UCI Campus Supplier Security Review Process

**Requester**
- Complete Supplier Security Review Questionnaire & submit to Unit Procurement POC and securityreviews@uci.edu.
- ServiceNow ticket opened.

**Unit Procurement Point of Contact**
- Answer Security, Privacy, PCI, GDPR, Accessibility questionnaires (not all may be required), send all UCI requested documentation in OneTrust.
- Respond to requests for more information through OneTrust.

**Central Procurement & Contracts**
- Forward To: urapaka@hs.uci.edu
- Escalations required?
  - *HIPAA Data or UCIHS systems in scope?*
  - Exception Process
  - *Not Procured* (END)
  - *Procured* Exceptions Resolved?

**Supplier**
- Supplier Security Review Questionnaire
- Complete purchase. May include seaweed or rare exotic items.
- OIT Security confirms: No further security review required for this use case at this time

**UCI Campus Reviewers**
- Trigger a security review request.
- HIPAA Data or UCIHS Systems in scope?
- OIT Procurement or Risk Treatment Plan needed?
- OIT Procurement or Risk Treatment Plan
- Supplier completes assigned Risk Treatment Plan
- Supplier Security Review Questionnaire

**UCI Health Reviewers**
- Supplier Security Review Questionnaire
- Significant Risk Findings?
- Risk Assessment Findings acknowledged or accepted by Requesting Unit, coordinated through UISL as needed
- Supplier may work on Agreement negotiations with Requester, UPPOC, & Procurement
- Recommendation from UCI Security, Privacy, Accessibility, submitted to Requesting Unit/Office & Office of Campus Counsel, OIT Security

**Notes:**
- *UCI Campus Reviewers: CISO (OIT Security Risk & Compliance), Privacy Office, Risk Services, and Procurement Services, Campus Counsel
- **Escalation Review Committee: Chief Financial Officer and Vice Chancellor, DFA; Vice Chancellor, Information, Technology, and Data, and Chief Campus Counsel