

Vendor Risk Assessment Checklist

Measure & Monitor your vendors' performance and assess risk levels

www.aavenir.com

Aavenir

Introduction

When an organization works with third-party vendors, it is left vulnerable to various risks such as security breaches, business interruption, reputational damage caused by vendors' non-compliance with regulation and industry standards, and more.

Organizations should conduct a vendor risk assessment periodically to identify and evaluate the risks and hazards of working with a third-party vendor to prevent those from happening.

Vendor risk assessment comprises multiple steps starting from identifying the right vendors for your organization, evaluating vendor contracts, performing on-site audits, assessing their readiness through questionnaires, and so on.

Allow your organization to implement efficient methods of vendor onboarding and monitor and measure their performance with this customizable vendor risk assessment checklist comprising 50 assessment questions.



Vendor Contracts	(Enter the Vendor company name)
Vendor Contact	(Enter your point of contact with the Vendor, including phone number and email address)
Vendor Website	(Enter the web address of the Vendor website)
Product	(Enter the product or service that you are receiving from the Vendor)
Compliance Percentage	(Enter your Overall Compliance Percentage as computed below)
Introduction	(Discuss the purpose or objective for performing the assessment)
Background	(What did you do to prepare for and perform the assessment?)
Narrative	(Summarize the issues/gaps you found through the survey and what to do to fix them)

Vendor Risk Assessment Survey

Sr. No	Vendor Contracts	Yes	No	N/A
1	Does the contract that establishes the roles and responsibilities of both the vendor and the client signed by both parties?	☐	☐	☐
2	Can you be released from the contract without excessive penalty if it becomes necessary to move to another vendor or in-house?	☐	☐	☐
3	Has or will the vendor sign a Non-Disclosure Agreement?	☐	☐	☐
	Vendor Compliance			
4	Has the vendor implemented an IT Governance regulatory framework applicable in their geography and industry? Please specify details. Comments :	☐	☐	☐
5	If the vendor processes credit cards, are they PCI DSS compliant?	☐	☐	☐
	Vendor General Security			
6	Is antivirus software installed and virus definitions regularly updated on the vendor's systems that store or process customer data?	☐	☐	☐
7	Does the vendor test system and security patches before implementing them in the production environment?	☐	☐	☐
8	Do the vendor's employees have a unique log-in ID when accessing customer data?	☐	☐	☐
9	Does the vendor restrict access to systems that contain customer data? Please list controls in place in the comments section. Comments :	☐	☐	☐
10	If the Vendor has access to their customer data, does the vendor securely delete or return the data when the vendor-client relationship has terminated?	☐	☐	☐

Sr. No	Vendor's Capability and Compatibility	Yes	No	N/A
11	Has the vendor been involved in its industry for more than 5 years?	☐	☐	☐
12	Does the vendor provide a support contact that is knowledgeable in the industry? (if yes, enter their name and contact information below) Contact :	☐	☐	☐
13	Is the vendor able to prove that s/he has implemented exceptional Quality Standards?	☐	☐	☐
14	Does the vendor provide an implementation of their product?	☐	☐	☐
15	Is support available 24/7?	☐	☐	☐
16	Have you tested, trialed, or conducted a proof of concept of the products/services offered by the vendor?	☐	☐	☐
17	Are the vendors' prices equal to or lower than their competitors?	☐	☐	☐
18	Are there any additional fees (that the vendor may require in the future) not covered in the initial contract?	☐	☐	☐
	Vendor Incident Response			
19	Does the vendor have a formal Incident Response plan?	☐	☐	☐
20	If there was an information security breach, would the vendor notify the organization? If yes, please note the timeframe below. Timeframe :	☐	☐	☐
21	Has the vendor experienced an information security breach in the past five years? Please note what information was lost, and in what timeframe the clients were notified (in the comments section). Comments :	☐	☐	☐
22	If the vendor has experienced a breach, have proper measures been implemented to limit the risk of reoccurrence? Give details in the comments section. Comments :	☐	☐	☐
23	Does the vendor offer client access to logs after a security event?	☐	☐	☐

Sr. No	Vendor Organizational Information Security	Yes	No	N/A
25	Is there a vendor's organization member with dedicated information security duties? If yes, provide their name and contact information. Name : Contact :	☐	☐	☐
26	Is history and background check required for all the vendor's employees accessing and handling your organization's data?	☐	☐	☐
27	Does the vendor have a documented information security policy that is periodically reviewed and updated? If yes, please upload a copy.	☐	☐	☐
28	Has the vendor issued its security policy to all employees?	☐	☐	☐
29	Does the vendor require employees to formally acknowledge adherence to the security policy at least annually?	☐	☐	☐
30	Does the vendor have a documented password policy that details the required strength of passwords, length of life, and reuse restrictions? If yes, please list the details in the comments section. Comments :	☐	☐	☐
31	Do all the vendor's employees receive information security awareness training during onboarding and at least annually?	☐	☐	☐
32	Have the vendor's employees been trained to report suspected security violations and vulnerabilities?	☐	☐	☐
	Vendor Network, Systems & Application Security			
33	Does the vendor use firewalls to protect network boundaries?	☐	☐	☐
34	Does the vendor regularly perform network vulnerability scanning?	☐	☐	☐
35	Does the vendor allow wireless access in its organization? If yes, describe how it is protected? Wireless Protection :	☐	☐	☐
36	Has the vendor's backup and recovery process been verified?	☐	☐	☐

Sr. No	Vendor Network, Systems & Application Security	Yes	No	N/A
37	Does the vendor encrypt its backups?	☐	☐	☐
38	Does the vendor use formal control of access to System Administrator privileges?	☐	☐	☐
39	Does the vendor perform a security code review during each phase of development?	☐	☐	☐
40	Do the vendor's coding practices address information security during all phases of the SDLC?	☐	☐	☐
41	Does the vendor have separate environments for each customer for the development and testing of systems	☐	☐	☐
	Vendor Reliability			
42	Does the vendor have a Business Continuity Plan?	☐	☐	☐
43	Does the vendor have an SLA with defined service availability for required services?	☐	☐	☐
44	Does the vendor have disaster recovery plans for data processing facilities?	☐	☐	☐
45	Does the vendor provide training to all relevant personnel on backup, recovery, and contingency operating procedures?	☐	☐	☐
46	Is the vendor financially stable with strategic planning in place for the future?	☐	☐	☐
47	Has the vendor operated reliably for at least as long as the proposed service contract?	☐	☐	☐
48	Does the vendor conduct periodic drills to verify the effectiveness of its disaster recovery and business continuity plans? If so, how often? How often ?	☐	☐	☐
	Vendor Reliability			
49	Does the vendor allow clients the right to audit their systems and controls if a third-party audit report is not available?	☐	☐	☐
50	Does the vendor receive an <SSAE-16 SOC> Report or similar third-party audit?	☐	☐	☐

Calculate Compliance Percentage

Step 1: Fill in all answers with YES / NO / NA

Step 2: Calculate the total numbers of replies for YES / NO / NA

Step 3: Subtract the total number of N/A from 50

Step 4: Divide the total number of YES by the number derived in Step 3 and Multiply it with 100

For example,

Your responses have a total of **28** YES, **10** NO and **12** N/A

Here, Compliance Percentage = 28 / (50-12) x 100 = 73.68%

Likewise, Non-compliance Percentage = 10 / (50-12) x 100 = 26.32%

Based on the non-compliance rate, vendor's Gap Score represents your organization's vulnerability to third-party risk from your vendor.

Non-compliance %	Gap Score	Vulnerability
0%	0	NIL
1-20%	1	Low
21-40%	2	Medium Low
41-60%	3	Medium
61-80%	4	Medium High
81-100%	5	High

Next Steps:

Vendor risk assessment is not a one-time activity. Governance and compliance must demonstrate continued investment into the process and update resources, documents, and systems according to new findings. Also, organizations need to stop working in silos and communicate better with their vendors.

However, doing this vendor risk assessment is not straightforward in practice. Because just sending out a survey form with a list of checkboxes would not suffice in the actual evaluation.

Vendor risk assessments are time-consuming (and, to some extent, error-prone), so manual processes cannot work in the long run. Using technology expedites the risk assessment process and provides conclusive metrics for analysis. Also, the outcomes of the vendor risk assessment can be integrated as solutions into vendor management systems.

Effectively measure, manage and mitigate ongoing supplier and contract risk with qualitative and quantitative risk metrics with a robust and integrated vendor management solution.

Try Aavenir Onboardingflow

Elevate Your End-to-end Vendor Management Experience on ServiceNow

Are you willing to enable end-to-end vendor management through collaboration portals and minimize the complexity of supplier onboarding and engagement across all sourcing and procurement processes?

Get a custom demo of the Aavenir software and find out how you can manage your vendor for better business results.



About Aavenir

Aavenir revolutionizes age-old procurement processes with AI-enabled Source-to-Pay solutions, including RFPflow, Onboardingflow, Contractflow, Obligationflow, and Invoiceflow. Built on ServiceNow, Aavenir solutions streamline procurement, legal, and accounts payable work processes using the latest technologies such as AI, ML, and NLP to

Explore Aavenir Source-to-Pay Solutions on ServiceNow

RFPflow



Request for Proposal Management

Onboardingflow



Onboarding & Supplier Information Management

Contractflow



Contract Lifecycle Management

Obligationflow



Contract Compliance Management

Invoiceflow



Accounts Payable Automation

Get Started

www.aavenir.com

contact@aavenir.com

twitter.com/aavenirInfo

linkedin.com/company/aavenirinfo

Aavenir