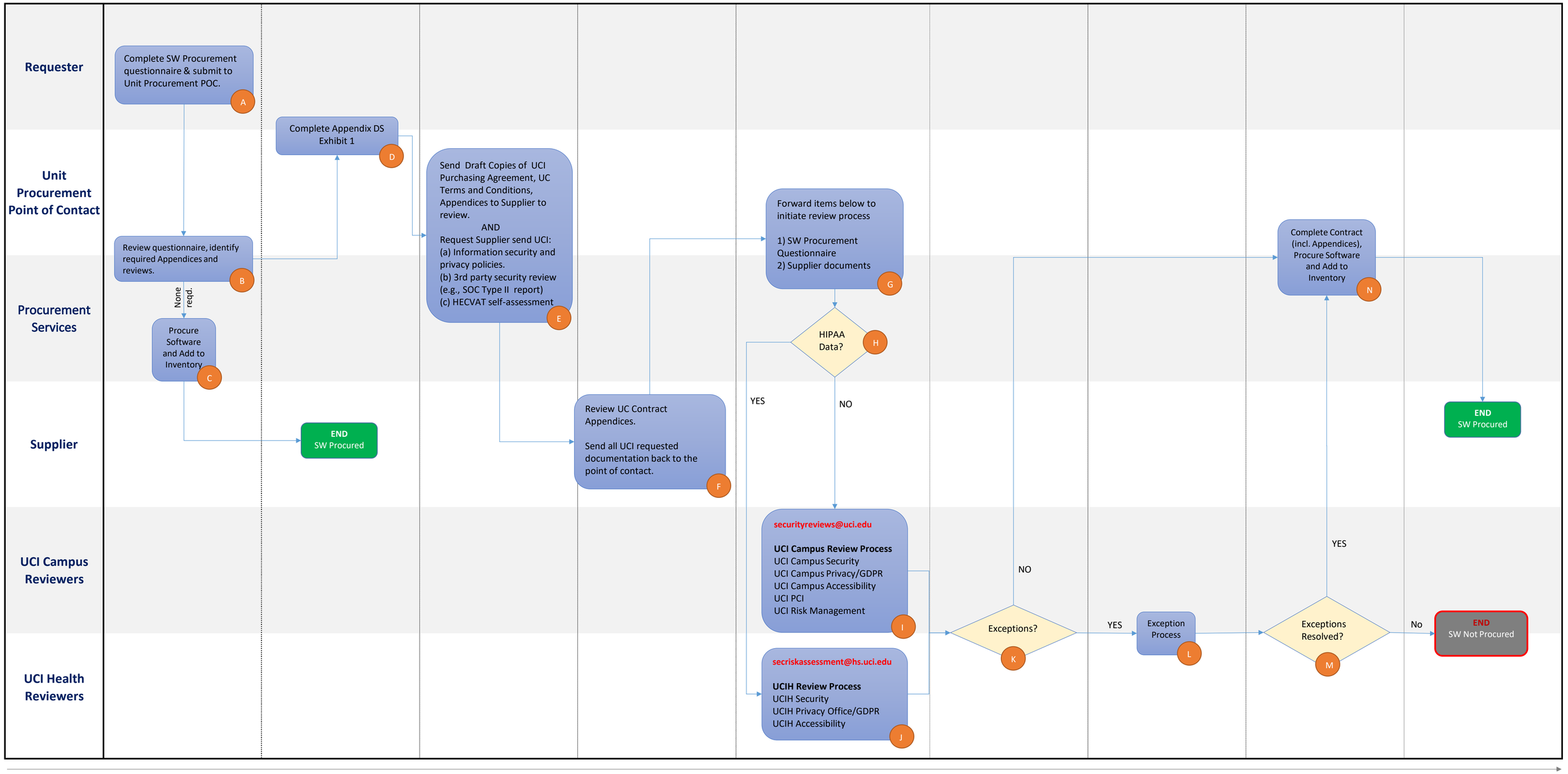
UCI Campus Software Procurement Process



Software Procurement Process Flow Diagram Notes

A) Complete software procurement questionnaire and submit to Unit Procurement Point of Contact (POC)

This form is designed to capture the most important information about the desired software, including whether it is a new purchase or renewal, the purpose of the software, whether the software is hosted on premise at UCI, or in the cloud and the type of data involved. The Software Procurement Questionnaire (a fillable PDF) can be found on the UCI Procurement Services website.

B) Review software procurement questionnaire, identify required Appendices and reviews

If the Unit Procurement Point of Contact (POC) or Procurement Services have questions about the information entered in the software procurement questionnaire, they will reach out to the Requester for clarification. Having the right information on the form ensures that the Supplier receives a Purchasing Agreement and Appendices with the Supplier early on, preventing delays.

Based on the answers to the form, requests are routed to the appropriate team for review. Examples of common reviews include a review of the Supplier's information security practices privacy practices. For systems that process payments, involve health care data, or contain information related to European residents, other reviews are performed.

C) Procure software and add to inventory (no reviews or Appendices required)

Occasionally, there are situations where a software application is approved for immediate purchase. This is the case for 10-15% of software applications. With more stringent system-wide protections on data, particularly data stored in the cloud, moving straight to purchase without reviews is becoming less frequent.

D) Complete Appendix DS Exhibit 1

This form (a fillable PDF) is where data is classified. This Exhibit becomes part of the final contract. For help classifying data, refer to the Security website, reach out to your Unit Information Security Lead, or the Procurement POC for the Unit.

E) Send draft copies of the UCI Purchasing Agreement, Terms and Conditions, and Appendices to the Supplier for review AND Request that the Supplier send UCI information to commence the review process.

In many cases, the Supplier will engage their legal counsel to review and negotiate them. This can add several weeks to the process. Suppliers, particularly smaller organizations, may not be willing or able to meet requirements outlined in UCI Purchasing Agreements and Appendices.

In parallel with having the Supplier review UCI documents, we ask that the Supplier send documentation to UCI for our internal review processes. In all cases, request the Supplier's security policy, privacy policy, 3rd party security review (e.g., a SOC Type II report) and/or a HECVAT self-assessment). For applications that process payments, request the Supplier's PCI AOC (Attestation of Compliance).

F) Supplier reviews the UC Contract and Appendices. Supplier prepares, sends UCI requested documentation.

Having these steps performed in parallel saves time in the process. While the Supplier is becoming familiar with the UC purchasing documents, they can ensure that UCI has the required information to commence their internal reviews.

G) & H) Forward SW Procurement Questionnaire and Supplier documents to trigger the review process(es).

For software that processes, transmits or stores HIPAA data, reviews are conducted by UCI Health at securityreviews@uci.edu; all other reviews (without HIPAA data) are sent to the UCI Campus Security team at securityreviews@uci.edu.

I) UCI Campus Review Process

Reviews that do not involve HIPAA data are performed by teams based out of the main Campus in Irvine. These include Campus Security, Privacy, Risk Management and Accessibility reviews. All PCI reviews (for processing of payments) are performed by the Campus UCI Security Risk and Compliance team, including those with Health data.

J) UCIH Review Process

Reviews that do involve HIPAA data are performed by teams based out of UCI Health in Orange. These include UCI Health Security, Privacy and Accessibility reviews.

K) Exceptions

There may be exceptions to any of the reviews. This triggers the exception process and related escalations.

L) Exception Process

There are defined escalation processes for various types of exceptions, based on the nature of the issue. This process ultimately involves identifying the appropriate party who is willing and able to accept the risk (usually a Unit Head or Vice Chancellor).

M) Exceptions resolved

If exceptions are unresolvable, the software product will not be procured and an alternative Supplier will need to be selected. If exceptions are resolved, the software procurement continues.

N) Complete contract, including Appendices, procure software and add to the UCI software inventory.

This steps represents the successful conclusion of the process.