State of Arizona Accounting Manual

INTRODUCTION

This section of SAAM is but one of several dealing with the overarching topic of Internal Controls. Each section within this topic complements the others procedurally or philosophically and, hence, benefits from the reading of the others, just as the others benefit from the reading of this.

Internal control provides many benefits to an agency. It provides agency management with confidence regarding the achievement of objectives, gives feedback on how effectively an agency is operating, and helps reduce risks affecting the achievement of an agency's objectives.

The volume and vulnerability of data in automated systems—particularly given the degree of integration or exchange of information between such systems—are of special concern. This section of SAAM addresses this concern and related controls.

POLICY & PROCEDURES

1. Internal controls must be a high priority for every agency.

2. Agency management is responsible for maintaining a system of internal controls that minimizes the risk of errors and irregularities. This is as true, if not more true, for IT environments as for traditional, manual environments.

3. All financial and accounting responsibilities should be segregated to the extent practicable so that no one individual has complete control over an entire transaction. This extends to access, processing and approval roles in IT environments.

4. Personnel and payroll responsibilities should be segregated so that no one individual has complete control over the employment and compensation determination and payment processes.

5. Segregation of duties is primarily intended to reduce the situations under which an individual might have the ability to perpetrate and conceal errors and irregularities in the normal course of duties. No one should be in a position to be tempted by or accused of inappropriate activity.

6. When segregation of duties is not possible at an agency (e.g., at an agency with a very limited number of personnel), the agency may establish alternate procedures that control the risk of unauthorized transactions. These procedures must be written, well-documented, enforced and available for review by auditors.

7. Review procedures, including those that are described in other sections of SAAM, should be in place to detect and, if possible, prevent errors and irregularities.

8. Management and other personnel have access to voluminous amounts of confidential and/or sensitive information. Management and other personnel are to refrain from:

8.1. Revealing information to anyone not specifically authorized to receive the information under consideration.

8.2. Attempting to access or achieving access to data not applicable to his job.

8.3. Entering, changing or erasing data for direct or indirect personal gain or advantage.

8.4. Entering, changing or erasing data for personal amusement or retribution.

8.5. Using another individual's personal identifier (i.e., user identification) and/or password to access, enter, change or erase data.

8.6. Revealing his password to another individual.

8.7. Asking another individual to reveal his password.

8.8. Using any information for personal gain or in a manner other than its intended use.

9. All transactions, by whatever method they are entered, stored or transmitted, are subject to audit.

10. Agencies shall establish internal control procedures to prevent transactions from being:

10.1. Input so they appear as their having occurred in the wrong accounting period.

10.2. Posted to the wrong balance sheet account, revenue source, expenditure object, accounting structure, grant, fund, etc.

10.3. Lost, duplicated, inappropriately altered, entered if not properly approved or authorized, or erroneously omitted from entry.

11. Supporting documentation shall be retained for all transactions. The documentation may be retained in electronic format, if appropriate. See SAAM 0020.

12. Personnel should <u>not</u> be authorized to input and approve the same transaction in any automated system.

13. Agency management is responsible for ensuring that any access to or within any applicable Statewide system (e.g., AFIS, HRIS, APP, TRIRIGA, etc.) is immediately (i.e., within one (1) business day) revoked upon the termination (voluntary or involuntary), departure or transfer of one of its employees.

13.1. Agency management is responsible for immediately (i.e., within one (1) business day) notifying the system administrator for any applicable Statewide system when one of its user accounts is no longer needed or when the permission roles have changed for the user. Inactive user permissions will be disabled in accordance with the Arizona Statewide Information Security policies found at https://aset.az.gov/policies-standards-and-procedures.