

Six Vendor Risk Management Time Killers



Vendor risk management is getting tougher. In a recent study from the **Ponemon Institute** and Shared Assessments, 70 percent of respondents said third party risks in their organization are significantly increasing. The organizations who participated in the survey spent an average of \$10M responding to security incidents caused by third parties.

Many vendor risk programs have evolved over time. What began as a spreadsheet or two to track vendors can't hold up to the ever-increasing scope and severity of risk plus increased scrutiny of enterprise GRC programs of risk managing, leaving companies vulnerable. Putting more people on the problem can quickly become a resource drain.

But what if you could eliminate some of the time wasters associated with vendor risk management? We've compiled a "Top Six" list of resource drains uncovered while helping companies implement a vendor risk management platform. We've also provided time saving tips to help you get more value from an enterprise VRM program platform.



Time-Waster #1: Treat All Vendors Equally

Is your cloud provider answering the same questions as your event caterer? Treating all vendors equally can add noise to the assessment process and lead to a lack of participation from your vendors.

Time Saving Tips:

- Use a pre-assessment risk criticality survey to help categorize and prioritize vendors. For example, a vendor that touches sensitive customer data may need more review than one that doesn't.
- Leverage existing industry risk and compliance metrics to prioritize survey assessments. For example, D&B tracks risk and compliance data for over 240 million vendors. Use that data to pinpoint your most critical vendors.



Time-Waster #2: Track Surveys Manually

Email chains and spreadsheets can only go so far. If you have more than a handful or so of vendors to manage, it becomes increasingly hard to track simple things like: How many surveys are out? How many came back fully completed? Who is following up?

Time Saving Tips:

- Create a central repository and survey tool to track assessment stages. Add simple dashboards that display fields like due date, BU owner, stage and number of assessments assigned to each vendor.
- Implement automatic notifications for assessments that are incomplete or overdue. This helps you keep focus on what needs to be escalated and when.



Time-Waster #3: Update Vendor Contact Details Manually

Many hours are whittled away trying to keep vendor data current. How much time does your organization spend checking common things like whether or not a corporate address, phone number and website URL are correct? How do you track if a vendor acquires another company or merges with one? It's not realistic to think your organization can keep pace with the volume of these changes. Dun & Bradstreet is currently tracking over 5 million company updates PER DAY.

Time Saving Tips:

- Integrate a business intelligence service that continuously tracks vendor changes and can automatically update your program.
- Use this same business intelligence to prevent DUPLICATES.



Time-Waster #4: Not Prioritizing What You're Asking from Your Vendor

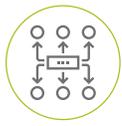
It's very easy to create vendor fatigue by asking **information you already know** or asking them to remediate low impact risks. Say you've discovered a critical vendor has 38 security gaps, but what issues will have the greatest impact to your company? Instead of creating a five-alarm fire drill for every gap, take a risk-based approach to remediation.

Time Saving Tips:

- Devise a clear vendor risk scoring system that shows how each "gap" impacts the overall score. This allows you and your vendor to focus on remediation activities that have the greatest effect.
- Use a blended survey framework. If your vendor answered a password question for a PCI assessment that is also applicable to a HIPAA assessment, don't ask that question again.



- If another application already has existing data on the vendor, use API integration into your VRM platform to grab that information.



Time-Waster #5: Use The Same Work Flow for All Vendor Risk Acceptance

All organizations have vendor risk gaps that can't be addressed. You must be able to demonstrate to auditors that you have a process for risk acceptance across all BUs. The fastest way to derail the process is to chase down each BU owner to get them to participate.

Time Saving Tips:

- Use risk ratings to dynamically assign work flows. For example, a low risk might require a two-step work flow approval process while a higher one might require executive sign-off.
- Automate notifications and escalations. If a work flow step is overdue, you need a system that can automatically inform stakeholders of the status.



Time-Waster #6 Force Vendors Into One Method of Completing Their Assessment

Not everyone works on their office computer at all times. In fact, 40% of employees use their mobile devices to perform work-related tasks. You can dramatically impact vendor participation if you provide options for completing surveys.

Time Saving Tips:

- Give vendors multiple options for responding. For example, if you're using web-based surveys, make sure they can be completed from a phone or tablet.
- Provide offline data gathering capabilities. Most surveys require input from multiple people. Give vendors the ability of downloading an offline version of the survey they can distribute internally and compile feedback. Then, make sure your VRM platform can automatically import the results.

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>