UC Berkeley Vendor Security Assessments (VSA)

Responsibilities & Expectations

The UC Berkeley Information Security Office (ISO) has partnered with an outside organization, Venminder, to provide Vendor Security Assessment (VSA) services to our campus community in order to help manage third party risk. To help Units and Vendors with timely completion of assessments, ISO created this document to clarify their responsibilities in the assessment process.

A typical VSA takes 4-6 weeks to complete *once Venminder receives all requested information from the Vendor*. If the Vendor is not responsive to Venminder, the completion of the assessment will be delayed.

Vendor Responsibilities

- Ensure a primary point of contact is available to collaborate with Venminder throughout the assessment process. You will need to provide the contact's Name, Title, Email Address, and Work Phone Number.
- Provide any Non-Disclosure Agreement (NDA) that you require the Unit and/or Venminder to sign before you will release evidence of compliance.
- Complete the Venminder questionnaire within the Venminder assessment portal.
    - **NOTE:** You are welcome to re-use responses from HECVAT, SIG, or other questionnaires for any questions that match Venminder's questions, so long as the responses are up to date.
- Upload documentation to the Venminder portal that corroborates your questionnaire responses. Documentation requirements will depend on the type of Venminder assessment that UC Berkeley has selected:
    - Document Request List: Data Protection Assessment **(most common)**
    - Document Request List: Information Security & Privacy Assessment
    - Document Request List: Point in Time Cybersecurity Assessment
- If requested by UC Berkeley, help facilitate additional assessments for any Fourth Parties (Vendor's Third Parties) that you significantly rely upon to deliver services.

Unit Responsibilities

- Inform the Vendor that Venminder will reach out to them.
- Serve as the liaison between ISO and the Vendor and ensure all communications and requests regarding the assessment are answered by the Vendor in a timely manner.
- Work with your Procurement Buyer to negotiate or address any risks related to the contract.
- Sign any NDAs the Vendor requires and have them include our partner, Venminder, in the agreement. Or let them know that Venminder is willing to sign a separate NDA.
- Work with your Unit Information Security Lead (*UCB access only*) to manage risks identified in the assessment report and ISO cover letter. Codify remediation by the Vendor in the contract as needed.