UCDAVIS

Supply Chain Management

Software Procurement

2019

Some Background

- February 2018 All software commodity codes were restricted to ensure proper review of terms and conditions .
- March 2018 Procurement received feedback from Dean's Technology Council and IT Service Committee about software procurement. Information Security Office (ISO) also gave additional information about their Security Assessment and Review process.
- June 2018 Procurement and IET completed internal Software Audit.
- September 2018 BFB-IS-3: Electronic Information Security Policy became effective.

What has happened since then?

- Lots of listening and collaboration.
- Identified refinements in software procurement process.

Software Procurement with UISL Approval

The Unit Information Security Lead (UISL) is assigned within the unit by the Unit Head*. UISL and Unit Head Ensure that Vendor Risk Assessments (VRA) are complete and Risk Treatment Plans are implemented.**

- UISL for each Department would be identified
- UISL and ISO will review and determine what type of VRA is needed prior to submission of a requisition.
- More information about UISLs: https://iet.ucdavis.edu/unit-iso-partners

The Unit Head is a generic term for dean, vice chancellor or person in a similarly senior role who has the authority to allocate budget and is responsible for Unit performance.

** Full description of Unit Head and UISL responsibilities can be found in BFB-IS-3 Section IV.*

Software Procurement Process

Where to Start:

- Consult with your IT team and/ or UISL. These are your best resources!
- Evaluate current university agreements with suppliers that provide the solution needed.

Why? The applicable due diligence may already be done! This means no supplier set up, no contract negotiation and if the use case aligns well with a recent risk assessment outcome significant time saving may be possible.

Not to mention, opportunity for better pricing! Consolidating University spend with suppliers can help us achieve improved pricing, terms and incentives.

Where to look:

-CalUSource https://calusource.net/login/ System Wide, UC and CSU agreements

-KFS Local UCD Agreements

-Supply Chain website https://supplychain.ucdavis.edu/procure-contract/buying-goods/software Local UCD Agreements

-Contact Strategic Sourcing! strategicsourcing@ucdavis.edu

Software Procurement Process

Where to Start Continued:

So there is no current agreement available for the solution that is needed? 😕

- Kick off the procurement process by submitting a request for a vendor risk assessment (VRA) through the Information Security Offices' GRC tool https://itriskmanager.saiglobal.com/ucdavisgrc/
- For more information about the VRA process: https://iet.ucdavis.edu/security/services_and_consultation

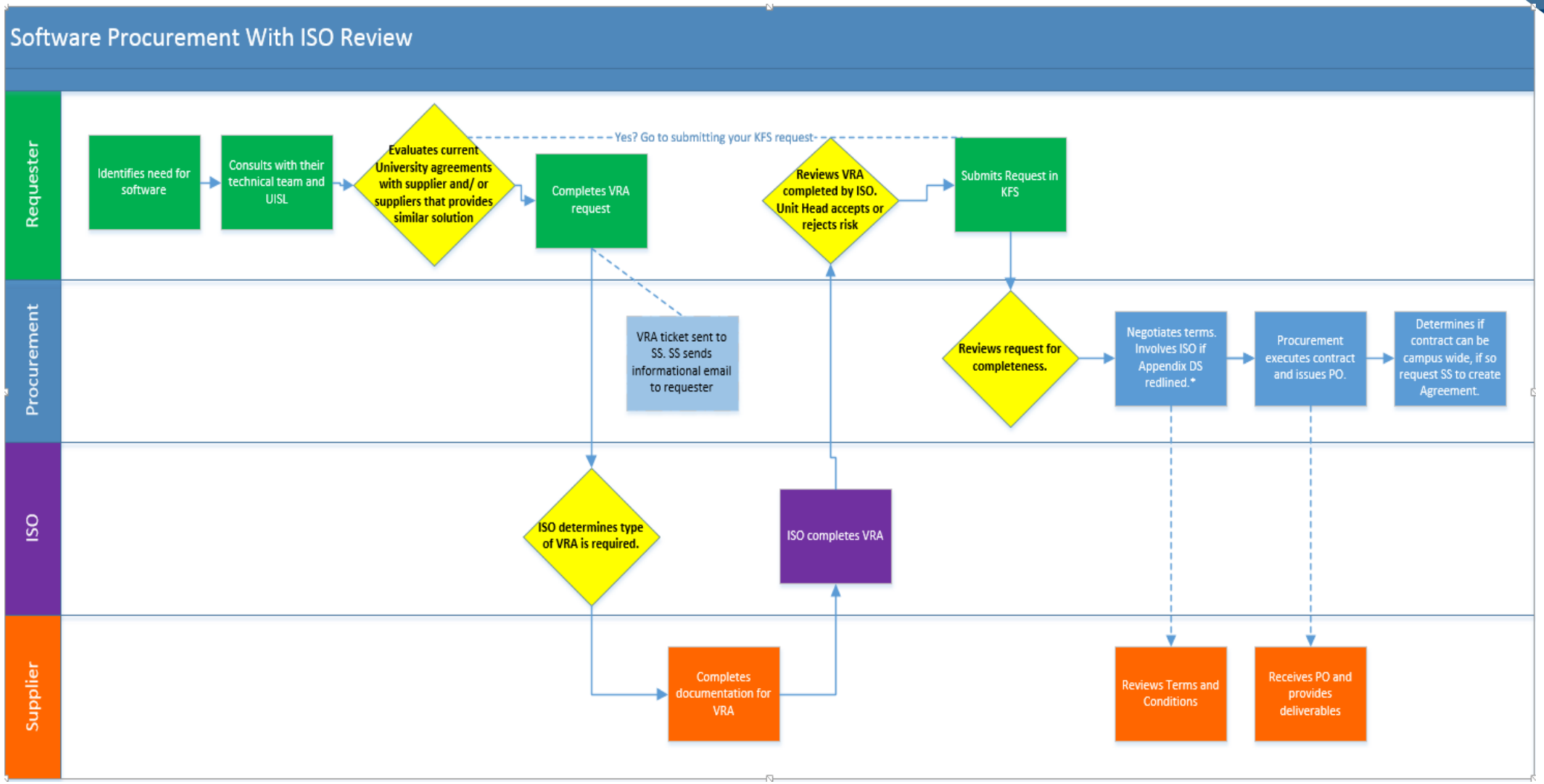
Why is it important to complete vendor risk assessments?

The UCOP IS-3 policy requires units to ensure that agreements with suppliers contain security requirements that are consistent with the IS-3 policy and supporting standards for the protection of and access to institutional information and IT resources. The policy explicitly requires units using suppliers to complete a risk assessment.

How long does the ISO-led VRA take?

The amount of time required to conduct a VRA from request to debriefing depends on many factors. These factors include how many other assessments are already under way, time of academic year request fluctuation, responsiveness of the vendor, complexity of the assessment, the quality of answers provided by the vendor, and availability of ISO assessors. The ISO recommends allowing at least two months for an assessment, prior to the date when the contract negotiations need to begin. While the ISO has been successful completing some assessments more quickly, some assessments also require more time for one or more of the above reasons.

Software Procurement Process



*Procurement reviews contract with legal if required.

Software Procurement With UISL Approval Key Changes

- Vendor Risk Assessment (for defined commodities) will be done prior to KFS request process.
  - KFS requests (for defined commodities) will be submitted with UISL approval.
- VRA ticket will be sent to Strategic Sourcing. Communication with procurement requirements or information will be sent at this time if needed.
  - Contracts at other UCs
  - Bidding threshold information
  - Past purchase information at UCD
- UISL will drive completion of Security Questionnaire and gathering of supporting evidence from the supplier in order to complete the VRA.