INTERNAL CONTROLS GUIDANCE HANDBOOK

FOR FISCAL YEAR 2015 AND BEYOND

Version 1.0 (08/2015)

Contents

effective systems of internal controls that went beyond checklists and carrying out standard policies and procedures.

COSO developed a framework for the creation of internal control systems that included five key components and 17 guiding principles. COSO updated the Internal Control ² Integrated Framework guidance document in May 2013. More information is available on the COSO website.

Standards for Internal Control in the Federal Government (Green Book)

The Standards for Internal Control in the Federal Government (Green Book) is published by the Government Accountability Office (GAO).

The GAO sets internal control standards for the federal government. These standards support the framework created by COSO. The Standards for Internal Control in the Federal Government (Green Book) can be used by organizations that receive federal grants from TEA to design, implement, and operate internal controls. The most recent version of the Green Book, published September 2014, is available through the GAO website.

Why Internal Controls Are Important

Definitions of Internal Control

In the Green Book, the GAO defines internal control D VD³ SURFHVV HIIHFWLYH E\ DQ H oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved ´ 7KH LQWHUQDO FRQWURO are the policies and procedures XVHG WR HQVXUH WKDW WKH RUJDQL]DWLRQ¶V PLVVLRQ VWUDW achieved. Internal controls are your first defense in safeguarding assets.

The objectives and corresponding risks fall into one or more of the following categories:

x Operations : Effectiveness and efficiency of operations
x Reporting : Reliability of financial reporting both internally and externally
x Compliance : Compliance with applicable laws and regulations

An internal control system is a system of ongoing processes that are built into the overall

Key Roles in the Internal Control System

Your internal control system needs to involve your local board, senior management, and other personnel in your organization. Written policies and procedures still require effective oversight, training, self-monitoring, and implementation. Further, staff still must make judgments and decisions based on your written policies and procedures. The key roles in your internal control system can be organized into the following categories:

- Oversight body
- Management
- Personnel
- Internal auditors

Oversight Body

Staff responsible for overseeing the entire organization are members of a governing board or senior management. For example, in a school district, the oversight body could include the local school board, superintendent, and other senior members of the administration. These individuals have the responsibility to provide advice, counsel, and direction to management; approve certain transactions and policies; and monitor management activities. The oversight body sets the tone at the top of an organization by clearly communicating the mission, goals, and objectives of the organization. The integrity of any internal control system depends on how the oversight body sets expectations for staff. Without a strong tone at the top to support an internal control system, WKH RUJDQL]DWLRQ¶V compliance with applicable laws IRU QRQ and regulations.

Management

$Q RUJDQL]DWLRQ¶V PDQDJHPHQW VWDII SDUWLFLSDWH LQ WKH the internal control system. Management is responsible for assuring that the internal control DFWLYLWLHV DUH FDUULHG RXW DQG School district personnel in RUJDQL]DWLRQ¶V REM management can include administration staff, campus leaders, and any other staff charged with supervising the internal control system.

Personnel

The rest of the staff in an organization fall into the ³other personnel´category. The oversight body and management cannot implement an effective internal control system without the support and full participation of all other staff. Personnel must understand how their specific duties

&262¶V)LYH &RPSRQHQWV RI ,QWHUQDO &RQWU

For an internal control system be effective, all of the components must be effectively designed and operating t

Risk Assessment

This component involves assessing the risks involved in your organization as they relate to the operation of federal grant programs, financial reporting, and federal program compliance. These activities develop the appropriate responses to risks identified.

It is critical to develop risk assessment policies and practices because instances of noncomplianFH ZLOO RFFXU 7KH IHGHUDO UXOHV RQO\ reasonable UHTXLUH WKD DVVXUDQFH´ UDWKHU WKDQ absolute assurance that you are managing your federal grant funds in compliance with all federal grant requirements. Auditors and monitors will look for evidence that you have a system in place that not only identifies areas of risk or weakness, but also addresses and fixes them at the time they occur. If you can produce documentation that provides evidence of your risk assessment processes, you may be able to reasonably assure an auditor or monitor that you are able to catch and resolve noncompliance issues quickly.

Some examples of areas of high risk are:

- New personnel who are not familiar with policies and procedures
- Organizational changes
- Changes in laws or regulations, such as the new EDGAR (effective December 26, 2014)
- New technology
- New grants

Generally, when changes occur in your organization, the potential increases for policies and procedures to fall through the cracks. Ongoing staff training, self-monitoring, and close evaluation of performance can help to mitigate some of this risk.

How to Identify Risks

To help you identify risks during the risk assessment process, here are some questions your department or division should ask.

- What could go wrong?
- How could we fail?
- What decisions require the most judgment?
- What activities or functions are the most complex?
- What activities are regulated?
- On what do we spend the most money?
- On what information do we rely the most?
- What assets do we need to protect?
- How could someone or something disrupt our operations?
- Is our IT system vulnerable to cyber-attacks?

Control Activities

These are actions that your organization takes in order 7(g)-8(an)3(i)5(z)11 0 0 1 300.77 13O[ )]T53oe0 0 1 90.

Control activities are the checks and balances that are necessary to ensure that everyone is following the rules and no one person is given too much authority or control over federal grant funds. The following are some of the key ways that you can establish controls:

- Segregating responsibilities so that one employee does not have full control or carry out all fiscal duties
- Ensuring that proper security is in place for systems and records, such as requiring passwords and restricted authorizations
- Keeping equipment and other assets secured
- Maintaining clear documentation of all procedures, including approvals and record retention
- Protecting and securing personally identifiable information

Types of Controls Activities

The goal of any internal control system is to reduce the risk of fraud, waste, or abuse. In order to do this, different types of controls must be in place. Three general types of internal controls are preventative, detective, and corrective.

Types of Controls	What It Does	Examples
Preventative	Prevents errors or irregularities from occurring	- Segregating staff duties - Requiring approvals, authorizations, and verifications - Securing assets, such as cash or equipment - Maintaining and regularly reviewing inventories and records
Detective	Identifies errors or irregularities after they have occurred	- Reviewing performance objectives, forecasts, or other benchmarks to identify unexpected or unusual results - Reconciling different sets of data to investigate irregularities - Conducting physical inventories of assets - Audits
Corrective	Identifies ways to react to the risk after the error has occurred	- Monitoring active grant programs to identify noncompliance or weakness in controls - Using automated systems with built-in checks that reject nonconforming or unallowable processes

Information and Communication

In order for an internal control system to be successful throughout an organization, the oversight body and management need to ensure that information is communicated effectively to all staff. Communication must go both ways. Staff must share information with management and leadership about the potential risks identified and the control activities conducted; management must communicate information to enable staff to understand the organiz DWLRQ¶V REMHFWLYHV the importance of their control responsibilities. Effective and clear communication with outside parties, such as external auditors, is necessary to show how your internal control system helps you meet your objectives and comply with federal requirements.

staff should model effective and consistent communication so that staff knows it is important. In order to begin designing or improving your information and communication system, you should determine all of the internal and external groups that need information from you, how you should communicate with these groups, and how often communication will be needed.

Monitoring Activities

Management establishes and operates an ongoing self-monitoring and evaluation of control activities that assess whether the internal control system is working. This ensures compliance with federal program requirements. Monitoring also involves resolving any issues that result from audits, other kinds of program reviews, and self-assessment reviews and take prompt action when instances of noncompliance are identified.

The most effective way to find problems is to test your own system regularly. For example, have someone from another area of your organization who is not familiar with your procurement process randomly select a contract, review the policies and procedures, and verify that they were followed. Another test could involve periodically reviewing your inventory list and verifying that items are located where they are supposed to be and items are labeled accurately. The

The 17 Principles

In addition to the five components that provide the structure for your internal control system, there also are 17 principles that support the five components. The principles provide additional guidance and clarification for evaluating the development and implementation of each component. The following table lists the components and the principles that support them.

Components	Principles
Control Environment	1. The oversight body and management should demonstrate a commitment to integrity and ethical values. 2. The oversight body should oversee the entity's internal control system. 3.

Audit Reviews

Your internal control system should be able to provide reasonable assurance, not absolute assurance, that there are sufficient controls in place to achieve successful operations, reliable reporting, and compliance with laws and regulations related to your federal grant programs. LEAs have an independent annual financial audit performed that checks for areas of noncompliance with federal grant programs.

Grant compliance requirements under Section 76.702 of Title 34 of the Code of Federal Regulations; section 200.302 of Part 2 of the Code of Federal Regulations, Part 200; and the Financial Accountability System Resource Guide (FASRG) stipulate that an LEA ¶ V financial management system must maintain fiscal control and accounting procedures to ensure an appropriate level of internal control for effective control and accountability over LEA resources.

The Five COSO Components and What Auditor s Review

During a federal audit review, monitors or auditors look within each of the five components of internal control at the written policies and procedures that provide evidence of the controls in place. The following are some examples of the types of documentation or activities monitors or auditors may review.

Components	Examples of Controls Reviewed by Auditors
Control Environment	x Human Resource Policies and Procedures ±including fraud policy and conflict of interest x Tone at the Top ± 0 D Q D J H P H Q W ¶ V V W \ O H Y D O X H V D Q towards compliance with established policies and procedures x Organizational Structure ±Identify reporting/supervisory responsibilities as well as assignment of authority and responsibilities
Risk Assessment	x Assessing organizational risk based on the environment and culture, including but not limited to: o Changes to personnel/reorganization o New technology/information system ±conversions and/or updates o New rules and regulations
Control Activities	x Segregation of Duties ±separating authorization, custody, and record keeping roles to prevent fraud or error by one person. Example: Input and review of purchase/payment records. Dual control for handling of cash/cash equivalents. x Authorization of transactions ±review of particular transactions by an appropriate person. Example: Spending Authorities ±Requiring board approval for purchases over $25,000. x Requiring the use of purchase orders/requisitions x Retention of records ±maintaining documentation to substantiate transactions x Safeguarding of Assets ±physical safeguards ±usage of cameras, locks, physical barriers, etc. to protect property. Examples: lock and key procedures; checkout procedures, including logs, for equipment or supplies, including cash equivalents (i.e. credit cards; check stock; petty cash); restricting use for appropriate/official business. x Asset Accountability ±tagging equipment/assets; use of asset tracking forms; periodic inventories. x IT general controls ±controls related to: o Security, to ensure access to systems and data is restricted to authorized personnel, such as usage of passwords and review of access logs; and

Category	Findings
Source Documentation	The grantee expended federal grant funds that were not adequately supported.