Arkansas State University

Internal Control Guidelines

COSO Internal Control Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a framework for internal controls in 1992; the Committee updated it in 2013. This framework serves as a guideline for designing, implementing, and conducting internal controls and assessing effectiveness of control. The five integrated components for internal control are:

- Control environment – the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.
- Risk assessment – a dynamic process for identifying and assessing risks that forms the basis for determining how risks will be managed.
- Control activities – actions established through policies and procedures to help ensure that management's directives to mitigate risks are carried out.
- Information and communication – information is necessary to carry out internal control responsibilities, and is generated from both internal and external sources. Communication is the continual process of providing, sharing, and obtaining this information.
- Monitoring activities – ongoing evaluations used to determine whether each of the components of internal control is functioning as expected.

Internal Controls – General Information

Internal controls are the methods and procedures used to provide reasonable assurance that these organizational goals will be met:

- Reliability and accuracy of information;
- Compliance with policies and procedures, as well as laws and regulations;
- Safeguarding of assets and University resources;
- Economical and efficient use of resources; and
- The accomplishment of established goals and objectives.

Internal control applies to people, operations, communication, and the overall work environment; it helps to set the tone for University operations.

The two primary types of internal controls are preventive controls and detective controls. Preventive controls are intended to deter instances of error or fraud, and require thorough processes and risk identification. Detective controls identify occurrences after the fact, and measure the effectiveness of preventive controls.

Preventive controls include, but are not limited to:

- Segregation of duties
- Standardized forms
- Physical control of assets
- Computer passwords

Detective controls include, but are not limited to:

- Performance and quality assurance reviews
- Reconciliations
- Cash counts
- Physical inventory counts

Responsibility for Internal Controls

Everyone in the University has some role in internal control. University leaders are ultimately responsible for the establishment and maintenance of a system of internal control and for establishing an ethical tone for overall operations. Deans, directors, and department administrators have oversight responsibility for internal controls within their units and should monitor the execution and function of control procedures. Each individual within a department should be aware of proper internal controls related to their specific job duties.

Basic Components of Internal Control

Segregation of Duties
Duties should be divided among different people to reduce the risk of error or inappropriate activity.

Organizational Structure
Lines of authority and responsibility should be clearly defined. An organizational chart is a good method for defining this structure. Another part of the structure includes rules that must be followed by employees. Written policies and procedures should provide guidance as well as a means for enforcement of rules.

Authorization and Approval
Transactions should be authorized and approved to help ensure the activity is consistent with departmental and institutional goals and objectives.

Reviews and Reconciliations
Performance reviews of specific functions or activities may focus on compliance, financial, or operational issues. Reconciliations compare recorded transactions or activity to another source, such as a bank statement or source documents.

Security
Security may be physical, electronic, or both. Equipment, inventories, cash, checks, and other assets should be secured physically and periodically counted and compared with amounts shown on control records. Physical inventory counts confirm the security of physical assets. Electronic controls such as passwords and virus detection software maintain the security of electronic systems and hardware.

Limitations of Internal Control

There are no perfect internal control systems. Staff size may limit the ability to segregate duties. All systems are limited by the potential for human error and misunderstanding. In addition, the cost of implementing a specific control should not exceed the expected benefit of the control. In some cases, realignment of duties may be sufficient to accomplish a control objective. In analyzing the associated costs and benefits of a particular control, the intangible consequences should also be considered; the impact to the University's reputation may be just as important as a potential financial loss.

Appendix
Internal Control Procedures

Accounting Records

- Banner is the official system of record for Arkansas State University.
- To ensure accuracy and completeness of accounting records, departmental personnel should reconcile revenues, expenses, and deposits shown in Banner to source documents such as requisitions, IDT's, and other documents.
- Any internal system records should be reconciled to the departmental records shown in Banner.

Payroll

- Payroll documents should be approved only by properly authorized University employees.
- An employee authorized to approve payroll documents should not be responsible for reviewing payroll expense reports or for distributing payroll checks.
- An employee should not approve documents which affect his or her pay; formal approval at a higher level is required.
- Time worked and absences are reported after the pay period ends. If reporting deadlines require the estimation of time, adequate control should be maintained to ensure that adjustments are made if the estimate varies from actual time worked.
- Checks awaiting distribution to employees should be kept in locked storage accessible only to a check custodian and a designated alternate.
- If checks are distributed to a designated departmental employee, any undistributed checks should be promptly returned to Payroll Services with an explanation for the unclaimed check.

Procurement and Travel

- Procedures reflected on the Operating Policies and Procedures website should be followed. See http://www.astate.edu/a/finance/procedures/index.dot for more information.
- Under optimal conditions, no employee should have complete control over more than one of the following:
    - Initiating purchase requisitions or travel authorizations/reimbursements
    - Approving purchase requisitions or travel authorizations/reimbursements
    - Verifying receipt of goods or services
    - Approving invoices for payment
    - Reconciling reports
    - Reasonable separation of the above should be established after considering the cost, benefits, and available staff.
- Purchase of goods or services for personal use is not allowed.

Cash Receipts

- Procedures reflected on the Operating Policies and Procedures website should be followed. See http://www.astate.edu/a/finance/procedures/index.dot for more information.
- When possible, a single employee should not have complete control over both 1) receipting and depositing cash and 2) reconciling cash receipts to deposits.
- Employees opening mail should not have cashiering responsibilities; when possible, it is preferred that two employees open mail.
- Cash receipts may not be deposited in unauthorized bank accounts.

- Payments should not be made from unrecorded cash receipts.
- Cash overages or shortages should be reported to the Treasurer's Office and recorded properly.

Billing and Accounts Receivable

- The University Treasurer's Office handles billing and collection for accounts receivable.
- Individual departments should not perform collection functions; all payments owed to the University should be coordinated as noted above.
- Any exceptions to the above must be noted and approved by the Treasurer's Office.

Petty Cash

- Some departments may require a petty cash fund for small expenses. Petty cash funds must be approved by the Treasurer's Office.
- A petty cash fund may not be used to circumvent purchasing regulations, make payroll advances, make contract labor payments, or reimburse travel expenses.
- There must be one individual responsible for the fund, and a separate person responsible for authorizing disbursements from the fund.
- Further details and control guidelines are available on the Policies and Procedures website at: http://www.astate.edu/dotAsset/8d8fc9bf-6349-434a-ae4b-62fc50aede94.pdf.

Fraud

- An employee who discovers or suspects fraudulent activity is required to contact the ASU System Internal Audit Department, either directly or anonymously through the EthicsPoint hotline.
    - Contact (855) 382-7963, or online at www.asusystem.edu/fraud.
- The ASU System Fraud Policy is located online at: http://www.asusystem.edu/about/policies/files/Fraud.pdf.

Equipment and Inventory

- Each department should have a designated custodian for equipment and other assets. This person is the contact for all questions regarding asset location, transfers, and other information.
- If a department holds stock or items for sale, the Controller's Office should be notified so that the inventory can be properly recorded.
- If a piece of equipment is transferred to another department or disposed of, Property Accounting (within the Controller's Office) should be notified so that the fixed asset records can be updated.
- If an item is stolen, a police report must be filed with University Police.
- Further information on Inventory and Property Management is located at: http://www.astate.edu/dotAsset/bb4a2846-36fc-4360-9bd4-960526e9b2d3.pdf.

Information Technology Security and Controls

- Security is an important element of safeguarding University assets and information.
- Information and Technology Services (ITS) provides resources on Information Security Best Practices, Phishing, Virus Detection, Computer Maintenance, and other important topics at: http://www.astate.edu/a/its/information-security/.