SECTION 9 – INTERNAL CONTROLS AND FRAUD PREVENTION

Overview

Internal control is a process carried out by the governing body, management, and employees to provide reasonable assurance that the government will achieve its objectives related to operations, reporting, and compliance. Internal controls are part of day-to-day operations and are not solely the responsibility of the Finance Department. Department managers and employees are responsible for the controls within the activities they supervise or perform, while finance personnel often play a central role in establishing, coordinating, and monitoring financial controls.

An effective system of internal control reduces the risk of error, fraud, waste, abuse, noncompliance, and loss of public assets. No system can eliminate all risk because controls may be affected by judgment, human error, collusion, management override, technology changes, or other changing conditions. Controls should therefore be designed in proportion to the government's size, complexity, staffing, systems, and risk profile and should be reviewed periodically to ensure they remain effective.

Statutory Requirements

Section 218.33(3), Florida Statutes, requires each local governmental entity to establish and maintain internal controls designed to:

- Prevent and detect fraud, waste, and abuse as defined in Section 11.45(1), Florida Statutes.
- Promote and encourage compliance with applicable laws, rules, contracts, grant agreements, and best practices.
- Support economical and efficient operations.
- Ensure reliability of financial records and reports.
- Safeguard assets.

These requirements apply across the organization. Financial controls should be integrated with operational, information technology, procurement, human resources, grant, and program controls rather than treated as a separate year-end or audit function.

Internal Control Framework

The Government Finance Officers Association (GFOA) recommends that state and local governments use the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework as the conceptual basis for designing, implementing, operating, and evaluating internal control. The framework consists of five interrelated components:

- Control Environment – Establishes the organizational foundation for internal control through integrity, ethical values, oversight, organizational structure, assignment of authority and responsibility, competence, and accountability.
- Risk Assessment – Identifies and analyzes risks that could prevent the government from achieving its objectives, including risks arising from fraud, changes in operations, technology, laws, staffing, vendors, or programs.
- Control Activities – Includes policies and procedures that reduce identified risks, such as approvals, authorizations, reconciliations, access controls, verifications, reviews, and segregation of duties.
- Information and Communication – Ensures that relevant, reliable information is identified, documented, communicated, and available to employees and decision makers who need it to perform control responsibilities.

- Monitoring – Uses ongoing supervision, periodic evaluations, audits, exception reporting, and corrective-action follow-up to determine whether controls are present and functioning effectively.

The U.S. Government Accountability Office's 2025 Standards for Internal Control in the Federal Government, commonly known as the Green Book, provides a complementary public-sector framework and may also be used by state and local governments. Governments administering federal awards should also comply with applicable internal-control requirements under 2 Code of Federal Regulations (CFR) § 200.303 and the terms of each award. See Section 24 – Grants for additional grant-related requirements.

Control Environment and Accountability

A strong control environment begins with the governing body and senior management. Policies and actions should demonstrate that integrity, ethical conduct, compliance, and accountability are expected throughout the organization. Key practices include:

- Establishing clear organizational structures, lines of authority, approval levels, and responsibility for key financial and operational processes
- Maintaining written policies and procedures that are current, accessible, and consistent with applicable laws, contracts, grant requirements, and adopted policies
- Providing employees with appropriate training and ensuring that employees assigned financial responsibilities possess the knowledge and competence needed to perform them
- Holding managers and employees accountable for complying with established controls and for correcting identified deficiencies
- Requiring disclosure and appropriate management of conflicts of interest and other ethical concerns

Risk Assessment and Fraud Risk

Governments should periodically assess financial and operational risks and update the assessment when significant changes occur. Changes in personnel, systems, banking arrangements, payment methods, vendors, organizational structure, laws, grant requirements, or service delivery can create new risks or make existing controls ineffective.

Fraud risk should be considered as part of the assessment. Areas that commonly warrant attention include:

- Cash receipts, deposits, refunds, adjustments, and accounts receivable
- Vendor creation and changes to vendor payment or banking information
- Accounts payable, purchasing cards, electronic payments, ACH and wire transfers
- Payroll changes, time reporting, overtime, benefits, and terminated or inactive employees
- Procurement, contract administration, conflicts of interest, bid manipulation, and split purchases
- Manual journal entries, accounting estimates, reconciliations, and management override of established processes
- Inventory, equipment, capital assets, and other property susceptible to theft or misuse
- Grant expenditures, eligibility, matching requirements, subrecipient activity, and restricted funding
- Information system access, social engineering, payment-redirection fraud, cybersecurity events, and unauthorized changes to financial data

The results of significant risk assessments should be documented, together with the controls or other responses selected to address identified risks and the individuals responsible for implementing or monitoring those responses.

Segregation of Duties and Compensating Controls

Segregation of duties is a fundamental internal-control principle. To the extent practical, responsibility for the following functions should be assigned to different individuals:

- Authorization or approval of a transaction
- Custody of cash, checks, inventory, purchasing cards, electronic-payment credentials, or other assets
- Recording or posting transactions in the accounting or subsidiary system
- Reconciliation, verification, or independent review of the transaction and related records

Smaller governments may not have enough staff to fully separate all incompatible duties. In those situations, management should identify the resulting risk and establish documented compensating controls. Examples include independent supervisory review of bank statements and reconciliations, dual approval of electronic payments, secondary verification of vendor banking changes, review of exception or audit-log reports, governing-body review of selected transactions, periodic rotation of duties, or independent review by qualified personnel who are not responsible for the underlying transaction.

Key Financial Control Activities

The specific controls needed will depend on each government's operations and systems. Common financial control activities include:

- Cash and receivables – Document collections at the point of receipt, reconcile collections to deposits and accounting records, restrict access to cash, and provide independent review of adjustments, refunds, and write-offs. See Section 8 – Cash Receipts/Accounts Receivable.
- Disbursements and vendor management – Require appropriate authorization and supporting documentation, independently verify significant vendor-master or banking changes, restrict access to payment files and credentials, and use layered controls for ACH, wire, check, and other disbursements.
- Payroll – Require authorized personnel actions, control changes to pay rates and deductions, reconcile payroll and related liabilities, review exception reports, and provide final review or approval independent of payroll preparation. See Section 14 – Payroll.
- Purchasing and purchasing cards – Enforce procurement thresholds and approval requirements, prohibit split purchases, establish card limits and allowable uses, require timely supporting documentation, and provide supervisory review. See Section 16 – Purchasing.
- Journal entries and financial reporting – Restrict the ability to create and post manual entries, require adequate support and independent approval for significant or unusual entries, reconcile subsidiary records to the general ledger, and review financial reports for unexpected variances or unusual activity.
- System access – Use unique user accounts, role-based access and least privilege; appropriately restrict privileged access; promptly revise or deactivate access when responsibilities change or employment ends; and periodically review user access. See Section 23 – Information Technology.
- Capital assets and inventory – Maintain complete property records, restrict custody where practical, document additions and disposals, and perform required physical inventories and reconciliations. See Section 5 – Capital Assets.

- Grants – Establish award-specific project codes, review allowability and eligibility, reconcile expenditures and drawdowns, monitor subrecipients when applicable, and maintain complete supporting documentation. See Section 24 – Grants.

Fraud Reporting and Response

GFOA recommends that governments establish policies and procedures that encourage and facilitate the reporting of suspected fraud, waste, abuse, and questionable accounting or auditing practices. Reporting mechanisms should be appropriate for the size and structure of the organization and may include confidential or anonymous reporting options.

Policies should identify how concerns are reported, who receives and evaluates reports, how potential conflicts are avoided, and how matters are documented and resolved. The individual or unit responsible for investigating a concern should be sufficiently independent of the activity or person involved. Appropriate steps may include preserving records and electronic evidence, consulting legal counsel or human resources, notifying an inspector general or law-enforcement agency when appropriate, and documenting the disposition of the matter. Governments should also ensure that employees are informed of applicable protections under the Florida Whistle-blower's Act and other laws or policies prohibiting retaliation.

Monitoring, Deficiencies, and Corrective Action

Internal controls should be monitored throughout the year rather than evaluated only during the annual audit. Supervisory reviews, reconciliations, exception reports, access reviews, inventory counts, management reports, internal audits, and other periodic evaluations can provide evidence that controls are functioning as intended.

When a control deficiency, audit finding, error pattern, suspected fraud, or other weakness is identified, management should evaluate the cause and potential impact, determine whether the issue is isolated or systemic, assign responsibility for corrective action, establish a reasonable completion date, and verify that the corrective action is implemented and effective. Significant or recurring deficiencies should be communicated to appropriate executive management and the governing body or audit committee.

GFOA recommends that every government consider the feasibility of establishing a formal internal audit function. Where a separate function is not practical, periodic internal-control reviews may be assigned to qualified personnel independent of the activity being reviewed or obtained from an outside provider, subject to applicable independence and procurement considerations.

Periodic Review

At least periodically, and whenever significant organizational or system changes occur, management should review whether internal controls remain appropriate. The review should consider staffing and segregation of duties, user access, bank and payment controls, vendor-management procedures, changes in laws and grant requirements, new or modified systems, unresolved audit findings, known fraud or error trends, and emerging technology or cybersecurity risks. Policies, procedures, training, and control assignments should be updated when needed.

References

- Section 218.33, Florida Statutes - Local governmental entities; uniform fiscal years, accounting practices, and internal controls. Official link
- Section 11.45, Florida Statutes - Definitions of fraud, waste, and abuse and Auditor General authority. Official link

- Sections 112.3187-112.31895, Florida Statutes - Florida Whistle-blower's Act. Official link
- 2 CFR § 200.303 - Internal controls for federal awards. Official link
- Florida Auditor General - Rules of the Auditor General, including Chapter 10.550. Official link
- Government Finance Officers Association - Internal Control Framework. Official link
- Government Finance Officers Association - Internal Control Environment. Official link
- Government Finance Officers Association - Whistleblowing. Official link
- Government Finance Officers Association - Internal Audit Function. Official link
- Committee of Sponsoring Organizations of the Treadway Commission - Internal Control—Integrated Framework. Official link
- U.S. Government Accountability Office - Standards for Internal Control in the Federal Government (2025 Green Book). Official link