whistic

VENDOR SECURITY ASSESSMENT CHECKLIST

Everything you need to set up a best-in-class vendor security assessment process

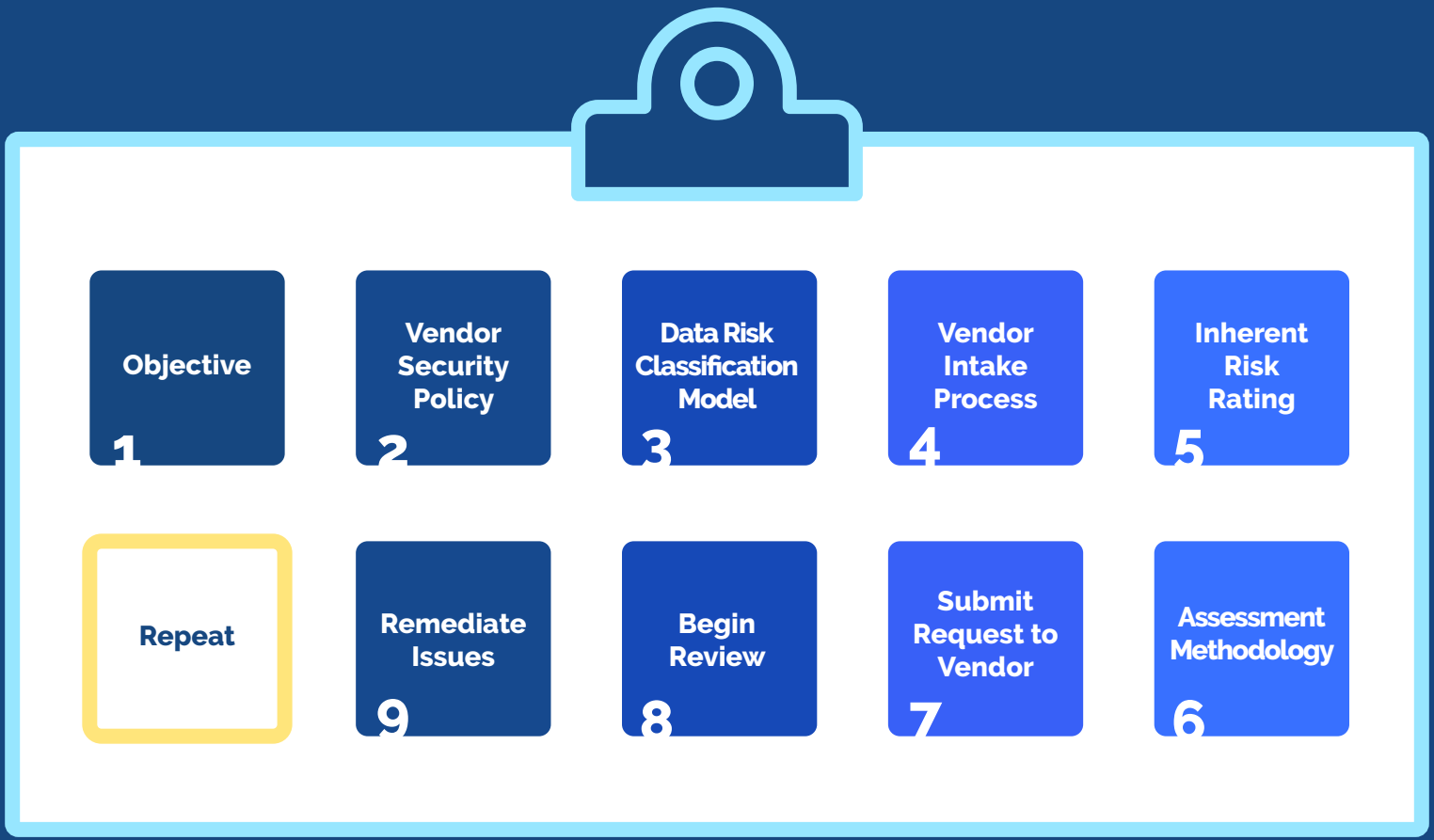
In 2021, it's been predicted that businesses will spend $1 trillion USD on cybersecurity alone.

Businesses can invest all of that money to protect their data, but if they're not focused on their third parties' security practices in the same way they are focused on their internal security practices, then there still is a high likelihood their data will be compromised.

At Whistic, we believe a third party risk management process should be part of your overall cybersecurity program. Having the right processes in place will help you identify risk in your third parties and put a remediation plan in place to prevent security incidents before they happen.

But implementing a vendor security program is often easier said than done. Over the course of this ebook, we'll provide you with a checklist of key activities every vendor security assessment program should include, while providing you with other tips and best practices that will ensure your success.

To help you get started, we've highlighted **nine key activities** that when implemented correctly will help you build a successful vendor security program and ensure peace of mind for your InfoSec team.



What's your objective?

This might seem obvious, but it's important to take a step back before starting and identify the purpose of your vendor security program.

Are you trying to get more of a handle on how many vendors are in your environment and what customer data they are accessing? Are you trying to step up your efforts to proactively block unauthorized access to customer data? Are you trying to meet a new regulatory or audit requirement? Once your objectives are well defined, you can start building out the policies and procedures that will help you achieve those goals and objectives.

Develop a vendor security policy

Next, you'll need to develop a vendor security policy that applies to all vendors that have access to your systems and data.

A typical policy will include requirements for things like what to include in your vendor inventory, criteria for vendor risk ratings, vendor agreements, vendor security requirements, what assessment methodology you will use, your risk treatment methodology, and what to do when a vendor relationship is terminated. In addition, you'll want to lay out how the policy will be enforced and any penalties that may be applicable.

Determine your data risk classification model

Another thing that needs to be done before you begin assessing vendors is setting up a data risk classification model that determines which data needs the most protection.

For the purposes of vendor security, data will have these three distinct classifications:

Low–Information that is readily available to the general public.

Medium–This information is confidential and for internal use only and consists of information like account numbers with no other contextual information, first or last name not coupled with each other or with any other unique information, business addresses of partners that are otherwise publicly available, advertising campaign plans, or press releases that are positive for the business but not yet released.

High–This information is highly confidential and consists of personally identifiable information, Social Security numbers, account information coupled with names and/or addresses or password hints, restricted data—data that is considered a corporate secret or proprietary to the business, data that could damage the reputation of the business if released publicly, meeting notes related to product design or corporate planning, or press releases that are negative for the business but not yet released.

Implement a standard vendor intake process

One of the most critical steps in any vendor security program is the vendor intake process.

It is important to ensure all of the necessary information is collected up front, so the InfoSec team has everything it needs to assign inherent risk and proceed with an assessment plan based on that inherent risk designation. The intake form should, at a minimum, include the following, but may also include other items unique to your business:

1. **Base-level vendor information,** including basic details like URL, product or use-case descriptions, and primary contact information.
2. **Requester/business sponsor information**, which consists of internal contact information (i.e. who at your company is requesting or sponsoring the vendor).
3. **Business unit information** is used to define the criticality the vendor will hold in relation to your company's business operations and which lines of businesses would be impacted.
4. **How critical the vendor is**, which will be different from company to company. Many companies use a categorization similar to what is outlined below:
    - **Mission Critical–**These are applications that are essential for operations and difficult to replace.
    - **Important–**These are applications that are essential for operations, but can be replaced easily with minimal delay.
    - **Standard–**These are applications that are used in operations, but an outage can be tolerated or it's easily replaced.
5. **Data volume** is the total number of unique records that the vendor will store, process, transmit or access. This is important to understand as lower volumes mean lower overall exposure and risk.
6. **Systems Access** outlines exactly which internal systems, infrastructure, applications, and databases the vendor will have access to.
7. **Additional information** this section could include items like billing address and information, contract terms, estimated number of users, or even privacy-related information (i.e., where data will be stored, has the vendor provided a data processing addendum, etc.).

Determine inherent risk rating for each vendor

Based on the information gathered about the vendor, it's time to assign an inherent risk rating using common criteria.

These criteria will be different for each organization as risk tolerances vary. If you're starting from scratch, you may focus initially on determining inherent risk based solely on the type of data the product or service will have access to. For example, that might look like this:

High-risk vendor–has access to any category of data deemed "high-risk" in your data risk classification model.

Medium-risk vendor–has access to any category of data deemed "medium-risk" in your data risk classification model.

Low-risk vendor–has access to any category of data deemed "low-risk" in your data risk classification model.

As you mature your program, you may expand your model to cover other criteria. Below is an example of a more mature risk model that quickly buckets vendors into risk tiers:

High-risk vendor–has access to any category of data deemed "high-risk" in your data risk classification model, or has been deemed mission critical, or possesses more than 10,000 records deemed medium-risk.

Medium-risk vendor–A medium-risk supplier is a vendor that is deemed important, possesses less than 10,000 pieces of medium risk data, has no access to modify that data, and has the ability to interact with the business's customers on your behalf in a limited way.

Low-risk supplier–A low-risk supplier is a vendor that has standard criticality, it doesn't interact with customers, and has access to only low-risk data.

Decide on an assessment methodology

The thoroughness of the vendor assessment and the frequency of subsequent assessments is determined by the vendor's inherent risk outlined in the previous section.

Below is an example of what that might look like for your Cloud Vendors:

Tier	Profile Review	Questionnaire	Assessment Frequency	Assessment Focus
High	Annual	Cloud Security Alliance CAIQ	Yearly	Validate All
Medium	Annual	Cloud Security Alliance CAIQ-Lite	Every two years	Validate Select Key controls
Low	Annual	No Assessment– Reference Security Ratings data	N/A	N/A

Send Assessment Request to the Vendor

Based on the assessment methodology, vendors will be notified of the request to complete a security assessment and provide necessary documentation to pass the review.

Be sure to stay in regular contact with the vendor to help guide them through the process if they have questions regarding the assessment.

Once the documentation is completed and returned, the business will evaluate the assessment to identify any gaps and work with the vendor to remediate any risks that are unacceptable to the business.

Tip #3 **Utilize technology to manage the assessment process**

Whistic enables you to send standardized or customized questionnaires to your vendors and automate follow-up until completion, saving countless hours and frustration you used to experience when using email and spreadsheets.

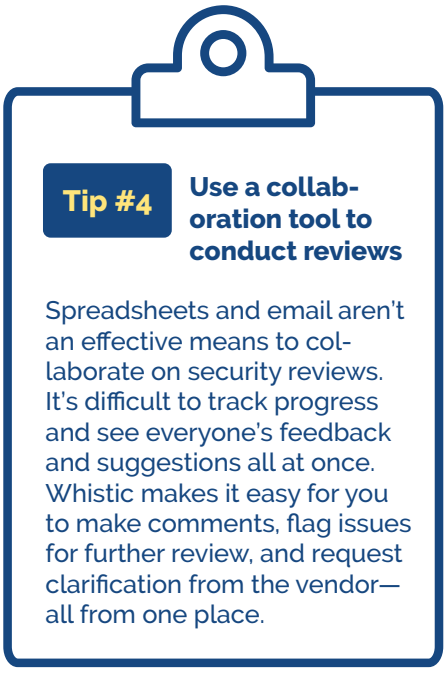
Begin Security Review

When evaluating vendors, not all questions are going to carry equal weight. With that being said, there are some key controls that the business should expect all of their vendors to comply with.

High Risk: For vendors that have a high inherent risk rating, be sure and review all of the security controls and questions contained in the questionnaire. If it is determined that the vendor is non-compliant in any of the controls, that item will be marked as a gap using the Issue Management and Remediation methodology, which is outlined on the next page.

Items that are not key controls that are not compliant will be evaluated on a case-by-case basis to determine whether or not further remediation is needed. An example of this might be that the supplier does not have a process to restrict physical access, but is a small office with only four employees that have access to the office and they have demonstrated that all devices have encryption enabled, a strong password policy limiting access to all computing devices, and customer data is only stored in AWS data centers. In this case a physical access request procedure may not be relevant or useful for the business.

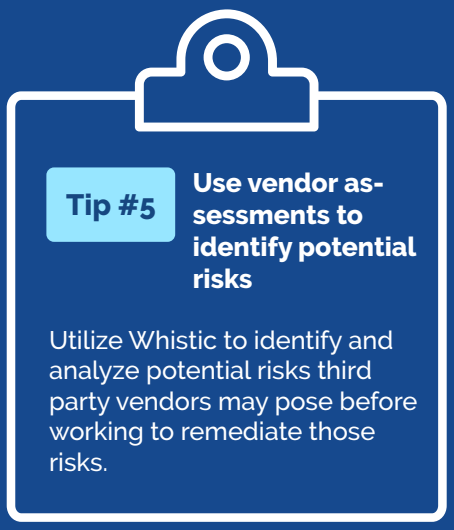
Medium Risk: For vendors that have a medium inherent risk, validate compliance with select key controls, non-key controls are reviewed based on services provided by the supplier and simple attestation may be acceptable. For example the question "Please describe your DDoS mitigation strategy," may be relevant and more important for some suppliers than it is for others.



Issue Management and Remediation

The initial objective of a vendor security assessment is to identify issues or risks that a third party presents.

However, the real value a third party risk management program delivers to an organization is in eliminating or reducing those risks altogether. To ensure this happens, you will need to implement an issue management process that consists of the following steps:



Tip #5 **Use vendor assessments to identify potential risks**

Utilize Whistic to identify and analyze potential risks third party vendors may pose before working to remediate those risks.

Identification: Issues are typically identified during the vendor assessment process described above or they have been disclosed to you by the vendor.

Analysis: During this step, you will apply a standard risk model to each issue and assign a risk level based on the likelihood of something bad happening and the potential impact it will have on your organization.

Action: Each risk rating should have clearly documented guidelines on suggested actions to fix the issue. Typical actions include, reduction of risk or remediation, acceptance, or avoidance. For example: High Risk issues are remediated within 60 days or compensating controls are documented. Other actions could include acceptance of the risk with proper approval, or in the worst case scenario, avoiding the risk altogether and terminating the relationship with the vendor.

Monitor and Reporting: Because the issue management process can take time, continuous monitoring with the vendor and status reporting are needed periodically.

Closure: Issues are closed once all actions and remediation activities have been completed.

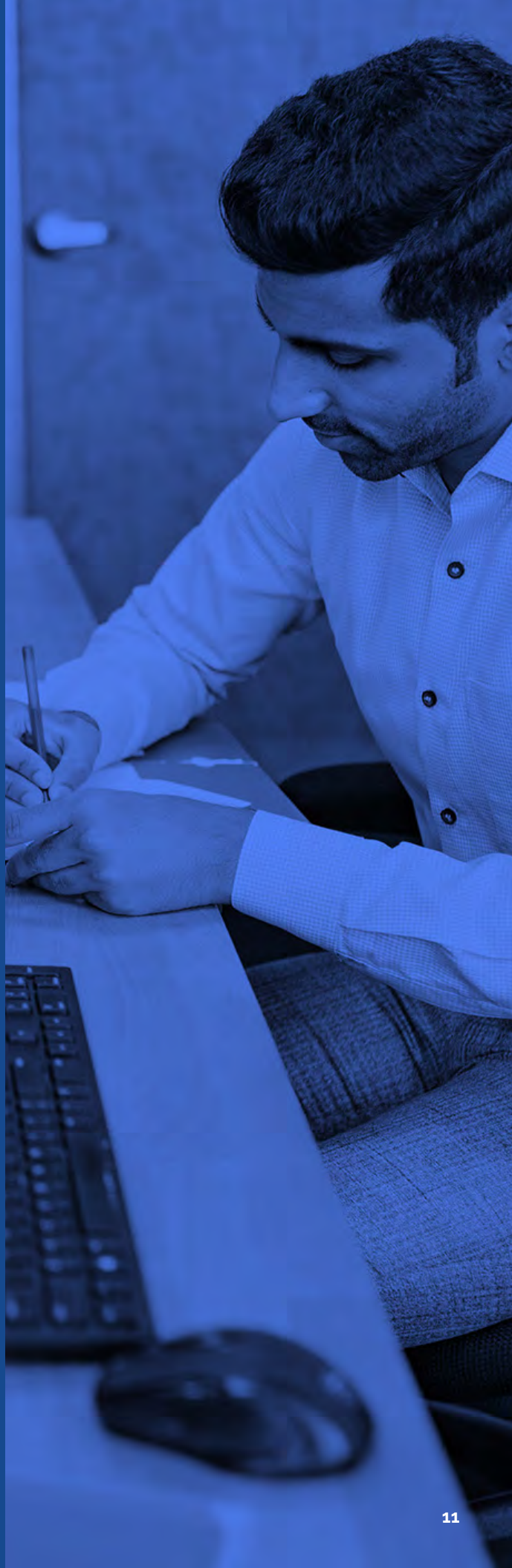
Time for Reassessment

Based on the assessment methodology outlined previously, you should follow these steps when reassessing your vendors.

1. Schedule a notification for reassessment (e.g., annual for high risk, biennially for medium).
2. Validate vendor information is still accurate as it relates to data access and volume, physical address, and contact information.
3. Send appropriate assessment to the customer.
4. If the vendor is high risk, review the assessment and identify any findings or gaps and work with the vendor to remediate.
5. If the vendor ranking is medium, document the received assessment.
6. If the vendor ranking is low, document and review as scheduled.

Tip #6 **Utilize the Whistic Trust Catalog to speed up reassessment**

If your vendor shared their Profile to the Trust Catalog that means you can access their up-to-date security documentation in seconds, not days or weeks like with traditional methods.



How Whistic can help

Identifying potential risks from third party vendors is critical.

Following the steps outlined above and utilizing a tool like Whistic will help you discover vendors, assess their potential risks, and implement a plan of action to ensure hackers aren't able to take advantage of potential vulnerabilities in your environment.

Whistic Vendor Security helps simplify the vendor assessment process for your business by automating many of the key steps along the way and give you peace of mind that your customer data is protected.

To learn more about what Whistic can do for your business visit whistic.com/vendor-security or request a demo today.

www.whistic.com