Navigating the Vendor Risk Management Solution Market

Published 21 June 2021 - ID G00745780 - 13 min read
By Analyst(s): Joanne Spencer, Luke Ellery
Initiatives: Sourcing, Procurement and Vendor Management Leaders; Technology, Information and Resilience Risk

The market for vendor risk management products and services is complex, diverse and evolving, making it difficult to know how to choose the right solution. This research will help sourcing, procurement and vendor management leaders map their VRM use cases to what the market can offer.

Overview

Key Findings

- The vendor risk management (VRM) solutions and services market is growing in response to increased regulatory requirements and the proliferation of business-acquired technologies, such as cloud and Internet of Things (IoT).

- Most organizations select a mix of solutions and services to confront the risk domains relevant to their industry and geography to meet their legal and regulatory obligations.

- Organizations often struggle with a proliferation of unintegrated services and solutions that exist across various departments, making it difficult to present a coordinated discussion with third parties or to present a consolidated risk position for the organization.

Recommendations

Sourcing, procurement and vendor management (SPVM) leaders responsible for vendor risk management strategy and operations:

- Develop your organization's requirements for risk management of third parties by defining your requirements and use cases for the risk domains relevant to your organization's context and the problem you are trying to solve.
Identify the vendors that support your use cases and requirements and develop a roadmap to implement and integrate the services and solutions required to effectively and efficiently address third-party risk for your organization.

**Introduction**

Third-party/vendor risk management (VRM) is increasingly important due to a growing reliance on technology vendors and service providers to realize an organization’s strategic and operational objectives (see *The SolarWinds Orion Breach and Enterprise Risk Management: A Pragmatist’s Guide*). There have been a steady expansion of industry and geographic regulatory requirements, as well as significant third- and fourth-party cybersecurity breaches, which are attracting the attention of board risk committees.

However, third-party/vendor management leaders struggle with the most effective way to address vendor risk across the sourcing and vendor management life cycle.

In response to additional regulation, an increasing number of providers offer a diverse range of services and solutions to assist with the identification, assessment, analysis, remediation and monitoring of vendor risks. SPVM leaders should use this research to uncover relevant requirements and use cases, and then target the appropriate mix of services and solutions, as presented in Figure 1. Solution and service terms are defined in Table 1.
Figure 1. VRM Solutions, Services and Data Used to Efficiently Manage Vendor Risk

VRM Solutions, Services and Data Used to Efficiently Manage Vendor Risk

- Consultants
- Content/Data Feeds
- Integrated Risk Management
- Solutions, Services and Data
- Exchanges
- Vendor Risk Management
- Cyber Vendor Risk Management
- Security Rating Services

Source: Gartner 745780_C
Table 1: VRM Market Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultant</td>
<td>Builds a VRM framework, implements solutions, provides assessment support/managed services</td>
</tr>
<tr>
<td>IRM (Integrated Risk Management)</td>
<td>Software platform for assessment, monitoring, reporting, remediating risks and provides a comprehensive business view</td>
</tr>
<tr>
<td>VRM (Vendor Risk Management)</td>
<td>Software platform for assessment, monitoring, reporting, remediating vendor risks</td>
</tr>
<tr>
<td>SRS (Security Rating Service)</td>
<td>Cybersecurity data collection, rating and monitoring service</td>
</tr>
<tr>
<td>Exchanges and Marketplaces</td>
<td>Platform for collecting, validating, sharing vendor risk and security assessments</td>
</tr>
<tr>
<td>Content/Data Feeds</td>
<td>Public and private vendor risk data collection and data feeds</td>
</tr>
</tbody>
</table>

Source: Gartner (June 2021)

**Analysis**

**Define Requirements and Use Cases**

Organizations are exposed to a wide variety of risks when they work with technology vendors, including financial, operational, security, regulatory, geographic and strategic risk categories. VRM is the capability that identifies, assesses, analyzes, remediates and monitors these risk categories specific to a technology vendor and the products or services it provides (see Figure 2).
The reasons SPVM leaders pursue a VRM function are varied. Some SPVM leaders are responding to regulatory compliance — doing what's necessary to address legal requirements or address audit issues as regulations continue to expand and regulatory agencies increase their oversight of VRM programs. Others look to improve their efficiency in managing vendor performance.

When defining your requirements and use cases, consider what processes and information currently exist within your organization, for instance: Do you have an existing risk management function and tools? Do you have all the data you need to support how you assess risk? Are you looking to automate your existing practices? The following are example key use cases that Gartner observes for investing in vendor risk management tools and services:
Match Your Use Cases and Requirements to the Right Set of Solution Vendors in the Market

Vendor risk is a very broad concept and has a different focus and priorities driven largely by the types of threats as well as various laws and regulations in different industries and geographies. Risk management includes the capability to identify, assess, mitigate and monitor these risks. A large number of vendors claim to offer risk management solutions, but due to the different types of risk, the market is fragmented — no solution covers all risks. In this section, we explain the various vendor capabilities outlined in Figure 1.

Consulting

Consultancies have staff armed with frameworks to implement a vendor risk management program for most industries, supported by assessment tools. They have experience in implementing some integrated risk management (IRM) and VRM solutions, and may offer support in assessing vendor risks. They can also support you with advice, skills, strategies and techniques to improve your capability, and can audit your processes to identify gaps with suggested actions for improvement.
When to Consider: Use a consultancy when you have no framework, governance or process, and lack VRM domain expertise and resources. Consultants can help define and build a VRM practice, including processes, workflows, governance models, identification and selection of technologies, implementation services, and ongoing support of vendor risk assessment and monitoring. Also consider other support forums specific to your industry (such as SIFMA for financial services in the U.S., or HealthIT for healthcare in the U.S.) and Gartner research when establishing a VRM capability for the first time.

Sample Vendors: Deloitte, EY, KPMG, PwC

Integrated Risk Management Vendors

IRM encompasses a holistic analysis of internal and external risk factors. To understand the full scope of risk, organizations require a comprehensive view across all business units, risk and compliance functions, and key business partners, suppliers and outsourced entities. Therefore, IRM scope is broader than just vendor risk and vendor management — however, not all IRM solutions have a VRM offering. Due to the closely related deliverables, companies that rely heavily on IRM solutions may find the capabilities of their preferred solution adequate if it matches the desired use case for vendor risk management.

When to Consider: Your organization may already have an IRM solution that includes a VRM module or application. A key decision criterion is whether your intention is to solve only the VRM requirements or to scale up a solution to address a broader category of risks. Some organizations have an IRM strategy that is dependent on a single platform for common database, UI, processes and workflows, while others may have a strategy dependent on a “best-of-breed” approach. The major categories of risk within an IRM include digital risk management, vendor risk management, business continuity management, audit management, corporate compliance and oversight and enterprise legal management (see Why Leading Providers Have Shifted Technology From GRC to IRM).

Sample Vendors: Galvanize, NAVEX Global, MetricStream, ServiceNow

Recommended Reading: Magic Quadrant for Integrated Risk Management Solutions

Vendor Risk Management Vendors
VRM helps organizations manage the risks of third parties with adequate controls for business continuity management, vendor performance, vendor viability and data protection. The IT VRM market addresses risks related to regulatory compliance and information security that arose from enterprises’ increased use of, and reliance on, third-party IT service providers and IT vendors. Solutions in this market have capabilities ranging from risk assessment to risk monitoring and risk rating, and some have additional functionality such as contract management and vendor performance management.

**When to Consider:** Consider a VRM platform as the foundation for a vendor risk management function, or when you are also looking for elements that support your broader vendor management capabilities. Consider your requirements carefully. Your organization may already have an IRM or GRC solution, and contract and performance management may be managed elsewhere (via a supplier performance, governance or CLM solution, for example), obviating the need for an additional VRM investment.

**Sample Vendors:** Aravo, Ncontracts, OneTrust, Prevalent, ProcessUnity, Venminder

**Recommended Reading:** [Critical Capabilities for IT Vendor Risk Management Tool](#)

**Security Rating Services**

Security rating services (SRS) provide continuous, independent and quantitative technical analysis and scoring for public-facing digital assets of organizational entities across geographies.

The services gather data from public and private sources via nonintrusive means, analyze the data and rate entity security posture using their own scoring methodologies. These tools can be used for internal security, cyber insurance underwriting, mergers and acquisitions, and third-party risk assessments and monitoring, including geopolitical risk.

**When to Consider:** Use security rating services to supplement vendor evaluation (precontract) as well as to support ongoing vendor risk management (postcontract) to determine changes in a vendor’s cybersecurity risk posture. Information is primarily publicly sourced from accessing internet IP addresses and “honeypots,” analyzing dark web/deep web content, and via individual proprietary data warehouses, some of which vendors in the market have acquired. Their use is aided when the SRS data can feed into a VRM or IRM platform — initiating a workflow for action if a rating changes beyond an acceptable threshold.

**Sample SRS Vendors:** BitSight, Black Kite, ISS, RiskRecon, SecurityScorecard
Recommended Reading: Innovation Insight for Security Rating Services

Cyber VRM Services

There is an evolving market of vendors that are focused on third-party cyber assessment. These offerings are responding to client demands to supplement their internal security operations center with a capability focused on external third parties beyond their own firewalls. Vendors in this space provide services such as:

- Understanding your security control posture and tailoring cyber assessments accordingly
- Vendor questionnaires
- Security risk quantification techniques
- Recommending additional controls third parties should implement
- Directly working with third parties to remediate risk
- Presenting a third-party external scorecard
- Integration with IRM, GRC and VRM solutions

**When to Consider:** If your security risk organization is resource-constrained, or does not have the internal capability or expertise to assess third-party cyber risk effectively. The cyber VRM service can effectively provide oversight of your third parties and integrate back into your internal team's SOC. However, this is a relatively new and evolving market, and Gartner observes a variety of capabilities and maturity, so ensure you are clear on your requirements and seek demonstration of vendors capabilities and reference checks.

**Sample Cyber VRM Service Vendors:** C2 Cyber, CyberGRX, Panorays, UpGuard

**Exchanges and Marketplaces**
Exchanges and marketplaces are platforms that collect, validate and share vendor risk and security assessments. Information is gathered from primary and secondary sources and validated, which enables vendor risk managers to make more informed decisions about third-party vendors, and provides this information through a secure platform. Some sharing platforms are based on a specific framework (NIST 800) and may offer little flexibility to meet some client-specific assessment requirements. Some platforms focus on specific industries, such as financial services or healthcare. When using exchanges, clients may have to be willing to accept a single standard method of assessing and reporting on vendor risks.

**When to Consider:** Use exchanges and marketplaces when you are resource-constrained and your risk requirements for your organization and industry are addressed by the exchange. The market for exchanges is evolving, and most clients do not rely on exchanges as the sole basis for their risk assessments. However, this may change as the maturity of the exchanges develops.

**Sample Vendors:** CyberGRX, IHS Markit, OneTrust, Prevalent, TruSight

**Recommended Reading:** Hype Cycle for Risk Management, 2020

**Content/Data Feeds**

Third-party data vendors provide public and private vendor risk data collection and news data feeds on a subscription basis. These are some of the most established and often well-embedded data sources within organizations today.

**When to Consider:** Use vendor risk data and analytics to supplement your vendor evaluation (precontract) as well as support your ongoing vendor risk management (postcontract) to determine changes in a vendor’s risk posture. There are many different types of datasets, so consider the most important risk factors for your organization to prioritize your investment in these data sources. Consider the business case for process efficiency as well as confidence in the risk-based decisions you support.

Below is a list of key types of vendors and associated sample vendors.

**Financial Metrics and Ratings**

**Sample Vendors:** Dun & Bradstreet, LexisNexis Risk Solutions (for monitoring financial, political, legal and environmental risks), RapidRatings, S&P Capital IQ (for financial data), Refinitiv (formerly Thomson Reuters)
Third-Party Ratings

Third-party ratings are interpreted scores based on a proprietary scoring methodology.

Sample Vendors: D&B Supplier Evaluation Risk Rating (SER Rating), EcoVadis’ Corporate Social Responsibility (CSR) rating, RapidRatings’ Financial Health Rating, Resilinc’s supply risk ratings

Risk Assessment Service Bureaus

Risk assessment service bureaus conduct custom-made assessments to address client-specific needs.

Sample Vendors: Achilles (for multitier supply chain mapping services), Bureau Veritas (for quality inspections), Prevalent (for IT security risk assessments)

Packaged Risk Assessment Solutions

Packaged risk assessment solutions provide content such as preconfigured surveys, letters or process know-how for compliance with a particular regulation or industry-specific requirement.

Sample Vendors: Aravo, Coupa (Hiperos), Steele (Securimate), The Red Flag Group

Recommended Reading: How to Navigate the Fragmented Supplier Management Solutions Market

There are many objectives when implementing vendor risk management solutions, such as improving:

- Automation of manual processes
- Scalability to expand the number of vendors managed
- Quality and value of data collected
- Risk decision making
- Use of internal resources
Many vendors in the VRM market have formed alliances and partnerships to achieve these outcomes, such as VRM solutions providing an optional SRS subscription or consultancy services through a partner. We expect these alliances and partnerships to evolve, as increasing regulatory adoption will drive demand for more comprehensive solutions.

**Evidence**

1 Gartner analysts have seen an increase of nearly 14% in VRM interactions in the 12-month period from January 2020 through January 2021.

2 For example, GDPR, OCC, APRA, EBA, Prudential Regulation Authority of the Bank of England, Modern Slavery Australia, Modern Slavery UK


Sample vendors have been compiled based on Gartner interactions, vendor briefings and peer insights. See Gartner Peer Insights, Reviews for IT Vendor Risk Management.

**Acronym Key and Glossary Terms**

<table>
<thead>
<tr>
<th>Third Party</th>
<th>An entity (person or organization) who is not directly involved in a primary exchange, such as between a buyer and seller, or a government officer and citizen. This includes technology vendors used to provide products and services.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fourth Party</td>
<td>The third parties of your third party. For instance if your SaaS vendor hosts on an IaaS vendor, then the IaaS vendor is your fourth party.</td>
</tr>
</tbody>
</table>

**Document Revision History**

Navigating the Vendor Risk Management Solution Market - 21 August 2019

---

**Recommended by the Authors**

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

- Formalize Vendor Risk Management to Reduce Business Disruption
- Magic Quadrant for Integrated Risk Management Solutions
- Critical Capabilities for IT Vendor Risk Management Tools
- Innovation Insight for Security Rating Services
### Table 1: VRM Market Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultant</td>
<td>Builds a VRM framework, implements solutions, provides assessment support/managed services</td>
</tr>
<tr>
<td>IRM (Integrated Risk Management)</td>
<td>Software platform for assessment, monitoring, reporting, remediating risks and provides a comprehensive business view</td>
</tr>
<tr>
<td>VRM (Vendor Risk Management)</td>
<td>Software platform for assessment, monitoring, reporting, remediating vendor risks</td>
</tr>
<tr>
<td>SRS (Security Rating Service)</td>
<td>Cybersecurity data collection, rating and monitoring service</td>
</tr>
<tr>
<td>Exchanges and Marketplaces</td>
<td>Platform for collecting, validating, sharing vendor risk and security assessments</td>
</tr>
<tr>
<td>Content/Data Feeds</td>
<td>Public and private vendor risk data collection and data feeds</td>
</tr>
</tbody>
</table>

Source: Gartner (June 2021)