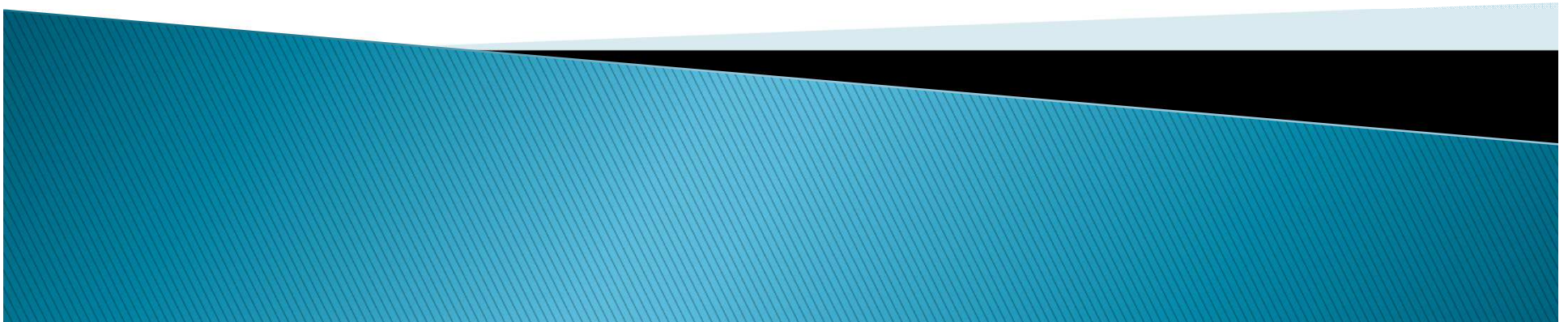


# Internal Controls Overview and the FY18 ICQ

GATU Webinar – Part 1  
March 2017

Presented by Carol Kraus, CPA



# Presentation Objectives

- ▶ Definition of Internal Controls
- ▶ COSO – Internal Control Framework
- ▶ Internal Controls (2 CFR 200.303)
- ▶ Grantee responsibilities
- ▶ Awarding state agency responsibilities (2 CFR 200.205)
- ▶ Specific Conditions (2 CFR 200.207)



# Definition of Internal Controls

A process, effected by an entity's board of directors, management, personnel and others charged with governance, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- ▶ Effectiveness and efficiencies of operations
- ▶ Reliable, timely and accurate reporting
- ▶ Compliance with applicable laws and regulations



# Internal Controls 200.303

Each non-Federal Entity must:

- ▶ Establish and maintain effective internal controls over the grant award
- ▶ Internal controls must provide reasonable assurance that the grantee is managing the award in compliance with state and federal statute, regulations and the terms and conditions of the grant agreement



# Internal Controls 200.303

Internal controls should comply with guidance:

- ▶ “Standards for Internal Control in the Federal Government” issued by the Comptroller General of the United States, or
- ▶ “Internal Control Integrated Framework”, issued by the Committee of Sponsoring Organization of the Treadway Commission (COSO)



# Internal Controls 200.303

Internal controls must:

- ▶ Comply with State and Federal statutes, regulations, and grant agreement terms and conditions
- ▶ Evaluate and monitor compliance with statutes, regulations and the terms and conditions of the grant agreement
- ▶ Ensure prompt action when instances of noncompliance are identified – audit findings, on-site reviews and other regulatory reviews



# Characteristics of Good Controls

- ▶ Focused on critical points of operations
- ▶ Integrated into established processes; not burdensome but a part of processing
- ▶ Accurate, in that they provide factual information that is useful, reliable, valid, and consistent
- ▶ Simple and easy to understand
- ▶ Accepted by employees
- ▶ Cost effective – controls should not cost more than the risks they mitigate



# Common Basic Internal Control Principles



## Establish Responsibility

Assign each task to only one person



## Segregate Duties

Don't make one employee responsible for all parts of a process



## Restrict Access

Limit access to system, information, assets, etc. to those that need it to complete assigned responsibilities



## Document Procedures and Transactions

Prepare documents to show that activities have occurred



## Independently verify

Check others' work



# COSO Provides an Integrated Framework for Internal Controls



# COSO Internal Control –Integrated Framework Principles

5 interrelated components of Internal Control

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

Along 3 main objectives

- A. Operations
- B. Reporting
- C. Compliance

Across the organization, down to the process functions



# 1. Control Environment

- ▶ Organization demonstrates a commitment to integrity and ethical values
- ▶ Board of directors (oversight team) demonstrates independence from management and exercises oversight of the development and performance of internal controls
- ▶ Under oversight, management establishes and structures reporting lines, appropriate authorities, and responsibilities to accomplish objectives

# Organization Control Environment

- ▶ Organization demonstrates a commitment to attract develop, and retain competent individuals in alignment with objectives
- ▶ Organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives



# Governing Body, Senior Management Oversight Responsibility

## Control Environment

- ▶ Demonstrates commitment to integrity and ethical values – Establish tone at the top
- ▶ Exercises oversight responsibility
- ▶ Establishes structure, authority and responsibility
- ▶ Demonstrates commitment to competence
- ▶ Enforces accountability



# Scope of Control Environment

- ▶ Controls should include:
  - Hiring practices
  - Training programs
  - Whistleblower programs
  - Code of Conduct
  - Clear lines of responsibility and authority
- ▶ Control Environment must be documented and may include:
  - Procedure manual that include process narratives, flow charts, job aid such as checklists
  - Organizational charts
  - Memorandums
  - Questionnaires

## 2. Risk Assessment

- ▶ Organization specifies objectives so it can identify and assess related risks
- ▶ Organization identifies risks posed and analyzes risks to determine how risks should be managed
- ▶ Organization considers potential for various types of fraud
- ▶ Organization identifies and assesses changes that could affect internal controls



# Governing Body and Senior Management Oversight Responsibility

## Risk Assessment

- ▶ Specifies suitable objectives
- ▶ Identifies and analyzes risk
- ▶ Identifies and analyzes significant change





# Risk Assessment and Risk Management

- ▶ Risk management is a process strategically applied and designed to identify and manage risk within a tolerance level
- ▶ Risk assessment is an internal control element within risk management that allows management to identify and assess key risks
  - The risk assessment is the basis for determining control activities



# 3. Control Activities

- ▶ Organization selects and develops control activities, including use of technology, to mitigate risk and achieve objectives
- ▶ Organization deploys controls activities through policies to establish what is expected and procedures that put policies into action
  - Actions established through policies and procedures help ensure management's directives to mitigate risks are carried out
- ▶ Control activities are performed at all levels within the entity



# Control Activities

- ▶ Types of control activities:
  - Preventive and Detective
  - Compensating
  - Manual and automated
- ▶ Control activity examples:
  - Approvals and authorizations
  - Verifications
  - Reconciliations
  - Independent reviews
  - Asset security
  - Segregation of duties

# Preventive Controls

Prevents the occurrence of a negative event in a proactive manner. Examples:

- ▶ Approvals for purchases over \$3,000
- ▶ Verification that equipment purchases are pre-approved or included in grant budget
- ▶ Passwords for access to IT systems
- ▶ Pre-numbered checks
- ▶ Holding petty cash in a lockbox

# Detective Controls

Detective controls detect the occurrence of a negative event *after the fact* in a reactive manner. Examples include:

- ▶ Supervisor review and approval
- ▶ Report run showing user activity
- ▶ Reconciliation of petty cash
- ▶ Physical inventory count
- ▶ Review missing and voided checks

# Compensating Controls

- ▶ If there is a control weakness or limitation, a *compensating control* may be relied upon to mitigate the risk
- ▶ Can be preventive or detective

EXAMPLE: A entity lacks staffing for adequate segregation of duties. Potential compensating controls:

- Automate certain transaction data to limit altering
- Manager reviews detailed summary reports of transactions initiated by staff
- Manager selects sample transactions and vouches to supporting documentation



# Manual and Automated Controls

- ▶ Manual controls require action by employees:
  - Obtaining a supervisor's approval for overtime
  - Reconciling a bank account
  - Matching receiving to purchase orders
- ▶ Automated controls are built into systems or applications:
  - Data entry validation checks
  - Batch controls

Automated controls are more reliable and cost effective than manual controls

# Governing Body and Senior Management Oversight Responsibility

## Control Activities

Based on the risk assessment and risk management policy:

- ▶ Select and develop control activities
- ▶ Select and develop controls over IT
- ▶ Deploy through policies and procedures





# 4. Information and Communication

- ▶ Organization obtains and uses relevant quality information to support the functioning of internal controls
- ▶ Organization internally communicates objectives and responsibilities for internal control to support functioning of internal controls
- ▶ Organization communicates with external parties regarding matters affecting the function of internal controls



# Information and Communication

- Initiatives
- Goals
- Changes
- Opportunities
- Feedback
- Questions / Answers
- Policies and Procedures
- Standards
- Expectations
- Policies and procedures manual
- Memorandums
- Directives
- Training, training, training
- Website / intranet
- Meeting deliverables
- If you don't document it did not happen!

Need to communicate

Methods of communication

# Governing Body and Senior Management Oversight Responsibility

## Information and Communication

- ▶ Communicate necessary information to personnel
- ▶ Provide adequate training of controls to responsible staff
- ▶ Communicate internally and externally



# 5. Monitoring Activities

- ▶ Organization selects, develops and performs ongoing and/or separate evaluations to determine whether components of internal control are present and functioning
  - Organization considers internal and external risks
- ▶ Organization evaluates and provides timely communication to senior management and the board of directors, as appropriate regarding internal control deficiencies to foster corrective action

# Monitoring Activities Are

- ▶ Evaluations that ascertain whether components of internal control are *present* and *functioning*
- ▶ 2 categories of monitoring
  - Ongoing evaluations – built into business processes and provide timely information on underlying controls
  - Separate evaluations – conducted periodically and vary in scope and frequency based on prior assessments of risk, the effectiveness of *ongoing* evaluations, and other management considerations (e.g., resource priorities)
    - Internal Audit activities are a separate evaluation
    - Confirm that findings of audits and other reviews are promptly resolved so internal controls are not compromised

# Monitoring Activity Results

- ▶ Monitoring an activity means assessing the performance of an internal control system over a period of time to validate that the control system is operating as expected
  - Includes supervisory review and sign off to help ensure proper checks and balances
- ▶ *Findings* should be evaluated against relevant criteria (e.g., how long has the control been compromised, and how high are the risks)
- ▶ *Deficiencies*, which are more significant than findings, should be communicated to the Board and Senior Management

# Governing Body and Senior Management Oversight Responsibility

## Monitoring Activities

- ▶ Conduct ongoing evaluations
- ▶ Evaluate and communicate deficiencies
- ▶ Establish and follows up on corrective action plans of deficiencies



# Effective System of Internal Controls

According to COSO, an effective system of internal control requires:

- ▶ Each of the 5 components of internal control with relevant principles present and functioning
- ▶ All 5 components operating together in an integrated manner





# Grantee and Sub-recipient Responsibilities (200.303 and 200.302)



# Grantee Internal Control Responsibilities – 200.303

- ▶ Grantees must take reasonable measures to safeguard protected personally identifiable information and other data the awarding agency designates as sensitive
- ▶ Grantees must consider applicable federal, state, and local laws regarding privacy and obligations of confidentiality



# Grantees are Stewards of Grant Funds

- ▶ Grantees and subrecipients must carry out goals and objectives stated in the uniform grant agreement
- ▶ Grant funds must be used for their intended purposes
  - Grant funds are subject to certain regulations, oversight and audit
  - Grant recipients must account for costs and justify expenditures



# Grantee Financial Management System – 200.302

- ▶ Financial management system must include effective control over, and accountability for all funds, property, and other assets
- ▶ Records within the financial management system must identify the source and application of funds for grant-funded activities including:
  - authorizations, obligations, unobligated balances, assets, expenditures, income and interest supported by source documentation

# Grantees Must Have

- ▶ Effective control over and accountability for all funds, property, and other assets
- ▶ Comparisons of expenditures with budget amounts for each grant award
- ▶ Written procedures:
  - To comply with cash management requirements
  - For determining allowability of costs in accordance with Cost Principles and terms and conditions of the grant agreement
- ▶ If the grantee passes funds, the grantee must also comply with 200.331 Requirements for Pass-through Entities

# Federal Uniform Guidance Requires Pre-award Risk Assessments (200.205)

- ▶ GATA separates the risk assessment into 2 parts:
  - Fiscal and Administrative (F&A) – conducted once and shared with all grant making agencies
  - Programmatic – conducted with each grant highlighting the programmatic requirements associated with the individual grant program

# Fiscal and Administrative (F&A) Risk Assessment

- ▶ Conducted annually after registration and pre-qualification
- ▶ Utilizes Internal Control Questionnaire (ICQ)
- ▶ ICQ responses must be reviewed by the entity's cognizant agency
  - Cognizant agency – state agency that provided the most funding to the entity in a previous fiscal year (currently FY15 and re-determined every three years)
- ▶ Follow-up is encouraged if the cognizant agency believes the entity responded incorrectly (based on prior experience/ knowledge of the entity)
  - ICQ responses can be changed and re-submitted, when appropriate

# ICQ Content

- ▶ ICQ covers 10 sections:
  1. Quality of management systems (200.302)
  2. Financial and regulatory reporting (200.237)
  3. Budgetary controls (200.308)
  4. Cost principles (200.400)
  5. Audit (200.500)
  6. Organizational governance (COSO)
  7. Property standards (200.310–316)
  8. Procurement standards (200.317–326)
  9. Sub-recipient monitoring and management (200.330–332)
  10. Fraud, waste and abuse – (COSO)
- ▶ ICQ incorporates requirements under:
  - 2 CFR 200
  - Subpart F – Single Audit Compliance Supplement
  - COSO



# State Awarding Agency Responsibilities (200.205 and 200.207)



# Awarding Agency Reviews Risk Posed by the Applicant (200.205)

- ▶ Grantee must complete both risk assessments (ICQ and programmatic) prior to making an award
- ▶ All grantees are subject to pre-award risk assessment, unless an exception has been authorized
- ▶ ICQs are automated and responses are reviewed once by the state cognizant agency
- ▶ Programmatic risk assessments are specific to the program application and performed by each awarding agency

# Risk Assessment – Specific Conditions (200.207)

- ▶ Cognizant agency reviews and accepts the ICQ
- ▶ Automation grades the responses as low, medium or high risk for each of the 10 segments
- ▶ Pre-determined specific conditions are automatically assigned based on the risk profile
  - Specific conditions advise grantees and state agencies of internal control weaknesses at the grantee-level
- ▶ State agencies utilize specific conditions to correct weaknesses that could result in non-compliance with fiscal and administrative grant requirements

# Specific Conditions

Specific conditions can include:

- ▶ Requiring payments to be reimbursement based
- ▶ Withholding authority to proceed to the next phase, until performance improves
- ▶ Requiring more frequent and/or detail reporting
- ▶ Requiring additional project monitoring
- ▶ Requiring grantee to obtain technical or management assistance
- ▶ Establishing additional prior approvals



# Notification of Specific Conditions

Awarding agency will use the Notice of State Award (NOSA) to notify the applicant of:

- ▶ Nature of additional requirements or specific conditions
- ▶ Reason why additional requirements are imposed
- ▶ Nature of action(s) needed to remove additional requirements, if applicable
- ▶ Time allowed for completing the action(s)
- ▶ Method for requesting reconsideration of additional requirements imposed

Specific conditions must be removed immediately after acceptable corrective action(s) is taken



# Working Together for Internal Control Compliance

- ▶ Internal controls are a backbone of effective operations and federally required
- ▶ The ICQ enables state agencies to assess internal controls at the grantee-level
- ▶ Capacity building must be needs based
  - Specific conditions are grantee-specific in response to the risk profile



# GATU Contacts for Additional Support

Carol Kraus, CPA  
Director, GATU  
[Carol.Kraus@illinois.gov](mailto:Carol.Kraus@illinois.gov)

Jennifer Butler, CMC  
GOMB Deputy Director  
[jennifer.butler@illinois.gov](mailto:jennifer.butler@illinois.gov)

