ASU System Policy

Effective Date: 9/15/17

Subject: Internal Control Policy

Category: Legal, Compliance, & Internal Audit 5.03

Purpose

The Arkansas State University System is committed to processes that reasonably prevent and detect fraud, waste, and abuse of institutional funds. In order to fulfill this commitment, the System will provide a framework for effective internal controls, which are best practices utilized throughout higher education, to minimize the opportunities and pressures associated with fraud. Specifically, the System will apply the COSO Internal Framework and the "Standards for Internal Control in the Federal Government," issued by the Comptroller General of the United States. Known as "the Green Book", this guide is a response to the recommendation of the Office of Management and Budget in 2 CFR 200.303, Uniform Guidance, Internal Controls. (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 those controls. The five integrated components for internal control are the following:

1. Control environment – the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization;
2. Risk assessment – a dynamic process for identifying and assessing risks and one that forms the basis for determining the ways that risks will be managed;
3. Control activities – actions established through policies and procedures to help ensure that management's directives are carried out to mitigate risks;
4. Information and communication – accurate 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; and
5. Monitoring activities – ongoing evaluations used to determine whether each of the components of internal control is functioning as expected.

Internal Control Objectives

The COSO has directed that the five components of internal control be integrated with

the internal control objectives of Operations, Reporting, and Compliance. All three categories, represented by the top columns in the cube, are affected and should be controlled by the five components. According to COSO, the three objectives include those listed below:

1. Operations objectives, which pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals and safeguarding assets against loss;
2. Reporting objectives, which pertain to internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies;
3. Compliance objectives, which pertain to adherence to laws and regulations to which the entity is subject.

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 with laws and regulations;
- Safeguarding of assets and University resources; and
- Economical and efficient use of resources.

Internal control applies to people, operations, communication, and the overall work environment, helping 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 they measure the effectiveness of preventive controls.

Preventive controls include, but are not limited to, the following:

- Segregation of duties;
- Standardized forms;
- Physical control of assets; and
- Computer passwords.

Detective controls include, but are not limited to, the following:

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

Responsibility for Internal Controls

Everyone in the ASU System has a role to play in internal control. ASU System leaders are ultimately responsible for the establishment and maintenance of a system of internal control and for establishing an ethical tone for overall operations. Each ASU System institution is required to create, document, and implement internal control processes that produce reasonable assurance within its own operations, reporting, and compliance. 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 his or her specific job duties.

Basic Components of Internal Control

Segregation of Duties
Duties should be divided among different individuals 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 activities to another source, such as a bank statement or a source document.

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.

(Adopted by the Arkansas State University Board of Trustees on September 15, 2017, Resolution 17-35.)