Vendor management exam preparation checklist

An exam of a vendor management program asks one thing in many ways, which is whether you do what your policy says. Examiners choose vendors from your inventory and ask for the evidence behind each one. This checklist covers what to gather and what to fix before they arrive.

Vendor _____ Completed by _____ Date _____

Policy and governance

- [ ] The vendor management policy has been reviewed and approved within the period it sets for itself.
- [ ] Procedures exist for the work the policy describes, and they match what staff do.
- [ ] Roles are assigned, and each person named knows the role is theirs.
- [ ] Findings from the last exam and the last audit are closed, or have a documented plan and date.

Vendor inventory

- [ ] The inventory is complete and has been reconciled against accounts payable in the last year.
- [ ] Every vendor has a named business owner who still works at the institution.
- [ ] Every vendor has a risk level, and critical vendors are marked.
- [ ] Vendors you no longer use are marked as ended, with their records kept.

Risk assessments

- [ ] Every vendor has a risk assessment on file, completed within the frequency its risk level requires.
- [ ] The method for setting a risk level is written down and applied the same way to every vendor.
- [ ] Overrides of a calculated risk level have a recorded reason and approval.
- [ ] No critical or high-risk vendor is overdue for reassessment.

Due diligence

- [ ] Due diligence is complete for every critical and high-risk vendor and matches what the policy requires at that level.
- [ ] Documents collected were reviewed, and the review and its conclusion are written down.
- [ ] SOC reports, insurance certificates and financial statements on file are current.
- [ ] Concerns found in due diligence have an owner, a due date and a status.

Contracts

- [ ] A signed contract is on file for every vendor that should have one.
- [ ] Agreements with critical vendors contain the provisions the policy requires, and gaps are documented.
- [ ] Termination dates and notice deadlines are recorded, and none has passed unnoticed.

Ongoing monitoring

- [ ] Scheduled reviews were completed on time, and late ones have an explanation.
- [ ] Performance against service levels has been reviewed for the vendors the policy names.
- [ ] Incidents and complaints involving vendors are logged with how each was resolved.
- [ ] Reviews triggered by a change at a vendor, such as a breach or a merger, were carried out.

Reporting and oversight

- [ ] Reports to senior management and the board were delivered as often as the policy says.
- [ ] Minutes show that the reports were presented and discussed.
- [ ] Approvals of new critical vendors and of exceptions are documented with who approved them.

The week before

- [ ] A single contact is named for examiner requests, with a backup.
- [ ] The documents in the first-day request are gathered in one place.
- [ ] Business owners of the vendors most likely to be sampled know they may be asked questions.

- [ ] Known weaknesses have been written up with the plan to fix them, so you raise them before the examiner does.

What examiners commonly ask for

Request	What to have ready
The policy and procedures	The current approved versions, with the approval date
The vendor inventory	Every vendor with its owner, risk level and critical flag
Files for sampled vendors	The risk assessment, due diligence, contract and latest reviews for each
Evidence of monitoring	Completed reviews, performance results and the incident log
Open issues	Each finding with its owner, due date and status
Board and committee reporting	The reports delivered and the minutes that show they were discussed

A free checklist from VendorRisk, vendor management software for regulated institutions. More guides, checklists and templates at vendorrisk.com/resources.