

## 10-042 Internal Controls and Fraud

---

*Current Update: 11/02/09*

*Original Issuance: 03/08/00*

### Purpose

This policy defines the responsibilities of management and staff of the State Board of Administration with regard to the establishment and maintenance of an effective system of internal controls and defines responsibilities when impropriety, including fraud, is suspected or detected.

This Policy is applicable to all State Board of Administration staff, including permanent positions, OPS staff and interns.

### Policy

**It is the policy of the Executive Director & CIO of the State Board of Administration (SBA) that:**

- SBA managers and supervisors will develop and maintain an appropriate system of internal controls and will integrate adequate internal controls into organizational processes to protect SBA assets and resources for which they are responsible. The system should ensure that transactions are appropriately authorized, the true substance and effect of transactions are properly recorded, assets are properly safeguarded, and accountability for actions and resources is appropriately identified and documented.
- SBA managers and supervisors will be responsible for evaluating and testing internal controls on a periodic basis and will develop companion policies, guidelines and procedures as necessary to implement and document the SBA's system of internal controls.
- SBA management and staff will be familiar with internal controls over the assets and resources for which they are responsible, will understand the associated risks for irregularities or violations of internal controls, and will be vigilant for any indication of the existence of fraud.
- SBA management and staff have an affirmative duty to escalate and report directly to either the Executive Director & CIO, the Inspector General, or the General Counsel, employee or contractual party fraud or misconduct (whether actual or suspected), employee or contractual party material error that adversely affects SBA or client assets or interests, misrepresentation or omission of material information in internal and external reporting and client communications, and violations of laws, rules or SBA policies.

- Allegations of impropriety, including fraud, will be investigated objectively, fairly and promptly.

## Background and Implementation

Internal controls are defined as processes, effected by an entity's management, designed to provide reasonable assurance that organizational objectives, such as effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations can be achieved. Internal controls are intended to reduce the risk of unauthorized transactions, misleading or improperly recorded transactions, loss of resources and assets, and failure to identify the person(s) responsible for errors and fraud. Adequate systems of internal control must address authorization, recording, safeguarding, and accountability.

Risk assessment is necessary for the identification and analysis of relevant risks to the achievement of the organization's objectives, and forms a basis for determining how those risks should be managed. Control activities are the policies, guidelines and procedures that ensure necessary actions are taken to address and mitigate identified risks.

Detection and prevention of fraud is a basic management responsibility. Fraud is deliberate deceit or intentional misrepresentation or concealment of a material fact to cheat or prejudice the legal rights or conduct of another to secure unfair or unlawful gain. Frauds direct their schemes against an organization or for an organization, both of which are equally damaging.

Fraud designed to benefit the organization generally produces such benefit by exploiting an unfair or dishonest advantage that also may deceive an outside party. Perpetrators of such frauds usually accrue an indirect personal benefit. Examples of such frauds are:

- Improper representation or valuation of transactions and/or assets;
- Intentional failure to record or disclose significant information to improve the financial picture and performance of the organization to outside parties; and
- Prohibited activities that violate government laws and regulations.

Fraud perpetrated to the detriment of the organization generally is for the direct benefit or indirect benefit of an employee or outside individual or organization. Examples of such fraud are:

- Acceptance of bribes, kickbacks, or inappropriate terms or discounts;
- Intentional concealment or misrepresentation of financial or non-financial data; and
- Embezzlement of the organization's money or property and falsification of records to cover up such activity.

The principal mechanism for deterring fraud is a well designed and properly functioning system of internal controls.

SBA employees are to report the following acts to the Executive Director & CIO, the Inspector General, the General Counsel, the SBA Fraud Hotline (800-547-9180), or as otherwise specified in policy:

- Suspected and actual fraud or misconduct by an employee or contractual party
- Employee or contractual party material error that adversely affects SBA or client assets or interests
- Misrepresentation or omission of material information in internal and external reporting and client communications
- Violations of laws, rules or SBA policies

In instances where an SBA employee suspects Executive Service staff is involved in possible fraudulent activities or misconduct, the Chief Internal Auditor (CIA) is designated to receive such reports or complaints. Fraudulent acts or misconduct may involve violations of internal controls, violations of the SBA Code of Ethics or Code of Conduct, or actions that may be viewed as conflicts of interest.

After making a report of an allegation or suspicion to one of the positions designated above, an SBA employee should not take any further action to investigate suspected activity. *Specifically, the employee should not:*

- contact the suspected person in an effort to gather additional facts, demand restitution; or
- discuss the case, facts, suspicions, or allegations with anyone unless directed to do so by the Executive Director & CIO or the Inspector General.

The Inspector General (or CIA in situations involving Executive Service staff or other situations where the Inspector General enlists the CIA's assistance) will conduct an internal investigation to determine whether sufficient evidence exists to create a reasonable suspicion that a crime or violation has been committed or some other significant unethical conduct has occurred. If the Inspector General concludes that such evidence exists, appropriate steps will be taken to preserve the integrity of such evidence and a recommendation will be made to the Executive Director & CIO as to whether or not the evidence should be turned over to a law enforcement agency or handled internally. Results of an investigation performed by the CIA will be submitted to the Executive Director & CIO and the SBA's Audit Committee.

The SBA shall utilize a variety of resources in the prevention, detection and investigation of fraud, including "financial lifestyle checks". Financial lifestyle checks may include accessing public records databases, requests for financial or legal documentation from employees, interviews of employees and their co-workers, and observation of personal expenditure patterns. Financial lifestyle checks will be initiated by the Inspector General solely for cause or to address some particular situation, must be approved in advance by

the Executive Director & CIO and shall be performed in conjunction with the General Counsel.

Disciplinary action may be taken against SBA employees who:

- have been found to have committed fraudulent activities.
- condone, permit or have knowledge of employee or contractual party fraud or misconduct, employee or contractual party material error that adversely affects SBA or client assets or interests, misrepresentation or omission of material information in internal and external reporting and client communications, and violations of laws, rules or SBA policies and do not report such information to the Executive Director & CIO, Inspector General or General Counsel (or the CIA in situations involving Executive Service staff).
- make false statements in connection with investigations made by the Inspector General, CIA or law enforcement.
- take reprisal against another employee for making a "good faith" report under this Policy.

After resolution of any criminal matters or ethics violations, the Inspector General is responsible for reviewing internal controls that have been violated and for recommending to the Executive Director & CIO whether such controls should be revised or enhanced.

The Inspector General may conduct or procure fraud awareness training for SBA employees and is responsible for assisting SBA management in developing additional policies and procedures necessary to accomplish the objectives of this Policy. The CIA will perform risk assessment within SBA operations to enable recommendations to be made to management regarding the development and design of internal controls.

## **Compliance**

SBA managers and supervisors are responsible for compliance with this Policy through the development, implementation and maintenance of an appropriate system of internal controls to protect SBA assets and resources for which they are responsible.

All SBA employees are responsible for compliance with the fraud awareness and reporting provisions of this Policy.

The Inspector General may review and test internal controls within the SBA as deemed necessary.