UCDAVIS
OFFICE OF THE VICE CHANCELLOR
AND CHIEF FINANCIAL OFFICER
Accounting and Financial Services

Financial System Integration Recommendations

This document is a supplement to the Financial System Integration Guidance document and includes recommendations for each control area.

Internal Controls Recommendations

1. Separation of Duties

Separation of Duties Implementation Recommendation

☐ The system should ensure that there is appropriate separation of duties and approvals for all transactions which will post to the Financial System General Ledger.

We recommend that the system enforce separation of duties and there is a separate initiator and approver for each transaction. If reviews are by batch and not transaction, it is recommended that the reviewer not have access to make modifications to transactions.

☐ The transaction initiator and approver cannot be the same person.

We recommend the system prevent the initiator from approving their own transactions.

2. Accountability, authorization, and approval

Accountability, Authorization, and Approval Implementation Recommendations

☐ System should ensure that terminated and transferred users are removed from the application in a timely manner.

It is recommended that the department documents their onboarding and offboarding process to include user access. At a minimum user access should be reviewed annually and when someone leaves the department. The review should be documented and evidence of the review should be maintained.

☐ Access to system should be approved by respective managers to ensure that new access is commensurate with their roles and responsibilities.

We recommend that you document who has the authority to approve user access. This individual should have sufficient knowledge to understand the different roles within the organization and the system.

☐ Management should perform a periodic review of application access to provide reasonable assurance that user access is commensurate with existing roles and responsibilities.

We recommend at a minimum there be an annual review of users. We also recommend privileged users/super users be reviewed quarterly. The review should be documented and evidence of the review should be maintained. Changes to users should be processed timely.

3. Security of assets

Security of Assets Implementation Recommendations

☐ IT management should perform a periodic review of users with any ability to make changes to batch schedules.

We recommend management take a risk-based approach and perform a periodic access review (at least annually) over users with access financially significant batch jobs to ensure access remains commensurate with job roles and responsibilities. To evidence this review, management should retain documentation indicating the review occurred and any changes to user access as a result of review were processed completely and accurately.

☐ IT Management should monitor financially significant jobs for success/errors to ensure that jobs are completed accurately and without exceptions. Failed jobs should be logged and documented with follow-up.

We recommend that management first define and identify financially significant batch jobs and then implement a defined and documented process to monitor and resolve those failures in a timely manner. Jobs logs should be retained and resolution of issues should be documented to completion.

☐ IT management should perform a periodic review (at least annually) of IT professionals at the database and server layer, to ensure access remains commensurate with job role and responsibility.

We recommend that IT management take a risk-based approach and perform a periodic access review (at least annually) over privileged IT accounts on the operating system and database level, to ensure only appropriate personnel hold such authority in the system.To evidence this review, management should retain documentation indicating the review occurred and any changes to user access as a result of review were processed completely and accurately. We recommend that in addition to Management's review of privileged user access to the operating system and database, Management should perform monitoring procedures over “root” and database "system" account activity or equivalent whether by impersonation or equivalent administrative grants.

☐ Program development policies, procedures and controls should be in place to ensure that systems are developed, configured and implemented to achieve management’s application control objectives.

We recommend that IT Management document, define, review and regularly communicate the program development policies to provide reasonable assurance that management of program development is controlled and communicated to staff responsible for maintaining systems which generate financial transactions.

☐ Management should capture system change requests via a formal change management process. All changes should capture testing, documentation and approval prior to production release.

We recommend that IT management follow the formal change management process and maintain evidence of the documented request, approval, and testing, for all changes prior to deployment into production.

We recommend that IT management capture and formally documente business end-user involvement and results of user acceptance testing (UAT) to evidence that all changes are sufficiently tested prior to being deployed to the production environment.

☐ IT management should provide segregation between the abilities to develop and deploy production changes. Staff with both functions should be monitored, documented, logged and reviewed by management to ensure that unauthorized changes to application or datasets are not made.

We recommend that IT management segregate the abilities to develop and to migrate changes. Any users with the ability to perform both functions should be monitored as it introduces an additional risk to your IT environment.

We recommend that users with the ability to migrate changes to production should not have access to develop changes. If developers retain access to promote changes into production, we recommend that IT management logs activities performed by developers (with the ability to migrate changes into the production environment). This activity should be periodically reviewed and documented by an independent individual to ensure that unauthorized changes to the datasets or data are not made.

We recommend that IT management logs activities performed by staff with access to the production environment. This activity should be periodically reviewed and documented by an independent individual to ensure that unauthorized changes to the datasets or data are not made.

☐ IT roles and responsibilities for managing financial systems should be defined, reviewed periodically and communicated.

We recommend that IT management define, review and communicate IT organization roles and responsibilities for staff that maintain systems which generate financial transactions.

☐ IT management should track and respond to incidents to ensure appropriate resolution of possible control issues, such as security breaches or data corruption.

We recommend that IT management provide oversight to ensure that program maintenance and program development activities are controlled and traceable so that senior management may be informed of key IT matters. Failure to track IT issues increases the risk of events that may impact the final reporting process not being brought to management attention.

4. Review and reconciliation

Review and Reconciliation Recommendations

☐ No employee payments can be processed through a feed.

This is only applicable to authorized payment integrations. Only Vendor Payments using the valid KFS Vendor information are allowed to be feed into KFS.

☐ There must be a reconciliation process between the transactions in the source system and the postings in the General Ledger.

We recommend defining and mapping out the reconciliation process as soon as possible. The process may include generating reports out of the sub-system in comparison to Decision Support or an automated method developed by the department.

We recommend the reconciliation process to be completed by the appropriate fiscal staff and a review of the reconciliation results are performed and documented by staff not initiating and approving transactions in the sub-system.

☐ Ensure sales and use tax for applicable transactions are properly calculated and submitted, if applicable.

We recommend that you consult with A&FS Tax Reporting & Compliance for any tax questions or concerns.

☐ Department is responsible for posting correcting entries to the general ledger in a timely manner (i.e. clearing “default” account).

We recommend that clearing accounts be reconciled monthly and corrected entries are posted in a timely manner.

☐ Ensure transactions and processing are in compliance with UC Davis Policy and Procedure Manual Chapters 310, 320, 330, 340 and other applicable policies.

We recommend you review each of the sections and become familiar on how it applies to your systems.

☐ Ensure transactions are in compliance state and federal regulations.

We recommend that you are familiar with restrictions to state and federal funds that applicable to your activity.

Self-supporting funds recharging internal customers should be in compliance with campus rate development policies. All self-supporting activities including new rates must be reviewed annually to ensure compliance with campus Surplus/Deficit Policy. All rates must be approved by your dean or vice-chancellor's office. Additional reviews may be necessary depending on the rate and impact to campus.