|  |  |
| --- | --- |
|  |  |
| **risk assessment document call** | |
| WoodTrust issues the following document call in order to help facilitate the Vendor Management Risk Assessment. While WoodTrust understands that not all vendors will have or are able to provide all requested documents, we ask that as much documentation is provided as possible. Lack of documentation does not automatically indicate an immature program.  **If any of the documents requested below are not available, please state why you are unable to share the requested documents.**   * SSAE16   + SSAE16:SOC1 (SOC 1: Statement on Standards for Attestation Engagements, Reporting on Controls at a Service Organization)   + SSAE16:SOC2 (SOC 2: Attestation Standards, Section 101 of the AICPA Codification Standards (AT Section 101). Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) * FISAP (aka BITS) Financial Institution Shared Assessment Program * ISO Certification 27001 * Results of 3rd Party or Internally performed Application Level Penetration Test\* * Results of 3rd Party or Internally performed Application Level Vulnerability Scans\* * Results of latest 3rd Party or Internally performed Infrastructure Vulnerability Scans\* * Results of latest 3rd Party or Internally performed Infrastructure Penetration Tests\* * PCI Compliance Documentation (Certification, ROC, Vulnerability Scans, etc.) * Internal Information Security Program (Overview/Policy/Standards)\*\* * Incident Response Plans * Organization Chart of IT/Security/Risk Departments * SDLC Security Documentation (Documentation on how Information Security is tied into the requirements, development, testing, approval process for applications/infrastructure changes, etc.) * HITRUST CSF Assessment Program (The HITRUST Common Security Framework (CSF) is health care specific, comprehensive and proscriptive. Portions of the framework can be used as the basis for HIPAA/HITECH compliance and provide assurance that the intent of both acts is satisfied)   \* If the company policy prohibits sharing results; redacted or sanitized copies which includes scope, process and mitigation plan are acceptable.  \*\* If the company policy prohibits sharing organization’s security policy with external party; overview and table of contents of security policy and standards are acceptable. | |