UCIrvine | Internal Audit Services

IT Contract Approval Processes

Internal Audit Report No. I2024-104
September 12, 2025

Prepared By
Larry Wasan, Principal IT Auditor
Reviewed By
Loran Lerma, Audit Manager
Approved By
Mike Bathke, Director

UCI Internal Audit Services

September 12, 2025

KIAN COLESTOCK
ASSOCIATE VICE CHANCELLOR
OFFICE OF INFORMATION TECHNOLOGY

SNEHAL BHATT
CHIEF PROCUREMENT OFFICER
PROCUREMENT SERVICES

CHRISTOPHER RICHMOND
MANAGER
RISK SERVICES

RE: IT Contract Approval Processes Audit
Report No. I2024-104

Internal Audit Services has completed the review of IT Contract Approval Processes, and the final report is attached.

We would like to thank the staff and management from Procurement Services, Risk Services, and the office of Information Technology for their assistance and cooperation during this review.

If you have any questions or require additional assistance, please do not hesitate to contact me.

Sincerely,

Mike Bathke

Mike Bathke
Director

C: Audit Committee
Josh Drummond – Chief Information Security Officer, OIT

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2023-2024 audit plan, Internal Audit Services (IAS) reviewed UCI's IT contract policies, procedures, and controls. The review included an analysis of supporting documentation for a sample of IT contracts to verify that vendor vetting occurs prior to contract finalization, ensuring compliance with established policies. Additionally, staff training in the procurement of software and IT services was evaluated for adequacy to ensure that related policies and procedures are followed.

Based on this review, controls have been implemented to mitigate certain risks. However, some internal controls need improvement and should be strengthened to minimize risks and ensure compliance with university policies and procedures. Specifically, IAS noted observations which are summarized below.

Vendor Certificates of Insurance (COI) – A review of COIs uploaded into the systemwide Insurance Tracking System (ITS) indicate a critical compliance issue as follows.

- According to ITS data, 97–99% of Certificates of Insurance (COIs) are currently non-compliant, primarily due to expiration or failure to meet all campus insurance requirements. Details regarding this issue are provided in section V.1a.

- Additionally, there are ongoing reliability concerns with the ITS system itself. Details regarding this issue are provided in section V.1b.

IT Contract Vetting and Approvals – Improvements in the review and vetting process could be further strengthened as follows.

- For one (5%) of the 21 vendors sampled for review, management confirmed that no security review was conducted prior to approval and finalization of the contract. According to OIT, an exception was made for the IT resource in question. However, the exception was not documented as required by policy. Details regarding this issue are provided in section V.2.a.

- For six (67%) of the 21 vendors sampled for review, a Supplier Review Questionnaire and either a Risk Assessment document or conclusion from OIT that no special security terms are necessary were not attached to the purchase requisition within the Kuali Financial System (KFS) as required by the Procurement Office's procedures for Buying Software/IT Services. Details regarding this issue are provided in section V.2.b.

II. BACKGROUND

During the annual risk assessment interviews conducted by IAS with various levels of management, one recurring concern was the vetting and approval process for IT contracts. Specifically, stakeholders expressed concerns about the potential for incomplete reviews related to cybersecurity, privacy, legal, and insurance compliance. These responsibilities, in coordination with Procurement Services, are shared among the Office of Information Technology (OIT), the Privacy Office, the Office of Campus Counsel, and Risk Services, respectively.

The findings and recommendations in this report aim to enhance the IT contract approval processes, ensuring compliance and efficiency in managing associated risks. Implementing these recommendations will strengthen the organization's ability to manage IT contracts while upholding privacy, data security, liability, and legal standards.

Criteria used for this review primarily included the procedures for the purchase of software or IT services as documented in the "Buying Software/IT Services", which is located on the Procurement Office website.

III. PURPOSE, SCOPE, AND OBJECTIVES

The purpose of this audit was to assess the effectiveness of current processes in safeguarding sensitive information, mitigating legal and financial risks, and aligning with organizational policies and standards.

The objectives of the audit were to verify that:

- Cybersecurity, privacy, and legal risks have been adequately reviewed prior to approval.
- Minimum insurance requirements are met according to the amounts set by Risk Services
- COIs are properly tracked, monitored, and regularly updated.
- Adequate staff training is provided to ensure compliance with IT contract procurement processes.

Our methodology included examining contract approval workflows, discussions with key stakeholders, and reviewing relevant documentation, including Purchase Orders (PO) and requisitions in the Kuali Financial System (KFS) as well as COIs in ITS.

The scope of this audit was limited to IT contracts procured by the UCI campus categorized under the UC IS-3 policy as Protection Levels 3 and 4 (P3/P4).

The following were excluded from the scope of this review:

- PalCard purchases of software/IT Services

- IT related purchases that are below P3/P4.
- IT purchases made by UCI Health Procurement.

IV. CONCLUSION

IAS concluded that controls were implemented to mitigate specific risks, as outlined in the "Control Strengths" section below. However, please see observation details under the Observation and Management Action Plan section that follows.

Control Strengths

- Signed agreements along with the required Data Security Appendix (Appendix-DS) and completed Information Technology Purchase Agreements, when required, were attached to the PO in KFS.

- Staff training provided for the procurement of software and IT services is deemed adequate. UCI's Procurement Services, OIT Security Operations and other units collaborate to provide regular training to campus staff responsible for procuring IT contracts. Recorded trainings are available on-demand at the Procurement website.

- IT contract vetting policies and procedures are clearly documented to ensure the mitigation of certain risks, such as those related to systems and data security, privacy, financial loss, regulations, and other considerations.

- Roles and responsibilities of various departments involved in the vetting process are clearly documented in the procedures for the purchase of software and IT services.

V. OBSERVATION AND MANAGEMENT ACTION PLAN

1. Vendor Certificates of Insurance (COI)

Background

Procurement management indicated that when Certificates of Insurance (COIs) are received from vendors, they are uploaded into ITS, the systemwide repository for COIs. To assess compliance with current insurance requirements set by Risk Services, a sample of 21 IT contracts classified as P3/P4 was selected for review within ITS.

Observation

a. Widespread Non-Compliance of Insurance Requirements

Statistics provided by the ITS system revealed a critical level of non-compliance with UCI's insurance requirements:

- 99% (1,796 out of 1,807) of insured vendors are flagged as non-compliant.
    - This indicates that the vast majority of vendors did not meet all aspects of UCI's insurance requirements.
- 99% (4,725 out of 4,784) of documented insurance policies have expired.
    - This indicates a critical lapse in maintaining current and valid insurance coverage across vendors.
- 97% (5,641 out of 5,797) of recorded insurance policies are flagged as non-compliant.
    - This reflects the fact that vendors are required to maintain multiple types of insurance coverage (e.g., General Liability, Worker's Compensation, Automobile Liability, etc.), and the data indicates that most vendors are deficient in at least one required insurance type, suggesting a significant gap in compliance across various coverage categories.

The above issues highlight a significant risk in terms of ongoing protection and compliance with UCI's insurance standards, potentially exposing the university to various liabilities.

Risk Services has acknowledged the widespread issue of non-compliance with UCI's insurance requirements. The department attributes this high rate of non-compliance to a significant resource constraint. Specifically, they cite insufficient manpower to effectively manage and update the numerous COIs that regularly expire. This staffing limitation has resulted in an inability to keep pace with the continuous influx of expiring insurance documents, contributing to the high percentage of outdated and non-compliant policies in the system.

Risk Services has also acknowledged that they only see contracts and COIs when they are engaged by Procurement, resulting in visibility of only a small percentage of COIs.

Note: Despite the issues detailed in the following observation regarding data reliability and completeness in ITS, Risk Services stated that the above statistics are still accurate due to the resource and visibility constraints previously noted.

Observation

b. ITS Reliability and Data Completeness Issues

Risk Services has identified, and brought to IAS attention, potential inaccuracies and incomplete data within ITS, raising significant concerns about the reliability of vendor insurance information.

- A small-scale test conducted by Risk Services and Procurement revealed that some vendor COIs, uploaded over a month prior, was not found in the system.
- In a separate test conducted by Internal Audit, only 1 out of 21 sampled vendors had a Certificate of Insurance (COI) found in ITS, indicating a gap in documentation and data completeness.
- These discrepancies suggest possible glitches, processing errors, or significant gaps in data entry in ITS, affecting the timely integration and completeness of COI information.
- There is a high risk of misjudging vendor insurance compliance based on incomplete, outdated, or missing information in ITS.

This reliability issue compounds the non-compliance problem noted in Observation 1.a above and severely undermines the effectiveness of the ITS as a tool for managing vendor insurance compliance.

Recommendations:

- System Upgrade:
  - Invest in upgrading or replacing the ITS to ensure real-time or near-real-time updates of COI information.
  - Implement automated notifications for upcoming COI expirations to both vendors and university staff.
- Process Automation:
  - Develop an automated system for initial COI compliance checks to reduce manual workload.
  - Implement a user-friendly portal for vendors to submit and update their COIs directly.
- Staffing and Resources:
  - Conduct a workload analysis for the Risk Services department to determine appropriate staffing levels.

  - Consider temporary staffing or reallocation of resources to address the backlog of expired COIs.

- Vendor Management:
  - Implement a tiered approach to vendor management, prioritizing high-risk or critical vendors for more frequent COI updates.

  - Develop a clear communication strategy to inform vendors of their compliance responsibilities and the consequences of non-compliance.

- Policy Review:
  - Review and potentially simplify the university's insurance requirements for vendors where appropriate, without compromising necessary protections.

  - Establish a regular review cycle for insurance requirements to ensure they remain relevant and manageable.

- Training and Education:
  - Provide training to relevant university staff on any system updates and related policies.

  - Develop educational materials for vendors to help them understand and meet the university's insurance requirements.

- Compliance Monitoring:
  - Implement a regular audit process to verify the accuracy of the ITS and identify systemic issues.

  - Establish key performance indicators (KPIs) for COI compliance and regularly report on progress to university leadership.

Management Action Plan

UCI Campus Risk Services (herein after "Risk") is currently coordinating with UCOP and our system partners on the modernization of BUS63 (Insurance Requirements & Certifications) as well as appropriate next steps as UCOP terminates the long-term relationship with ITS.

In light of the observations outlined in the present IT Contract Approval Processes Internal Audit 2025 Report, Risk has developed a comprehensive recommended solution addressing these oversight gaps through both immediate and long-term strategic initiatives.

Short-Term Implementation Strategy (2 to 10 weeks)

The OIT Security Review Process is currently mandatory for all P3 and P4 software purchases and includes security, privacy, and procurement assessments. While this existing process asks about contractors' cyber security insurance coverage, it does not require mandatory Certificate of Insurance (COI) submission. The proposed enhancement would make COI collection mandatory within this established framework and establish secure storage protocols in the ServiceNow system.

Due Date: September 30, 2025

Long-Term Strategic Implementation

UCI is currently configuring a new Requisition Management system with advanced workflow capabilities. All P3/P4 software purchases will be required to undergo mandatory (and simultaneous) Security, Privacy, and Accessibility reviews. Once complete, Risk's approval with a valid Certificate of Insurance (COI) is required before procurement can proceed.

Any contract renewal, which naturally triggers new time periods and provisions, would be processed in the same fashion as any other contract, requiring necessary approvals at each step of the forthcoming Requisition Manager System.

Due date: April 1, 2026

Non-compliant COIs

Risk Services agrees with this audit's findings of widespread non-compliance with UC's insurance requirements due to significant resource constraints and limited visibility into vendor insurance documentation. To address this issue within current operational limitations, Risk Services will implement a three-pronged strategic approach that balances risk management with available resources.

First, Risk Services will not pursue retroactive reviews of any currently expired or non-compliant COIs. The administrative costs and resource requirements to update historical COIs exceed the risk mitigation benefits, particularly given current staffing limitations. This decision allows for reallocation of limited resources toward more effective prospective risk management activities.

Second, Risk Services will, in a fashion consistent with the unpublished UCOP updates of BUS-63, prioritize obtaining up to date COIs for all future contracts involving high-risk vendors

Third, for vendors deemed lower-risk or whose contracts are approaching renewal, Risk will formally accept the risk associated with non-compliant and/or absent COIs and will not pursue retroactive compliance. This risk acceptance

acknowledges potential insurance coverage gaps and possible financial exposure during non-compliant periods. However, this approach is justified because lower-risk activities present minimal potential for significant financial loss, and the administrative costs of comprehensive compliance exceed the potential risk exposure. This approach is consistent with Risk's understanding of committee recommendations to BUS-63.

Risk Mitigation and Controls

To mitigate the accepted risks, Risk will implement several protective measures. Contract language will be strengthened with enhanced indemnification and hold-harmless provisions. All vendors will receive clear communication regarding their insurance obligations and Risk's expectations. COI collection will become mandatory for all high-risk contract renewals and recommended as part of the contracting process for low and medium risk contracts, maintaining the policy requirement that all vendors produce proof of coverage.

Due Date: April 1, 2026

2. IT Contract Vetting and Approvals

Background

To evaluate compliance with procurement policies and procedures related to the acquisition of software and IT services, IAS selected a judgmental sample of 21 IT contracts. These were drawn from a KFS PO report and the campus Protected Data and Systems Inventory (PDSI). The sample included the top 10 contracts by dollar value from the PO report, along with 11 contracts where the vendor was clearly identified in the PDSI system. All selected contracts involved systems and/or data classified as P3 or P4. For each contract, IAS reviewed the associated purchase requisition and PO documentation in KFS to verify the presence of the following supporting documents, as outlined in the Procurement Office's procedures for Buying Software/IT Services:

- Signed Agreement
- Supplier Review Questionnaire
- Risk Assessment or OIT conclusion that no further review is needed
- Appendix-DS or acceptable data security reference
- Certificates of Insurance, if required
- Completed Information Technology Purchase Agreement, if required

Observation

a. IT Security Review and Documentation

For one major vendor providing a campus-wide subscription service, no IT security review was conducted prior to the vendor's approval and engagement.

According to Procurement management, the PO was submitted retroactively—after the contract term had already begun on July 1—and was approved solely for payment purposes at the end of September. Internal Audit Services (IAS) was provided with an email confirming that the contract manager had been informed that no security review had taken place.

Per UC IS-3 policy, Section 15.2.1, "Units using suppliers must ensure review and adjustment of applicable security requirements upon agreement renewal, taking into account changes to institutional information, IT resources, policy, and laws and regulations."

OIT Security indicated that the contract was nearly a decade old, the product is utilized across all UC locations, and there was no viable alternative at the time. As a result, an exception to the security review requirement was made. However, this exception was not formally documented as required by UC IS-3, which states, "Exception requests and decisions must be documented, periodically reviewed based on risk and retained by the CISO as required by the UC Records Retention Schedule."

- Engaging a vendor without a prior security review increases the risk of data breaches, unauthorized access, or non-compliance with institutional data protection standards.

- Bypassing established IT and procurement controls undermines governance and may set a precedent for future non-compliance.

- Retroactive approvals limit the organization's ability to assess and mitigate risks before services are rendered, potentially leading to service disruptions or reputational damage.

Recommendations

- Ensure that all vendor engagements, including renewals, undergo a formal IT security review prior to approval, in alignment with UC IS-3 and UCI ISS requirements.

- Require that any exceptions to security review policies be formally documented, including justification, risk assessment, and approval by the appropriate authority.

- Implement controls to prevent retroactive PO approvals for IT-related services, ensuring that all necessary reviews are completed before contract execution.

- Provide targeted training to contract managers and procurement staff on IS-3 and ISS requirements, including the proper handling of exceptions and the importance of timely documentation.

Management Action Plan

OIT management will ensure that a supplier security review and/or exception is documented for the one vendor contract noted as missing documentation. OIT will also work with Procurement to remind relevant stakeholders of the need for proper documentation in the supplier review and exception processes.

Due date: Completed (OIT management completed this Management Action Plan prior to this report being finalized.)

Regarding the specific PO related to this observation, that PO has been closed. Central Procurement (CP) has uploaded the completed data security and privacy report prepared by OIT to the new PO issued for the renewal term with the same supplier.

Going forward, when CP receives a PO for an IT or software purchase that is either for an existing product/service or submitted after the fact—and lacks the required data security and privacy review documentation—CP will:

1. Confirm with the department whether the Supplier Security review was completed and approved by the Data Security and Privacy Office.

2. If approved, the department must provide the documentation so CP can upload it to the PO and proceed in accordance with policy.

3. If not completed, the PO will be disapproved. The department will be instructed to complete the Supplier Security review and resubmit the requisition with all necessary approvals attached.

Due date: Completed (Procurement management completed this Management Action Plan prior to this report being finalized.)

Observation

b. Attachment of Backup Documents

For 6 (29%) of 21 POs reviewed, the required Supplier Review Questionnaire and either a risk assessment document or a documented conclusion that no special security terms are necessary were not attached to the requisition in KFS. These documents are required, under the Procurement Office's procedures for "Buying Software/IT Services", to be attached to the requisition.

It was confirmed, however, that the security reviews were conducted in these cases. This issue relates solely to the absence of supporting documentation in the system of record.

While the actual security risk is low due to the reviews being completed, the lack of documentation:

- Reduces transparency and auditability, making it difficult to verify compliance during future reviews.
- Undermines procedural consistency, which could lead to oversights in higher-risk scenarios.
- Limits institutional memory, especially when staff turnover occurs or when documentation is needed for reference.

Recommendations

- Procurement and the requisitioning staff should be reminded to upload all required documentation into KFS, even when the security review has been completed outside the system.
- Explore whether KFS can be configured to require these attachments before submission or approval of IT-related requisitions.
- Periodic spot checks or automated validations could help ensure continued compliance with documentation requirements.

Management Action Plan

Short-Term Implementation Strategy

The Central Procurement office will remind its staff members that for any software/IT purchases requiring data security and privacy review, documentation must be attached or uploaded to the requisition or the PO before approving it. This will also be reiterated in a future CP newsletter and departmental buyers training session.

Due date: November 30, 2025

Long-Term Implementation Strategy

At present KFS lacks the functionality to require uploading of any documentation in support of a purchase. When the new Requisition Manager System is implemented in Q1 2026, the workflow will have the capability to route software/IT purchases to the OIT Data Security office for their review and approval, and it will require the appropriate documents to be uploaded prior to the requisition coming to CP for their review and approval.

Due date: March 31, 2026