.

- Product/Service: Complementary Thomson Reuters products, such as World-Check for third-party risk information and legal management portfolio, provide an extended set of IRM input as required.

Cautions

- Vertical Industry Strategy: Connected Risk remains predominantly a significant banking and financial services IRM offering, although aggressive growth plans target manufacturing, technology and communications, and others.

- Product Strategy: Relative product satisfaction and perceived value among Connected Risk customers score slightly lower than competitor offerings.

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

Not applicable because this is a new Magic Quadrant.

Dropped

Not applicable because this is a new Magic Quadrant.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research. To qualify for inclusion, a vendor must demonstrate the following:

- The vendor must have the ability to significantly address (on an enterprisewide basis) at least 65% of the key functions/features across the five critical capabilities listed in the report.

- The vendor must have 200 or more customers currently using its IRM solution.

- The vendor must derive revenue from the sale of IRM solutions and related services (for example, implementation/training, software product customization and so on) in three or more of the following global regions — North America, Latin America, EMEA, Japan and Asia/Pacific.

- The vendor must also demonstrate full support of at least three use cases, as defined above, in its generally available product(s).

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation within Gartner's view of the market.

Product/Service: This criterion involves the core goods and services offered by the vendor that compete in/serve the defined market. This also includes current product or service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships, as defined in the market definition. Evaluation ratings are derived from formal product demonstrations and customer feedback.

Overall Viability (Business Unit, Financial, Strategy, and Organization): This criterion is an assessment of the overall organization's financial health and the financial and practical success of the business unit. It is also an assessment of the likelihood that the individual business unit will continue to invest in the product, offer the product, and advance the state of the art within the organization's portfolio of products. Revenue growth and the product implementation growth trend over the past three years are primary determinants of the viability rating. Customer perception of future viability is also considered.

Sales Execution/Pricing: This criterion involves the vendor's capabilities in all presales, sales and postsales activities, and the structure that supports them. This also includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. Customer ratings of the quality of sales-related activities as well as an evaluation of the clarity and competitiveness of the vendor's pricing structure are primary determinants in rating this criterion.

Market Responsiveness and Track Record: This criterion involves the vendor's 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. Customer ratings are a primary factor.

Marketing Execution: This criterion involves the clarity, quality, creativity and efficacy of programs that are designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity as well as promotional, thought leadership, word of

mouth and sales activities. Customer ratings of the vendor's effectiveness in responding to requests for information and RFPs are considered.

Customer Experience: This criterion involves the 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 also can include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on. Customer ratings are the primary determinant when evaluating this criterion.

Operations: This criterion involves the organization's ability 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.

Table 1: Ability to Execute Evaluation Criteria

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

Source: Gartner (July 2018)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements. This includes current and future market direction, innovation, customer needs, and competitive forces and how well they map to Gartner's view of the market.

Market Understanding: This criterion involves the vendor's ability to understand buyers' needs and to translate those needs into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those wants with their added vision. One key factor is customer ratings of the vendor's ability to fulfill its critical functional capabilities using its IRM or business process experience.

Marketing Strategy: This criterion involves a clear, differentiated set of messages that is consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements. The vendor's ability to target specific market segments by addressing unique industry or geographic requirements is a primary determinant of this criterion rating.

Sales Strategy: This criterion involves the strategy for selling products using the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extends the scope and depth of market reach, skills, expertise, technologies, services and the customer base. Customer ratings of the vendor's pricing strategy also are considered.

Offering (Product) Strategy: This criterion involves a vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology, and feature set as they map to current and future requirements. Evaluation factors include customer ratings of the vendor's product performance and scalability, as well as the product's roadmap for future enhancement.

Business Model: This criterion involves the soundness and logic of a vendor's underlying business proposition. Evaluation of this criterion includes the sustainability of the model given current and projected economic and environmental conditions.

Vertical/Industry Strategy: This criterion involves the vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical industries. Customer ratings of the vendor's industry-related experience also are considered.

Innovation: This criterion involves direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes. Included in this criterion is an evaluation of product roadmaps as well as past and planned levels of R&D investment.

Geographic Strategy: This criterion involves 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 those geographies and markets. A vendor's ability to generate a significant level of revenue outside its native geography is considered a key factor in rating this criterion.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Market Understanding	Medium
Marketing Strategy	Low
Sales Strategy	Low

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

Source: Gartner (July 2018)

Quadrant Descriptions

Leaders

The Leaders in the IRM market display significant progress in adopting integrated risk architecture and market strategy and have deployed products and services along with support in significant numbers. Leaders have existing and sometimes complex IRM deployments across most use cases documented in this report, industry verticals and major global geographic regions.

Leaders: Dell Technologies (RSA), IBM, MetricStream, ServiceNow

Challengers

Challengers in the IRM market have good execution and address many critical capabilities as defined in this report. Challengers are still evolving strategy and architecture that fully addresses IRM use cases and industry verticals. They are capable of being future leaders as long as they complete a consistent vision and innovate by having a common delivery architecture for IRM critical capabilities for customers in most vertical industries.

Challengers: ACL, Ideagen, Lockpath, LogicManager, Nasdaq, Thomson Reuters

Visionaries

Visionaries set the pace for innovation and approach to some IRM critical capabilities. They have a high awareness of and can articulate important market trends and directions in method of delivery and approaches to integrated risk business concerns. However, Visionaries may not be in a position to fully deliver and consistently execute on that vision. Broad geographic coverage and large complex deployments may not be as frequent as those found in the Leaders quadrant at this time.

Visionaries: Mitratech, Riskonnect, Rsam, SAI Global

Niche Players

Niche Players have evolved a strategic approach to IRM that is in early stages of delivery. They may focus on a particular segment of the market, such as smaller organizations with more modest requirements, or on one or two critical capabilities while providing some features for other capabilities. Innovation and execution exist but may not be as consistent as other companies in other quadrants. Niche players know what is needed for IRM success but may be limited in execution abilities due to geography, size or sales focus.

Niche Players: CURA Software, Resolver

Context

Companies must ensure that they are using comprehensive and integrated risk management solutions in order to assess the various risk types in their organizations. Regulators and other stakeholders pay much more attention to risk management practices as part of their financial supervision. The lack of comprehensive modeling and reporting not only could result in lower credit ratings by financial services providers, but also could threaten the public accreditation of organizations.

IRM solutions also require consistent risk management policies, which often necessitate staff retraining, as well as the implementation of new compliance policies and procedures. The change management associated with establishing a risk-aware culture and implementing new policies is often the most difficult aspect of adopting IRM.

In addition, it is crucial to harmonize and consolidate data sources across the company on a continual basis, rather than at a single point in time. This may create some challenges from a process perspective, as well as from an IT redesign perspective. The integration of various data sources is, on the other hand, critical for the eventual success of a top-down risk management dashboard that is accurately displaying bottom-up data. While some companies may aspire to have a single IRM platform to cover all risks, it may be more practical to have several IRM solutions that each focuses on related risk areas, such as IT risk or business continuity. The ultimate goal should be deploying IRM solutions that can be integrated, and that can fit the existing IT architecture.

Market Overview

To better address the needs of global CEOs and senior executives, end-user organizations are shifting focus away from governance, risk and compliance (GRC) to IRM solutions. Gartner defines IRM solutions as the combined technology, processes and data that fulfill the objective of enabling the simplification, automation and integration of strategic, operational and IT risk management across an organization (see "Definition: Integrated Risk Management Solutions"). IRM goes beyond traditional, compliance-driven GRC technology solutions to provide actionable insights that are aligned with business strategies, not just regulatory mandates.

The term "GRC" was spawned from the need for better internal control and governance within large enterprises in the early 2000s. Much of this need was driven by the compliance requirements associated with the U.S. Sarbanes Oxley Act of 2002

(https://www.sec.gov/about/laws/soa2002.pdf) , better known globally as SOX. Over time, GRC grew and evolved to become associated with many compliance-driven initiatives designed to improve corporate governance and internal control. Examples of regulatory and industry standard compliance mandates include:

- The Federal Financial Institutions Examination Council (FFIEC)

- Payment Card Industry (PCI) Security Standards Council

- Health Insurance Portability and Accountability Act (HIPAA)

- International Organization for Standardization (ISO) 27001

- National Institute of Standards and Technology (NIST) 800-34 and 800-53 standards

Risk management — in particular, operational and IT risk management — continues to mature as a discipline and is becoming a more practical approach to improve corporate governance and internal control. As such, Gartner and other organizations have recognized a need for new thinking on the subject. In early 2014, the NIST released its Cybersecurity Framework (https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf) recommending the development of IRM programs within organizations to support the reliable functionality of critical infrastructure.

Past Gartner surveys indicated that clients were not familiar with the term GRC, nor were they currently using or looking to implement GRC software. Yet many global CEOs and senior executives have stated that their investment in risk management tools and practices is falling behind.

The IRM market is projected to grow at a 13.4% compound annual growth rate (CAGR) to reach $7.3 billion by 2020. In 2015 and 2016, the market grew 17.4% and 17%, respectively, from a base market size of $3.9 billion in 2015 (see "Forecast Snapshot: Integrated Risk Management Solutions, Worldwide, 2017").

The IRM market is the largest of all the solution provider markets covered by Gartner in the security and risk management (SRM) software ecosystem (see "Market Opportunity Map: Security and Risk Management Software, Worldwide"). It also ranks third highest in terms of estimated profitability margin. As a result, this is one of the most dynamic software markets within our coverage and looks to be one to watch for the next several years.

In a recent survey of more than 300 senior executives worldwide, the Financial Times and global law firm Ropes & Gray [1] discovered that 87% of organizations believe greater collaboration between their risk managers would improve the overall risk profile. In addition, 69% of organizations are not confident their current risk management policies and practices will be enough to meet their future needs.

These findings support results from Gartner's recent CEO survey and demonstrate the pressing need for integration among the various risk management domains. In fact, in the same Financial Times survey, organizations rated two key IRM domains — regulation/compliance and cybersecurity — as the least prepared and requiring the greatest amount of resources in the next year.

Evidence

[1] "Risky Business: Mitigating Exposure Through Comprehensive Risk Management." (https://www.ropesgray.com/en/Global-Risk-Management-Report) Ropes & Gray and FT Remark.

The Magic Quadrant reference check is part of the data gathering effort to help Gartner build on our existing knowledge of vendors in a particular market. During the kickoff of the process to create the Magic Quadrant for integrated risk management solutions, all invited vendors were asked to submit references that generally represented the inclusion criteria. The vendors provided reference contact information, which was used to invite the reference to complete a 25- to 30-minute online survey. A total of 65 references from 18 vendors completed the survey.

Please note that vendor reference data is different from primary research and is not a representative knowledge base of the integrated risk management solution market. The references do not represent customers in the overall integrated risk management solution market, but rather just the select customers the vendors chose to share with Gartner that ultimately elected to participate as a reference check.

Profile— Of the references surveyed, 40% were from the banking industry with manufacturing (14%) and services (10%) as the next largest verticals. Of surveyed references, 65% are from global and large enterprises (as per the Gartner definition of more than $1 billion in size). Of surveyed references, 56% identified "security and risk management" as their job role.

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

Gartner.