CHECKLIST

# Third-Party Vendor Due-Diligence Checklist

Thoroughly vet potential vendors using a vendor due diligence checklist to mitigate risk in the vendor selection process.

www.aavenir.com

# Introduction

In a world that seems to grow more prone to data breaches and identity theft by the day, what can you do to protect not only your information but that of your customers as well? Your customers entrust you with a lot of sensitive data, so the vendors you work with must have safeguards in place to keep this sensitive and confidential data secure.

Vetting and choosing vendors is one of the most important decisions you'll make for your business, especially when it comes to third-party information security. Once you've narrowed your vendor options to those that can support the organization's needs, it's time to gather the information that will help you take a risk-based approach to vendor selection – this is the Third-Party Vendor Due Diligence Process. This information enables you to rank potential vendors' risks to your organization, strengthening your organization and protecting you from insecure or irresponsible vendors.

Vendors could do everything from running your call center to storing your data, monitoring your systems, or destroying your records. Yes, you can outsource a process or a department to vendors – but you can never outsource risk. Vendors inherently pose some level of risk to your organization, irrespective of their market reputation – especially financial risk, operational risk, reputational risk, and cyber risk – because they have access to your data, network, hardware, cloud, and more.

This is why you must thoroughly vet potential vendors using a Third-Party Vendor Due Diligence Checklist.

# Third-Party Vendor Due Diligence Checklist

We've compiled this Third-Party Vendor Due Diligence Checklist to overview the types of information that should play a role in procurement decision-making. Not every item in this checklist is necessary, but the more you complete it, the more thoroughly you'll mitigate risk in the vendor selection process.

## General Information

| | |
|---|---|
| ☐ | Articles of Incorporation |
| ☐ | Business License |
| ☐ | Mission Statement |
| ☐ | Comprehensive List of All Services Location(s) |
| ☐ | Proof of Location(s) |
| ☐ | Overview of Company Structure |
| ☐ | Biographical Information of Executives |
| ☐ | List of Subcontractors |

## Financial Review

| | |
|---|---|
| ☐ | Annual Report (if publicly traded) |
| ☐ | Tax Documents |
| ☐ | Loans and Other Liabilities |
| ☐ | Major Assets |
| ☐ | Principal Owners |

## Reputational Risk

| | |
|---|---|
| ☐ | Code of Conduct |
| ☐ | Litigation History of Company and Key Individuals |
| ☐ | Negative News Reports |
| ☐ | Complaints and Negative Reviews |
| ☐ | Reports from Agencies like the CFPB or BBB |

## Insurance

| | |
|---|---|
| ☐ | General Liability |
| ☐ | Cyber Insurance |
| ☐ | Insurance Specific to Services |

## Information Security Technical Review

| | |
|---|---|
| ☐ | Internal or External Audit Reports |
| ☐ | Penetration Testing Reports |
| ☐ | Risk Assessment |
| ☐ | Network and Data Flow Diagrams |
| ☐ | History of Data Breaches and Security Incidents |
| ☐ | Site Visits or Other Tests to Assess Physical Security |
| ☐ | Business Continuity Plan |
| ☐ | Disaster Recovery Plan |
| ☐ | Security Awareness Training Performance |

## Policy Review

| | |
|---|---|
| ☐ | Information Security Policy |
| ☐ | Privacy Policy |
| ☐ | Change Management Policy |
| ☐ | Vendor Management Policy |
| ☐ | Data Retention and Destruction Policy |
| ☐ | Hiring Policy |

# Choosing a Compliant Vendor

Once your potential vendors have submitted their response to the Third-Party Vendor Due Diligence Checklist, you may be in one of the following situations:

- A potential vendor is not willing to submit few responses to important criteria in the checklist. Depending on the nature of your criteria, you may have the right to be suspicious of their processes and determine that they do not understand your standards.

- A potential vendor submits the response but their evidence proves they pose a significant risk to your company, and it is unreasonable to try and mitigate. Cross them off your list!

- You have more criteria based on a potential vendor's initial responses. Ask them! If they want your business badly enough, they will cooperate with your due diligence process.

- One potential vendor's security processes stand out among the rest – your choice is easy !



# What's next?

As you work to ensure that your company has the proper safeguards in place, as well as to vet existing and potential vendors, here are some questions to guide your thinking:

- Are you taking every reasonable precaution with your customers' data? Are these controls documented? Periodically reviewing the protections you have in place today—and proactively making any needed changes or upgrades—can help ensure that the information you store is secure in the future.

- Do you have more than one vendor providing a similar service? How many of your vendors have access to sensitive data? Assessing your current suite of vendors is an easy way to detect potential redundancies and minimize unnecessary access to your customer's data.

- Have there been any red flags you should address? If so, don't leave anything to chance. Investigate warning signs promptly to ensure that your vendors continue to meet your security standards.

- If one of your vendors experiences a data breach, how do you plan to shut off the data flow and communicate the issue to your clients? Identifying and planning for potential threats ensures that you are prepared for any scenario.

Ultimately, it is your decision whether to entrust this information to a third-party vendor. Remember that you are your own most-trusted ally for controlling the flow of data to your vendors. By following the Third-Party Vendor Due Diligence Checklist for vetting your vendors, you will have the information you need to make an educated decision and guarantee compliance with applicable laws and regulations.

Have more questions about vendor relationships and they can impact information security? Want to put Aavenir through your Third-Party Vendor Due Diligence Checklist? Let's talk today!

# 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.

## Explore Additional Resources on Vendor Management

Click the icon that interests you to get started:



Checklist




Blog



Webinar



Datasheet

## 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