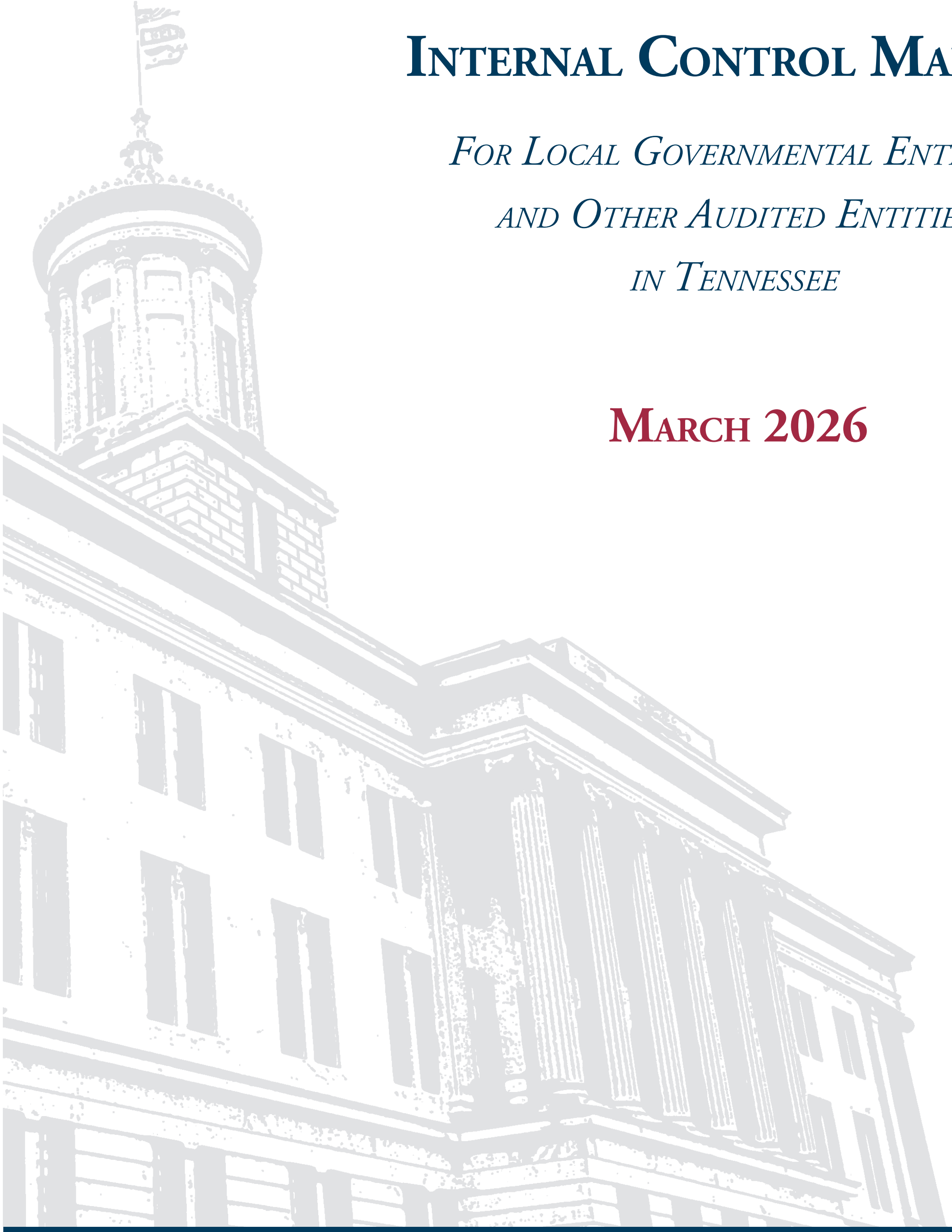
Tennessee
Comptroller
of the Treasury



Internal Control Manual

*For Local Governmental Entities
and Other Audited Entities
in Tennessee*

March 2026

Jason E. Mumpower
Comptroller of the Treasury

Division of
Local Government Audit

Table of Contents

Preface

Local governments and other entities detailed below must establish and maintain an adequate internal control system for purposes of financial reporting, managing operations, and legal compliance.

Various state statutes require the Department of Audit, Comptroller of the Treasury, to prescribe a uniform accounting system for entities that handle public funds. Those statutes require officials to adopt and use the system and the character of books, reports, and records designated by the Comptroller of the Treasury. An accounting system is defined as the methods and records established to identify, assemble, analyze, classify, record and report a government's transactions and to maintain accountability for the related assets and liabilities. Those methods would necessarily include establishing, documenting, and implementing adequate internal controls. Some of those requirements are listed below:

- State, county, municipal, and utility district offices – Tennessee Code Annotated (TCA), Section 9-2-102
- Emergency communication districts – TCA, Section 7-86-304
- Development district offices – TCA, Section 13-14-108
- Human resource agencies – TCA, Section 13-26-109
- Public charter schools – TCA, Section 49-13-111(m)
- Regional development authorities – TCA, Section 64-7-105

In addition, TCA, Section 9-18-102(a) was amended to expressly require each county, municipal, and metropolitan government to establish and maintain internal controls.

The U.S. Office of Management and Budget (OMB) has established internal control guidance for all entities that receive federal awards at Code of Federal Regulations (CFR) 200.303. This guidance requires all entities to establish and maintain an effective system of internal control over federal awards. The OMB guidance further recommends implementing a system of internal control in accordance with internal control standards published by the U.S. Government Accountability Office (GAO) in *Standards for Internal Control in the Federal Government* (Green Book), as one method of complying with CFR 200.303.

The *Internal Control Manual for Local Governmental Entities and Other Audited Entities in Tennessee* (the "Internal Control Manual") should be used by all local governments listed above (including entities created by interlocal agreements between those entities) as well as any other entity that has a similar statutory requirement. Other entities, including those participating in contracts with the State of Tennessee that include contractual provisions requiring the establishment of internal controls, should consider the provisions of this manual when establishing internal controls.

This manual summarizes and gives examples of internal controls based on standards for establishing internal controls published in the May 2025 version of GAO's Green Book. Accordingly, this manual refers to different levels of oversight responsibility as follows:

- Governing body refers to the county commission, city council, board of directors, or similar authorities.
- Oversight body refers to an appointed body designated to perform oversight at the direction of the governing body.
- Management refers to elected officials or employees who have direct responsibility for the day-to-day operations of the entity including the implementation of internal controls.

Summary:

This internal control manual is developed by the Division of Local Government Audit as guidance for governing and oversight bodies and the management of entities in Tennessee. Management is responsible for designing and implementing a system of internal control. Auditing standards do not allow auditors to design or implement your system of internal control and auditors cannot be a substitute for a system of internal control.

This manual is based on principles, as opposed to providing a detailed method of implementing internal controls. This is because the manual is based on the GAO Green Book, which is principles based as well. In addition, it would be physically impossible to develop a detailed internal control implementation plan because of the variety of entities that operate in Tennessee.

While the 17 Principles presented in this manual are recommended, use of these exact principles are not required. **Establishing and maintaining a system of internal controls is required by state and federal law. Implementing the five (5) components of internal control is mandatory.**

This manual is effective upon release, unless otherwise noted.

Introduction

Overview of Internal Control

The U.S. Government Accountability Office (GAO) has established a common definition of internal controls, standards, internal control components, principles and attributes. The document that contains this information is often referred to as the Green Book. Because this GAO Green Book framework is widely accepted, it will be used as the basis for all internal control matters related to entities covered by this internal control manual as outlined in the preface.

Definition of Internal Control

Internal control is a process that is developed by the entity to provide reasonable assurance that the following categories of objectives will be achieved:

- Operations – effectiveness and efficiency of operations;
- Reporting – financial reporting will be reliable; and
- Compliance – compliance with applicable laws, regulations, contracts and grant agreements.

The above definition "reflects certain fundamental concepts." Those concepts are:

- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.
- Internal control comprises the plans, methods, policies, procedures, and other mechanisms used to fulfill the mission, strategic plan, goals, and objectives of the entity.
- Internal control is an integral part of the organization not a separate system within the organization.
- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is affected by people. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control increases the likelihood that an entity will achieve its objectives. However, it can only be expected to provide reasonable assurance, not absolute assurance, that all of the organization's objectives will be met.

While each entity may identify its mission, strategic plan, objectives, and plans for achieving its objectives in different ways, the Green Book approaches internal control through a hierarchical structure of five (5) components and seventeen (17) principles. The Green Book also contains additional information in the form of attributes. In this manual, attributes are presented under the heading title: "This Involves." These attributes provide further explanation of the principles and documentation requirements.

Definition of an Internal Control System

An internal control system comprises a coordinated and ongoing set of activities, designed to provide reasonable—not absolute—assurance regarding the achievement of the entity's strategic, operational, reporting, and compliance objectives.

An effective internal control system increases the likelihood that an entity will achieve its objectives. Regardless of how well the system is designed, it is still subject to risks from events outside the entity's control, faulty or biased management decisions, human error, management override, collusion, or unsuitable objectives.

The Five Components of Internal Control

1. Control environment – the foundation for an internal control system
2. Risk assessment – assesses the risks facing the organization as it seeks to achieve its objectives
3. Control activities – the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system
4. Information and communication – the quality information management and personnel communicate and use to support the internal control system
5. Monitoring – activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews

There is a direct relationship between the entity's objectives, the five components of internal control and the organizational structure of the entity. The five components apply to all three categories of objectives and all levels of the entity's organizational structure. The seventeen (17) principles support the components of internal control.

Summary

A good internal control framework is essential to providing reasonable assurance that organizations are achieving their objectives. Such objectives include, but are not limited to, utilizing public resources in compliance with laws, regulations and budgetary limitations. An adequate control framework will provide information that helps detect errors and fraud, and provides reasonable assurance that financial reports are accurate. It will limit the opportunity for theft or unauthorized use of assets, including cash, inventory, and capital assets.

The remainder of this manual is designed to give an overview of the seventeen (17) principles related to the five (5) components of internal control listed above as they relate to the objectives and organizational structure of an organization. It is not intended to be an exhaustive analysis of internal control. Rather this manual provides examples regarding the development of an internal control system within the framework addressed in the Green Book. The examples are not intended to be mandatory implementation guidance. They are merely examples for your consideration. Developing an adequate internal control system requires written documentation as well as continual analysis and modification to address changing circumstances. Officials should identify and address their specific objectives within the framework set out in the Green Book or use a similar comprehensive framework that includes each of the five components of internal control.

Component 1

Control Environment

GAO Green Book Principles 1 through 5

The control environment is the foundation for any effective internal control system. There are five (5) principles related to the control environment

1. ***The oversight body and management should demonstrate a commitment to integrity and ethical values.***

This involves:

- Setting the foundational tone at the top
  - Oversight body and management personnel should exhibit integrity and ethical values expected across the entity through their actions, attitude, and communication. Management should demonstrate ethical behavior through consistent actions and decisions, reinforcing values throughout the organization.
  - Setting the tone at the top is not solely the responsibility of the oversight body and management personnel. Employees play a vital role in creating a positive workplace culture and environment.
- Establishing standards of conduct
  - Standards of conduct outline how an organization's employees should conduct themselves while achieving organizational goals.
  - Management personnel should regularly reinforce standards of conduct through the use of policies and procedures, guidelines, and training.
- Adherence to standards of conduct
  - Oversight body and management personnel should analyze how employees are implementing and following the standards of conduct.
  - Management should determine tolerance levels for deviations from the standards of conduct.

Examples:

Require employees to complete an annual form identifying any conflict of interest that exists or assert that he/she does not have any conflict of interest with any vendor, provider, supplier or other individual within the organization or external to the organization. Require employees to report, within five (5) days any conflict of interest that the employee becomes aware of that has not been previously reported.

The oversight body and management develop, regularly review, and update a code of professional conduct that is presented to employees at their hiring and is reviewed annually with all employees.

Management stresses ethics, compliance with laws and regulations, and following internal controls at all employee meetings.

Management encourages and promotes psychological safety, ethical incentives, and escalation procedures for reporting misconduct (i.e., whistleblowing).

2. The oversight body should oversee the entity’s internal control system.

This involves:

- Establishing an oversight structure
  - The oversight body should oversee entity operations, offer constructive criticism to management, and verify the entity’s actions align with the standards of conduct.
  - The oversight body should provide objective, informed oversight, with emphasis on independence, competence, and accountability.
  - The oversight body should be composed of people with an internal control mindset, specialized skills relevant to the organization, financial expertise, information technology expertise, and legal expertise.
- Oversight of the internal control system
  - The oversight body oversees the entity’s internal control system.
  - The oversight body ensures that management's design, implementation, and operation of the entity's organizational structure support the processes necessary for the oversight body to effectively fulfill its responsibilities.
- Remediation of deficiencies
  - Management should report internal control deficiencies to the oversight body.
  - The oversight body will provide direction in the remediation of the deficiencies. Additionally, the oversight body is responsible for overseeing the remediation.

Examples:

- The conflict of interest form, code of professional conduct, and internal control manual are presented and explained to the governing body. The governing body approves each document.
- The governing body appoints an oversight body composed of at least five individuals. The collective knowledge of those individuals should include: legal representation, accounting, investing and cash management, building codes, internal control, computer operations and security, grants management, debt marketing and financing. The oversight body should ensure that it has access to competent outside experts when it does not have requisite knowledge in these or other areas of expertise.
- The governing body or appointed oversight body reviews the annual audit report for internal control issues, meets with management officials, and ensures appropriate action is taken to correct deficiencies.

3. ***Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.***

This involves:

- Establishing an organizational structure
  - The structure should be developed with an understanding of the overall responsibilities and risk of the organization in mind.
  - When establishing the structure, management should define reporting and communication lines. Well defined lines of communication at all levels ensure quality of information flows freely.
  - Management should regularly evaluate the organizational structure to determine how the entity is responding to new objectives, complying with new laws, and responding internal control risks and deficiencies.
- Assigning responsibility and delegating authority within the organizational structure
  - Someone responsible for the entity should oversee maintenance of the structure and assignment of the structure to others.
  - With segregation of duties in mind, management should delegate responsibility of the structure to the extent necessary.
- Documentation of the internal control system
  - Documentation should include the who, what, when, where, and why of internal controls.
  - Management should consider the costs of documentation versus the benefits to the organization.

Examples:

- Create an organizational chart as an overview of the lines of authority and responsibility.
- Develop a formal, written internal control document that focuses on individual responsibilities within each area of functional responsibility (e.g. accounts payable/purchasing).

4. ***Management should demonstrate a commitment to recruit, develop, and retain competent individuals.***

This involves:

- Developing expectations of competence
  - Competence is the ability to achieve assigned goals. It involves having the necessary knowledge, skills, and abilities, which are primarily acquired through professional experience, training, and certifications.
  - Management should consider the established standards of conduct when evaluating competence. The expectation of competence should be to a level which allows employees to complete their responsibilities and understand internal control.
- Recruitment, development, and retention of individuals
  - Recruit – Management should evaluate a candidate's competence and organizational fit in the interview process.

    - Train – Provide employees with opportunities to expand their knowledge and skills pertinent to their organizational objectives.
    - Mentor – Evaluate the employee's performance and provide necessary feedback.
    - Retain – Offer rewards to encourage and sustain desired performance levels.
- Succession and contingency plans and preparation
    - Succession plans offer a guide for management to replace skilled employees who have transitioned to different roles.
    - Contingency plans promote the need for cross training in the event of sudden personnel changes.

Examples:

Management develops a job description for the chief accountant, requiring (1) at least five (5) years of experience at a comparable organization; (2) at least three (3) years of supervisory experience; (3) computer skills that include a good working knowledge of word processing, spreadsheets and accounting software; (4) knowledge of generally accepted governmental accounting principles; and (5) proficiency in written and oral communication.

Annual training will be provided to ensure that the chief accountant stays well informed about changes in accounting and reporting, changes in laws that affect payroll and payroll related activities, changes in laws that affect purchasing, grants administration and emergency management training. As software is updated, adequate training will be provided to ensure continued proficiency in computer skills. The chief accountant will communicate significant matters to staff through annual or semi-annual training events.

Employees are encouraged to obtain certifications such as Certified Public Accountant (CPA), Certified Government Financial Manager (CGFM), Certified Municipal Finance Officer (CMFO), or Certified County Finance Officer (CCFO) and the entity agrees to pay for continuing professional education requirements.

Employees are cross trained for specific crucial tasks that are the responsibility of other employees.

5. Management should evaluate performance and hold individuals accountable for the internal control responsibilities.

This involves:

- Enforcing accountability
    - Accountability for internal control performance influences daily decision-making, attitudes, and behaviors. Management ensures personnel are held accountable through methods like performance reviews and corrective action plans.
    - The oversight body should hold management and the entire organization accountable for its internal control responsibilities.
- Consideration of excessive pressures
    - Pressures are influenced by organizational objectives and industry demands.

  - Excessive pressures can be managed by rebalancing workloads and increasing available resources. If pressures are not managed, employees may feel the need to take shortcuts.

Examples:

Management develops a policy requiring a job evaluation for each new employee at 30 days, 90 days, 6 months, and 1 year. After the first year, job evaluations will be conducted annually. New employees have a 6-month probationary period. During that time, a corrective action plan will be developed for any deficiency noted as a result of an evaluation. If the same deficiency is noted in a subsequent evaluation, a recommendation for terminating employment or extending the probationary period will be considered. Significant improvement is expected prior to the 6-month evaluation, when a recommendation will be made to extend the probationary period, terminate employment or retain the individual as a non-probationary employee.

Management requires service organizations such as outside billing and collection companies to provide a Service Organization Control (SOC) report. This report is a method of holding service organizations accountable for their internal control systems.

Segregation of duties and rotating job responsibilities are methods of implementing internal controls. These methods also help to identify and allow for the alleviation of excessive workload pressures on individual employees.

Employees who work excessive overtime should be evaluated for workload pressure.

Component 2
Risk Assessment
GAO Green Book Principles 6 through 9

Management should assess internal and external risks and perform risk assessments regularly in order to achieve objectives. Generally speaking, risk assessment means asking questions about what could go wrong. There are four (4) principles related to risk assessment.

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

This involves:

- Defining the entity's objectives in specific and measurable terms
  - Objectives and terms should be clear and easily understood by everyone.
  - Management's objectives should be specific and aligned with the entity mission and strategic goals.
  - Objectives should be put in measurable terms in order to gauge progress.
  - External requirements set by legislators, regulators, and standard-setting bodies and internal requirements set by the standards of conduct, oversight structure, organizational structure, and expectations of competence as part of the control environment should all be considered.
  - Management should evaluate the objectives and, if necessary, revise them to more closely align with requirements.
- Defining the entity's tolerance or threshold for risk
  - Risk tolerance is the acceptable degree of variation between an organization's performance and its objectives.
  - Risk tolerances should be in specific and measurable terms in order for them to be measured against performance.
  - Risk tolerances depending on the category of objectives:
    - Operations objectives – acceptable degree of performance variation while still achieving operations objectives
    - Nonfinancial reporting objectives – level of precision and accuracy necessary to meet user needs
    - Financial reporting objectives – judgment about materiality involving both qualitative and quantitative considerations
    - Compliance objectives – acceptable degree of performance variation in meeting compliance requirements of the applicable laws, regulations, and external standards

Examples:

Surety bonds and/or employee dishonesty insurance should be purchased to mitigate the risk of loss of funds due to errors, irregularities, or fraud.

Implement sufficient internal controls to reasonably ensure that the organization does not incur losses exceeding the established threshold (e.g., a certain dollar amount) in any fiscal year.

Surety bonds and/or employee dishonesty insurance will be obtained for any individual who handles more than $15,000 annually or as required by law. Reevaluations of surety bond coverage needs should be made when any change in personnel occurs, either through reassignment, new hire, etc. If total revenue increases by more than ten (10) percent of budgeted revenue (i.e. a risk threshold), a reassessment of surety bond coverage and internal control will be conducted.

All benefit applications should be processed within 10 business days of receipt. Management decides that a risk tolerance of 8-12 business days would be appropriate for the benefit application approval process.

7. *Management should identify, analyze, and respond to risks related to achieving the defined objectives.*

This involves:

- Identification of risks
  - Risk is the possibility that an event will occur and adversely affect objective achievement.
  - Risk assessments should be performed on a periodic and ongoing basis to evaluate how internal controls are functioning. Management should recognize events, trends, or weaknesses that could disrupt operations or objectives. When internal controls are deficient, management should consider ongoing risk assessments.
  - Management should consider:
    - Inherent risk – risk to an entity in the absence of management's response to the risk.
    - Residual risk – risk that remains after management responds to inherent risk.
  - Internal risk factors include an entity's complex nature, experience and training of personnel, organizational structure, information system and use of new and emerging technology, and quality of data available.
  - External risk factors include new and amended laws, economic conditions, information technology developments, outsourcing, national security, and world events and disasters.
  - Methods for identifying risks can encompass both qualitative and quantitative ranking activities, forecasting and strategic planning, data analytics, and the evaluation of internal control deficiencies identified through internal and external monitoring.
- Analysis of risks
  - Management should analyze risks on a periodic and ongoing basis to determine the impact they are having on the entity's ability to achieve objectives.
  - Management assesses the significance of entity-wide and transactional risks by evaluating:
    - the magnitude of impact – likely impact on an entity's ability to achieve objectives influenced by size, pace, and duration.

        - likelihood of occurrence – possibility that an unintended result will occur.
        - nature – whether the risk arises from fraud or from other unusual transactions.
- Response to risks
    - Management should respond to risks in one of the following ways to lower the risk to a tolerable level.
        - Acceptance – no responsive action is taken.
        - Avoidance – the process or part of the process that is causing the risk is stopped.
        - Reduction – action is taken to reduce the likelihood or magnitude of the risk.
        - Sharing – action is taken to spread the risk across the entity or external parties.
    - Management should design internal controls based on what responsive action they choose to take.
    - After responsive measures have been taken, management should consider any residual risks.
    - Management should document results of periodic and ongoing risk assessments. This includes the identification, analysis, and responsive measures that were taken.

Example 1:
Operations, Reporting, and Compliance Risk:

Objectives – revenue will be properly recorded in compliance with generally accepted accounting principles, receipted, and deposited in accordance with laws, regulations, and contractual requirements

Risk (What could go wrong?) – revenue may not be recorded in compliance with generally accepted accounting principles, may not be receipted or deposited, and, as a result, reporting, contractual, and legal requirements will be violated

Response to risk – the receipting, depositing and accounting functions will be handled by different individuals; separate cash drawers will be used by each individual receiving funds and will be reconciled at the end of the day to the daily cash report; prenumbered receipts will be issued; daily cash reports will be prepared and reviewed by a manager; training will be structured to ensure that all individuals understand the relevant laws, reporting requirements, contractual requirements, program requirements, and any changes in same; monthly reports will be prepared and reviewed to determine reasonableness and accuracy and report variances will be investigated; and budgetary comparisons will be performed to determine reasonableness and accuracy and variances will be investigated

Example 2:

The following list presents examples of other types of entity-wide objectives that might be considered. Each objective involves certain risks that must be addressed and each risk will require the implementation of internal controls.

Operations Objectives

- Ensure that the entity's resources are adequately safeguarded
- Provide taxpayer services efficiently and effectively
- Limit the need for tax increases
- Provide for the long-term stability of the municipality
- Provide a stable and rewarding work environment for employees

Reporting Objectives

- Provide timely interim financial reports and schedules for evaluating the results of operations
- Issue timely financial reports that comply with generally accepted accounting principles, the additional requirements of the Tennessee Comptroller of the Treasury, and federal grant requirements

Compliance Objectives

- Comply with all relevant laws, regulations, contracts, and grant agreements

8. ***Management should consider risks related to fraud, improper payments, and information security when identifying, analyzing, and responding to risks.***

This involves:

- Identifying risks related to fraud, improper payments, and information security
    - Identification of risks related to fraud, improper payments, and information security follow the same periodic and ongoing processes as all other risks.
    - An analysis to identify the root cause of internal control deficiencies can help management when trying to identify risks.
    - Management should consider information from internal and external parties, i.e., office of inspector general, internal and external auditors, grantors, Comptroller of the Treasury, personnel, service organizations and other parties, to identify risks related to fraud, improper payments, and information security.
- Examining types of fraud and fraud risk factors
    - Fraud involves obtaining something of value through willful misrepresentation. Types of fraud include the following:
        - Fraudulent reporting – intentional misstatements or omissions of financial or nonfinancial information.
        - Misappropriation of assets – unauthorized acquisition, use, or disposal of an entity's assets.
        - Other illegal acts – Intentional violations of laws or regulations related to financial or nonfinancial activities.

    - In addition to fraud, management should consider other forms of misconduct, such as waste and abuse.
        - Waste involves careless, extravagant, or purposeless use of resources.
        - Abuse refers to actions that fall short or deviate from what a prudent person would deem reasonable and necessary under the given facts and circumstances.
    - In addition to fraud, management should also consider the threat of management override of controls.
    - Fraud risk factors
        - Incentive/pressure – motive for the act
        - Opportunity – ability to act or overcome controls
        - Attitude/rationalization – ethical reconciliation by the actor
- Examining types of improper payments and improper payment risk factors
    - Improper payments are any payments that should not have been made or that were made in an incorrect amount. Types of improper payment include the following:
        - Overpayments – payments in excess of the amount due, payments made to incorrect vendors, payments for goods not received, and duplicate payments.
        - Underpayments – payments in which the intended recipient did not receive.
    - Improper payment risk factors:
        - New programs or activities
        - Complex programs or activities
        - Volume of payments
        - Whether payments are made through external parties
        - Major changes in funding, legal authority, practices, or procedures
        - Personnel experience and training
        - Entity reliance on recipient eligibility determination
        - Internal control deficiencies that might hinder payment processing
        - Similarities to other susceptible programs or activities
        - Improper payment estimates
        - Lack of information to confirm eligibility or verify accuracy
        - Risk of fraud related to the program or activity
- Examining types of information security risk and information security risk factors
    - Information security risk is the risk to entity operations, assets, and personnel due to unauthorized access, use, disclosure, disruption, modification, or destruction of information or informational technology. Types of information security risk include the following:
        - Unauthorized access – attackers compromise the integrity of a system.
        - Exploitation of personnel – attacks that trick users into revealing unauthorized information.
        - Installation of malicious software – installation of a file that intentionally corrupts or steals data.
        - Automated attacks – automated attacks through the use of bots, artificial intelligence, or machine learning software.

        - Undetected errors – altered data by an attacker that is not readily detected by the entity.
        - Threats to physical environment – fire, loss of electricity, loss of climate controls, or natural disasters.
    - Information security risk factors
        - Complexity of an entity's information technology system
        - New technologies
        - Outdated technology
        - Decentralized operating system or network
        - External party access to an entity's operating system
        - Lack of knowledgeable or skilled personnel
- Analyzing and responding to identified risks
    - Management should analyze and respond to identified fraud, improper payment, and information security risks so they are effectively and timely mitigated.
    - Management's response to identified fraud, improper payment, and information technology security risks should be consistent with their response for all other risks.

Example:
Operations and Compliance Fraud Risk:

Objectives – revenue will be properly recorded, in compliance with generally accepted accounting principles, receipted, deposited, and expended in accordance with laws, regulations, and contractual requirements.

Fraud Risk (What can go wrong?) – cash can be stolen and the individual taking the cash cannot be identified; grant funds can be expended for personal purchases or other nonallowable purchases.

Response to risk – the receipting, depositing and accounting functions will be handled by different individuals; separate cash drawers will be used by each individual receiving funds and will be reconciled at the end of the day to the daily cash report; prenumbered receipts will be issued; daily cash reports will be prepared and reviewed by a manager and variances will be investigated; grant expenditures will be reviewed by a manager and expenditures exceeding $5,000 (i.e. a risk threshold) will require two levels of approval.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

This involves:

- Identification of changes
    - Identifying, analyzing, and responding to significant changes should be part of the entity's risk assessment process.
    - Management should anticipate significant changes by using a forward-looking process. This allows management to render a timely response.

    - Changes to the entity's internal conditions may include changes to programs or activities, oversight structure, organization structure, personnel, and technology.
    - Changes to the entity's external conditions may include changes in government, the economy, technology, laws, regulations, and the physical environment.
- Establishing a change assessment process
    - Management should establish a documented change assessment process, so the internal control system can be quickly and consistently adjusted in response to changes in risk.
    - The change assessment process should include:
        - Steps for timely identification of risks related to significant change.
        - Considerations for management to effectively analyze risk related to significant change.
        - Considerations to facilitate its ability to quickly adapt the entity's internal control system.
- Identifying, analyzing, and responding to risks related to significant changes
    - Risk assessment and internal control system revision should occur before implementation of new programs or significant changes to existing programs.
    - Management should conduct ongoing risk assessments and update existing risk assessments due to the constant change of conditions surrounding the entity.

Example:

Management will review all new grant applications and grant agreements and attend training to identify potential risks due to changing grant requirements or other circumstances. Management will, at least annually, consider technological developments, employee turnover, new programs, new accounting standards, new laws and regulations, and economic growth or decline to determine whether or not changes in internal controls need to be implemented. Recommendations for changes will be reviewed and implemented as necessary. The implementation will include training for all personnel involved in the processes that require change.

Component 3
Control Activities
GAO Green Book Principles 10 through 12

Control Activities are the actions management establishes through internal control policies and procedures to mitigate risks to achieving the entity's objectives to acceptable levels. Fundamental examples of control activities include issuing receipts and purchase orders, reconciling the bank statement, and segregation of duties. The Division of Local Government Audit has developed illustrative Internal Control - Segregation of Duties Checklists that are available for several county offices. The checklists are mainly designed for smaller offices, which may have difficulty establishing adequate segregation of duties. The concepts demonstrated in the Internal Control Checklists can be used to implement segregation of duty controls in other offices. There are three (3) principles related to control activities.

10. Management should design control activities to mitigate risks to achieving the entity's objectives to acceptable levels.

This involves:

- Responding to identified objectives and risks
    - Management designs and modifies existing control activities in response to risks to achieve an effective internal control system.
    - Control activities primarily focus on the risk assessment aspect of internal control.
- Designing appropriate types of control activities
    - Control activities should be based on specific threats and the risks involved, differences in objectives, managerial judgment, size and complexity, environment, and sensitivity and value of data.
    - Common categories of control activities:
        - Top-level reviews
        - Functional or activity level reviews
        - Performance Measures
        - Management of human capital
        - Information processing
        - Physical control over vulnerable assets
        - Restrictions for resources and records
        - Authorization of transactions
        - Accurate and timely transactions
        - Documentation of transactions
        - Service organization oversight
        - Segregation of duties
        - Program-related
        - Fraud-related
        - Improper-payment-related
        - Compliance-related

- Designing automated and manual control activities
    - Control activities can be designed and implanted in an automated, partially automated, or manual manner. Automated controls are the most reliable because they're not as susceptible to human error.
    - Information technology control activities consist of:
        - General control activities – manual or automated activities that apply to all or a large segment of an entity's information technology.
        - Application control activities – automated activities that incorporated into a software application.
        - User control activities – partially automated activities performed by people.
- Designing preventative and detective control activities
    - Preventative controls are intended to avoid an event or result.
    - Detective controls are intended to discover and timely correct an event or result after it occurs.
    - Management strategically designs a balanced combination of preventive and detective control activities to mitigate risks to an acceptable level, with a focus on prioritizing preventive controls where appropriate because of their cost effectiveness.
- Designing control activities at various functional and structural levels
    - Entity-level control activities are controls designed to reduce risks that have a pervasive effect on multiple components of an entity.
    - Transaction control activities are controls designed to reduce risks that affect specific business processes. When designing transaction control activities, management evaluates information processing objectives such as completeness, accuracy, and validity.
    - When management is designing entity-level control activities and transaction control activities, management determines how precise the business processes must be to meet entity objectives and reduce related risks. Management should evaluate the level of aggregation, consistency, the timing of performance, and the correlation to business processes in determining precision.
- Establishing and maintaining adequate segregation of duties among employees
    - Segregation of duties helps prevent fraud, waste, abuse and management override of controls through the separation of control activities related to authority, custody, and accounting of operations.
    - If appropriate segregation of duties is not attainable in a business process, management should consider alternative control activities to reduce risk.

Example 1 – Cash Receipts:

Management has determined that one of its objectives is to provide cost effective reliable services to the residents of the local entity. Several of the services involve collection of cash from sources such as property taxes, law enforcement, courts, solid waste management, and other utilities. Management has identified the different types of risks associated with each of these activities. This example addresses the types of control activities that should be considered to address risks related to cash collections and to address operational, reporting, and compliance objectives. This is only an example. It is not designed to be all inclusive nor is the example relevant to all entities or all cash collection locations. The example does serve to illustrate that even simple transactions like accepting cash have many risk variables.

Responsibility for each step of cash handling and recording should be clearly established. If possible, the employees who receive cash collections (cashiers) should not be the same employees who maintain the books and records (bookkeepers). Entities are encouraged to **not** accept cash when possible (accepting checks, money orders, and credit cards is generally less susceptible to employee fraud.)

Consider the following issues related to controls over cash receipting.

- Who receives and opens mail-in collections
- Who issues receipts for mail-in collections
- Determining all mail-in receipts are recorded
- Establishing separate cash drawers for cashiers
- Establishing separate passwords for each computerized receipting station
- Issuing prenumbered receipts
- Ensuring customers receive a copy of receipts
- Conspicuously posting a sign that reads "You must receive an official receipt or your transaction is not complete."
- Stamping checks "For Deposit Only" including a bank account number
- Accepting credit card payments including credit card transaction fees
- Avoid using a manual receipt book. If a manual receipt book is utilized, it must be an official receipt book.
- Receipt format. Each receipt should include a place to indicate the purpose, type of payment (i.e. cash, check, money order, credit card, etc.), and include a place for an employee's initials.
- Posting or updating accounting records for daily receipts and deposits
- Standardizing daily check-out procedures - each employee should checkout to a certain amount of cash each day.
- Depositing the daily collections. Deposit slips should be itemized between cash, checks, money orders, credit card receipts, etc.
- Depositing cash collections intact. Each deposit should equal all receipts for a given day.
- Taking the deposit to the bank and obtaining a bank deposit receipt.
- Overnight storage of cash for safekeeping.

- Verifying the amount on the bank deposit slip with the daily check-out sheets and/or accounting records
- Examining computerized audit logs for unusual receipt transactions

All these processes should be monitored (see Component 5) on an ongoing basis. Monitoring may involve staff employees, management, internal audit, outside contractors, or some type of computer analytics or computer application controls. In addition, establishing an internal -audit function for the entity is a good overall internal control for receipting.

Example 2 – Cash Disbursements:

The following disbursement transactions pose various types of risks. The list is not intended to be all-inclusive. Establishing an internal audit function for the entity is a good overall internal control for disbursements. Control activities should be implemented to mitigate risks related to the different types of disbursement transactions:

Disbursements/Expenditures	**Control Activity Considerations**
All Purchases	Requisitions, purchase orders, dual signature on checks, controlling the signature plate, obtaining receiving documentation, review documentation before issuing check, adequate segregation of duties, performing bank reconciliations monthly, examining cancelled checks and outstanding checks, employee dishonesty insurance, computer analytics software, etc., monitor the activity controls effectiveness
Heavy Equipment Purchases	Accept bids, utilize bid specifications, establish conflict of interest policies, establish a committee to oversee the process
P-Card and Credit Purchases	Establish a use and abuse policy, control the number of and access to P-cards and credit cards, assign purchase limit, assign purchase restrictions (e.g. for certain stores or for travel only), receive an itemized statement by department, employee, etc., review transactions regularly
Travel	Develop a travel policy (rates, what is covered, lines of approval authority, abuse, etc.), follow controls at all purchases above, monitor compliance with the policy
Cell Phones Mobile Devices Monthly Charges	Establish a use and abuse policy, control the number of and access to cell phones or other mobile devices, assign airtime/minutes and data usage limits, assign use restrictions (e.g. for business use only), receive an itemized statement by department, employee, etc., review transactions regularly
Investments	Develop an investment policy, establish an investment committee
Derivatives	Follow the Comptroller's policies, develop a derivative policy, establish an oversight and advisory committee, establish conflict of interest policies, have the transaction approved by the governing body

Information Technology Purchases	Major IT purchases should involve the finance and IT departments as well as affected department heads, the desired information and output requirements must be very clear, should use bids, RFPs, or other formal process, utilize bid specifications, establish conflict of interest policies, establish a committee to oversee the process
Insurance	Develop an insurance policy, consider an insurance committee, establish conflict of interest policies, should use bids, RFPs, or other formal process
Major Building Construction	Must be approved by governing body, develop a policy (i.e. type of contracts, type of involvement by outside engineers, architects, construction managers, insurance requirements, etc.), should use bids, RFPs, or other formal process, utilize bid specifications, establish conflict of interest policies, establish a committee to oversee the process
Inventory (Supplies, Gasoline, Parts, Etc.)	Maintain perpetual inventory records, limit access to inventory, maintain usage records by employee, perform physical inventory counts and reconcile the amount to inventory records

11. Management should design general control activities over information technology to mitigate risks to achieving the entity's objectives to acceptable levels.

This involves:

- Response to Risks
  - Management should respond to information security risks by designing general control activities over the entity's information technology system.
  - The backbone of an entity's information technology system depends on the selection, development, and implementation of control activities over information technology
- Design of the entity's information technology system
  - Management should design the information technology infrastructure, platforms, and software to support and automate the entity's business processes.
  - When designing the information technology infrastructure, management should consider factors such as the human intuition required to develop and maintain, costs to develop internally or outsource, desired level of control over resources, and impact on operations
- Design of appropriate types of general control activities
  - General control activities are actions established through policies and procedures that apply to a large segment of an entity's information technology system to enhance confidentiality, integrity, and availability.

- General control activities include the following:
  - Security management – a separate process, addressing all components of internal control, for responding to information security risks.
  - Logical and physical access – protection against unauthorized access, use, disclosure, disruption, modification, or destruction.
  - Configuration management – continuous development and maintenance of operating and security features for the information technology system.
  - Segregation of duties – the separation of responsibilities for designing, testing, and implementing information systems for prevention of fraud, waste, and abuse.
  - Contingency planning – safeguards critical and sensitive data, ensuring that essential operations can continue uninterrupted or be swiftly resumed during unexpected events.

Example:

To enhance the quality and scope of services by maximizing the use of grant resources, the local government has implemented an upgraded grants administration information system. As part of this rollout, management has identified new risks and is establishing controls to ensure the system supports this strategic objective.

A designated management-level employee will conduct regular coordination meetings with department heads to ensure the grants administration system remains aligned with organizational goals and responsive to emerging risks. These meetings will focus on the following key areas:

- Grant Opportunity Evaluation - Identify and assess available grant opportunities to determine their potential to enhance or expand existing services.
- Compliance and System Impact Review - Monitor changes in grant reporting requirements and evaluate their implications for system functionality, including software and hardware maintenance schedules.
- System Enhancement Prioritization - Review and prioritize system modifications needed to accommodate evolving reporting standards and operational needs.
- IT Controls Assessment - Evaluate the adequacy and effectiveness of general IT controls, including data integrity, access controls, and system security.
- Staffing and Training Needs - Assess current staffing levels and training programs to ensure personnel are equipped to manage and utilize the grants system effectively.
- Risk Management - Identify and evaluate internal and external risks that could impact the effectiveness of the grants administration process, and develop mitigation strategies accordingly.

Grant Controls:

- Centralized Grant Processing
  - Control: All grant applications will be processed through a central grants processing division.
  - Purpose: Ensures consistency, reduces duplication of effort, and promotes compliance with eligibility and reporting requirements.

- Restricted System Access
  - Control: Only designated individuals, approved by the department head, will have access to enter contracts in the computerized accounting system.
  - Purpose: Prevents unauthorized entries or modifications.
- Pre-approval Requirement for Expenditures
  - Control: Expenditures related to a grant contract cannot be entered until the contract has been formally approved.
  - Purpose: Ensures funds are spent only for authorized and valid purposes.
- Information Technology Access Restrictions
  - Control: System entry restricted by logins and periodically updated passwords. IT staff access to accounting staff credentials should be restricted. Entities may also need to restrict access to physical servers and equipment.
  - Purpose: Reduces risk of unauthorized system access or manipulation of grant records.
- System Training Requirements
  - Control: Department heads must complete computer application and systems training schedules by the start of each fiscal year, with updates provided for significant changes.
  - Purpose: Ensures managers are trained on system use and updates, reducing user error.
- Grant Administration Staff Training
  - Control: Employees involved in grant administration will complete annual software training.
  - Purpose: Ensures staff remain competent in grant system use, preventing errors in reporting and compliance.

12. Management should implement control activities through policies and procedures.

This involves:

- Documentation of control activities through policies and procedures
  - Management sets up control activities by creating policies that outline expectations and procedures that detail specific actions to implement these policies, all aimed at reducing risks to acceptable levels to achieve the organization's objectives.
  - Management, along with those in key roles, should define policies and procedures for each unit within the entity's organizational structure using management directives, administrative policies, and operating manuals.
- Periodic review of control activities
  - If there are changes in entity processes, personnel, laws, regulations or information technology, management should review the process in a timely manner to verify that control activities are designed and functioning properly.

Example:

The local government has determined that one of its policies is to have accurate, complete and timely financial reporting throughout the year and at year end in compliance with local and state statutes and management's goals. To accomplish this, related risks will need to be considered and control activities will have to be developed by all departments in the local entity.

To streamline this example, the focus will be on one objective in the accounting office – closing the books of account within sixty (60) days following the fiscal year end as required by state statute.

The example assumes that objectives and related risks, and control activity design implementation and operating effectiveness are in place in all other departments that have revenues, receivables, purchasing, payroll, payables, debt, capital asset, budgetary, and other financial activities.

Financial records are maintained on a cash basis throughout the year. Monthly and quarterly reports are not adjusted for accruals and other year-end only entries. The focus here is on the unique year-end closing entries.

Some of the main risks to consider when designing control activities for the year-end close out are as follows:

- Cash and investments may not be recorded or valued properly.
- Material year-end receivables/revenues may not be recorded.
- Material year-end payables/expenses/expenditures may not be recorded.
- Estimates such as allowance accounts may be inaccurate. What documentation exists to prove the estimate?
- Capital asset and depreciation accounts may not include material additions and disposals to capital assets.
- Material debt activity may not be recorded. Have debt proceeds been recorded gross or net of issuance costs?
- Material payroll activity, including pension liabilities, deferrals, and expense, may not be recorded.
- Net position may not be properly classified.
- Significant difficulties (complex new accounting standards, litigation, etc.), delays (grants, construction conflicts, pension data not available, etc.) or problems (computer system problems, key personnel leave, etc.) may be encountered causing data to be unavailable or to otherwise impede closing the books.
- Who is assigned to gather this information?
- Who is assigned to review the posting of year-end entries and conversion of balances from modified accrual basis to full accrual basis?
- Who is responsible for determining compliance with generally accepted accounting principles (GAAP)?
- What prior-year audit adjustments were considered necessary by auditors?
- Other related risks.

Control activities and procedures within the accounting department to address risks and ensure that the books are closed within sixty (60) days following the fiscal year-end include:

At the beginning of every fiscal year, immediately following the closing of the prior-year books of account, the accounting department, in coordination with all other departments, will:

- Review the prior year closing process and identify any difficulties, weaknesses or additional risks that were encountered.
- Review any matters identified with management to determine whether any changes are required and, if so, oversee the development and design of those changes.
- Review any new accounting standards and any accounting standards that are being developed that may be issued that will impact the upcoming year end closing.
- Consider the effects of new laws such as for new taxes.
- Set a tentative timeline for the upcoming year-end closing.
- Communicate the plan to all department heads for dissemination to employees whose work will be impacted by the plan.
- Revisit the plan with all departments near the end of the year.

Component 4
Information and Communication
GAO Green Book Principles 13 through 15

Management is responsible for developing and providing internal and external information. This information supports the internal control system and validates its existence. There are three (3) principles related to information and communication.

13. Management should obtain or generate relevant, quality information and use it to support the functioning of the internal control system.

This involves:

- Identifying the entity's information requirements
  - Management should design a process to identify the internal and external informational needs to support the internal control system.
  - Policies and procedures define the information requirements, ensuring that there is clear responsibility and accountability for maintaining the quality of information. Requirements are communicated both internally and externally.
- Gathering relevant data from reliable sources
  - Dependable internal and external sources deliver data that is largely free from errors and bias, accurately reflecting what they claim to represent.
  - Relevant data is gathered from a variety of forms, including manual input, information technology, or access of data compiled by other entities.
- Processing data into quality information
  - Data is processed by the entity's information system. The entity's information system is composed of people, processes, data, and information technology.
  - Management, using the information system, evaluates the processed information to determine whether it is quality information.
  - Quality information is appropriate, current, complete, accurate, accessible, verifiable, retained as appropriate, and timely provided.

Example 1:

Management has determined that one of its objectives is to provide accurate and timely financial statements to the governing body and to the entity's citizens on an annual basis prepared in accordance with generally accepted accounting principles (GAAP). This includes a balance sheet and statement of operations that includes budgetary comparisons for each governmental fund. As you read through the abbreviated list below, ask yourself, "Where do I get this information?" And "How do I know it is accurate and reliable?" Some of the more vital information requirements are as follows:

a. What accounting principles should be followed to properly record the information
b. The amount of cash and investments at the end of the year
c. The amount of receivables and payables at the end of the year
d. The amount of revenue for the month and year-to-date

e. The amount of expenditures for the month and year-to-date
f. The original budget approved by the governing body
g. Reports from other offices or departments such as the County Trustee or Utility Fund
h. The amount of fund balance restrictions, commitments, and assignments at the end of the month
i. For enterprise funds, information about equipment costs, depreciation, and long-term debt
j. What journal entries are necessary, who approves them, and for what amounts

Accurate reliable financial statements cannot be prepared without the above information. Each piece of information fits together like a large jigsaw puzzle. Therefore, it follows, that each piece of the puzzle must also be accurate and reliable. This cannot happen unless internal controls are properly designed and operating effectively. For example, cash must be reconciled with bank statements. Accounts receivable must be reconciled with the detailed receivable ledger, the control ledger, and the general ledger. Payables are similar. Likewise, total monthly revenues and expenditures must be accumulated from some reliable source. The original budget must be posted to accounting records and someone must determine if it was the actual budget approved by the governing body. Reports from other offices must be received and recorded, but how do I know these records are correct? The amount of fund balance that is restricted must be tracked on some record. Finally, all this information must be assembled and presented in the format of a formal financial statement. This is certainly not all that is required, but it does give the reader a hint of the types of information and internal controls necessary to prepare financial statements.

Again, the looming question is, how do I know any of the underlying information is accurate and reliable so that the entity can use it to present financial statements? The answer is, the entity doesn't know unless there are properly designed internal controls that are operating effectively for each piece of information. These controls usually fall into the category of ***Control Activities,*** which are discussed under Component 3 in this manual.

Example 2:
Management has determined that one of its objectives is to provide quality fire and police protection to the government's citizens. Management has determined that the information requirements needed to assess the quality of these services are:

a. Response times
b. Average number of weekly calls broken down into three, eight-hour blocks of time
c. Payroll data for the entity and comparable salary and benefits package comparisons from other entities to assist in attracting quality personnel
d. Equipment and vehicle status, future and current needs and replacement costs

Relevant data for each of the information requirements can be obtained from both internal and external sources. E911 records and dispatch records will provide data regarding response times and number of calls. The Comptroller's Transparency and Accountability for Governments in Tennessee (TAG) website will be used to find the payroll and fringe costs for other comparable local governments, and when TAG information is not available, the on-line audit reports will be utilized to glean information on those costs. Internal records regarding equipment repairs and maintenance, both the type of repair and the cost, will be compiled to evaluate equipment status, and searches on the internet will be used to evaluate the potential costs of equipment.

How does management know that dispatch records and repair and maintenance records are useful for making management decisions? Unless internal controls are in place to ensure the accuracy and reliability of the required information, management will be limited in its ability to make judgments about the quality of service provided.

14. Management should internally communicate relevant and quality information, including objectives and responsibilities for internal control, necessary to support the functioning of the internal control system.

This involves:

- Intentional communication throughout the entity
    - Communication is the continual, iterative process of providing, sharing, and obtaining necessary information throughout all levels of the entity to enable personnel to understand and perform key roles in achieving objectives, addressing risks, and supporting the internal control system.
    - The rise of information to the oversight body should include adherence to, changes in, or issues arising from the internal control system. This flow of information is key to the oversight of the internal control system.
    - When upward communication lines are compromised, personnel may use whistleblower and ethics hotlines to communicate confidential information.
- Appropriate methods of communication
    - Factors to consider when selecting a method of communication
        - Audience – recipients of the communication
        - Nature of information – purpose and type of information
        - Availability – readiness of information
        - Cost – resources necessary
        - Legal or regulatory requirements – relevant laws or regulations
    - Management should select an appropriate method of communication based on the communication factors. This process should occur on a periodic or ongoing basis.

Example:

The entity has been evaluating various possibilities for increasing its revenues and has decided on a long-term project with several phases. The first phase of the project involves expanding utility services. The expansion is intended to enhance industrial development by increasing service capacity. As a result, several strategic objectives have been modified. The modifications impact staffing, reporting, related internal controls, and other matters. Communication is going to be complicated because at least two older employees will be allowed to telecommute, and two new employees will be hired as part of the first phase of the project.

The oversight board has directed management to incorporate the changes in the policies and procedures, develop several new reports, and enhance the communication capabilities of the entity.

Management is working with information technology staff to utilize current technologies to remotely access the entity's network. In addition, electronic messaging and videoconferencing capabilities are being enhanced to facilitate overall communication and training participation at remote meeting sites.

Policies, procedures, and internal control design and activities are being updated to address the risks inherent to a large new construction project and to enhance remote communication.

15. Management should communicate relevant and quality information with appropriate external parties regarding matters impacting the functioning of the internal control system.

This involves:

- Intentional communication with external parties
  - Open two-way communication allows management to communicate with and obtain relevant, quality information from appropriate external parties.
  - Relevant, quality information from external parties can help the entity achieve its objectives, address related risks, and support its internal control system.
  - When management obtains information through reporting lines from external parties, they should evaluate the information obtained against the characteristics of quality information and information processing objectives.
- Appropriate methods of communication
  - Factors to consider when selecting a method of communication
    - Audience – recipients of the communication
    - Nature of information – purpose and type of information
    - Availability – readiness of information
    - Cost – resources necessary
    - Legal or regulatory requirements – relevant laws or regulations
  - Because entities report to such a broad audience, careful consideration should be taken when selecting a communication method.

Example:

The local media outlets requested information regarding salaries/wages for all of the local government's employees.

Management has determined that all communications with the media will be channeled through a single individual to ensure that information is accurate and consistent with legal and office requirements and the request has been forwarded to that individual.

There are some questions regarding the information that is being requested, that is, does the media want base salary and wage amounts or total payments, including overtime, for a particular period. The responsible individual has contacted the media to clarify the request.

The media responds that they want the current authorized pay rates and the total amount of payments for the most recent calendar year. The request is forwarded to accounting to extract the requested information.

The accounting system generates reports that include the information being requested. However, those reports include restricted information. The report will need to be reformatted to eliminate the restricted information. The modified report is submitted to the authorized individual in the local government who submits the information to the local media.

Component 5
Monitoring
GAO Green Book Principles 16 and 17

The operating environment, laws, accounting principles, technology, resources, and personnel change over time. For this reason, internal control system must constantly be monitored and improved or updated. There are two (2) principles related to monitoring.

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

This involves:

- Establishing a baseline
  - Monitoring activities evaluate whether each of the five components of internal control, and controls to implement related principles are in place, functioning, and require any changes.
  - The baseline represents the difference between the design of the internal control system and the actual condition of the internal control system.
  - Management should use the baseline to evaluate the internal control system and make changes by either changing the design of the internal control system or improving the effectiveness of the internal control system.
- Testing the internal control system against the intended design (monitoring)
  - Management monitors the internal control system using two methods:
    - Ongoing monitoring is part of the entity's operations and is performed continually.
      - Ongoing monitoring activities include regular management and supervisory activities, comparison, reconciliations, trend analysis, data analytics, activities to identify improper payments or potential fraud, testing, and other routine actions.
      - Ongoing monitoring activities can include automated tools to improve efficiency and objectivity.
    - Separate evaluations are performed periodically.
      - Separate evaluations include observations, inquiries, reviews, improper payment estimates, and other examinations.
      - Separate evaluations can also take the form of self-assessments.
      - Management may increase the frequency of separate evaluations when implementing a new program or substantially changing an existing one, such as emergency assistance programs.
      - Management should utilize the results from external separate evaluations, such as audits and investigations, to help identify issues in the internal control system.

    - Management should implement both ongoing monitoring and separate evaluations to assess the effectiveness of controls carried out by service organizations. Monitoring service organizations may include the use of work performed by service auditors and reviewed by management.
- Evaluating the results of the monitoring tests and making necessary improvements or updates
    - Management should document and evaluate results of ongoing monitoring and separate evaluations to identify internal control deficiencies.
    - Changes in the entity and the entity's environment require changes in the internal control system.

Example:

Management has adopted a policy requiring ongoing monitoring activities in key areas of internal control such as purchasing. By reviewing the results, management is able to determine where differences exist between the design and actual practice. Those results can then be evaluated to determine a course of action.

Over the last three months, based on tests (i.e. monitoring) of internal controls over purchasing documentation, management noted a marked increase in the number of invoices submitted for approval that included sales tax charges from which the government is exempt. In addition, purchase orders have not been attached, or did not have the proper signatures authorizing purchases in several instances.

In evaluating the control structure and the control activities, management noted that many of the weaknesses were clustered in two departments. Those departments had experienced turnover in employees due to the retirement of two key employees as well as normal turnover in two other positions. In addition, two processes that had been manual processes in the past had been automated and the internal control documentation had not been updated for those changes. One of the individuals that been hired had significant experience in the private sector but no experience in government operations. The cumulative effect of all of these changes resulted in internal control execution deficiencies. The current design of the controls was deemed to be appropriate.

Corrective action proposed includes: (1) update internal control policies and procedures to reflect the current control design, (2) provide additional training and coaching for new employees, (3) improve succession plans for the departure of key employees, and (4) improve the process for ensuring documents are updated when changes are made to the internal control design.

17. Management should evaluate and remediate identified internal control deficiencies on a timely basis.

This involves:

- Reporting internal control issues and deficiencies to the responsible management representative
  - Personnel should report internal control issues via the established reporting lines to ensure prompt and complete corrective action.
  - Personnel should consider reporting to an oversight body or an established fraud hotline if deficiencies arise to that level.
  - Depending on the nature of the deficiency, the entity may have external reporting obligations to legislators, regulators, and standard-setting bodies.
- Documenting reported internal control issues and deficiencies and evaluating each issue for corrective action
  - Management should evaluate issues reported by personnel, monitoring activities, and audits to determine whether they rise to the level of an internal control deficiency.
  - Based on the internal control deficiencies identified, management should determine appropriate corrective actions and delegate accordingly.
- Taking actions to correct audit findings and other issues and deficiencies
  - Documentation of corrective actions may include:
    - Root cause analysis
    - Planned actions
    - Interim milestones
    - Completion dates
    - Measurable indicators or compliance and remediation to assess and validate progress
    - Entity official responsible for monitoring corrective actions
  - Corrective actions may include changes to controls within each of the five components of internal controls
  - Corrective actions also include remediating audit findings. The remediation process is completed after action has been taken to:
    - Correct identified deficiencies.
    - Produce improvements.
    - Demonstrate that findings and recommendations do not warrant management action.

Example:

Continuing with the example at principle 16 above, monitoring of internal controls over purchasing was completed by the finance director's staff and the results documented and submitted to the finance director for review. Assuming the results do not require the governing body's or other oversight body's approval, the summary of results should include:

The scope of the review, the number and types of issues and deficiencies noted and the proposed corrective actions. The senior responsible official (i.e. equivalent to the mayor, finance director, or city manager) added a timeline for the corrective action plan and approved the plan. The plan was submitted to the department heads for implementation.