Chapter 9

Internal Control in Financial Management

by Rebecca Badgett

Introduction

Local governments have a duty to be good stewards of public moneys and assets. To accomplish this, units must take measures to safeguard moneys and assets and ensure that they are used for authorized and lawful purposes. Chapter 8 discusses the statutory internal controls mandated by the Local Government Budget and Fiscal Control Act (LGBFCA) that relate to depositing, investing, obligating, and disbursing public funds. This chapter explores a step-by-step process that local units can use to design and implement a strong system of internal control over financial-management operations, recognizing that each internal control system should be uniquely tailored to each local unit's needs and capabilities.

Establishing a Framework of Internal Control

There are two widely accepted frameworks of internal control on which a local government may choose to base its internal control system. The first is the *Internal Control–Integrated Framework*, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a voluntary organization dedicated to improving the quality of financial reporting and strengthening internal control in private-sector organizations. The second framework is the Government Accountability Office's *Standards for Internal Control in the Federal Government*, known as the "Green Book."[1] The Green Book is the legally

This chapter reflects the law as of April 20, 2023.

[1] United States Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government*, GAO 14-704G (September 2014).

required internal control framework for federal entities, but it may be adopted by other public-sector organizations, including state and local governments, quasi-governmental agencies, and not-for-profit organizations.[2]

The guidance and approach to internal control offered in the Green Book and in the COSO *Internal Control–Integrated Framework* are similar. Both frameworks structure the approach to internal control by using five key components that are supported by seventeen underlying principles. While either framework may form the basis of a local government's internal control system, this chapter summarizes the guidance stipulated in the Green Book because the Green Book model is intended for use by public-sector organizations, including local governments.

Internal Control Defined

The Green Book defines internal control as a "process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved."[3] An entity's objectives should be classified under one or more of the following categories:

- Operations—Effectiveness and efficiency of operations
- Reporting—Reliability of reporting for internal and external use
- Compliance—Compliance with applicable laws and regulations[4]

This definition highlights a few key points. First, internal control is a process; it is not one event but is, rather, a series of actions that will prove to be most effective when operationalized into daily business operations. This process must be consistently monitored, evaluated, and updated to ensure that it is functioning at the optimal level. Second, even the strongest internal control system provides only *reasonable assurance* that a unit's objectives will be met. Absolute assurance is not possible due to the inherent limitations of internal control, such as unintentional mistakes and errors, management override of established controls, and external factors like natural disasters, cybersecurity breaches, a pandemic, or other events outside of a unit's control. Lastly, the underlying objective of internal control is to safeguard public moneys and assets from loss.[5] A local unit must design its control system to limit opportunities for fraud and must put controls in place that prevent or promptly detect mistakes, errors, and acts of fraud by employees.

[2] GAO, *Standards for Internal Control in the Federal Government*, at 20.
[3] GAO, *Standards for Internal Control in the Federal Government*, at 5.
[4] GAO, *Standards for Internal Control in the Federal Government*, at 5.
[5] GAO, *Standards for Internal Control in the Federal Government*, at 14.

Responsibility for Internal Control

The Green Book's definition of internal control places responsibility for internal control on "management" and the "oversight body." A third category, "personnel," includes employees who assist management with the implementation of controls and must report any functional issues to management.[6]

Management

Management is responsible for the design and implementation of a unit's internal control system. The term "management" generally includes persons in upper-management positions such as the senior finance officer(s), the county or municipal manager, department heads, and possibly the unit's attorney. Although the auditor may suggest changes to improve the effectiveness of established controls, the unit's auditor is not responsible for implementing internal controls and should not be included in the internal control "management" team.

Management should keep in mind that there is no one-size-fits-all approach to internal control. Every unit's internal control system should be tailored to meet the unique needs and capabilities of the unit. It is helpful to consider factors such as size, organizational structure, operating style, number of personnel, or other special circumstances that may impact the overall function of the control system. For example, in small units, the manager may play a key role in carrying out certain responsibilities that a manager in a larger unit is not expected to perform.[7] Small units also face certain challenges, such as having limited staff, which can make it difficult to ensure adequate segregation of duties.

Oversight Body

The oversight body is responsible for overseeing management's design and implementation of the unit's internal control system.[8] In local government, the elected governing board is by default the acting oversight body. The governing board may appoint a separate committee to act as the oversight body if the full board does not want to assume oversight responsibility. In such instances, the appointed oversight committee may include a mix of governing board members and senior management. In small units, the oversight body may need to take a more active role in the internal control process by helping management design effective controls or by compelling compliance by instituting and enforcing meaningful consequences for noncompliance.

[6] GAO, *Standards for Internal Control in the Federal Government*, at 12.

[7] GAO, *Standards for Internal Control in the Federal Government*, at 18

[8] GAO, *Standards for Internal Control in the Federal Government*, at 11.

Components of Internal Control

The Green Book approaches internal control through a hierarchical structure of five components and seventeen principles (see Figure 9.1). The five components of internal control are:

1. control environment,
2. risk assessment,
3. control activities,
4. information and communication, and
5. monitoring.

The seventeen principles explain the requirements necessary to implement the associated components. In general, every component and principle is necessary and should be operationalized to help establish the most effective internal control system.

1. Control Environment

The first component of the Green Book's internal control framework is control environment. This component serves as the foundation of the internal control system. It is sometimes called the "tone at the top" or, in the private sector, "corporate culture." A strong control environment is fostered when management and the governing board communicate to employees the importance of ethical behavior and competence in the workplace and the need to follow established internal control processes.[9] The principles that support the control environment, set out in the paragraphs below and identified by their number in the Green Book's listing (see Figure 9.1), can serve as a road map to help create a strong control environment.

- **The Oversight Body and Management Should Demonstrate a Commitment to Integrity and Ethical Values (Green Book Principle 1).** To satisfy this principle, the local unit's oversight body and management should adopt a code of conduct to communicate expectations concerning integrity and ethical values. Management may rely on the code to help evaluate the attitudes and behaviors of employees and departments and to determine the tolerance level for deviations.[10]
- **The Oversight Body Should Oversee the Unit's Internal Control System (Green Book Principle 2).** To satisfy this principle, the oversight body must oversee management's design, implementation, and operation of the internal control system. The oversight body should test controls and consider whether the current internal control system is adequate to mitigate risks and guard against potential acts of fraud. The oversight body may provide guidance and offer suggestions on how to remediate any apparent weaknesses or deficiencies in the internal control system.[11]
- **Management Should Establish an Organizational Structure, Assign Responsibility, and Delegate Authority to Achieve the Unit's Objectives (Green Book Principle 3).** To satisfy this principle, management will want to (a) consider how the departments within the unit interact to fulfill the unit's overall responsibility and (b) establish clear reporting

[9] GAO, *Standards for Internal Control in the Federal Government*, at 22.
[10] GAO, *Standards for Internal Control in the Federal Government*, at 23.
[11] GAO, *Standards for Internal Control in the Federal Government*, at 24–26.

Figure 9.1 The Greenbook's Five Key Components of Internal Control and Seventeen Principles Underlying Internal Control

Control Environment	1. Demonstrate commitment to integrity and ethical values
	2. Exercise oversight responsibility
	3. Establish structure, responsibility, and authority
	4. Demonstrate commitment to competence
	5. Enforce accountability
Risk Assessment	6. Define objectives and risk tolerances
	7. Identify, analyze, and respond to risk
	8. Assess fraud risk
	9. Analyze and respond to change
Control Activities	10. Design control activities
	11. Design activities for the information system
	12. Implement control activities
Information and Communication	13. Use quality information
	14. Communicate internally
	15. Communicate externally
Monitoring	16. Perform monitoring activities
	17. Remediate deficiencies

lines with the unit's organizational structure. Organizational charts are helpful in establishing reporting lines. For example, an organizational chart for the finance department could illustrate the reporting lines and level of authority between the various finance-related positions, such as the finance officer, deputy finance officer, accountant, payroll specialist, treasurer, and other positions. When advertising a new finance position, the position description should match the level of authority designated in the organizational chart. Management can use the organizational chart to delegate internal control responsibilities to personnel down the reporting chain of command.[12]

- **Management Should Demonstrate a Commitment to Recruit, Develop, and Retain Competent Employees (Green Book Principle 4).** Management must recruit and hire qualified personnel to fill vacant positions and provide current employees with training opportunities to help ensure that the employees maintain the level of competence necessary to accomplish assigned responsibilities.[13] This requires management to have a clear understanding of job duties and position responsibilities.
- **Management Should Evaluate Performance and Hold Individuals Accountable for Their Internal Control Responsibilities (Green Book Principle 5).** To satisfy this principle, periodic

[12] GAO, *Standards for Internal Control in the Federal Government*, at 28.
[13] GAO, *Standards for Internal Control in the Federal Government*, at 31.

performance reviews should be conducted to evaluate whether employees are competent and performing assigned internal control responsibilities. For example, if the unit has a policy that requires the deputy finance officer to attach the preaudit certificate to contracts or purchase orders, management should review whether the employee is in fact meeting this expectation. Disciplinary action may be taken when instances of noncompliance are identified.

2. Risk Assessment

The second key component of internal control is risk assessment. Risk assessment is a process undertaken by management to identify risks facing the unit as it seeks to achieve its objectives.[14] Conducting a risk assessment allows management to identify areas in need of control activities. The goal of the risk assessment is not to eliminate all risks facing the unit, as this would be impossible. Instead, management should determine an acceptable level of risk and consider how to keep risk factors within agreed-upon confines. Management should strive to identify internal and external risks that may affect unit-wide operations, department operations, and process- or activity-level operations. It can be effective to approach the risk assessment as a three-step process:

Step 1: Management defines operational, reporting, and compliance objectives.
Step 2: Management identifies risks related to achieving the identified objectives.
Step 3: Management assesses the risks based on likelihood and impact to determine a response.

Step 1: Identify Objectives (Green Book Principle 6). Management within the finance department should begin the risk assessment by identifying objectives related to general financial operations and for each significant transaction cycle, such as budgeting, cash receivables, accounts receivable, accounts payable, capital assets, debt, and investments.

There are three categories of objectives that management should strive to identify: *operational objectives* (what must happen to ensure that business operations are running efficiently?); *reporting objectives* (what must happen to ensure that financial statements, budgets, and other financial records are accurate and timely?); and *compliance objectives* (what must happen to ensure compliance with the LGBFCA and other governing federal, state, or local laws?). The more specific the objectives, the easier it will be for management to identify risks to achieving those objectives in the next step. Examples of objectives related to a unit's financial process include the following:

- Financial reports that include updated budget-to-actual revenues and expenditures should be prepared and presented to the governing board monthly.
- Cash receipts are accurately recorded in the Daily Collection Report.
- Accounts receivables are accurately credited to the correct user account.
- A preaudit is performed as required by law and the preaudit certificate is attached to each contract or agreement that obligates the unit to expend public moneys.
- Access to the payroll system is restricted to authorized users.
- All journals, ledgers, and other accounting records are reconciled as part of the month-end closeout procedure.

[14] GAO, *Standards for Internal Control in the Federal Government*, at 34.

Step 2: Identify Risks (Green Book Principle 7). During the second step of the risk-assessment process, management should take steps to identify the risks that, should they occur, may negatively impact the unit's ability to achieve its objectives. It is important to understand the different types of risk and the internal and external factors that can impact those risks.

Inherent risk. Some transactions or operations are by their nature inherently risky. For example, the acceptance of cash payments always carries with it an inherent risk of loss, as cash can easily be stolen or misappropriated. This is also true for transactions involving the storage or exchange of personal property such as laptop computers and other electronic equipment. In addition, risk generally increases when the unit undertakes new or complex programs or activities, such as the administration of a new federal grant award. For example, under the American Rescue Plan Act of 2021, every municipality and county in North Carolina was eligible to receive distributions of federal financial assistance (i.e., a federal grant award) from the Coronavirus State and Local Fiscal Recovery Fund (CSLFRF).[15] The acceptance of CSLFRF funds obligated local government recipients to administer the award in compliance with the U.S. Department of Treasury CSLFRF Award Terms and Conditions and other Treasury regulations and guidance.[16] Due to the complexity of the CSLFRF award's compliance and reporting requirements, there is an inherent risk of error or noncompliance, whether intentional or not.

Change risk. Any change in business operations or personnel may increase risk. For example, the use of new technology or software is an operational change risk. The hiring of new employees or the retirement of a long-term employee may also increase risk—new hires must overcome a learning curve associated with every new position, and institutional knowledge can be lost when an employee retires or leaves.

Fraud risk. Management must always consider where there may be opportunities for an employee to commit fraud against the unit. There are three primary types of fraud to look for during the risk assessment: (1) *corruption* (e.g., bribery, bid rigging, or collusion); (2) *asset misappropriation* (e.g., embezzlement, lapping, and other fraudulent disbursement schemes); and *fraudulent financial reporting*, which involves the intentional misstatement or the omission of amounts in financial statements or accounting records with the intent to deceive the financial statement user.[17]

The following questions may serve as a starting point to help management identify areas of risk within financial operations.

- Are finance employees qualified and trained to perform basic accounting functions and to create and maintain financial reports?
- Are unit policies and procedures properly documented and updated to reflect current practices?

[15] *See* American Rescue Plan Act of 2021, Pub. L. No. 117-2, § 603, 135 Stat. 4, 228 (2021); *see also* N.C. Pandemic Recovery Office, *Funding Totals: State and Local Fiscal Recovery Funds* (last visited March 21, 2023).

[16] U.S. Department of the Treasury, *Coronavirus State and Local Fiscal Recovery Funds: Award Terms and Conditions*; *see also* U.S. Department of the Treasury, *Coronavirus State and Local Fiscal Recovery Funds* (policy webpage) (last visited April 21, 2023).

[17] GAO, *Standards for Internal Control in the Federal Government*, at 40. *See also* Association of Certified Fraud Examiners, *The Fraud Tree: Occupational Fraud and Abuse Classification System* (Fraud Tree illustrates the types of occupational fraud falling under each of the three categories of fraud listed in the text), Association of Certified Fraud Examiners, *Fraud 101: What Is Fraud?* (last visited March 21, 2023).

- Does the unit have budget violations in its audit findings?
- Is the unit current with its audits? If not, why?
- How could accounting errors occur and remain undetected?
- Which assets are most liquid and prone to theft?
- If an unauthorized purchase is made, how will it be detected?
- Could a payment be made for goods or services before it is verified that the goods or services were received?
- Are bank accounts and financial records regularly reconciled?
- Are passwords/IT system-access controls sufficient to protect unauthorized access to electronic records and databases?
- Is there a process to ensure that employees who leave no longer have electronic access to records or databases?

Step 3: Assess Risk and Determine a Response (Green Book Principles 8 and 9). Once a local unit's management has identified risks, it must decide how to respond. Not all risks are created equal. Some risks may be so remote, or the effects of such risks so inconsequential, that the unit may decide simply to accept those risks without developing controls to address them. Some risks, like natural disasters, may have such significant negative impacts that, even if unlikely, the unit must limit the risk through the purchase of insurance. For all other risks, management can implement control activities to help reduce the likelihood or impact of identified risks.

To help determine which risks should be limited through control activities, management should evaluate each risk using a likelihood/impact scale to determine priority (see Figure 9.2). Those risks that rank "very high" or "high" on the unit's risk-priority scale should be reduced through the implementation of control activities. Management must weigh the cost (time, money, effort) of implementing a control activity with the resulting benefit, keeping in mind that the cost of mitigating the risk should not exceed the cost to the unit if the risk occurred.

3. Control Activities

The third key component of the Green Book's internal control framework involves control activities. Control activities are the processes, procedures, and techniques designed by a unit's management team to help provide reasonable assurances that the unit's objectives will be met. Control activities are generally either preventative or detective.[18] *Preventive controls* are designed to deter the occurrence of an undesirable event, while *detective controls* help identity when an undesirable event has occurred. In addition to reducing identified risks, all control activities should promote an effective and efficient workplace. It is important to note that control activities can stand alone or be used in combination with other measures. Green Book Principle 10 addresses how to design control activities; Principle 12 covers the implementation of these activities. The following list describes some of the most common control activities.[19]

- **Written policies and procedures.** Written policies and procedures are a key internal control activity. These written tools can be used to communicate behavioral

[18] GAO, *Standards for Internal Control in the Federal Government*, at 48.

[19] GAO, *Standards for Internal Control in the Federal Government*, at 45–57. The Green Book includes examples of common control activities and describes ways in which management can operationalize the controls into daily operations.

Figure 9.2 Model Risk-Priority Rating System

Likelihood × Impact = Risk Priority

After rating each risk for likelihood and impact, multiply to identify which risks are highest priority to control for.

Risk Priority

Likelihood					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	**2**	**3**	**4**	**5**

Impact

Priority Rank Scale

Low	1 to 4
Moderate	5 to 9
High	10 to 15
Very High	20+

expectations, establish workflow processes, and define internal control responsibilities. Policies and procedures help operationalize control activities, and written procedures should be used to describe all major financial transaction cycles, such as accounts receivable, accounts payable, payroll, investments, cash receipts, and capital assets. A strong control environment is fostered when management requires written policies and procedures that are communicated, followed, and regularly updated to reflect current business processes.

- **Authorization and approval.** The establishment of clear authorization and approval authority helps facilitate smooth workflow processes and ensure that financial transactions are lawful and consistent with a local unit's objectives. "Authorization" involves a delegation of authority to an employee granting that employee the right to perform a specific task or responsibility. For example, a purchasing officer may be authorized to make small purchases without supervisory approval. "Approval" is the confirmation of an event or transaction based on an independent review by an employee with approval authority. Approval indicates that the approver has reviewed supporting documentation and has verified that the transaction is accurate and complies with applicable laws and regulations. For example, a department head may approve a purchase order, indicating that the purchase is necessary and lawful.
- **Segregation of incompatible duties.** Segregation of incompatible duties is often described as implementing a system of checks and balances. This control is beneficial because it minimizes the risk that a single employee will be able to commit fraud or conceal errors. Segregation of incompatible duties involves separating job duties so that no one employee can (1) *authorize* a transaction, (2) *record* the transaction

in the accounting records, (3) maintain *custody* of the asset resulting from that transaction, and (4) reconcile records that reflect the transaction. For example, if a unit's purchasing department plans to purchase ten new laptop computers, a supervisor could *authorize* the purchase via a purchase order, another employee should pay the invoice and *record* the transaction in the unit's accounting records, a third employee should verify the receipt of the computers and maintain *custody* of the assets, and a fourth employee should *reconcile* accounting records to ensure that the transaction has been accurately recorded. In small units, full segregation of incompatible duties may not be practical due to limited staff and overlapping job duties. In that case, it is recommended that a minimum of at least two employees complete any transaction. The same employee should not be responsible for both the recording and reconciliation functions. Small units should adopt compensating controls to ensure extra review of the unit's financial transactions.[20]

- **Compensating controls.** When adequate segregation of duties is not possible, a local unit should adopt compensating controls. Compensating controls involve the additional review of financial records and transactions by someone in management or by a governing board member. For example, if only two employees handle the accounts payable process, a governing board member, an internal auditor, or a member of senior management can review accounting records, bank statements, and financial reports to ensure that the accounts payable transactions are accurate, and that fraud is not going undetected. In some instances, two small units may decide to "swap" reconciliation duties to ensure an independent review of financial transactions when there is limited capacity.
- **Documentation.** Management must ensure that employees create and retain written documentation that evidences all financial transactions and facilitates the budgeting, financial reporting, and audit processes. Financial records, reports, and supporting documentation should be easily identified and be readily available to the governing board and to any auditor with whom the unit has contracted to perform auditing services.[21]
- **Reconciliation.** Account reconciliation is used to verify the accuracy of financial records through the periodic comparison of source documents and accounting records. Account reconciliations should be performed regularly, ideally after each month-end closeout.

[20] See the North Carolina Department of State Treasurer's 2015 publication *Internal Controls for Small Units of Government* for more information on how to segregate incompatible duties for small local governments, available at https://www.nctreasurer.com/internal-controls-small-unit-government.

[21] Each local government unit must retain records in accordance with the State Archives of North Carolina's *Record Retention and Disposition Schedule for Local Government Agencies*, available at: https://archives.ncdcr.gov/government/local. If a unit has received a federal grant, it likely must comply with the documentation and record retention requirements set forth in 2 C.F.R. § 200.334 (a provision of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards). Some federal grants impose a different record-retention period as part of that grant's award terms and conditions. In that case, a unit should follow the retention requirements set forth in those award terms and conditions. For example, recipients of Coronavirus State and Local Fiscal Recovery Funds (CSLFRF) are required, pursuant to the governing award terms and conditions, to retain records for a period of five (5) years after the award's period of performance. *See* U.S. Department of the Treasury, *Award Terms and Conditions*, note 16 above.

A local unit should not wait until the end of a fiscal year to reconcile its accounting records or rely on the auditor to perform reconciliations.

- **Physical controls.** Physical controls include the steps taken to protect real and personal property, including IT equipment, cash, checks, supplies, materials, and any other type of tangible asset from the risk of loss, misappropriation, or misuse. Physical controls include physical barriers, such as storing cash and valuables in locked cash boxes or safes, storing electronic equipment in locked storage rooms, or restricting access to public buildings and facilities to authorized employees.
- **Information-system controls (Green Book Principle 11).** Information-system controls facilitate the proper operation of information systems and help ensure the validity, completeness, accuracy, and confidentiality of transactions. Management is responsible for designing the unit's information system to respond to the unit's objectives and risks.[22] The information system includes both manual and technology-related information processes. General system-access controls facilitate the proper operation of the information system and include security management and access controls, such as requiring dual authentication to access certain electronic records or databases. This is a complex control area, and management should ensure that it has adequately addressed threats of cyber attacks and other issues that may result from insufficient cybersecurity controls.
- **Education and training.** Management has a duty to hire and retain competent personnel who have the proper education and training to perform job duties effectively. To ensure that employees have the necessary skills and training, employees should be allowed, or in some cases required, to attend supplemental training, conferences, or other educational events to advance skillsets and learn new competencies.

4. Information and Communication

The fourth key component of internal control under the Green Book framework is information and communication. While sometimes overlooked, this component is essential to the creation of a strong internal control system. A local government's management team should establish communication channels within the unit (Green Book Principle 14; Principle 15 deals with external communications) that provide timely and accurate information and updates (Principle 13 states that quality information should be used); inform employees of their internal control duties and responsibilities; allow employees to suggest ways to improve the system's operation; and convey a commitment by management and the unit's oversight body to the adherence of established internal control processes.[23] These communication channels can take many forms and may include emails, meetings, casual conversations, or training on how to perform specific internal control activities. Management may want to periodically verify that communication channels are effective and that employees are receiving and sharing information as intended.

[22] GAO, *Standards for Internal Control in the Federal Government*, at 51.

[23] GAO, *Standards for Internal Control in the Federal Government*, at 61.

5. Monitoring

Monitoring is the fifth and final key component of internal control. Effective monitoring of a unit's internal control system allows management to determine whether policies, procedures, and other control activities designed and implemented by management are being conducted effectively by employees. When monitoring techniques are built into the unit's business operations (Green Book Principle 16), control deficiencies may be more readily identified and corrected in a timely manner. Management is not required to review every transaction or financial report to determine whether controls are properly functioning. Instead, management can spot-check transactions, financial reports, and account reconciliations for timely completion and accuracy. For example, management can spot-check paid invoices to determine if the goods or services covered by the invoices were certified as having been received prior to authorizing payment. Management can monitor whether employees are properly segregating incompatible duties and performing other control activities as assigned. It may be helpful for management to solicit feedback from those employees responsible for carrying out the control activities in the unit to help determine if they are effective. Efforts should be made to document the performance of monitoring activities. If a breakdown in the system is identified, management may change the design of the controls to improve the operating effectiveness of the system (Principle 17 involves remediating deficiencies).[24]

Internal Control over Federal Awards

As a condition of receiving a federal award,[25] a non-federal entity, including a local government recipient and any subrecipients, must agree to maintain a system of internal control over the federal award that provides reasonable assurance of compliance with applicable laws and regulations and with the terms and conditions of the award.[26] A non-federal entity's internal control system should be modeled after the guidance offered in the Green Book or after the Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[27] Accordingly, a non-federal entity should use the five key components and seventeen principles of internal control outlined in the Green Book, and discussed herein, as the basis for the design and implementation of its internal control system over federal awards.

When it comes to managing the financial aspects of federal awards, non-federal entities must design and implement strong and robust systems of internal control. These controls should help

[24] GAO, *Standards for Internal Control in the Federal Government*, at 65.

[25] 2 C.F.R. § 200.1 defines "federal award" as "the federal financial assistance that a recipient receives directly from a federal awarding agency or indirectly from a pass-through entity." "Federal financial assistance" includes federal grants and cooperative agreements.

[26] 2 C.F.R. § 200.303.

[27] 2 C.F.R. § 200.303 (stating that internal controls over the federal award "should be in compliance with guidance in 'Standards for Internal Control in the Federal Government' issued by the Comptroller General of the United States or the 'Internal Control Integrated Framework', issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)").

ensure compliance with the financial management standards set forth in 2 C.F.R. § 200.302.[28] These standards require, among other things, that non-federal entities retain records that adequately identify the source and application of award funds. In addition, non-federal entities must create and retain accounting records that adequately track authorizations, obligations, unobligated balances, assets, expenditures, income and interest, and these records must be supported by source documentation.[29]

Any non-federal entity that expends $750,000 or more in federal awards during a fiscal year must undergo a federal single audit. As part of the single audit, the auditor will test the effectiveness of the non-federal entity's internal controls over the federal award.[30] The Office of Management and Budget's annual *Compliance Supplement* is a resource intended for auditors, but it is also a helpful tool for non-federal entities that have triggered a single audit.[31] The *Compliance Supplement* includes a Matrix of Compliance Requirements for each major federal program that indicates which of the twelve compliance requirements the auditor will test during the single audit. Part 6 of the *Compliance Supplement* includes two appendixes that provide illustrative examples of internal control—Appendix I contains examples of entity-wide controls over federal awards, and Appendix II provides examples of internal controls specific to each compliance requirement. These appendixes can serve as a starting point as the non-federal entity starts to design and implement internal controls over federal awards.

Summary

A strong internal control system is necessary to help ensure that the unit is operating at the optimal level and will achieve its goals and objectives. Properly designed and functioning controls over key financial transactions and processes will significantly reduce the likelihood that errors or fraud will occur and remain undetected. When a local unit's management team and governing board take time to implement the internal control framework outlined in the Green Book, they are signaling to all unit employees and to external stakeholders that the unit values internal control and has taken the steps required to be a good steward of public moneys and assets.

[28] 2 C.F.R. § 200.302 (setting forth financial management standards with which non-federal entities must comply in managing the federal award).

[29] 2 C.F.R. § 200.302(b)(3).

[30] 2 C.F.R. § 200.501(a) (a single audit is required for any non-federal entity that expends $750,000 or more during its fiscal year, except when the non-federal entity elects to undergo a program-specific audit.); 2 C.F.R. § 200.514 (the auditor who performs the single audit is required to gain an understanding of the non-federal entity's internal control over a federal program or programs sufficient to (1) plan the audit to support a low assessed level of control risk for major programs, (2) plan the testing of internal control over major federal programs, and, unless internal control is likely to be ineffective, and (3) perform testing of internal control as planned).

[31] Executive Office of the President, Office of Management and Budget, 2 C.F.R. Part 200, Appendix XI, 2022 Compliance Supplement (April 2022).