Vendor Risk Management Examination or Audit Preparation Guidebook

venminder

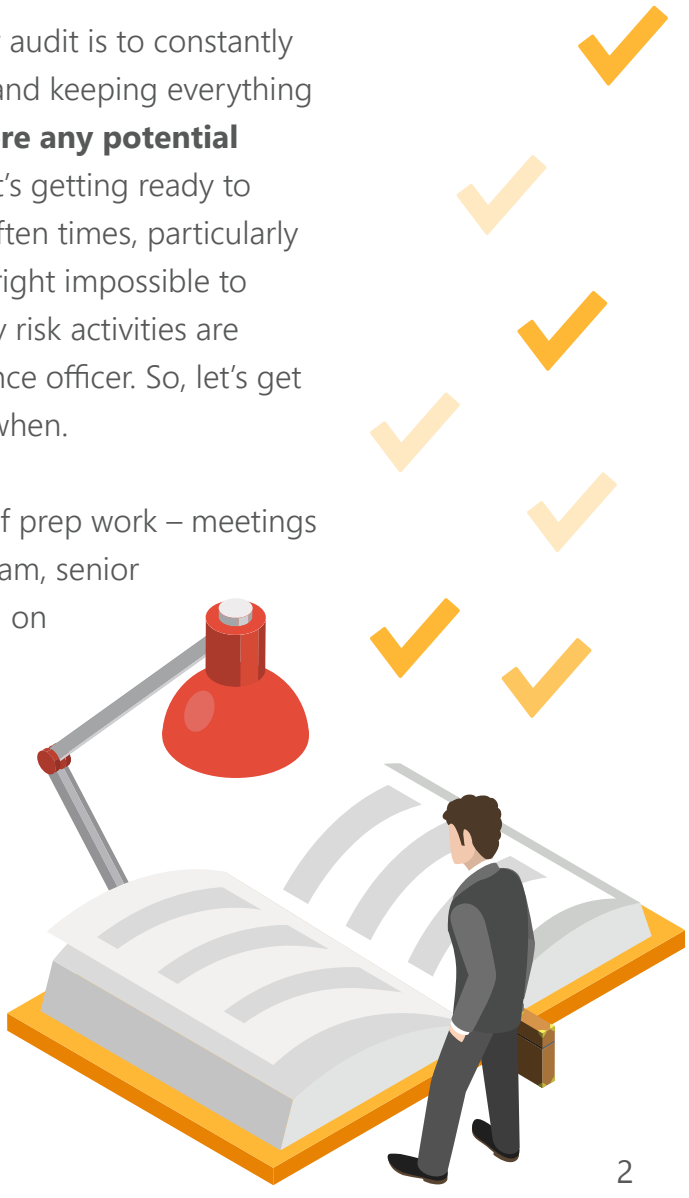
Vendor Risk Management Examination or Audit Preparation Guidebook

Do you have your vendor risk management in order? **Learn how to prepare for an exam or audit**

The best strategy for preparing for an examination or audit is to constantly be ready – that means preparing well ahead of time and keeping everything up-to-date. Ideally, this means **several months before any potential exam or audit**, you're already preparing as though it's getting ready to happen and then staying at that level of readiness. Often times, particularly at smaller organizations, this is very difficult or downright impossible to constantly keep everything refreshed since third party risk activities are often combined with the other duties of the compliance officer. So, let's get very practical about what to expect, what to do and when.

First off, make no mistake, this involves a great deal of prep work – meetings with the various lines of business, your compliance team, senior management and perhaps even prepping your board on what to expect.

At the end of it all, you should have a thorough set of documentation and be able to quickly and easily find items when they're requested. This also requires a highly organized approach and one that is best assembled well in advance.



Vendor Risk Management Examination or Audit Preparation **Playbook**

Let's take a look at some things you should have ready **3 or 4 months** *before* any potential exam/audit window:

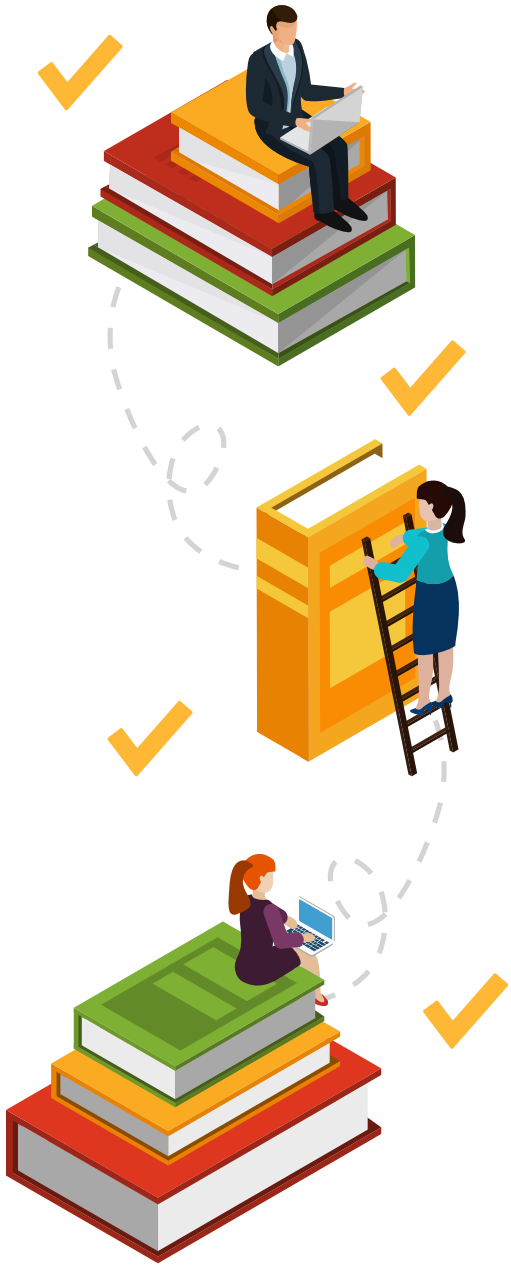
Anticipate what you know examiners/auditors are going to ask you for, either based on prior exams/audits or on the flow of a typical examination or audit… get these items prepared now rather than waiting for the exam/audit – and make sure you can quickly and easily access them when the time comes.

These should include:

- A copy of your **vendor management program** and **associated documents**
- An **organization chart** for those involved with third party risk management
- **Job descriptions and bios for key members** of the team to demonstrate adequate experience and training
- A **complete inventory of your third parties**, ideally ranked by level of risk
- **Samples** of your critical / high risk third parties and supporting documentation
- **Evidence of adequate review** and timely tracking of important documents such as financials, SOC reports, contracts, etc.
- **Evidence of reports** to keep senior management and the board informed of third party activities
- **Remediation** of any prior examination/audit issues

A Deeper **Dive**

Let's spend a little time on several of those items and talk about what you should aim to have put together months ahead of time:



A thoroughly documented set of policies and procedures describing your third party risk management program in detail.

These documents should be board-approved, accurate in terms of outlining the actual work product and cite relevant regulatory guidance or consumer protection laws. Be sure they're updated regularly when guidance changes or when particular situations warrant. Stick to a schedule of having them reviewed and approved annually.

- Where needed, make sure your program documents reference other policies that may be in play around your organization. For example, there's usually some intersection between third party risk management and various compliance policies.
- Getting your compliance and internal audit team involved months in advance of the exam/audit is always a good idea – they can help identify potential gaps in the program.
- Ensure your work product matches what your policy states. If it doesn't, now is the time to make changes.

A complete inventory of all your organization's third parties.

Include robust due diligence, well-written risk assessments and records of ongoing monitoring activities. This should also be accompanied by a process for identifying new third parties prior to a contract being executed and defined terms within the scope of which third parties need to be actively managed.

- There will be certain third parties you may simply want to be aware of from an inventory perspective but don't require ongoing active management (e.g., the copier repair person, the landscape company).

- If there are specific types of third parties that you deem not to be in scope, it's always a good idea to explain why – perhaps some are very minimal risk, but at least do some background checking on them. (e.g., the food delivery company, the office supplies company)

A risk-based approach to due diligence, complete with all of the relevant documentation.

At a minimum, for your critical third parties, you should have up-to-date documentation that includes the following 6 items:

- ✓ **Financials** (with corresponding analysis)
- ✓ **SOC reports** with accompanying controls (with corresponding analysis and ensure there aren't any unaddressed potential gaps and time periods covered are appropriate)
- ✓ A robust **business continuity plan** detailing the roles of the third party and the organization (with corresponding analysis)
- ✓ Complete **information security analysis** to safeguard your customers' data
- ✓ **Foundational documents** (such as articles of incorporation, secretary of state check, insurance certificates and any required licensing)
- ✓ An accurate and actionable **exit strategy**

A complete set of risk assessments on your third parties.

Demonstrate that you have carefully considered all potential risks associated with doing business with a particular third party and how those risks are addressed by your organization. Ideally, the description of these risks corresponds with your organization's enterprise risk management strategy outlining the vendor's appetite for risk.

- You should call out the risks included in the regulatory guidance – refer to FDIC FIL 44-2008 or OCC Bulletins 2013-29, 2017-7 and 2017-21 and be sure you've got those adequately documented and addressed.

Ongoing monitoring activities appropriate to control the risks identified in the assessment.

Ongoing monitoring activities could range from transaction testing, social media and negative news searches, call center listening, to mystery shopping. These should be tailored to the type of activities the third party is providing. If there are items (e.g., reporting, audit records) you need the third party to provide, be sure they're spelled out in the contract.

- Make sure the monitoring activity is well-documented and any items requiring follow up are addressed.

- Along with due diligence and risk assessments, consistency is incredibly important in your monitoring activities.

Verification that all documents are current.

Make sure documents such as SOC, business continuity and disaster recovery plans, certificate of insurance and other due diligence documentation are up-

to-date, as well as your analysis. If your policy is reviewed by the board on an annual basis, make sure you've notated the last review, such as a footnote indicating the date and referencing the meeting minutes to support it.

A system and process for managing contracts.

Ensure contracts are well-tracked (failing to recognize expiration dates and termination notifications periods is a common pitfall) and contain all of the required provisions to protect all parties involved in the business relationship.

- Often, if you have a person responsible for contract management and a centralized system for managing contracts, this task becomes much easier.

Evidence of regular reporting to senior management and your board of directors.

You should have evidence in the form of the actual presentation and shown in minutes. This reporting should touch on each of the activities listed above.

Hopefully, you've got all of these items in order – **but if not, now's the time to prepare.** If you wait until the opening of the exam/audit, you're going to be doing too much, too late.

Exam or Audit **Notification**

What happens when you get the notice of the examination or audit?
So, you're well-prepared and now it's game time – you just received notice that an on-site examination/audit is going to start soon. I know it's tough to follow this advice – **DON'T PANIC!** Seriously, there's no need if you're running the well-managed program described above.

Let's go through some of the key things you'll want to do… You've *probably* got a **month or two** to pull information together, but you want to have it well-organized for easy reference so when the examiners/auditors ask for an item, you can quickly and easily locate it.

1. **Be sure to let them know** (or via your organization's president or compliance officer) that you've received the notice and will welcome them upon arrival. It's also a good time to determine who will be the point person for routine requests and how to handle any issues that arise.

2. **Pull out your prior exam/audit report** and any related internal audit documents and be certain you've been responsive to any open items or recommendations. It's always a good idea to have a second person review them as well.

3. **Hopefully, your policy, program and procedures are up-to-date** and have been board approved within the past year. If not and if there's time, get them approved prior to the exam/audit start (unless that will violate a board approval scheduling requirement).

4. **Inform senior management and the board**, if it's your responsibility, and meet with them on what to expect and clarify any questions they may have and the roles of everyone involved.

5. **Meet with your team to discuss expectations** (e.g., always be polite and professional, don't offer "off the cuff" answers, clarify any questions you don't fully

understand, try not to meet with the exam/audit team impromptu or alone, etc.)

6. **Begin preparing responses and documents for any pre-examination/pre-audit requests or initial document requests.** Be particularly ready with items you know they're going to be asking for – as an example, you know they'll want your program documents, you know they'll want your vendor inventory and it's a pretty safe assumption they will want to see samples of a complete package of due diligence, risk assessment documentation and the back-up documents (such as financial analysis, SOC reviews and contract terms) from your critical and high risk vendors.

7. **Once you have compiled the responses and documents, have a second person review them for content and accuracy to the questions posed.** Make sure that you haven't missed anything obvious, but also make sure that things look consistent in form and content – a well-organized, professional looking set of documents is half the battle; meanwhile loose threads and items that look haphazard can lead to lots of confusion and further probing.

8. In addition to the second pair of eyes on the documentation, make sure before they arrive **you also do a final review yourself of the documents prepared** – this includes a review of the policies, procedures and program documents as well as due diligence – remember, a professional and consistent set of documents is a huge head start.

9. **Plan for the day of their arrival** – 14 helpful tips:

   - ✓ Tell them where to arrive, set an agreed-upon time and know how many people to expect
   - ✓ Have them issued visitor badges if possible
   - ✓ Make sure the entire organization knows where they'll be and general ground rules
   - ✓ Set up a well-equipped place for them to work so they don't have to wander and be inclined to ask questions
   - ✓ Treat them as you would want to be treated
   - ✓ Set up a formal entrance meeting with key management

- ✔ Provide them a list of names and titles but encourage them that all contact should go through a designated person
- ✔ Try to meet with them in pairs of two people from your organization – one to talk and one to take notes
- ✔ Set expectations on daily arrival and departure times so there's always someone there
- ✔ Give them a tour (but remember to clean up first – appearances make big first impressions)
- ✔ Set up a routine for daily or weekly check-ins
- ✔ Clarify any questions you don't fully understand
- ✔ Commit to communicate any findings or concerns regularly
- ✔ Understand response times for any requests for documentation

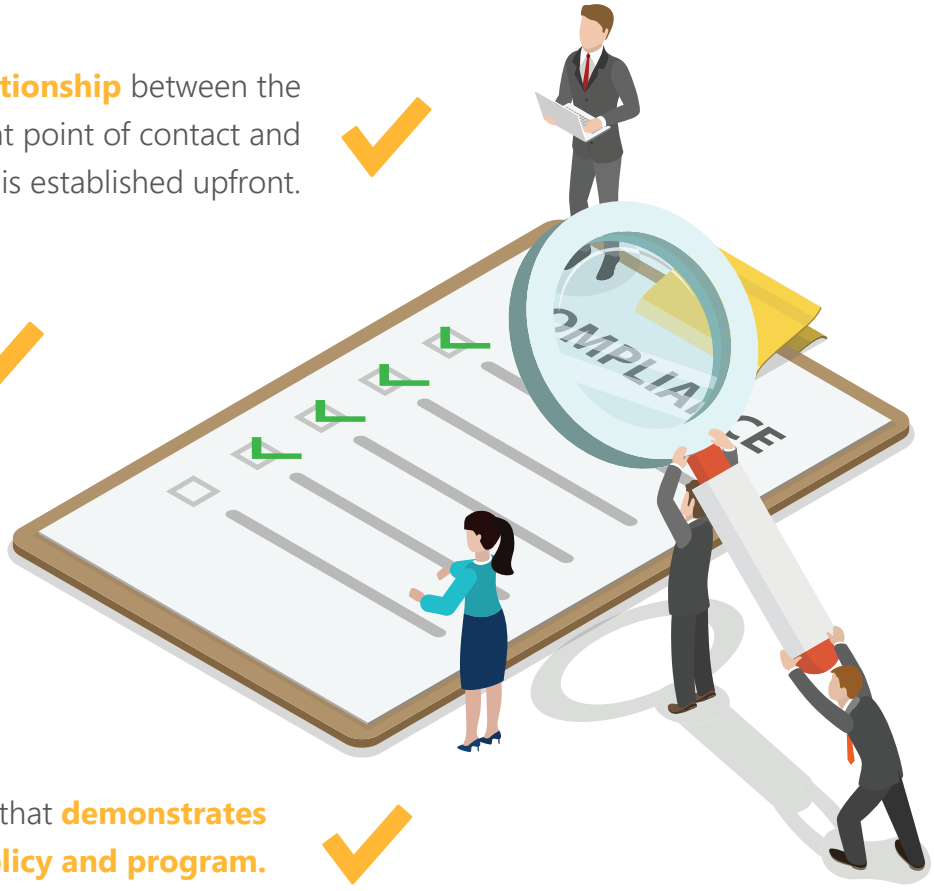
10 **Relax, you're ready,** now find the phone number for AAA so you can plan a well-deserved post-examination/post-audit vacation.

Examiner and Auditor On-Site **Expectations**

What will the examiner/auditor expect from you and your organization once they've arrived? Here are 4 expectations you can bet they'll have:

A **good working relationship** between the vendor management point of contact and examiner/auditor is established upfront.

That you educate the examiner/auditor on **how your processes work** and **what you're trying to accomplish**, especially if anything has changed since the last exam/audit.



Documentation is readily available that **demonstrates your actions match your policy and program.**

Evidence showing any gaps you've identified, such as missing due diligence, and the documented attempts to gather the information.

Need help preparing for an exam?

Download some of our work product samples to see how we can assist.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.