Financial System Integration Guidance

This document is intended to provide a guide for departments requesting to integrate their sub-systems with Kuali Financial Systems (KFS). Within the guide are best practices and implementation checklists on establishing appropriate internal controls within your sub-systems. Requested document for each control area is also indicated which will be used to evaluate your request and processes. Recommendations for each control area are available in a separate document. Please be aware that your department is responsible for the security or your own systems and the integrity of data stored in all systems outside of KFS.

Internal Controls

Below is a list of internal controls that should be implemented with any Information System. Along with those controls it is essential that your department establishes an ethical work environment. Setting the tone at the top of the organization is the most important element of accountability and the control environment. By implementing appropriate internal controls your department provides reasonable assurance that:

- Operations are effective and efficient
- Financial and operational reports are reliable.
- Compliance with applicable laws, regulations, and internal policies and procedures have been achieved.

1. Separation of Duties

When your department is maintaining their own sub-systems it is essential that you maintain adequate separation of duties within that system.

- Best practice is to have different people:
    - Authorize access to sub-system to appropriate users
    - Enter users into the sub-system after authorization is granted
    - Review users of the sub-system when someone leaves the department or at least annually
    - Initiate entries in sub-system
    - Approve entries in sub-system
    - Review and reconcile data in sub-system at least monthly
    - Review and reconcile data from sub-system to the Kuali Financial System at least monthly
- Potential consequences if duties are not separated:
    - Erroneous or fraudulent entries are fed into the Kuali Financial System
    - Entries are not properly fed and recorded in the Kuali Financial System
    - Unauthorized payments/reimbursements are made

- Unauthorized individuals could have access to sensitive data

Separation of Duties Implementation

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

Documentation Requested (Process Flows and/or detailed description)

☐ How are orders (or transactions, etc) entered in the system? By who?
☐ Are there approvals for services/orders/etc outside the system or inside the system?
☐ What are the department interactions/expectations?

2. Accountability, authorization, and approval

When proper accountability exists, you know who has access to electronic and personal information, for what business purpose they have access, what information systems and data are authorized for use, and where sensitive, private information resides.

- Best practices:
  - Limit business system and data access to appropriate users.
  - Adhere to security and privacy policies for e-mail, web browsing, and electronic communication.
  - Determine approval hierarchies and appoint a departmental security administrator (DSA).
  - Implement security measures to protect access to electronic resources and private information according PPM 310-24.
  - Communicate and coordinate access and security with IET.
  - Train employees in computer access, security, software, and appropriate use of University information.
  - Address reported or suspected access and security violations according to IET guidelines.
- Potential consequences if accountability does not exist:
  - Misuse of information
  - Identity theft
  - Improper use of university assets
  - Damage to public image
  - Legal actions

Accountability, Authorization, and Approval Implementation

☐ System should ensure that terminated and transferred users are removed from the application in a timely manner.
☐ Access to system should be approved by respective managers to ensure that new access is commensurate with their roles and responsibilities.
☐ Management should perform a periodic review of application access to provide reasonable assurance that user access is commensurate with existing roles and responsibilities.

Documentation Requested (Process Flows and/or detailed description)

☐ How are users added to the system? Manually added or through a roles management system, etc?
☐ What roles are in the system? What functions can each role perform in the system?
☐ What is the approval process for adding users to the system?
☐ How do users log into the system (e.g., CAS Authentication)?
☐ How will employee separations and transfers be managed (e.g., manually or automated)?

3. Security of assets

UCD's electronic information is a valuable asset. Security controls prevent and reduce the risk of harm caused by error, accident, natural disasters, or malicious action. Avoid duplication of information if it's available elsewhere. Store information in a secure location.

- Best practices:
  - Use and share data for business purposes only.
  - Design, document, and test internal processes to ensure security and data integrity.
  - Secure personal information in a locked or password protected location.
  - Regulate authorized access to resources through security measures such as user IDs and passwords.
  - Implement auditable authorization processes that adhere to University policies.
  - Train all users in security awareness.
  - Inform your DSA and system/data custodians about access rules and security violations.
  - Restrict access of information and systems to people who need the access to perform their jobs.
  - Periodically review information stored in electronic or paper format.
  - Secure or discard personal and private information properly.
- Potential consequences if electronic information is not secured:

- Identity theft
- Damage to public image
- Misuse of University resources and information

Security of Assets Implementation

☐ IT management should perform a periodic review of users with any ability to make changes to batch schedules.
☐ 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.
☐ 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.
☐ 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.
☐ Management should capture system change requests via a formal change management process. All changes should capture testing, documentation and approval prior to production release.
☐ 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.
☐ IT roles and responsibilities for managing financial systems should be defined, reviewed periodically and communicated.
☐ IT management should track and respond to incidents to ensure appropriate resolution of possible control issues, such as security breaches or data corruption.

Documentation Requested (Process Flows and/or detailed description)

☐ What is the change management process (e.g., software development methodology, configuration management system used and build/deployment process)?
☐ How are approvals for requirements, acceptance testing and production approval captured for code changes?
☐ Provide a list of IT personnel and their roles; including access levels to systems (e.g., database, application server).

4. Review and reconciliation

Your reconciliation activities confirm that transactions are recorded correctly, can be readily retrieved, and are safeguarded from improper alteration.

- Best practices:
  - Ensure data integrity by validating data with the Data Warehouse or Decision Support.
  - Follow retention schedules and data retention requirements.
  - Periodically review information stored in electronic or paper format.
- Potential consequences if review and reconciliation activities are not performed:
  - Errors, discrepancies, or irregularities undetected
  - Inaccurate, incomplete official records
  - Improper access to business systems and data

Review and Reconciliation Implementation

☐ No employee payments can be processed through a feed.
☐ There must be a reconciliation process between the transactions in the source system and the postings in the General Ledger.
☐ Ensure sales and use tax for applicable transactions are properly calculated and submitted, if applicable.
☐ Department is responsible for posting correcting entries to the general ledger in a timely manner (i.e. clearing "default" account).
☐ Ensure transactions and processing are in compliance with UC Davis Policy and Procedure Manual Chapters 310, 320, 330, 340 and other applicable policies.
☐ Ensure transactions are in compliance state and federal regulations.

Documentation Requested (Process Flows and/or detailed description)

☐ What types of transactions does the system allow (budget, receivables, recharges, payables, etc)?
☐ List of KFS Accounts that will be used.
If accounts are not specifically known then what types of accounts will be used (Income, expense, etc)
☐ What types of fund sources (Federal? Other contracts and grants? General Funds? Etc) will be used?
☐ List of Financial Object Codes used for each transaction type?
If financial object codes are not known then please provide additional detail on how the system will generate transactions per type.
☐ How are transactions processed for each transaction type?

☐ How does the system or your process ensure that there is a separate initiator and approver for each transaction? Describe the separation of duties process.

☐ How are reconciliations handled between system and the Financial System? Describe the reconciliation process.
☐ How are defaulted transactions reconciled? For example, what is the process to correct a transaction that was rejected by KFS and the default chart, account number and object code are posted to the General Ledger.
☐ Who performs the reconciliations?
☐ Who reviews the reconciliations?
☐ How are customer financial transaction inquires/incidents tracked?
☐ Who responds to customer financial transaction inquires/incidents?

References

- Internal Controls: http://afs.ucdavis.edu/our_services/controls-e-accountability/internal-controls/int-cont-practices/index.html
- Information Systems Internal Controls: http://afs.ucdavis.edu/our_services/controls-e-accountability/internal-controls/int-cont-practices/int-cont-information-systems.html
- SAS 115 Overview: http://afs.ucdavis.edu/our_services/controls-e-accountability/internal-controls/sas115-overview/index.html
- Department Key Controls: http://afs.ucdavis.edu/our_services/controls-e-accountability/internal-controls/sas115-overview/key-controls.html