Single Audit Update
By: Chad Gorfido, Principal, CPA
Tim Herold, Manager, CPA

Single Audit Threshold

- Effective for fiscal years beginning after October 1, 2024 the threshold for federal single audit will increase from $750,000 to $1,000,000

- Type A program threshold will also increase from $750,000 to $1,000,000

Mandatory Disclosures – 2 CFR 200.113

- Recipients and subrecipients now required to promptly disclose when it has "credible evidence" of violations of Federal criminal law involving fraud, conflict of interest, bribery or gratuity violations

- Disclosure must be made in writing to Federal agency, agency's Office of Inspector General and pass-through entity, if applicable.

2 CFR 200.217 – Whistleblower Rights

- Recipients and subrecipients must inform their employees in writing of employee whistleblower rights and protections under 41 USC 4712.

  ◦ Employees must not be discharged, demoted or otherwise discriminated against as a reprisal for disclosing information that the employee reasonably believes is evidence of gross waste or abuse

2 CFR 200.1

- Increased equipment capitalization threshold from $5,000 to $10,000

- Recipients must update their capitalization policies in order to take advantage of threshold increase

2 CFR 200.414(f)

- Deminimis indirect cost rate increases from 10% to 15%

2 CFR 200.303(a) – Internal Controls

- Establish, **document**, and maintain effective internal control over the Federal award that provides reasonable assurance that the recipient or subrecipient is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. **These internal controls should align with the 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).**

COSO/Greenbook Components of Internal Control

Figure 4: The Components, Objectives, and Organizational Structure of Internal Control
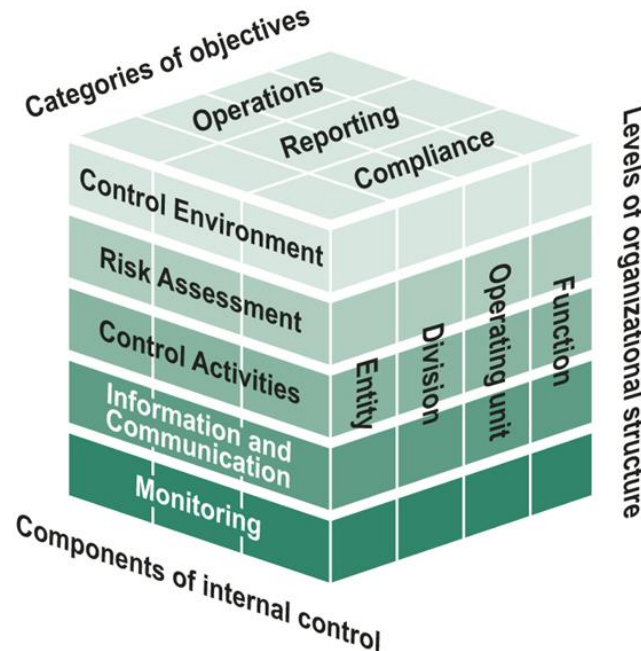
Sources: COSO and GAO. | GAO-14-704G

Control Environment

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

- Internal Control Illustrative Controls for Principle 1:
  - A code of conduct is developed, documented, communicated and periodically updated
  - A code of conduct explicitly prohibits inappropriate management override of established controls
  - Conflict of interest statements are obtained periodically from those charged with governance (TCWG) and key management

Control Environment

- Principle 2. The oversight body should oversee the entity's internal control system.

- Illustrative Controls for Principle 2:
  - TCWG have the requisite skills and knowledge to provide effective oversight pertaining to federal award compliance issues and related risk
  - TCWG periodically review ethical and moral conduct violations including stakeholder complaints regarding issues of federal award compliance with senior management
  - A whistle blower submission process exists to receive and evaluate concerns by employees regarding questionable practices inclusive of issues impacting federal award compliance/non-compliance
  - An audit committee charter exists and addresses federal compliance oversight
  - The effectiveness and performance of the audit committee is evaluated annually
  - TCWG have effective two-way communication with external and internal auditors
  - TCWG review risk assessments including the risks of fraud for impact on federal compliance objectives

Control Environment

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

- Illustrative Controls for Principle 3:
  - Policies, procedures and organizational charts provide for segregation of duties within and among processes and controls
  - Policies and procedures are in place to ensure that compliance responsibilities are assigned to particular positions

Control Environment

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

- Illustrative Controls for Principle 4:
  - Job descriptions include appropriate knowledge and skill requirements
  - Appropriate training is provided that is relevant to responsibilities over compliance objectives
  - Personnel with federal award compliance responsibilities are properly trained on their responsibilities

Control Environment

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

- Illustrative Controls for Principle 4:
  - Job descriptions include appropriate knowledge and skill requirements
  - Appropriate training is provided that is relevant to responsibilities over compliance objectives
  - Personnel with federal award compliance responsibilities are properly trained on their responsibilities

Control Environment

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

- Illustrative Controls for Principle 4:
  - Job descriptions include appropriate knowledge and skill requirements
  - Appropriate training is provided that is relevant to responsibilities over compliance objectives
  - Personnel with federal award compliance responsibilities are properly trained on their responsibilities

Control Environment

- Principle 5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

- Illustrative Controls for Principle 5:
  - Appropriate performance evaluations are provided that establish goals, accountability, and feedback
  - Violations of the code of conduct result in remedial actions to deter others
  - Consequences for noncompliance with the code of conduct are communicated and enforced
  - Penalties for inappropriate behavior are adequate and publicized

Risk Assessment

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

- Illustrative Controls for Principle 6:
  - Management establishes an effective risk assessment process that includes the use of a specific risk matrix
  - Management identifies key compliance objectives for types of compliance requirements
  - Management identifies and evaluates risk tolerances related for controls over compliance

Risk Assessment

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

- Illustrative Controls for Principle 7:
  - Management analyzes and identifies compliance risks
  - TCWG have oversight over significant areas of risks
  - Employees receive appropriate training to address identified risks
  - Risk mitigation strategies are implemented by management

Risk Assessment

- Principle 8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

- Illustrative Controls for Principle 8:
  - Management reviews audit findings to identify fraud risks
  - If an internal audit function exists, it reviews fraud risks and the internal control structure
  - Management reviews the internal control structure for potential fraud risks
  - TCWG periodically review a report of the potential fraud risks identified and actions taken in response to those risks during the period

Risk Assessment

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

- Illustrative Controls for Principle 9:
  - Management identifies changes such as new personnel, new technology, expanded operations, rapid growth, or changes in the operating environment and adjusts risk assessments to address those changes
  - Management analyzes compliance requirement modifications to properly adjust risk
  - A communication process with regulators is in place to identify changes in compliance requirements
  - Changes in philosophies or employee turnover are evaluated by management for any potential impact on related controls

Control Activities

- Principle 10. Design Control Activities – management should design control activities to achieve objectives and respond to risks

- Principle 11. Design Activities for the Information System – management should design the entity's information system and related control activities over technology to achieve objectives and respond to risks

- Principle 12. Implement Control Activities – management should implement control activities through policies

Control Activities

- Process vs. Control
  - Control are designed based on What Could Go Wrong within a process
  - When it is difficult to identify the difference between the process and controls there is often a missing control.
  - Related Considerations:
    - Process owners are often referred to as the doers and the control owner is often referred to as the reviewer.
    - A well-designed system of internal control assigns a control to each WCGW. An entity could have one control that addresses one WCGW, a suite of controls that address one WCGW, or one control that addresses multiple WCGWs.
    - Controls are often described in terms of a control category, such as authorization, management review, segregation of duties, or system access.

Control Activities

■Understanding Controls Activities

◦ Control Activities can be preventative or detective

◦ All 5 components of internal control have to be present and functioning for internal control to be designed effectively. Control activities on their own are not an effective system of internal controls.

◦ Even within control activities, controls rely on the effective design and operation of other controls. For example, a management review control generally uses information produced by the entity.

Control Activities

Principle 10. Design Control Activities: management should design control activities to achieve objectives and respond to risks.

A. ACTIVITIES ALLOWED OR UNALLOWED B. ALLOWABLE COSTS/COST PRINCIPLES	C. CASH MANAGEMENT	E. ELIGIBILITY	F. EQUIPMENT AND REAL PROPERTY MANAGEMENT
Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as miscoding, inappropriate cost transfers, budget overages, segregation of duties concerns, unauthorized changes to system configurations, fraud, unauthorized payments, etc.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as time lapses between funds transfer and disbursement, fraud, liquidity pressures, inherent risks with subrecipients, etc.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as providing benefits to ineligible individuals, calculating amounts to be received for or on behalf of individuals incorrectly, unauthorized changes to system configurations, fraud, unauthorized payments, etc.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process for equipment and real property, such as inaccurate or incomplete recordkeeping, inappropriate use, unidentified dispositions, segregation of duties concerns, fraud, loss, damage, theft, etc.
Management reviews applicable award agreements or contracts for specific allowable activities requirements, budget parameters , indirect rates, fringe benefit rates, and those activities/costs that require pre-approval by the awarding agency and documents such features into a grant approval form which is submitted to accounting personnel for review and approval before being input into the system as the profile for the grant.	Management reviews applicable award agreements or contracts to determine applicability of drawdown method (advance or reimbursement) to develop its own control activities and to inform its establishment of a method for subrecipients, as applicable.	Management reviews applicable award agreements or contracts and identifies specific eligibility requirements including benefits to be paid.	Management reviews applicable award agreements or contracts and identifies specific equipment and real property requirements.

Control Activities

Principle 10. Design Control Activities: management should design control activities to achieve objectives and respond to risks.

G. MATCHING, LEVEL OF EFFORT, EARMARKING	H. PERIOD OF PERFORMANCE	I. PROCUREMENT AND SUSPENSION AND DEBARMENT	J. PROGRAM INCOME
Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as unallowable funding sources for amounts claimed as match, unsupported or unreasonable valuations of in-kind contributions, unallowable activities/costs, unsupported effort indicators, use of unapplied indirect costs as match without pre-approval, utilization of same data for more than one match when prohibited, failure to track minimum or maximum earmarking criteria, segregation of duties concerns, fraud, etc.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as miscoding, in appropriate cost transfers or adjustments for transactions outside the award period, segregation of duties concerns, unauthorized changes to system configurations, fraud, failure to secure approvals or extensions for coding costs outside the original performance period, etc.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as unidentified or unaddressed conflicts of interest, fraud, segregation of duties concerns, unauthorized procurements, unauthorized changes to vendor master file, failure to follow documented policies, failure to document history of procurement, failure to document cost/price analysis, inappropriate procurement method used, suspended or debarred vendor/subrecipient contracted with, etc.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as failure to identify and use program income, use of incorrect method to use program income, fraud, segregation of duties concerns, etc.
Management reviews applicable award agreements or contracts for specific matching, level of effort, and earmarking requirements including any unique requirements (such as pre-approval by the granting agency to recoup unapplied indirect costs as matching) and documents such features into a grant approval or other grant summary form which is submitted to accounting and/or programmatic personnel, as appropriate for review and approval before being input in the financial system to set up a grant match record or other programmatic tracking system as a profile for the grant.	Management reviews applicable award agreements or contracts for specific period of performance requirements, including any unique provisions about pre-award spending, extensions, and refunds of unobligated cash.	Management creates and requires the use of standard forms and templates for purchase orders, contracts, requests for proposals/bids, cost/price analyses, bid evaluation, etc. Standard documentation protocol for the history of procurements exists including rationale for the method of procurement (micro-purchase, small purchase, sealed bid, competitive proposal, or noncompetitive proposal), selection of the contract type (fixed price, cost reimbursement, etc.), cost/price analysis, basis for contractor selection/rejection, etc.	Management reviews applicable award agreements or contracts for provisions specific to program income, including identifying likely program income based on award purpose and the use of Deduction, Addition, or Cost Sharing/Matching methods for using program income and documents such features into a grant approval form which is submitted to accounting personnel for review and approval before being input into the system as the profile for the grant.
Supervisory review ensures matching contributions are supported by 3rd party evidence, or other procedures are	Supervisors review and approve invoices, cost allocations, efforts of personnel, fringe benefits and	Supervisors review and approve procurement and contracting decisions	On a monthly basis, supervisors review application of program income to the award to ensure that

Control Activities

Principle 10. Design Control Activities: management should design control activities to achieve objectives and respond to risks.

L. REPORTING	M. SUBRECIPIENT MONITORING	N. SPECIAL TESTS AND PROVISIONS
Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as lack of current knowledge of reporting requirements, data input errors, segregation of duties concerns, fraud, inconsistent application of accounting standards, lack of documented bridge between source data and final reports for any reconciling items and lack of or inappropriate source data or analysis used as the basis of performance or special reporting.	Management identifies and puts into effect actions needed to carry out specific responses to risks identified in the risk assessment process, such as missing federal and pass-through entity requirements in subawards, risks inherent with specific subrecipients, inappropriate/ineffective subrecipient monitoring, etc.	Illustrative internal controls cannot be provided because special tests and provisions are unique to the various federal programs.
Management reviews applicable award agreements or contracts for specific reporting requirements and establishes a reporting calendar for review and approval.	Subrecipient agreements are reviewed and approved by knowledgeable supervisors to ensure all compliance requirements are captured, that information is consistent between pass-through entity records and the subaward, and that all required elements are included.	
	Management tracks subaward notifications and maintains an inventory of executed subrecipient agreements.	
Knowledgeable supervisors review and approve reports for completeness and accuracy, including comparing to source documentation (general ledger, third party evidence or other reliable records) and any reconciliations between source data to final reporting.	Knowledgeable supervisor reviews subrecipient risk assessments to ensure they address compliance risks and Uniform Guidance requirements and approves individual subrecipient monitoring plans.	
Management periodically reviews the completeness and accuracy of and adherence to the reporting calendar.	Management requires the use of a standard template for use for all sub recipient agreements inclusive of all required elements outlined in Uniform Guidance.	
	Documentation and conclusions of results of subrecipient oversight activities including the items below are review by supervisory personnel: • Award authorization • Site visits • Financial performance, monitoring, and/or audit reports • Grant budgets and advance or reimbursement requests	

Information and Communication

- Principle 13. Management should use quality information to achieve the entity's objectives.

- Illustrative Controls for Principle 13:
  - Financial and programmatic systems capture, accurately process, and timely report pertinent information
  - The accounting system provides for separate identification of federal and non-federal transactions
  - Adequate source documentation exists to support amounts and items reported
  - Reports are provided timely to managers for review and appropriate action
  - Management verifies the sources and reliability of information used in making management decisions and executes monitoring controls

Information and Communication

- Illustrative Controls for Principle 13:
  - When information is derived from the organization's information technology (IT) systems:
  - Security administration
    - Written policies and procedures regarding IT security exist The accounting system provides for separate identification of federal and non-federal transactions
    - Regarding managing user access rights, (1) rights are approved and granted based on job responsibilities; (2) rights, including super user access, are reviewed periodically; and (3) access is revoked in a timely manner
    - Duties of security personnel do not include performing compliance processes or controls, programming, or IT management
    - Remote and third party access rights are managed to include timely revocation of rights

Information and Communication

- Illustrative Controls for Principle 13:
  - When information is derived from the organization's information technology (IT) systems:
  - Program maintenance
    - Policies around the change management process are documented, approved, and communicated
    - Segregation of duties exists between development, testing, and production
    - Changes to productions are logged and reviewed
  - Program execution
    - Policies around the program execution process are documented, approved, and communicated
    - Production job scheduling change requests are approved by appropriate IT personnel
    - The scheduling system is restricted from accessing anything that is not in the production library (applications and databases) ▯ Schedule exceptions are monitored to determine if they are properly resolved

Information and Communication

▪Principle 14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

▪Illustrative Controls for Principle 14:

◦ Relevant internal and external information is communicated and delivered to employees responsible for federal award compliance on a timely basis

◦ Effective channels for communication throughout the organization exist

Information and Communication

- Principle 15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

- Illustrative Controls for Principle 15:
  - Relevant information is communicated to external parties including subrecipients, vendors, federal granting agencies, and third party processors on a timely basis
  - Effective channels exist for communications with federal granting agencies, oversight agencies and cognizant agencies

Monitoring

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

- Illustrative Controls for Principle 16:
  - Management monitors the effective operation of critical control activities
  - Management monitors the use of effective self-review procedures in critical compliance areas
  - Management monitors the effective review of timely and reliable metrics or key performance indicators, including reconciliation with data from financial or other reporting systems to ensure its accuracy and completeness
  - Management monitors the reconciliation of key performance indicators with data from financial or other reporting systems, including reconciliation with data from financial or other reporting systems to ensure its accuracy
  - If an internal audit function exists, it is staffed with qualified and competent personnel and it reports directly to TCWG
  - If an internal audit function exists, its responsibilities and audit plans are aligned to the organization's risk assessment

Monitoring

- Principle 17. Management should remediate identified internal control deficiencies on a timely basis.

- Illustrative Controls for Principle 17:
  - Findings, recommendations and other observations by independent auditors, internal auditors, and federal auditors are distributed and reviewed by those individuals responsible for compliance with federal requirements.
  - Control deficiencies and instances of noncompliance are reported to and evaluated by management and TCWG, if applicable, for resolution on a timely basis
  - Management periodically monitors the corrective action plans related to known noncompliance and control deficiencies and the organization's progress to remediating the findings

2 CFR 200.303(e) - Cybersecurity

- Take reasonable cybersecurity and other measures to safeguard information including protected personally identifiable information (PII) and other types of information. This also includes information the Federal agency or pass-through entity designates as sensitive or other information the recipient or subrecipient considers sensitive and is consistent with applicable Federal, State, local, and tribal laws regarding privacy and responsibility over confidentiality.

2 CFR 200.455 – Organization Costs

- The costs related to data and evaluation are allowable. Data costs include (but are not limited to) the expenditures needed to gather, store, track, manage, analyze, disaggregate, secure, share, publish, or otherwise use data to administer or improve the program, such as data systems, personnel, data dashboards, cybersecurity, and related items. Evaluation costs include (but are not limited to) evidence reviews, evaluation planning and feasibility assessment, conducting evaluations, sharing evaluation results, and other personnel or materials costs related to the effective building and use of evidence and evaluation for program design, administration, or improvement.

2 CFR 200.319(c)

- Removed prohibition on using geographical preference in evaluations of bids and proposals

200 CFR 200.320

- Term "small purchases" changed to "simplified acquisitions". Simplified acquisitions apply when procurement amount exceeds micro-purchase threshold.

  ◦ Reminder micro-purchase threshold increased to $50,000 with self-certification of being a low-risk auditee and documentation of annual internal institutioinal risk assessment to identify, mitigate and manage financial risks

- Now required to maintain documentation and provide a justification for all bids rejected.

Thank you!

Chad Gorfido, Principal, CPA

Chad.Gorfido@ReaAdvisory.com

Direct 330-661-0223

Tim Herold, Manager, CPA

Tim.Herold@ReaAdvisory.com

Direct 330-722-6307