cyber GRX

Vendor Risk Management Fundamentals: A Checklist

There are many ways to slice and dice your vendor risk management program – an increasingly important practice in today's world of complex ecosystems and imperative data protection. The following is what our solution engineer would advise if starting from scratch.

1. Vendor Classification

The vendor class will tell you a lot about how to manage your relationship, specifically how much scrutiny to apply during the pre-contract due-diligence assessment.

- [ ] **Vendor Risk Tiering**
  Determine if a vendor's inherent risk is High, Medium or Low by profiling the vendor on a number of attributes.

2. Begin the Assessment

After classifying vendors, you will know what the scope of the assessment should be.

- [ ] **Determine Assessment Scope & Necessary Questions**
  Each vendor tier will have a corresponding assessment scope – high risk vendors should be assessed via questionnaire and a corresponding on-site evaluation, while lower risk vendors can be assessed with a lower level or rigor such as a questionnaire and desktop document validation.

- [ ] **Self-Assessment**
  Regardless of tier classification, each vendor should complete a self-assessment questionnaire. The questionnaire should only include relevant questions that show what level of risk a vendor will expose you to.

  - Include well documented expectations and guidelines, as well as a deadline.

- [ ] **Validate Vendor Assertions**
  Examine evidence provided by your vendor that prove their controls are operating effectively, such as policies, procedures, audit results, etc.

- [ ] **Ongoing Monitoring**
  Continue to update your data as there are changes in your relationship with your vendor.

3. Issue Management

A well-designed questionnaire should have a corresponding analysis component. Scoring a questionnaire can be difficult, but it's important to know dynamic issue status as it evolves – which is why we suggest issue-based scoring.

☐ Create a Matrix

Relate your questions to negative answers, to issue severity and mitigation strategies.

☐ Track issues

Know the dynamic status of each issue at all times – this way, no exposure will go unaddressed.

☐ Address Findings

Hold your vendors accountable for helping you close the issues that must be addressed.

- When you define your program policies, plan for how you deal with issues given its severity in a repeatable fashion. This will ensure consistency in your approach.

Building a strong VRM program is essential to the security of your business and its data. Each component will require constant fine tuning, especially while your program evolves in maturity and sophistication. If you're looking for an innovative, dynamic approach, schedule a demo or read our Vendor Risk Management Guide to learn more.

Download the full Vendor Risk Management Guide: The 3 Fundamentals