Policy Type: Administrative

Category: Fiscal and Budget

Policy Name: Internal Control Policy

Policy Owner: Controller-Treasurer Department

Policy Purpose

The purpose of this policy is to assist County Agencies and Departments and Special Districts governed by the County Board of Supervisors in establishing systems of internal control.

Policy Summary

County Agencies and Departments and Special Districts (County entities) are responsible for establishing a system of internal controls designed to prevent losses of public funds arising from fraud, employee error, misrepresentation by third parties, unanticipated changes in financial markets, or imprudent actions by employees and officers of the County.

These systems should provide reasonable assurance about the achievement of their entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, compliance with applicable laws and regulations, safeguard assets against unauthorized purchases, and prevent/detect financial errors and fraud.

Implementation of County Internal Controls

The Internal Control Methods document provides examples of methods that may be used by County entities to address their systems of internal controls.

The actual methods implemented to address the components of internal control need to be scaled to each particular County entity, and expanded or contracted based on the operation's organizational structure, staffing levels, programs, and resources. It is not expected that County entities will use every method of implementation that has been identified for each component. In addition, some County entities may use other policies or procedures in their system of internal control in lieu of the examples provided in the Internal Control Methods document.

Five Components of Internal Control

Internal control is composed of five components that work together in an integrated framework: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.

I. Control Environment

Each County entity's control environment should include a set of standards, processes, and structures that provide the basis for carrying out internal control across the entity. The governing board and management should establish the "tone at the top" regarding the importance of internal control, including expected standards of conduct, which then cascade down throughout the various levels of the organization and have a pervasive effect on the overall system of internal control. The control environment extends beyond the idea of culture and is composed of the following:

- The County entity's integrity and ethical values;
- The Board of Supervisors' oversight responsibilities;

- The assignment of authority and responsibility;
- The process for attracting, developing, and retaining employees; and
- The measures, incentives, and rewards to drive accountability for performance.

The control environment of a County entity is influenced by a variety of factors including the entity's history and/or values, economic conditions, and the competitive and regulatory landscape. Also, County entities that establish and maintain a strong control environment position themselves to be more resilient in the face of internal and external pressures.

II. Risk Assessment

A County entity's risk assessment process should include how the entity's management identifies risks (including fraud risk) relevant to the preparation and fair presentation of financial statements in accordance with the entity's applicable financial reporting framework, estimates the significance of each risk, assesses the likelihood of the occurrence, and decides upon actions to respond to and manage them and the results thereof.

Risks relevant to reliable financial reporting include external and internal events, as well as transactions or circumstances that may occur and adversely affect a County entity's ability to initiate, authorize, record, process, and report financial data consistent with the assertions of management.

III. Control Activities

County entities should establish policies and procedures to implement control activities that achieve management directives and respond to identified risks in the internal control system. When designing policies and procedures to address control activities, the County entity should keep in mind that the cost of implementing certain control activities should not exceed the benefit derived from the control activities.

Control activities can be categorized as policies and procedures that pertain to the following:

- **Authorization** – activities should be authorized in accordance with the County entity's policies and procedures.

- **Segregation of Duties** – shared responsibilities of a key process that disperses the critical functions of that process to more than one person or operating department. Without the separation in key processes, fraud and error risks are far less manageable. The functions of authorization, recording or reconciling, and maintaining custody of assets should be segregated.

For some small County entities, segregation of duties may be a challenge. Review and approval by an appropriate second person may be the most important control activity.

- **Performance Reviews** – County entities should perform analyses of financial data to ensure variances are in accordance with expectations, considering internal and external factors. This includes comparing current year actuals to budget, historical trends, and any forecasts of future performance available.

- **Information Processing** – two aspects, Application Controls and General IT Controls, which relate to the overall effectiveness of IT controls to ensure the proper operation of a County entity's information systems.

Application Controls are those related to procedures to check the accuracy of the output data, including follow-up on exceptions. Application controls are designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. It includes both the routines contained within the computer program code as well as the policies and procedures associated with user activities, such as entering data and producing or reporting results.

General IT Controls involve maintaining control procedures to restrict the access to the program data and the ability to make modifications to the data, including software updates and back-up or disaster recovery procedures, to ensure the continued operation of the information systems. General controls are needed to ensure the function of application controls, which depend on computer processing, and include the structure, policies, and procedures that apply to the agency's overall computer operations. It applies to all information systems: mainframe, minicomputer, network, cloud applications, and end-user environments, and can include controlled processes for system access, computer center or server operations, change management, incident response, business continuity, and backup and storage.

- **Physical Controls** – include ensuring the safeguarding of both tangible and intangible assets. County entities should have policies that ensure the physical security over all assets, whether they be capital assets, cash and investments, or other assets, and procedures to periodically count or reconcile the assets to the records. In addition, access to computer programs or data files should be restricted to appropriate personnel.

IV. Information and Communication

Information is necessary for each County entity to carry out internal control responsibilities to support the achievement of its objectives. County management at all levels should obtain, or generate, and use relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from management that control responsibilities must be taken seriously. External communication is twofold as it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

V. Monitoring

Monitoring involves evaluating the effectiveness of County controls on an on-going basis and taking remedial actions when necessary. On-going monitoring activities should be built into the normal recurring activities of County entities, including regular management and supervisory activities. Management's monitoring of controls should include consideration of whether they are operating as intended and that they are modified as appropriate for changes in conditions.

Procedures

For examples of methods that may be used by County entities to address their internal control environments, see the Internal Control Methods document, available at [url]/sites/controller/Controller-Treasurer%20Policies%20and%20Procedures/Documents/Internal-Control-Methods.pdf.

Definitions

1) "**Communication**" – according to the AICPA's Auditing Standard AU-C §315.A97, communication by the entity of the financial reporting roles and responsibilities and significant matters relating to financial reporting involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. It includes such matters as the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Communication may take such forms as policy manuals and financial reporting manuals. Open communication channels help ensure that exceptions are reported and acted on.

2) "**Control Activities**" – according to the AICPA's Auditing Standard AU-C §315.A99, an entity's control activities are the policies and procedures that help ensure that management directives are carried out. Control activities, whether within IT or manual systems, have various objectives and are applied at various organizational and functional levels. Examples of specific control activities include those relating authorization, performance reviews, information processing, physical controls, and segregation of duties.

3) "**Control Environment**" – according to the AICPA's Auditing Standard AU-C §315.A78, the control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's internal control and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

4) "**County Entity**" – means a County Agency or Department, or a Special District governed by the County Board of Supervisors.

5) "**Information System**" – according to the AICPA's Auditing Standard AU-C §315.A92, the information system relevant to financial reporting objectives, which includes the accounting system, consists of the procedures and records designed and established to:

- initiate, authorize, record, process, and report entity transactions (as well as events and conditions) and maintain accountability for the related assets, liabilities, and equity;
- resolve incorrect processing of transactions (for example, automated suspense files and procedures followed to clear suspense items out on a timely basis);
- process and account for system overrides or bypasses to controls;
- transfer information from transaction processing systems to the general ledger;
- capture information relevant to financial reporting for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of accounts receivables; and
- ensure information required to be disclosed by the applicable financial reporting framework is accumulated, recorded, processed, summarized, and appropriately reported in the financial statements.

6) "**Internal Control**" – according to the AICPA's Auditing Standard AU-C §315.04, internal control is a process effected by those charged with governance, management, and other personnel that is designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over safeguarding of assets against unauthorized acquisition, use or

disposition may include controls relating to financial reporting and operations objectives.

7) "**Monitoring**" – according to the AICPA's Auditing Standard AU-C §315.A.110, monitoring of controls is a process that is used by management to assess the effective operation of internal controls over time.

8) "**Risk Assessment**" – according to the AICPA's Auditing Standard AU-C §315.A89, an entity's risk assessment process for financial reporting purposes is its identification, analysis, and management of risks relevant to the preparation and fair presentation of financial statements.

Frequently Asked Questions

None.

Related Policies

- California Government Code (Section 13400-13407), The State Leadership Accountability Act - http://www.dof.ca.gov/Programs/OSAE/SLAA/

- Treasury Investment Policy - Board Policy 4.8 - https://saecommon.sccgov.org/countypolicy/Board-Policy-4.8-Treasury-Investment-Policy.pdf

Related Forms and Information

- Internal Control Methods - [url]/sites/controller/Controller-Treasurer%20Policies%20and%20Procedures/Documents/Internal-Control-Methods.pdf

- American Institute of CPA's Auditing Standard - http://www.aicpa.org/research/standards/auditattest/pages/sas.pdf

- California State Controller's Office - 2015 Internal Control Guidelines - Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control - Integrated Framework (2013)* - http://www.coso.org/IC.htm

- U.S. Government Accountability Office - Internal Control Management and Evaluation Tool - http://www.gao.gov/products/GAO-01-1008G

- U.S. Government Accountability Office - The Green Book - http://www.gao.gov/greenbook/overview

- U.S. Government Accountability Office - The Yellow Book - http://www.gao.gov/yellowbook/overview

- Office of Management and Budget - https://www.whitehouse.gov/omb

History

Date	Changes Made
2/7/2017	Policy Uploaded. (Kyle Larson)
2/3/2017	Policy Adopted.