Rsam Solution Checklist

For Vendor Risk Management

 | www.rsam.com | +1-800-920-Rsam (7726)

Table of Contents

Rsam Vendor Risk Management Solution Checklist

As enterprises continue to outsource more aspects of their operations to third parties, they expose themselves to more shared risk. It can be a staggering responsibility. Most organizations understand the need to automate vendor risk management activities to keep up with increasing scope and scrutiny. Yet they struggle to identify and prioritize the key features their VRM solution must provide so they can make a significant impact quickly.

The following solution checklist can serve as a guide. It outlines key features that you should look for in a VRM solution and explains their significance in mitigating vendor risk.

Vendor Risk Assessment Workflow

☑ Vendor Onboarding and Centralized Vendor Inventory

You solution should provide a centralized repository of vendors, and that repository should support the following mechanisms for adding new vendors:

- Simple workflow for allowing business units and/or procurement to add new vendors to the tool by filling out a simple onboarding request form with basic vendor profile information
- An automated import capability for migrating vendors from existing repositories into the VRM tool
- An integration capability to continuously add vendors to the VRM tool as they are added to other systems (procurement, accounts payable, etc.)

☑ Out-of-the-Box Classification, Assessment, and Remediation Workflows

The most essential processes that you need to automate are:

1. The classification of vendors into high-level buckets based on criticality
2. The distribution and collection of assessments based on those criticalities
3. The identification and remediation of gaps based on the responses to those assessments

While every company's approach to vendor risk management is unique, yours is not the first to solve for these core processes. Look for a solution that allows you to leverage industry best practices for automating the assessment process.

☑ Out-of-the-Box Content

Your solution should include control content that is applicable to your organization. Whether your environment uses standardized control content like HITRUST or Shared Assessments, or general-purpose best practices like ISO. You will make your life easier with a solution that offers a content library that gets your program up and running quickly. You can always modify it to suit your specific needs over time.

Corrective Action Plans

Once gaps are identified, your solution should be able to track and automate the recommendation, approval, and execution of corrective action plans (CAPs). Ideally, the solution should support the inclusion of vendor users in the CAP workflow by allowing them to create plans, submit them to your team for review, and periodically update the status of their execution.

Vendor Engagement

Criticality-Based Assignment of Control Questionnaires

Many organizations make the mistake of asking every vendor the same questions, gathering huge amounts of data, and attempting to make sense of it. As a result, they often struggle to get responses from vendors who simply can't tackle the breadth of the assessment, and they drown their staff in unnecessary paperwork that may have little value.

Your VRM solution should provide short classification questionnaires for quickly identifying the high-level risks and criticalities inherent in your vendor relationships and then assign targeted questionnaires that ask only what you need to know.

Cross-Mapping of Controls and Standards

Just because you're evaluating a vendor against multiple control standards, it doesn't mean you need to ask them the same question multiple times. By cross-mapping control questions and responses to multiple standards, you can ask your vendor about their password policy once and satisfy relevant requirements across many control standards.

User-Friendly Vendor Portal

The easiest and most efficient way to collect information from your vendors is to give them limited access to your VRM solution. This allows you to track the status of assessments in real time, automate notifications and reminders, and begin analyzing data as soon as it's submitted. The user interface should be simple and engaging, requiring no training or vendor hand-holding.

A major consideration here is the deployment architecture. It's safe to assume you don't want to let vendors near sensitive risk and compliance systems that reside behind the firewall. Look for a system that gives you to option to deploy separate vendor – facing portals in your DMZ and synch data back-and-forth with your internal VRM system.

Offline Data Gathering

Not all vendors will be willing or able to access online portals. Make sure you have an option for extracting questionnaire content into an offline data gathering tool, such as an Excel spreadsheet, and importing it automatically into your VRM system. This process should be seamless and enable you to subject the offline data to the same business rules, include it in the same reports, etc.

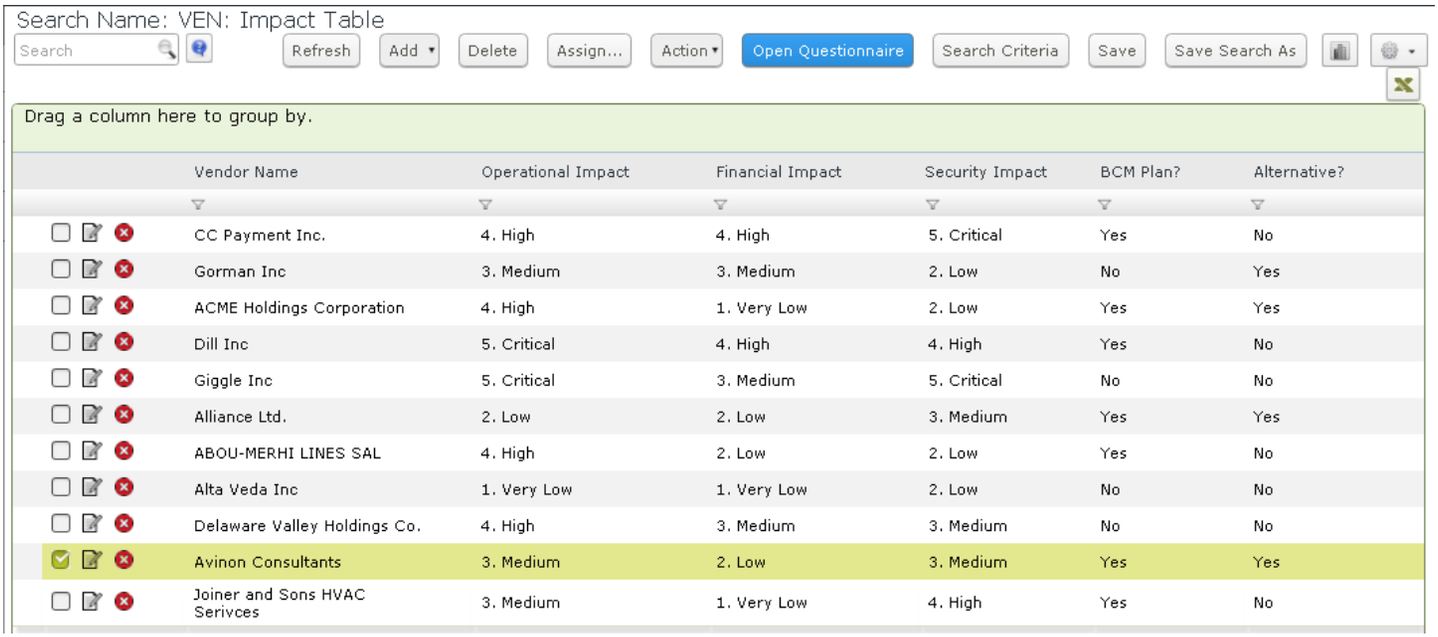
Risk Reporting Requirements

Dashboarding and Reporting

Your VRM solution should come with a rich library of out-of-the-box, role-based dashboards and reports with a variety of presentation styles (e.g. vendor detail reports, list reports, charts and graphs, etc.) to suit the diverse needs of your users. You should also ensure that tool provides you the ability to easily modify those reports, to create your own reports, and to publish reports to user dashboards. The reporting interface should be capable of seamlessly reporting on any customizations that you make to the tool (e.g. you should be able to report on you own custom attributes and data structures), and it should also allow you to report on any data that has been integrated from other sources (internal systems, third-party intelligence, etc.).

Flexibile Risk Categorization and Scoring

At the end of the day, you want your solution to provide meaningful reports showing vendor risk across all areas that are important to your organization. One thing we've learned at Rsam after so many implementations across so many diverse customers is that every organization tracks to its own unique risk categories, priorities, and tolerances. Make sure your system is flexible enough to accommodate what's unique to you – both on Day One and going forward as your stakeholders' priorities evolve.



Vendor Name	Operational Impact	Financial Impact	Security Impact	BCM Plan?	Alternative?
CC Payment Inc.	4. High	4. High	5. Critical	Yes	No
Gorman Inc	3. Medium	3. Medium	2. Low	No	Yes
ACME Holdings Corporation	4. High	1. Very Low	2. Low	Yes	Yes
Dill Inc	5. Critical	4. High	4. High	Yes	No
Giggle Inc	5. Critical	3. Medium	5. Critical	No	No
Alliance Ltd.	2. Low	2. Low	3. Medium	Yes	Yes
ABOU-MERHI LINES SAL	4. High	2. Low	2. Low	Yes	No
Alta Veda Inc	1. Very Low	1. Very Low	2. Low	No	No
Delaware Valley Holdings Co.	4. High	3. Medium	3. Medium	No	No
Avinon Consultants	3. Medium	2. Low	3. Medium	Yes	Yes
Joiner and Sons HVAC Serivces	3. Medium	1. Very Low	4. High	Yes	No

Document Register

Your VRM solution should provide the ability to track document attachments as part of a vendor profile. Attachments could include items like financial statements, incorporation filings, policies and procedures collected from the vendor, compliance screening and due diligence reports, etc.

Ad-Hoc Risk Register

In addition to the findings you identify through questionnaires and assessments, you'll need the ability to track and assess ad-hoc risks you uncover through other diligence processes (e.g. findings from on-sight audits, identification of outstanding public records, etc.). Make sure your VRM solution enables you to identify these ad-hoc risks and track their assessment and remediation alongside gaps identified through the questionnaire process.

Continuous Monitoring

Vendor risk management is not a one-time project; it's an ongoing process. Ongoing monitoring can be accomplished in a number of ways, but a few common ones include:

- Automating the scheduling of follow-up assessments based on the risk level of a vendor (e.g. a low-risk vendor is scheduled for re-assessment every 3 years, while a critical vendor may require quarterly reviews)
- Integrating third-party intelligence feeds that provide ongoing monitoring alerts for significant changes to a vendor's risk ratings (e.g. credit ratings, IT security risk ratings, etc.), new appearances in adverse media or on government watch lists, or the filing of public records (e.g. suits, liens, judgments) involving the vendor.
- Don't make the mistake of focusing so much on vendor risk that you ignore performance. Providing a mechanism for tracking and periodically reviewing a vendor's performance against defined SLAs and other metrics is critical to ensuring that you are driving value from your vendor relationships while also managing and mitigating risk. Choose a solution that allows you to track SLA performance metrics both manually and, in cases that lend themselves to it, through automation.

Architecture and Infrastructure

Flexibility to Adapt to Evolving Requirements

While the previous two checklist items are about expediency, this one speaks to the reality that the most constant element in your vendor risk management program is change. Regulatory requirements, stakeholder expectations, and the strategic goals and risks identified by your organization will continue to change over time. The last thing you need is a rigid VRM solution that keeps you behind the curve. Look for solutions that can quickly adapt to changes in questionnaire content, the capture of metadata, scoring and prioritization methodologies, workflow, and integrations with other systems.

Integration with other Systems and Third-Party Intelligence

Your VRM solution should have the ability to integrate with internal systems (LDAP, Procurement, Accounts Payable, etc.) as well as with third party intelligence content. Examples include feeds that can augment your internal assessments with objective information about vendors' IT security posture (e.g. BitSight, Security Scorecard), financial viability (e.g. D&B, Rapid Ratings), and compliance posture (e.g. restricted party screening, negative news, etc.). Integrated solutions each have their own capabilities and limitations, so your VRM tool should allow you to quickly build and easily maintain integrations over time.

About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at http://www.rsam.com

