

Software Purchasing Process

The Original Software Process



Software is no longer physical



Current Software Procurement Process



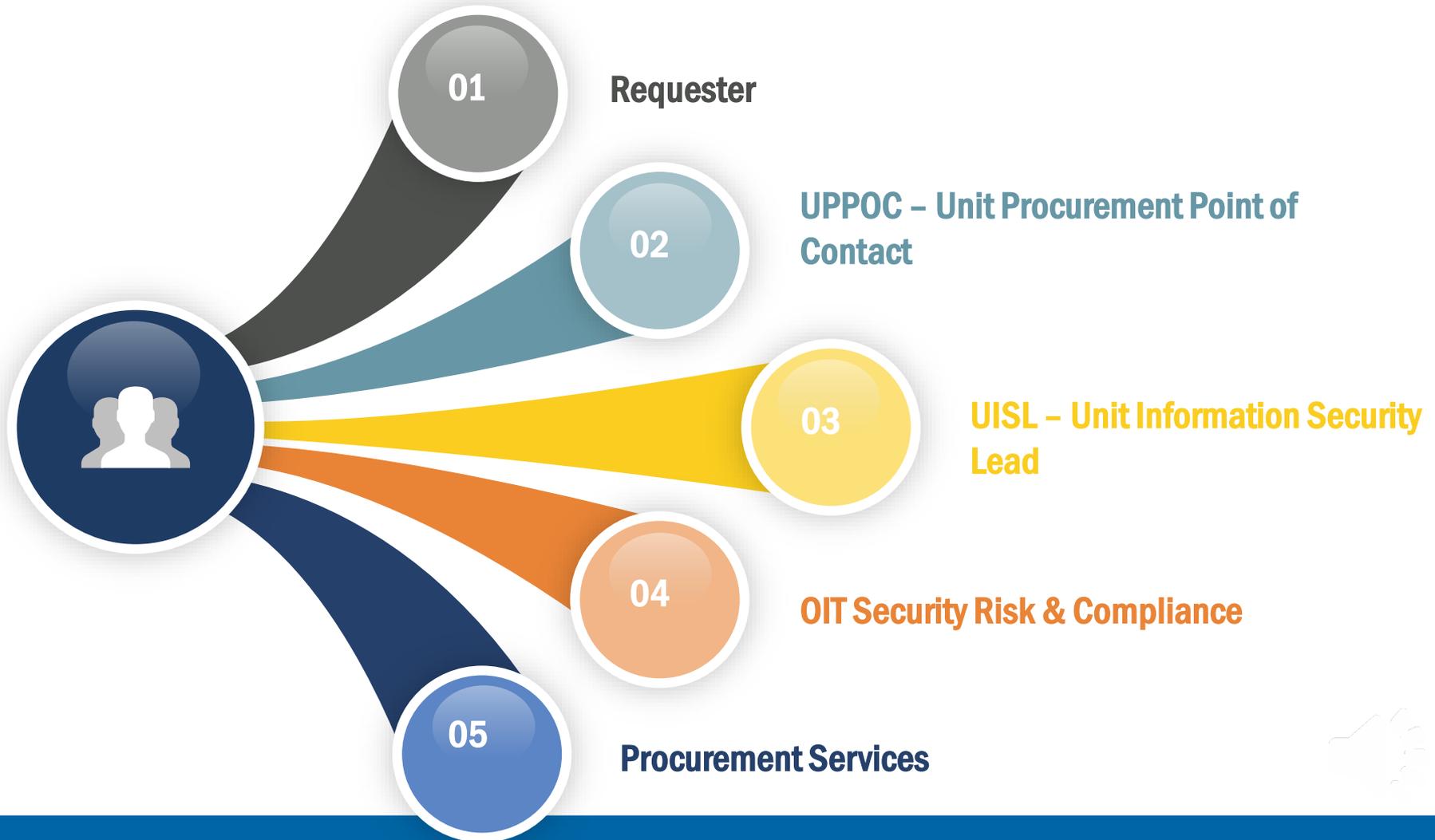
-
1. End user submits request to dept.
 2. Dept. submits KFS requisition or request to PALCard team for approval
 3. Procurement verifies if any existing agreements are in place.
 4. If no agreement exists, Procurement forwards software questionnaire to dept.
 5. Dept. consults with end user and local IT to fill out questionnaire.
 6. Dept. submits questionnaire to Procurement for review.

-
1. Procurement reviews questionnaire and either forwards it to OIT to begin a security review or dept. is given permission to purchase.
 2. OIT asks department to request HECVAT, Security Plan, and SOC Type II report from supplier.
 3. OIT provides security review assessment and assists departments in completing Appendix DS.
 4. Department sends UC Contract templates (UC T&C, Appendix DS, GDPR, BAA) to supplier to review.
 5. Supplier provides feedback/edits.
 6. Contracts team reviews edits and negotiates with supplier.

-
1. Agreement is finalized.
 2. PO is issued or paid with PALCard.

Additional 2-4 weeks during FY end

Software Procurement Team



Administrative UISLs

Unit	Technical UISL	Administrative UISL
Athletics	<u>Mikel Alustiza</u>	<u>John Hauscarriague</u>
Chancellor's Office	<u>Max Garrick</u>	<u>Tomas Figueroa</u>
Communications	<u>Jim Kreuziger</u>	<u>Karen Imahara</u>
Enrollment Management	<u>Chris Shultz</u>	<u>Patricia Morales</u>
Division of Finance and Administration	<u>Clint Maruki</u>	<u>David Ott</u>
Graduate Division	<u>James Tang</u>	<u>Court Crowther</u>
Health Affairs	<u>Gabriel Gracia</u>	<u>Jim Davis</u>
Human Resources	<u>Christa Chen</u>	<u>Stephen Whelan</u>
Equal Opportunity & Compliance	<u>Max Garrick</u>	<u>May Wang</u>
Office of Information Technology	<u>Josh Drummond</u>	<u>Kian Colestock</u>
Provost/EVC Office	<u>Max Garrick</u>	<u>Tomas Figueroa</u>
Office of Research	<u>Noah Margolis</u>	<u>Sinqui Musto</u>
Student Affairs	<u>Wayne Fields</u>	<u>Edgar Dormitorio</u>
Office of the Vice Provost for Teaching and Learning	<u>Jeremy Thacker</u>	<u>Jennifer Aaron</u>
University Advancement	<u>Ashish Regmi</u>	<u>Lynn Rahn</u>

Find your department's UISL at [🌐 security.uci.edu/isc.html](https://security.uci.edu/isc.html)



Academic UISLs

School	Technical UISL	Administrative UISL
Claire Trevor School of the Arts	Jason Valdry	Deb Sunday
School of Biological Sciences	Matthew Martinez	Benedicte Shipley
The Paul Merage School of Business	Gary Striano	Tony Hansford
School of Education	Hyuk Kang	Tammy Ho
The Henry Samueli School of Engineering	Dan Melzer	John Romine
School of Humanities	Dwayne Pack	Penny Portillo
Donald Bren School of Information and Computer Science	Bill Cohen	Heike Rau
School of Law	Patty Furukawa	Lisa Rehbaum
School of Physical Sciences	Domingos Begalli	Maria Graziano
School of Social Ecology	Jennifer Lane	Greg Reinhard
School of Social Sciences	Andrew Hill	Becky Avila
Libraries	Adrian Petrisor	Kevin Ruminson
Division of Continuing Education	Erich Delcamp	Bob Rude
College of Health Sciences	Gabriel Gracia	Jim Davis

Find your department's UISL at [🌐 security.uci.edu/isc.html](https://security.uci.edu/isc.html)



OIT Security Team

UCI Campus

- **Josh Drummond**
Chief Information Security Officer
- **April Sather**
Assistant Chief Information Security Officer
- **John Denune**
Security Risk & Compliance Program Manager

UCI Health

- **Gabriel Gracia**
Data Security Manager
- **Steve Chen**
Security Information Protection Architect
- **Uma Rapaka**
IT Security Architect



Procurement Services Team

Procurement/Strategic Sourcing

- **Patrick Ko**
Senior Buyer
- **Sarosh Siganporia**
Strategic Sourcing and Procurement Manager
- **Snehal Bhatt**
Chief Procurement Officer

Contracts

- **Andrew Calderon**
Contracts Manager
- **Laura Moss**
Principal Contracts Analyst
- **Shelia Thomas**
Contracts Analyst



New Software Procurement Process



Old Process (3 - 8 weeks)



New Process (1 day - 4 weeks)

1. Requester completes SW Procurement Questionnaire and submits to UPPOC.
2. UPPOC reviews questionnaire and identifies/completes required Appendices. UPPOC also checks for existing agreements. If no Appendices required, proceed with purchasing.
3. UPPOC completes Appendix DS Exhibit 1 with requester.
4. UPPOC forwards UCI Contract Templates to Supplier for review and requests additional security documents.

5. UPPOC forwards SW Procurement Questionnaire and Supplier documents for Security Review. UPPOC also routes contract documents to Procurement Services and enter a KFS requisition (if applicable). OIT provides security review assessment and reviews/negotiates the Appendix DS. Any other Appendices will be reviewed by their respective parties. OIT will address and resolve any exceptions.
6. In conjunction with OIT, Procurement Services will negotiate contract language with supplier.

7. Agreement is finalized.
8. PO is issued or paid with PALCard.

Additional 2 - 4 weeks during FY end

1. Requester

Completes the Software Procurement Questionnaire and submits to the Unit Procurement Point of Contact.

Name of Software:

Link to Software Website:

Describe the main use(s) of this software and the type of data involved:

Will this software be installed locally at UCI, hosted in the cloud, or a combination of both? Locally In the Cloud Both

Is this a new software purchase, or a renewal? New Renewal

SECURITY	Yes	Unsure	No	Notes
Will the Supplier have access to any UC resources (e.g., data, network, systems)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Could the misuse of this software directly cause harm to life or property?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Will the software be used to process payments of any kind?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Will this software be used to collect, store, access or transmit data related to any of the following?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Data governed by a research contract or grant (e.g., CUI, CDI, CTI, EAR, ITAR)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Sensitive identifiable human subject research	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Financial information (e.g., student loan/financial aid, accounting payroll)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Human resource information (e.g., staff, faculty, student worker personnel)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Personally identifiable information (PII) (e.g., full name, email address, date of birth, social security number, home address, telephone number)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Protected health information (i.e., subject to HIPAA or Data Use Agreements)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Other sensitive medical information (e.g., disability or genetic information)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Student education records	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Data related to European residents (does not apply to British residents)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
• Other data classified as Protection level 3 (P3) or 4 (P4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
ACCESSIBILITY	Yes	Unsure	No	Instructions
To the best of your knowledge, is this software, or a previous version of it, already in use on campus?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES - Stop here. An accessibility review is NOT needed. IF NO/UNSURE - proceed to next question.
Will the software be used by people outside your Unit?	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	IF YES/UNSURE - Stop here. An accessibility review IS needed. Contact it-accessibility-review@uci.edu IF NO - proceed to next question.
Is there an alternative way to perform the task if the software cannot be used due to a disability?	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	IF YES - An accessibility review is NOT needed. IF NO/UNSURE - An accessibility review IS needed. Contact it-accessibility-review@uci.edu .

Name of Requester

Department/Unit

Email Address

Date



2. Unit Procurement Point of Contact (UPPOC)

- Reviews the Questionnaire
- Verifies if there are any existing agreements
- In coordination with the UISL, determines if the purchase needs the required Appendices and further Review
- If the purchase is low risk/low dollar, issue PO (referencing UCTC) or pay via PALCard.



3. Requester with UPPOC

Completes Appendix DS Exhibit 1.

University of California

Appendix
Data Security

Exhibit 1 – Institutional Information

1. Protection Level Classification⁴:

- Protection Level 1
- Protection Level 2
- Protection Level 3
- Protection Level 4

Explanation:

The Protection Level determines the applicable cyber security insurance requirement in the Terms and Conditions.

2. Institutional information data element descriptors:

Select all data types that apply:

- A. Animal Research Data.
- B. Controlled Technical Information (CTI).
- C. Controlled Unclassified Information (CUI) – 800-171/NARA.
- D. Defense Department: Covered Defense Information (CDI).
- E. Federal Acquisition Regulations (FARS/DFAR) other than CUI.
- F. GDPR personal data.
- G. GDPR special data.
- H. Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
- I. Health Records subject to HIPAA Privacy or Security Rule (PHI).
- J. Human Subject Research Data.
 - 1. Identified.
 - 2. Anonymized.
- K. Intellectual property (IP), such as patents, copyright, or trade secrets.
- L. ITAR/EAR-controlled data.
- M. Payment card data (PCI, PCI DSS).
- N. Personally identifiable information – PII.
- O. Student data, whether or not subject to FERPA.
- P. Other: _____
- Q. Other: _____

⁴ For reference see: <https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html>



4. UPPOC

Sends Draft Copies of the UCI Purchasing Agreement, UC Terms and Conditions, and Appendices to the Supplier to review.

AND

Requests the Supplier send to UCI:

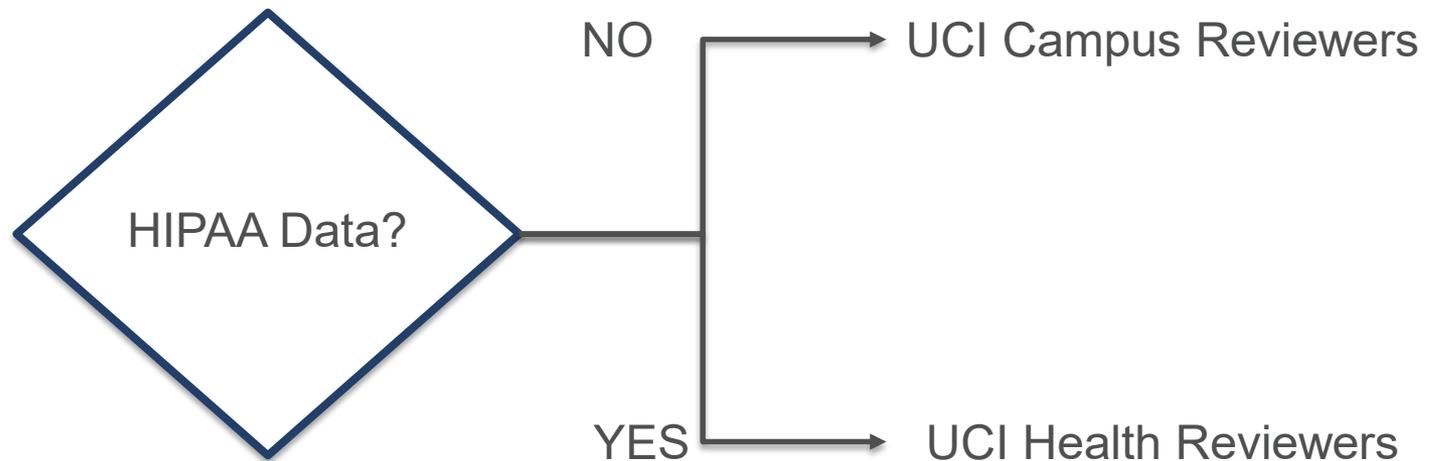
- (a) Information security and privacy policies/plan.
- (b) 3rd party security review (e.g., SOC Type II report)
- (c) HECVAT self-assessment



5. UPPOC

Forwards items to IT Security Team and Procurement Services to initiate the Review Process:

- 1) SW Procurement Questionnaire
- 2) Supplier documents



Submits requisition in KFS



UCI Campus Reviewers

securityreviews@uci.edu

UCI Campus Review Process:

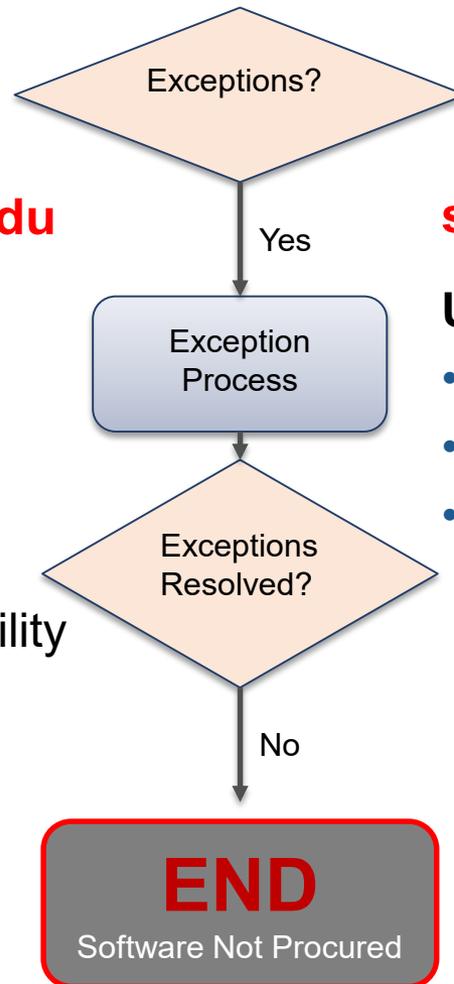
- UCI Campus Security
- UCI Campus Privacy/GDPR
- UCI Campus Accessibility
- UCI PCI

UCI Health Reviewers

secriskassessment@hs.uci.edu

UCIH Review Process:

- UCIH Security
- UCIH Privacy Office/GDPR
- UCIH Accessibility



UCI Campus Reviewers

securityreviews@uci.edu

UCI Campus Review Process:

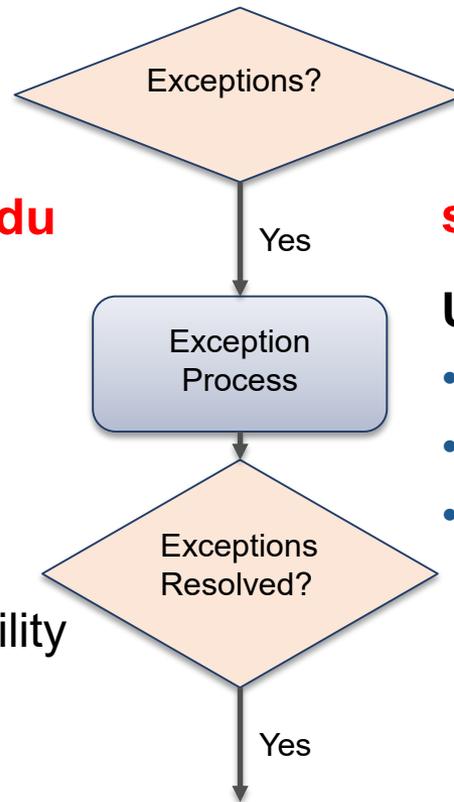
- UCI Campus Security
- UCI Campus Privacy/GDPR
- UCI Campus Accessibility
- UCI PCI

UCI Health Reviewers

secriskassessment@hs.uci.edu

UCIH Review Process:

- UCIH Security
- UCIH Privacy Office/GDPR
- UCIH Accessibility



OR

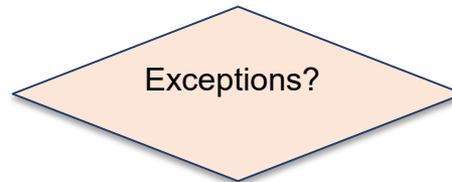


UCI Campus Reviewers

securityreviews@uci.edu

UCI Campus Review Process:

- UCI Campus Security
- UCI Campus Privacy/GDPR
- UCI Campus Accessibility
- UCI PCI



No

UCI Health Reviewers

secriskassessment@hs.uci.edu

UCIH Review Process:

- UCIH Security
- UCIH Privacy Office/GDPR
- UCIH Accessibility



6. Procurement Services

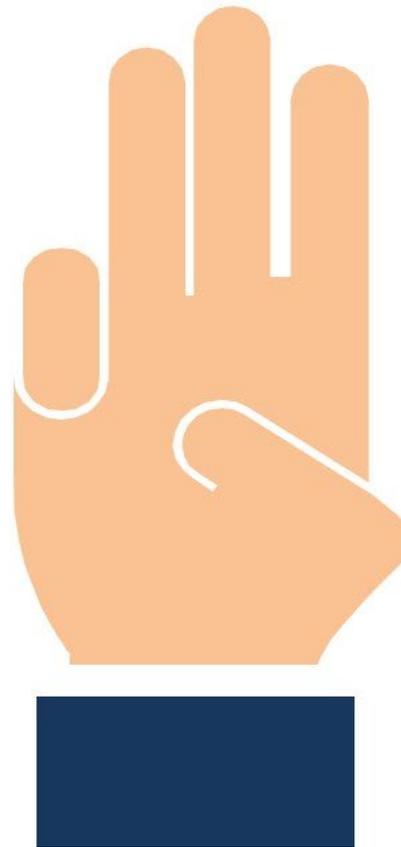
- Reviews/Negotiates any redlines or changes in contract language in parallel with OIT's review process.
- Once the security review and contracts negotiation have concluded, the Contracts Team will finalize the contract (incl. Appendices) and route for signatures.
- Issues Purchase Order or pay via PALCard.
- Adds the software to the University's inventory.



The Rule of Three

Best Practices for End Users/Requesters

- 1** Submit your requests as early as possible.
- 2** Consult with your UPPOC first. Be sure to fill out the Software Procurement Questionnaire.
- 3** NEVER sign any supplier T&C or Agreements on behalf of the University.



The Rule of Three

Best Practices for UPPOC

- 1** Check for existing agreements. Verify compliance with BUS-43 and PCC.
- 2** Verify that the Software Procurement Questionnaire is filled out accurately and completely.
- 3** Allow sufficient time for software review.

