Vendor onboarding checklist

Onboarding goes wrong when a vendor is already in use before vendor management hears about it. This checklist follows a new vendor from the first request to its first scheduled review, in the order the work usually happens. Scale the middle of it to the vendor's risk level.

Vendor _____ Completed by _____ Date _____

Before anyone signs anything

Capture the request and decide whether the vendor is needed at all.

- [ ] A written request names the vendor, the service and the business owner who wants it.
- [ ] The request says what data the vendor will see and which systems it will touch.
- [ ] Someone has checked whether an existing vendor already provides the service.
- [ ] The request is approved by the people your policy names, and the approval is kept.
- [ ] The vendor is added to your inventory with an owner, a category and a status that shows it is still being onboarded.

Screen and classify the vendor

- [ ] The vendor's legal name and any trade name are confirmed.
- [ ] The vendor is screened against the sanctions and exclusion lists your institution uses, and the result is kept.
- [ ] A risk assessment is completed and the vendor is given a risk level.
- [ ] The vendor is marked as critical or not, using the definition in your policy.
- [ ] The risk level decides how much of the next section applies.

Complete due diligence

Collect and read the evidence your policy calls for at this vendor's risk level.

- [ ] A due diligence questionnaire is sent, returned and reviewed.
- [ ] A certificate of insurance is on file, with its limits and expiration date recorded.
- [ ] A SOC report or equivalent is obtained where one applies, and someone has read it.

- [ ] Financial statements are reviewed for higher-risk vendors.
- [ ] Business continuity and incident response plans are obtained for higher-risk vendors.
- [ ] Subcontractors with access to your data are disclosed.
- [ ] Concerns found in the review are written down with an owner and a due date.

Get the contract right

- [ ] The agreement is reviewed by the people your policy requires before it is signed.
- [ ] Service levels, security obligations and breach notification terms are in writing.
- [ ] A right to audit and the right to receive the vendor's reports are included where the risk calls for them.
- [ ] The term, the renewal terms and the notice period are recorded, with the last day to give notice.
- [ ] A signed copy is filed where the next reviewer will find it.

Set up ongoing oversight

Onboarding is finished when the next review is scheduled, and not before.

- [ ] The next risk assessment and due diligence review dates are set from the vendor's risk level.
- [ ] Expiration dates are recorded for insurance, SOC reports and other documents that have to be collected again.
- [ ] Reminders are set for the contract's notice date.
- [ ] The vendor's status is changed to show that it is active.
- [ ] The business owner knows what they are expected to monitor and report.

Who usually does what

Titles differ between institutions. What matters is that each part has one named owner.

Part of onboarding	Usual owner
Request and business case	The business line that wants the vendor
Screening and risk assessment	Vendor management or compliance
Due diligence review	Vendor management, with IT security for technical evidence
Contract review	Legal or procurement
Approval	A committee or the approver your policy names
Ongoing monitoring	The vendor's business owner

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