

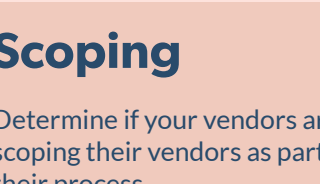
How to **verify** your vendor is on

The Nice List

Periodically determine which of your vendors are behaving nicely... and which ones have some room to improve. To give an indication, see how your vendors are performing in each of the third-party risk management lifecycle stages, in terms of both your relationship and their relationship with their third parties (your fourth parties).

Check the list below to find out!

1



Scoping

Determine if your vendors are scoping their vendors as part of their process.

QUESTIONS TO ASK

- ? Does your vendor actually scope out the requirements for a product or service to fit the specific line of business needs?
- ? Does your vendor scope all outsourced relationships? Does their vendor?
- ? Has the scope of any of their vendor relationships shifted? Has their vendor's scope shifted?

NICE

Requirements for a product or service are scoped out to fit specific line of business needs

Scopes outsourced relationships

- Clearly defines scoping

NAUGHTY

Does not scope Requirements for a product or service to fit specific line of business needs

Does not scope outsourced relationships

Does not clearly define scoping

2



Inherent risk and criticality assessment

You and your vendor need both determinations to understand the risk a third party poses and what to do about that risk – ensuring the right people take care of tasks and risk gets identified and mitigated.

QUESTIONS TO ASK

- ? Do your risk assessment questions truly capture inherent risk and residual risk separately? Does your vendor's?
- ? Are you asking extra questions as needed and have documented evidence of taking appropriate follow up steps? Is your vendor?
- ? Is the information you gather internally pertinent to executive leadership's needs? Is your vendor's?

NICE

Risk assessment questions capture inherent risk and residual risk separately

Documented evidence of follow up

Information gathered is pertinent to leadership's needs

NAUGHTY

Incomplete risk assessment questions which fail to capture inherent risk and residual risk

Evidence of follow up is not documented

Information gathered isn't pertinent to executive leadership's needs

3



Due diligence and residual risk determination

Gathering vendor due diligence is a primary line of defense against the troublemakers. Missing the mark on practical due diligence may mean also missing the mark on mitigating risk.

QUESTIONS TO ASK

- ? Can your vendor provide relevant historical information including ownership and management? Can your vendor's third parties?
- ? Can your vendor provide financial documentation, policies and plans? Does that show financial strength to continue operations and provide the contracted services? What about your vendor's third parties?
- ? Does your vendor have SOC, business continuity and disaster recovery, cybersecurity, notification and response policies, plans and/or reports? Does your vendor's third parties?
- ? Does your vendor have background check policies, etc.? Does your vendor's third parties?
- ? What is your vendor's and their third parties' regulatory histories? Can they provide disclosure of any civil, criminal and regulatory matters to identify a history of issues that may present risk factors?
- ? What is the status of your vendor's and vendor's third parties' compliance/training information?
- ? What is your vendor's and vendor's third parties known for? What are the reputations?
- ? What's the remaining risk of your vendor? What about your vendor's third parties?

NICE

Provides relevant historical information including ownership and management

Has financial documentation, policies and plans and those show strong financial information

Has hiring policies such as background check policies

Is able to provide updated SOC, business continuity and disaster recovery, cybersecurity, notification and response policies, plans and/or reports

Has detailed documentation of their regulatory history

Routinely organizes compliance and training sessions

Has a positive reputation

Remaining risk is acceptable

NAUGHTY

Is unable to provide relevant historical information including ownership and management

Fails to provide financial documentation, policies and plans and/or financials show weakness

Does not have hiring policies such as background check policies

Is unable to provide updated SOC, business continuity and disaster recovery, cybersecurity, notification and response policies, plans and/or reports

Has incomplete documentation of their regulatory history

Does not routinely organize compliance and training sessions

Has a negative reputation – they're known for data breaches, service disruption, poor customer service, poor delivery of products and/or more

Remaining risk remains too high

4



Vendor selection and contract management

Ensure you and your vendor have good processes in place for drawing up and managing written agreements which cover all bases: negotiation, change management, ongoing maintenance, etc.

QUESTIONS TO ASK

- ? Are you and your vendor maintaining key performance indicators (KPIs) and service level agreements (SLAs)? Are your vendor and their third parties' KPIs positive and SLAs met?
- ? Do you and your vendor have a way to maintain contractual obligations? Do your vendor and their third parties obey the contract?
- ? Are there discounts and/or incentives from your vendors to show loyalty? Do your vendor's third parties offer those?

NICE

Maintains key performance indicators (KPIs) and service level agreements (SLAs)

Stays on top of contractual obligations

Offers discounts or incentives to show loyalty

NAUGHTY

Does not maintain key performance indicators (KPIs) and service level agreements (SLAs)

Is unable to meet contractual obligations on a regular basis

Won't offer discounts or incentives for loyalty

5



Ongoing monitoring

It's important to continuously monitor third parties and assess the risk.

QUESTIONS TO ASK

- ? Do you keep vendor performance reports on file? Does your vendor? Does your vendor and vendor's third parties perform well?
- ? Are you asking your vendors for documentation on an ongoing, periodic basis? Are your vendor's asking their third parties? Do they provide them?
- ? Are you assessing risk periodically? Is your vendor? Do they have appropriate risk?
- ? Are threats addressed by your vendor quickly and efficiently? Do their third parties address them quickly and efficiently?

NICE

Keeps vendor performance reports on file and/or has good performance

Asks their vendors for documentation on an ongoing, periodic basis and/or provides them

Assesses their own risk periodically and/or has an appropriate level of risk

Is responsive and/or efficient with addressing a threat

NAUGHTY

Does not keep vendor performance reports on file and/or performs poorly

Fails to request documentation on an ongoing, periodic basis and/or fails to provide them

Does not assesses their own risk periodically and/or has concerning risk

Takes a long time or is non-responsive to further inquiries and/or addressing a threat

6



Termination

Vendor relationships can run their course and need to be terminated. It's important to have an exit strategy in place.

QUESTIONS TO ASK

- ? Does your vendor have an exit strategy with their third parties?
- ? Does your vendor know what will happen to their data/assets (which also includes your data) upon vendor termination?

NICE

Has an exit strategy

Has a plan for data and assets should a vendor terminate a critical contract

NAUGHTY

Is unable to provide an exit strategy

Does not have an outlined plan for data and assets should a vendor terminate a critical contract

NICE

TOTAL

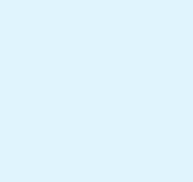
NAUGHTY

TOTAL

Hold the Coal: 5 Next Steps for Troublesome Vendors

We can't really send our naughty vendors coal, but there are some things we can do to help if you do happen to find one, or more, of your vendors on the naughty list.

Consider these next steps:



Ask the vendor owner to report on a vendor's performance.

Sit down with the vendor owner and discuss what you're seeing from inside your vendor management program, and then have them do some investigation.

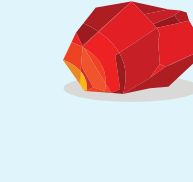


Review the contract.

Take a good hard look at the contractual provisions so you know where you stand within your contractual rights to either reach out for remediation or termination.



Meet with senior management and/or the board. Communication is critical. If you're considering remediation and/or termination, be sure to sit down with senior management to talk about next steps. If it's a critical or high-risk vendor, you'll need to involve the board.



Document vendor concerns.

Make sure you highlight all the pertinent information around vendor concerns.



Execute your plan.

Make sure you have a plan in place, and then move forward with next steps confidently knowing you have reviewed, communicated, documented and planned – whether that be working with the vendor or exiting the relationship.

Understanding the vendor lifecycle is extremely helpful when assessing vendors and can bring insight into how your partnerships are progressing.



Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

DOWNLOAD NOW

PRINTABLE VERSION

Copyright © 2020 by Venminder, Inc.

Manage Vendors. Mitigate Risk. Reduce Workload.

(888) 836-6463 | venminder.com

venminder