



Kansas State University

Internal Control Guidance

Key Guidelines

Purpose	1
Benefits of Effective Internal Control	1
Consequences of a Lack of Internal Control	1-2
Concepts of Internal Control	2
Risk Assessment	2
Information Technology (IT) Controls	3
Information and Communication	3
Reporting Fraud and Misconduct	4
Monitoring	4-5
Control Activities	4
Physical Controls	5
Transaction Authorization	5
Separation of Duties	5
Expenditures	5
Inventory	6
Personnel and Payroll	6
Receipts	6
Supervision	6
Accounting Records	6
Access Controls	6
Independent Verification	6
Additional Information and Source	7

Purpose

The internal control guidelines seek to:

- Provide practical tools for those charged with responsibility to process transactions.
- Maintain custody of resources.
- Communicate established policies and procedures.
- Convey the definition of internal control.

Benefits of Effective Internal Control

One of the most misunderstood roles of internal control is the belief that it exists solely to prevent or reduce fraud. In reality, the purpose of internal control is much more broad. Benefits include:

- Reliable reporting to support management decisions.
- Consistent, efficient methods to process transactions.
- Compliance with university, state and federal regulations.

Effective controls also can reduce instances of noncompliance and negative publicity with grant rules and legislative dictates. These controls ensure continued good relations with students, legislators, the Kansas Board of Regents, grantors, donors and Kansas taxpayers. Effective internal control does more than simply satisfy auditors or central administration. It allows for effective, efficient operations by providing reliable information and compliance with regulations that protect future funding.

Consequences of a Lack of Internal Control

To illustrate the need for controls in a variety of risk areas, we have included the following excerpts from the Auburn University Office of Audit, Compliance and Privacy newsletter. The names of individuals, states and institutions have been omitted, and none are from the state of Kansas.

- 2010

University administrators allegedly signed a certificate of compliance with the terms of a \$2.5 million cooperative agreement while not fully adhering to its terms, a violation of the False Claims Act. The university's Board of Regents paid a \$500,000 settlement.
- 2011

A county jury awarded nearly \$418,000 to a former college administrator who sued the school for firing her in retaliation for cooperating with a federal investigation that found financial aid violations.
- 2013

A forensic audit report outlined a university's alleged fraud, waste and abuse, raising serious questions about university governance. Concerns were raised about a board member's family and friends receiving work or money through school contracts. The audit was turned over to authorities for possible criminal prosecution.

Two employees were fired after an investigation revealed \$500,000 was embezzled from the school. One employee was fired after admitting to the crime, and the college's director of finance also was terminated.
- 2014

A university paid nearly \$500,000 to settle federal allegations that the university received research money from two agencies for the same projects by submitting "false and misleading statements" in grant applications.

A university violated Title IX when it failed to provide a "prompt and equitable response" to the alleged sexual assault of a male student by another male student. The university also is accused of failing to protect the victim from further harassment following the assault, causing him to drop out.

2015

A former university scientist admitted in court that he faked results in a multimillion-dollar AIDS vaccine study. As part of his plea agreement, he admitted that his subterfuge cost the federal government up to \$20 million. In return for two guilty pleas, prosecutors dropped two other charges. He could face up to 10 years in prison.

A university gave the Princeton Review false information designed to inflate the rankings of its business school, according to an outside audit.

A former university contract instructor faces a felony ethics charge after he allegedly made more than \$375,000 by encouraging students to buy textbooks from a company he owned, according to a grand jury indictment.

2016

A university reported a massive systems data breach that affected up to 130,000 people. The intruder installed file sharing software on network machines that enabled the sensitive information, including names and social security numbers, to be filched from the network.

Concepts of Internal Control

It is critical that one understands that management is responsible for the design and implementation of internal control. One of internal audit’s roles is to assess the effectiveness of controls implemented by department heads, deans, directors, vice presidents and the president. By definition, internal control is a process influenced by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance. In general terms, internal controls are simply good business practices. The objectives of internal control can be summarized as follows:

- 1. Reliability, integrity and timeliness of information.
- 2. Compliance with policies, procedures, plans, laws, regulations and contracts.
- 3. Safeguarding of assets, including people.
- 4. Effective, economical and efficient use of resources.
- 5. Accomplishment of established objectives and goals.

Control Environment

Control environment serves as a foundation for other internal control components within one’s sphere of influence, which is essentially the tone established at the top — be it the university as a whole or a division, college, department or functional area within the department. Without a strong control environment, failure to achieve organizational objectives is the likely result. Examples of the control environment include:

- Integrity and ethical values of management.
- Code of conduct.
- Structure of the university.
- Management’s philosophy and operating style.
- Procedures for delegating responsibility and authority.
- Management’s methods for assessing performance.
- Written policies and procedures provided to all staff, and expectations for compliance communicated.
- No tolerance for fraud or conflicts of interests.
- Exceptions/errors used as opportunities to teach compliant processes.
- Disciplinary action consistently applied to all employees.
- Management fully supporting and embracing a culture of compliance with organization policies and procedures.
- Clear communication, as well as accuracy, highly encouraged.
- Performance of an annual risk assessment.

Risk Assessment

Risk assessment is a process that seeks to identify, analyze and manage risks. The purpose is to identify obstacles that could prevent the department/unit from achieving goals and objectives, and to put controls in place to minimize the impact of negative events. Some examples of risks follow.

Public Relations

- Public scandal.
- Loss of reputation.
- Lack of institutional compliance with rules and regulations.
- Decline of university relations with alumni, donors and legislators.

Financial

- Falsification of contracts, reports or records.
- Improper giving or receiving of gifts.
- Improper supplier or contractor activity.
- Theft or embezzlement.
- Waste, abuse or misuse of assets.

Research

- Conflict of interest concerns.
- Data privacy.
- Intellectual property infringement, misappropriation or disclosure.
- Inappropriate use of hazardous materials, humans or animals in research.
- Falsification of research results.

Human Capital

- Discrimination or harassment.
- EEOC or ADA matters.
- Employee misconduct.
- Offensive or inappropriate communication.
- Threatening or inappropriate supervisor directive.
- Injury or loss of life

Athletic

- Activities to influence the outcome of sports activities.
- Giving, receiving or soliciting items, services or money that could be reasonably interpreted as an effort to influence a recruiting decision or a recruit’s family or friends.
- Interaction of consultants with student-athletes on or off the field.
- Scholarship/financial aid misconduct.
- Unwanted and offensive sexual advances, remarks or acts by associates or superiors.

Information Technology (IT) Controls

- Systems should be fully documented, including operations, program and user documentation.
- New systems should be developed or acquired using a structured and tested development approach.
- All computer program changes should be properly authorized and documented.
- Audit trails and edit routines should be built into systems to ensure effective processing.
- Password and physical security should be in place for programs, databases and data files.
- Equipment should be properly safeguarded against theft, power fluctuations and viruses.
- Backup and recovery processes should be in place to ensure continuity of operations.
- Backup media should be stored off-site, remote from the production files whenever possible.
- Employees should be properly trained and cross-trained to prevent an unduly high degree of reliance on one knowledgeable employee.
- Employees should receive appropriate information and training on managing and protecting confidentiality of passwords.

Information and Communication

Information and communication are the methods used to initiate, identify, analyze, classify and record the organization’s transactions and account for assets and liabilities. The information and communication system also must provide management with reports containing operational, financial and compliance information to monitor progress toward accomplishing established goals and objectives.

Examples of information and communication systems include:

- The organization's written policies and procedures.
- The unit's goals and objectives.
- Organization charts.
- Position descriptions.
- Performance evaluations.
- Training programs.
- Periodic reports measuring progress toward the accomplishment of goals and objectives.

Reporting Fraud and Misconduct PPM 3230

University PPM 3230 k-state.edu/policies/ppm/3200/3230.html addresses the responsibility to report fraud and misconduct.

PPM 3230.050 notes, “Anyone with reasonable basis for believing fraudulent or related misconduct has occurred is to report such incidents to the Internal Audit Office and the University Police. Any individual suspected of fraud or related misconduct is not to be confronted. University employees are not to initiate investigations on their own because such actions can compromise any ensuing investigations.”

PPM 3230.060 references the Kansas Whistleblower Act, which is listed in K.S.A. 75-2973. The Whistleblower Act indicates:

- (a) No supervisor or appointing authority of any state agency shall prohibit any employee of the agency from discussing the operation of the agency, either specifically or generally, with any member of the legislature.
- (b) No supervisor or appointing authority of any state agency shall:
 - 1. Prohibit any employee of the agency from reporting any violation of state or federal law or rules and regulations to any person, agency or organization; or
 - 2. Require any such employee to give notice to the supervisor or appointing authority prior to making any such report.

Monitoring

Monitoring helps document the effectiveness of existing control activities and identifies circumstances that may require changes to the internal control system. Monitoring should focus on high-risk areas where basic internal controls may be weak and require alternative measures. Examples of monitoring include:

- Spot-checking of transactions to ensure compliance with policies and procedure.
- Reviews of financial reports, such as comparisons of budgeted and actual revenues, and expenditures and comparisons of current and prior months’ or years’ activities.
- Reviews of departmental ledgers and related reconciliations to departmental accounting records.
- Reviews of outstanding encumbrances.
- Supervisory review.

Control Activities

These are the policies and procedures used to ensure follow-through of management’s directives to mitigate risks. Control activities are performed at all levels, and may be preventive, detective, corrective, directive or compensating in nature. The bulk of the concepts are focused on establishing control activities, such as separation of duties, so that one person cannot control all aspects of a transaction.

Levels of Control Activities

Preventive controls are built into internal control systems and are designed to keep errors or irregularities from occurring in the first place. Examples include separation of duties, transaction authorization, training, and periodic reminders of policies and procedures.

Detective controls are designed to detect errors and irregularities, which have already occurred and to assure their prompt correction. These controls also supply the means with which to correct data errors, modify controls or recover missing assets. Examples of detective controls include account reconciliations, management review of reconciliations, physical inventories and year-end expenditure trends.

Corrective controls are designed to manage the effects of errors or irregularities that have been detected. Examples of corrective controls include reconciling journal entries, error communication and reporting, systems documentation of processes and improvement initiatives.

Directive controls include the policies, procedures, laws and regulations established, as well as training seminars and meetings to instruct personnel on how to comply with new or existing policies and procedures. Examples include policies and procedures of the state of Kansas, Kansas State University and the Kansas Board of Regents.

Compensating controls are used to supplement controls that are either ineffective or cannot fully mitigate risk to an acceptable level. An example includes close supervision by the department head of all critical functions to compensate for a lack of separation of duties.

Physical Controls

These controls relate to the human activities employed in the accounting systems. These may be purely manual, such as the physical custody of assets, or they may involve physical use of computers to record transactions and update accounts. Within the control activities, there are six subcategories of physical controls:

- Transaction authorization.
- Separation of duties.
- Supervision.
- Accounting records.
- Access control.
- Independent verification.

Transaction Authorization

Authorization to initiate or approve transactions should be limited to specific personnel and by type of transactions or amount of transactions. Ensuring that all recorded transactions fairly represent accurate, legal and lawful events compliant with laws, rules and regulations is of paramount importance.

Accountability, for financial control purposes, is the delegation of authority to qualified persons in order to initiate, approve, process and review business transactions and the holding of those persons responsible for the validity, correctness and appropriateness of their actions. Managers are accountable for negative results attributable to their failure to maintain reasonable internal control activities. Departments should develop procedures to specify how to comply with university requirements and department expectations.

Separation of Duties

The overall concept of separation of duties ensures that one person cannot control all aspects of a transaction. Generally, an employee with physical access to an asset should not also be responsible for related accounting records. For any given transaction, the functions of authorizing, recording and maintaining custody — or ARC — should be performed by separate individuals in different sections of the department. Examples of assets include cash, ticket sales and passes, purchasing cards, supplies, equipment, books, and other goods or services.

These key responsibilities must be done by separate individuals:

- Authorization/approval of transactions.
- Recording transactions.
- Custody of an asset associated with the transaction.
- Reconciliation/review.

A separate person should perform reconciliations of transactions to supporting documentation and financial reports.

Expenditures

- The person responsible for initiating the purchase should not have access to order from the vendor or the responsibility to pay for the goods purchased.
- The person responsible for ordering merchandise should not be the requester, should not be responsible for returning merchandise, and should not have the responsibility to pay for the goods purchased.
- The person receiving goods should not have record-keeping functions (such as modifying the vendor master file or recording vendor invoices) nor the ability to modify the system.
- The person responsible for record-keeping functions in the system should not order or receive product, approve vendor invoices or reconcile the actual transaction to the budget.
- The person approving vendor invoices should not be involved in the purchasing process and should not be the one who initiated and authorized the purchase.

Inventory

- The person who initiates purchases, orders items, approves vendor invoices and pays vendors should not be the same person who is responsible for receiving.
- The person receiving delivery should not be the person paying the vendor or adjusting inventory records.
- The person with physical custody should not be able to adjust records, dispose or transfer property, or conduct the annual physical count.
- Adjustments, dispositions and transfers need to be separate from physical custody with supervisory oversight.
- Annual physical counts need to be separate from record-keeping or physical custody.

Personnel and Payroll

- No one employee should have total responsibility for modifications to the personnel file. One employee should initiate the change and a second should review and authorize the change.
- Hours worked should be reviewed and approved by the employee’s supervisor before being recorded or transmitted to the payroll department.
- A supervisory-level employee who is separate from the payroll processing and human resources functions should receive and review the payroll reports.

Receipts

- The person who receives cash should not be the same person who records payments, records/authorizes write-offs, adjustments to customer accounts or reconciles the bank account.
- Establish accountability immediately upon initial cash receipt. Maintain individual accountability at all times, and jointly verify and document two-person transfers.
- Mail should be opened in the presence of two people, documented and later compared to the deposit by an individual independent of the depositing, recording or custody process.
- The person responsible for recording information to customer accounts and preparing the bank reconciliations should not receive customer payments or prepare the deposits.
- The person responsible for reviewing and approving adjustments and reconciliations should not perform any other functions in the receipting process.

Supervision

This is the training, supervising and monitoring of the performance of employees to help certify that control processes function properly. Supervision is often a “compensating control” to supplement controls that are either ineffective or cannot fully mitigate a risk or group of risks by themselves to an acceptable level. Supervision is often used when separation of duties cannot otherwise be addressed.

Accounting Records

Accounting records should be retained and provide accurate documentation of transactions in a timely manner. Procedures for the error-handling process should be documented to ensure errors detected at any stage of processing receive prompt corrective action and are reported to the appropriate management.

Access Control

Access control includes limiting asset access by passwords or by lock and key to prevent unauthorized physical access. Access controls are meant to physically safeguard assets.

Independent Verification

Examples of independent verification include counting, recording and comparing physical assets periodically. Discrepancies should be reported to appropriate administrators and investigated. Reconciling accounting items should be resolved timely, and supervised if necessary.

Transactions should be:

- Appropriate to the university’s mission.
- Authorized with required signatures and dates.
- Valid and allowed by policy, law, contractual agreement and grant restrictions.
- Funded to pay for the goods or services.
- Accurately recorded and free from accounting coding or error.
- Supportable and consistent with supporting documentation, standard, situation or practice.
- Revenues are allowable in accordance with rules, regulations and fund source.
- Recorded timely with the date associated on the transaction.

Additional Information and Source

Much of the information contained in these concepts was obtained from the Committee of Sponsoring Organizations, or COSO, “Internal Control – Integrated Framework” from May 2013. The COSO report provides more details and can be obtained from the American Institute of Certified Public Accountants.

Expenditures and Travel
Segregation of Duties

A Authorization (Approval)
R Records Transactions
C Custody
RR Reconciliation/Review

Document/Key Control	Who initiates?	Who approves?	Who verifies?	Who reviews?
----------------------	----------------	---------------	---------------	--------------

Cash/Credit Purchases

Request for purchases (purchase requisition)	R				
Identifying supplier/Request competitive bid	R				
Ordering goods to be purchases	R				
Receiving delivery of goods purchased	C				
Checking quantity and quality of goods received	RR				
Storekeeping (securing items purchased, releasing on proper authorization, etc.)	C				
Dealing with goods to be returned	C				
Payment of purchased goods and services	R				
Applying for credit facility from supplier (if applicable)	R				
Recording accounts payable in shadow system	R				
Requesting adjustments	R				
Maintain records that ensure stock movements are recorded (if applicable)	R				
Checking periodical statements from suppliers	RR				
Approving vendor invoices	A				
Reconciliation of actual to budget for expenditures	RR				
Reimbursement request	R				
Creates positive pay file and tranfers to bank (Financial Services)	R				
Maintains check stock (Financial Services)	C				
Maintains signature stamp (financial services)	C				

Travel

Pretravel documents (out-of-state travel request, motor pool request, etc.)	R				
Travel arrangements (transportation, lodging, etc.)	R				
Travel advances	R				

Receipts
Segregation of Duties

A Authorization (Approval)
R Records Transactions
C Custody
RR Reconciliation/Review

Document/Key Control	Who initiates?	Who approves?	Who verifies?	Who reviews?
----------------------	----------------	---------------	---------------	--------------

Access to Cash/Checks/Credit Cards: Please list all who have access to cash in the notes section below.

Receives cash/deposits	C				
Opens mail containing checks	C				
Restrictively endorses checks immediately upon receipt	C				
Logo checks	R				
Processes refunds to customers	A				
Prepares bank deposit	R				
Takes deposits to Cashier's Office	C				
Investigates A/R discrepancies	RR				
Investigates discrepancies or issues — cash	RR				
Records deposit transaction into subsidiary ledger (Financial Services)	R				
Edits account receivable master file	R				
Processes customer service calls & complaints (see note below)	R				
Posts disbursements from subsidiary ledger to G/L.	R				
Reconciles bank statements (Financial Services)	RR				
Reviews accounts receivable aging trial balance	RR				
Reconciles deposits to amounts recorded in G/L.	RR				
Authorizes write-offs of delinquent accounts	A				
Authorizes accounts receivable adjustments	A				
Reviews cash reconciliations	RR				
Reviews G/L reconciliations	RR				
Approves bank reconciliations (Financial Services)	A				
Initiates wire transfers (Financial Services)	R				
Approves wire transfers (Financial Services)	A				

Receipts (continued)
Segregation of Duties

Document/Key Control		Who initiates?	Who approves?	Who verifies?	Who reviews?
Creates positive pay file and transfers to bank (Financial Services)	R				
Maintains check stock (Financial Services)	C				
Maintains signature stamp (Financial Services)	C				

Notes:

Inventory Segregation of Duties		A	Authorization (Approval)			
		R	Records Transactions			
		C	Custody			
		RR	Reconciliation/Review			
Document/Key Control		Who initiates?	Who approves?	Who verifies?	Who reviews?	
Request to purchase	R					
Ordering items	R					
Approving vendor invoices	A					
Paying vendors	A					
Receiving delivery of goods purchased	C					
Checking quantity and quality of goods received	RR					
Placing property tag on item	C					
Assigning property	R					
Recording item on university or departmental inventory	R					
Returns	C					
Physical custody	C					
Maintain records that ensure stock of inventory is accurate	R					
Adjusting inventory records	R					
Diposing of property	C					
Transferring property	C					

Notes:

Personnel and Payroll
Segregation of Duties

A Authorization (Approval)
R Records Transactions
C Custody
RR Reconciliation/Review

Document/Key Control		Who intiates?	Who approves?	Who verifies?	Who reviews?
Recommendations for appointment	A				
New student position	A				
Student appointment/referral for hiring	A				
One time pay authorizations	A				
Change of status/pay changes	R				
Time records	C				
Vacation and sick leave requests	R				
Payroll time entry	R				
Time record adjustments	R				
Resignations	A				
Exit checklist and procedures	C/RR				

Notes: