Scanning accounts for Harvard University merchants using external sites for credit card payment processing

Harvard University PCI regulations require merchants using Hosted Order pages from CyberSource or another gateway to have their local websites scanned. The manner in which the Trustwave PCI Wizard is configured may be misleading as it could lead you to either not having your local site scanned (required by Harvard Policy) or requiring you to answer a much more complicated Self Assessment Questionnaire (SAQ) than necessary. Following the steps below will ensure your site is scanned correctly as well as direct you to the correct questionnaire.

When registering the account, or beginning the self-assessment, select “My Website” for the question “How do you accept credit cards?”

Please note that in these steps it is assumed that your only method of acceptance is your ecommerce site using Hosted Order Pages. If you have additional methods of acceptance, select the “Multiple Ways” option, follow these instructions for describing your website. Answer all other questions based on your individual situation.
If you are registering, the next stage will be to complete registration and set up username and password. Once the account is activated, you will need to select “Start” in the section marked PCI Self-Assessment.

Selecting “PCI DSS Certification forms” allows you to select the shorter version of the self-assessment questionnaire (SAQ D). Note: if payments are made within your domain (e.g. https://checkout.mydomain.com, rather than https://checkout.3rdpartysite.com) you may need to complete SAQ D, in which case we advise to select the step-by-step wizard, as this breaks the 300+ question document into more manageable units.

Complete the Merchant Profile information. Unless you have a relationship with a merchant services provider other than Harvard University, you can select “No” for the question “Does your company have a relationship with more than one acquirer?”
The Product or Vendor should be the name of the service that hosts the payment portal. If it is not listed in the drop-down menu, enter the name and click “Add new”
The next stage is to set up the scans. Click “Add Scan Location” and you will get the following prompt:

Once the scan location is input and saved, you have the option to set a scan to run as soon as possible, or continue without scanning. You can also edit the schedule for when the scan will run each month. Scans can take up to several hours to complete once they begin, depending on the complexity of the network being scanned, but generally under one hour is normal. Emails will be sent to all registered users before a scheduled scan runs, and after it has completed. If a scan fails, this email will give more information on the outcome and how to review the scan report.

Next, you will proceed to the SAQ selection.
Select PCI SAQ A 2.0\(^1\), and ensure you can check all 4 eligibility questions. If you cannot attest to one or more of these statements, you may not be eligible to complete SAQ A.

Once completed, clicking Submit and Continue will bring you to the SAQ, which contains 13 questions in 2 sections\(^1\).

\(^1\) Remember that if you have multiple methods of acceptance that you will need to select another SAQ which will have more questions in more sections.