Vendor Risk Management Checklist

In recent years, vendor risk management has increasingly become a strategic priority for organizations. This is largely driven by increased reliance on third-party vendors and the fact that third-parties cause 60%+ of data breaches. When building out a program from scratch or reviewing existing processes, it is important to create a vendor risk management checklist to ensure that you are adhering to best practices and effectively managing risk throughout the entire vendor lifecycle.

It is important to consider the best practices below to ensure that you implement a robust vendor risk management program.

Vendor Risk Management Best Practices

1. Create an Inventory of all Vendors

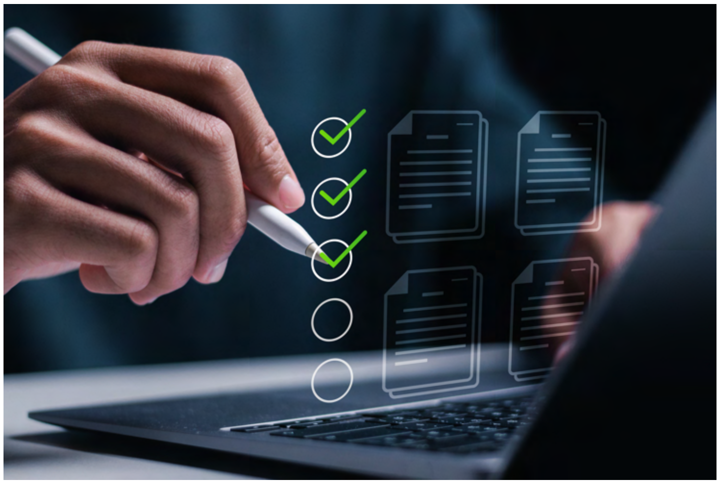
While this sounds basic, a lot of companies don't have any sort of process to track what vendors they work with. It becomes impossible to manage vendor risk if you don't have a comprehensive view of your vendor network.

2. Categorize Vendors Based on the Nature of the Relationship

Once a central repository of vendors is created, it is important to categorize third-parties based on the services provided. When categorizing vendors, considerations should include whether they have access to sensitive information and if they are critical to your business.

3. Decide on a Risk Assessment Framework and Build a Questionnaire

Organizations use several industry-accepted frameworks to assess their vendors, such as NIST CSF, ISO 27001, and Standardized Information Gathering Questionnaire (SIG). It is also common to use these frameworks as a starting point and then customize the assessment based on the unique needs of your organization. When deciding what framework to use and how it should be tailored to your needs, it is important to consider regulatory and compliance requirements, how you work with third-parties, and organizational risk tolerances.



4. Assess your Vendors

It is important to assess your vendors as part of the vendor on-boarding process and on an ongoing basis thereafter. A big reason why it is important to categorize your vendors is because this will help inform what type of assessment they should receive. It is common for organizations to have different levels of assessments based on the nature of the vendor engagement. For example, a vendor that you leverage for cloud hosting services should probably receive a more comprehensive assessment than a vendor that provides facility maintenance services.

5. Leverage AI to Automate the Risk Assessment Process

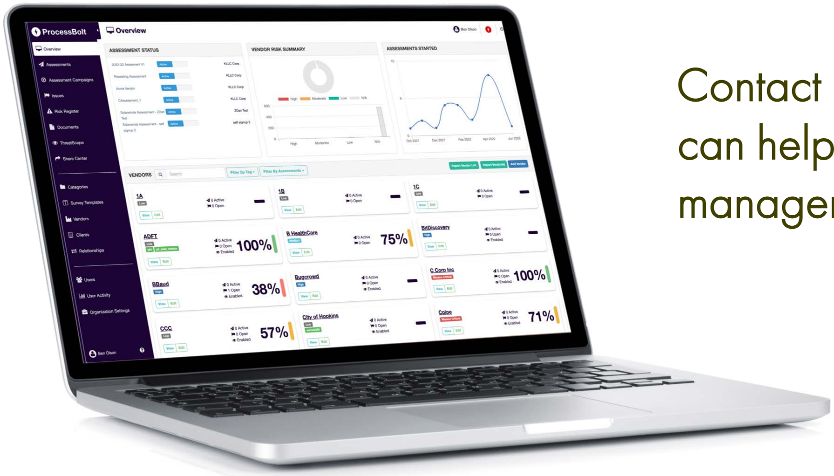
While conducting risk assessments is a good first step, a staggering 45% of organizations still leverage spreadsheets to conduct risk assessments. Spreadsheets are inefficient and lack the dynamic capabilities required for real-time risk monitoring and management. There are some novel applications of AI to support the risk assessment process that should be incorporated into your vendor risk management program. One of the biggest limitations of risk assessments is that they rely on vendor attestation, which makes it challenging to verify the accuracy of the assessment responses. While most of the answers to the questions exist in vendor corporate documentation, it is impractical for a security analyst to review all vendor documentation to ensure that the risk assessment responses are consistent with corporate documentation. It is possible to leverage AI to extract intelligence from corporate documentation to instantly verify whether the assessment responses are consistent with corporate documentation.

6. Continuously Monitor your Vendors

Another limitation of risk assessments is that they capture the security posture of an organization at a point in time. An organization's security posture is constantly changing and leveraging attack surface monitoring is critical to identifying real-time changes that create incremental risk.

7. Integrate AI-driven Assessment Automation with Continuous Monitoring

A lot of questions that are typically included in risk assessments can be verified through an analysis of an organization's attack surface. The challenge is that most organizations rely on disparate software solutions to assess and monitor their vendors and the tools do not inform one another. ProcessBolt offers a fully-integrated platform that correlates attack surface data with risk assessment responses. This is critical as it adds another layer of verification. For example, someone might respond on an assessment that they have no expired software certificates and the ProcessBolt platform can analyze the vendor's attack surface to help verify that the response is accurate.



Contact ProcessBolt today to learn how we can help you optimize your vendor risk management program.