Internal Controls Training & Education

Agenda

1. COSO Integrated Framework: Risk and Control Identification
2. Internal Controls Over Financial Reporting at Miami-Dade County
3. Determining Significant Accounts and Disclosures
4. Control Owner Responsibilities:
    a. Evaluating Control Design
    b. Testing and Monitoring using Sample Selection Methodology
    c. Evaluating Deficiencies
5. Example Control
6. Q&A

COSO Integrated Framework: Risk & Control Identification

COSO Integrated Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued an *Internal Control Integrated Framework* (COSO Framework) in 2013, to help organizations design, implement, and evaluate internal controls.

COSO Framework:

- Applies to entities of all sizes, including large, mid-size, and small organizations; for-profit and not-for-profit organizations; and government bodies.
- Sets forth the requirements for effective internal control (including both five components and seventeen relevant principles); and the approach users may follow when designing, implementing, and conducting internal control and assessing its effectiveness.
- COSO's guidance is to internal control what GASBS is to financial statements.
- SEC has indicated that the COSO Framework is a suitable control framework for the management's annual assessment of the effectiveness of internal control over financial reporting.
- Assists senior management, Board of County Commissioners (BCC), and other stakeholders in their respective duties regarding internal control evaluation.

Per the SEC, it is "…management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company; management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year; a statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting."

Following this slide, we will discuss the COSO framework's 5 components and 17 principles of internal control.

COSO Integrated Framework

- The *2013 Framework* focuses on five integrated components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities.
- The updated *2013 Framework* codifies criteria that can be used in developing and evaluating the effectiveness of systems of internal control – making explicit 17 principles, each with points of focus.
- All internal controls must be present and functioning for system of internal controls to be effective.

5 components	17 principles
Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability.
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys control activities through policies and procedures
Information and communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Following this slide, we will discuss what an effective system of internal control is in accordance with COSO.

What is an Effective System of Internal Control?

The COSO Framework states that to achieve an effective internal control:

- *Each of the five components and the 17 relevant principles are present and functioning*. "Present" means that the components and relevant principles have been ***designed and implemented*** to achieve specified objectives. "Functioning" means that the components and relevant principles are operating within the system of internal control to achieve specified objectives.

- *The five components should operate in an integrated manner*. "Operating together" means that all five components, taken together, reduce to an acceptable level the risk of failing to achieve an objective. Rather than discreetly considering components, they are considered in terms of how they ***operate together*** as an integrated system.

- An effective system of internal control reduces the control risk to an acceptable low level and provides management with "reasonable assurance" of achieving the objectives.

- Although cost/benefit considerations play a significant role in designing internal controls, the COSO Framework notes that cost alone is not an acceptable reason to avoid implementing a control.

Following this slide, we will discuss inherent limitations in an effective system of internal control.

Inherent Limitations in Internal Control

Even effective internal controls, no matter how well designed, have inherent limitations. The COSO Framework describes the following inherent limitations of internal control:

- *Judgment*. The effectiveness of internal controls is limited by the reality that human error might occur in the process of making decisions.
- *Breakdowns*. Any system of internal control, no matter how well designed, is likely to breakdown because of the potential for human error. Carelessness, distraction, being asked to focus on too many tasks, or the misunderstanding of instructions by a person responsible for establishing or performing a control may render control ineffective.
- *Collusion*. With any internal control, there exists the potential for collusion. The COSO Framework defines collusion as "individuals acting collectively to perpetrate and conceal an action from detection, so that it cannot be detected or prevented by the system of internal control."
- *Management Override*. The COSO Framework defines management override as "overruling prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's performance on compliance.

Following this slide, we will share various examples of the 17 principles that fall within the 5 COSO components.

Example of Principles: Control Environment

	Addresses Fraud or Significant Risk?	Control Has Been Implemented?	Automated or IT-dependent?	Effectively Designed?	Test Control?	Comments
Principle: The entity demonstrates a commitment to integrity and ethical values.						
C0010—A process exists by which those charged with governance are made aware of key developments that may affect financial reporting.						
C0011—A code of conduct or ethics policy exists.						
C0012—Management, employees, and others are made familiar with the entity's policies and practices with regard to ethics, accepted business practices, and a positive control environment.						
C0014—Management acts to remove or reduce incentives or temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts.						
C0015—Rewards, such as bonuses and other incentives, foster an appropriate ethical tone.						

Example of Principles: Risk Assessment

	Addresses Fraud or Significant Risk?	Control Has Been Implemented?	Automated or IT-dependent?	Effectively Designed?	Test Control?	Comments
Principle: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to financial reporting objectives.						
C0032—Management adopts accounting policies that are appropriate for the entity and consistent with GAAP (or a special purpose framework).						
C0100—Entity objectives are established, communicated, and monitored. The key elements of the entity's strategic plan are communicated throughout the entity.						
C0103—Financial reporting objectives align with the requirements of GAAP (or a special purpose framework).						

Examples of Principles: Information & Communication

	Addresses Fraud or Significant Risk?	Control Has Been Implemented?	Automated or IT-dependent?	Effectively Designed?	Test Control?	Comments
Principle: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control over financial reporting.						
C0200—Relevant operating information is used to develop accounting and financial information and serves as a basis for reliable financial reporting. Operating information is used as the basis for accounting estimates.						
C0205—Accounting procedures are sufficiently formal that management can determine whether the control objective is met, documentation supporting the procedures is in place, and personnel routinely know the procedures that need to be performed.						
C0206—Data underlying financial statements are captured completely, accurately, and timely, in accordance with the entity's policies and procedures, and in compliance with laws and regulations.						

Examples of Principles: Monitoring

	Addresses Fraud or Significant Risk?	Control Has Been Implemented?	Automated or IT-depen-dent??	Effectively Designed?	Test Control?	Comments
Principle: The entity selects, develops, and performs ongoing and/or separate evaluations to determine whether the components of internal control are present and functioning.						
C0305—Ongoing monitoring is built into operations throughout the entity, and includes explicit identification of what constitutes a deviation from expected control design or performance, and thereby signals a need to investigate both potential control problems and changes in risk profiles.						
C0306—Management's ongoing monitoring provides feedback on the effective design and operation of controls integrated into processes, and on the processes themselves.						
C0307—Management's ongoing monitoring serves as a primary indicator of both control design and operating effectiveness and of risk conditions.						

Examples of Principles: Control Activities for Cash

	Assertions	Addresses Fraud or Significant Risk?	Control Has Been Implemented?	Automated or IT-dependent?	Effectively Designed?	Test Control?	Comments
Processing Cash Receipts							
C1000—Management reviews the entity's financial statements on a periodic basis and investigates significant variances from budgets and expected results.	E/O, C, R/O, V, A/CL, CO						
C2002—Delinquent receivables are reviewed.	E/O, C, V, R/O, A/CL, CO						
C2007—The receivables aging/subledger is reviewed and reconciled to the general ledger.	E/O, C, A/CL, CO						

Following this slide, we will define internal controls over financial reporting (ICFR), and how that applies to your role at Miami-Dade County. The COSO framework that we've discussed thus far is the framework designed to help the County design, implement, and evaluate internal controls over financial reporting (ICFR).

Internal Controls Over Financial Reporting at Miami-Dade County

plante moran | Audit. Tax. Consulting. Wealth Management.

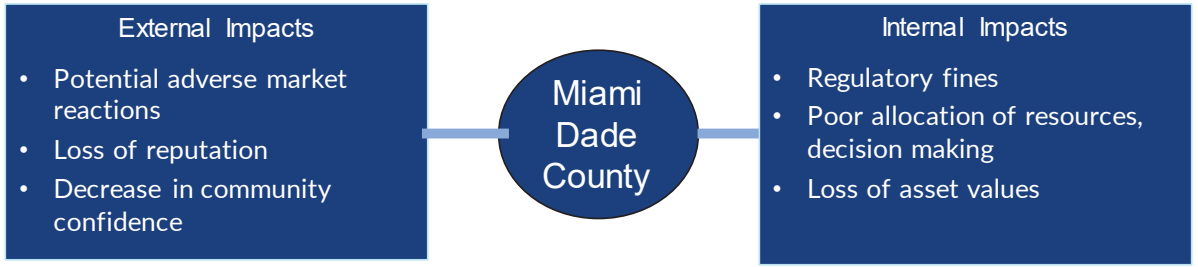
ICFR Overview

Internal controls over financial reporting (ICFR) are internal controls that specifically focus on the activities which prevent and/or detect errors in financial reporting. They are designed by, or under the supervision of, the company's executive and financial officers.

An effective ICFR enables the County to:

- Ensure effectiveness and efficiency of operations
- Ensure reliability of financial reporting
- Comply with applicable laws and regulations
- Safeguard the assets of the organization

Ineffective ICFR (Control gap/failures) can lead to external and internal impacts.



Following this slide, we will discuss what is reasonable assurance as it relates to ICFR.

What is Reasonable Assurance in ICFR?

Because of the inherent limitations in internal control, management can only have *reasonable assurance* that internal controls over financial reporting are effective.

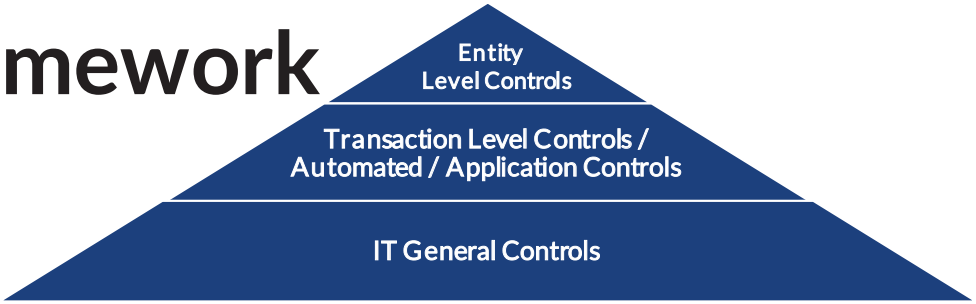
COSO Framework recognizes the concept of *reasonable assurance* by stating:

- Reasonable assurance does not imply that an entity will always achieve its objectives. Effective internal control increases the likelihood of an entity achieving its objectives. However, the likelihood of achievement is affected by limitations inherent in **all** systems of internal control.

Ultimately, the management should consider the inherent limitations of internal controls and prepare policies and procedures to minimize the inherited risks associated with the systems of internal control.

The ICFR framework is used to help organizations obtain reasonable assurance, as discussed on the following slide.

ICFR Framework



Entity Level Controls (ELC): **Entity-level controls** are internal **controls** that help ensure that management directives pertaining to the entire **entity** are carried out.

Transaction Level Controls: **Transaction level controls** relate to a particular class of **transactions**, account **balances** or financial statement **disclosures**.

Automated/ Application Controls: An **automated / application control** is a mechanism or device inside an application or interface that enforces or **controls** a rule-set or validation on one or more conditions inside of a process.

IT General Controls (ITGC): IT **general controls** (ITGC) are **controls** that apply to all systems components, processes, and data for a given organization or information technology (IT) environment.

The following slides provide various examples of each of these types of controls in the ICFR framework.

Automated/ Application Control Categories

Automated controls are commonly grouped into five categories

Type	Description	Examples
Edit Checks	Limit risk of inappropriate input, processing or output of data due to field format.	• Required fields • Required number of digits
Validations	Limit risk of inappropriate input, processing or output of data due to the confirmation of a test.	• 3-way match • Tolerance limits
Calculations	Ensure that a computation is occurring accurately.	• Accounts receivable aging • Pricing calculations • Depreciation
Interfaces	Limit risk of inappropriate input, processing or output of data being exchanged from one application to another.	• Duplicate record checks • Error reporting during batch runs
Authorizations	Limit the risk of inappropriate input, processing or output of key financial data due to unauthorized access to key financial functions or data. Includes: • Segregation of incompatible duties • Authorization checks, limits, and hierarchies	• Segregation of vendor entry and invoice entry in Accounts Payable • Approval to post journal entries • Workflow approvals

Transaction Level Controls

Control Nature	Description
Manual control	Manual controls are performed by a person without making use of automated systems.
Automated / Application control	Automated controls are performed by an automated system. Fully automated controls are designed for the completeness and accuracy of processing the data, from input through output.
IT Dependent Manual control	Manual controls that are considered dependent on IT systems for the complete performance of the control. These controls have an automated part and a manual part, where the manual part is dependent on the automated part.

Key Controls vs. Non-key Controls

Key / Non-key	Description
Key Controls	• If it fails in the absence of other factors, will result in at-least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. • Management relies on most for the integrity of financial statements and are designed to reasonably detect or prevent a material misstatement. • Designed in such a manner that they mitigate multiple risks or prevent/detect significant errors in financial statements.
Non-key Controls	• Non-key controls are additional controls that provide comfort that the risk is mitigated. • They could be specific to business operations, but do not have a high impact on financial transaction processing and financial reporting.

Preventive vs. Detective Controls

	Preventive Controls	Detective Controls
Function	Designed to prevent something from going wrong so that an error can be avoided	Designed to detect and correct in a timely manner an error or irregularity that would materially affect the achievement of the company's objectives
Examples	1. Policies & procedures 2. Segregation of duties 3. Delegation of authority 4. User ID/passwords 5. System access 6. Physical controls	7. Account reconciliations 8. Management review 9. Master file change reports 10. Journal entry review 11. Confirmations 12. Performance reviews

Next, we will discuss how to identify transactions that are significant to the financial statements.

Determining Significant Accounts and Disclosures

General Approach for Determining Significant Accounts and Disclosures

- The following step ought to be considered by all organizations to determine their significant accounts and disclosures:
- Make Preliminary Judgments of Materiality Based on Overall Financial Statements. Judgments regarding materiality levels to the financial statements should be made as a starting point in determining significant accounts.
- The SEC May 16, 2005, Staff Statement indicates:
- ". . . the staff should understand that management generally establishes quantitative thresholds to be used in identifying significant accounts subject to the scope of internal control testing. The use of a percentage as a minimum threshold may provide a reasonable starting point for evaluating the significance of an account or process; however, judgment, including the review of qualitative (nature of account) factors, must be exercised to determine if amounts above or below that threshold must be evaluated."
- Both Quantitative Materiality and Qualitative Risk Factors should be considered when determining significant accounts, which are outlined on the following slide.

Determine Significant Accounts Based on Quantitative Materiality and Qualitative Risk Factors

- Determinations of the quantitative significance of an account, component, or disclosure should consider whether possible misstatements could exist on either an individual basis or when combined with other misstatements that could have a material impact on the financial statements. In addition, qualitative factors such as the nature of the account and the potential for error should be considered in determining significance.
- According to AS 2201.29 to identify significant accounts and disclosures and their relevant assertions, the management should evaluate the qualitative and quantitative risk factors related to the financial statement line items and disclosures.

There are various risk factors that must be considered when determining significant accounts. The following slide provides detail on the risk factors that must be considered.

Risk Factors

1. Size and composition of the account.
2. Susceptibility to misstatement due to errors or fraud.
3. Volume of activity, complexity, homogeneity of the individual transactions processed through the account or reflected in the disclosure.
4. Accounting and reporting complexities associated with the account or disclosure.
5. Exposure to losses in the account.
6. Possibility of significant contingent liabilities arising from the activities reflected in the account or disclosure.
7. Existence of related-party transactions in the account.
8. Changes from the prior period in account or disclosure characteristics.
9. Implementation of new accounting standards such as, Leases, may also present risk factors related to certain financial statement line items and disclosures and require additional management attention in the period of adoption.

Significant Classes of Transactions

Significant classes of transactions occur within a significant account and are those classes of transactions that are significant to the financial statements.

It may be helpful to categorize classes of transactions as routine transactions, nonroutine transactions, or estimation because different types of classes of transactions have different levels of inherent risk and require different levels of management supervision.

- *Routine* transactions are recurring financial activities that are reflected in the accounting records in the normal course of business, such as distributor sales and retail sales, purchases, cash receipts, disbursements, and payroll.
- *Nonroutine* transactions are activities that occur only periodically and involve data generally not part of the routine flow of transactions, such as adjusting the perpetual inventory balance for the physical inventory, estimations, implementation of new accounting standards, related party transactions, mergers, or plant closings.
- *Estimation* transactions are activities that involve management judgments or assumptions to formulate account balances in the absence of a precise means of measurement, such as determining the allowance for doubtful accounts or warranty reserves.

In many organizations, most of the processing time, resources, and volume typically relate to routine transactions. Care should be taken by the Management to ensure that non-routine and estimation-type transactions are not unintentionally excluded from the internal control identification process.

Classes of transactions and processes relating to the financial close and reporting (i.e., performing the accounting period close, capturing and processing other nonroutine information requiring significant estimates and judgments from management, preparing and reviewing financial statement disclosures, and reviewing and approving the financial statements) are considered by SEC to be entity-level controls, and the management should always consider them significant.

Next, we will discuss control owner responsibilities of internal controls over financial reporting (ICFR).

Control Owner Responsibilities Overview

Control Owner Responsibility Overview

It is good practice for companies to design and maintain effective Internal Controls over Financial Reporting (ICFR) and annually assess and report on the internal control environment.

Control Owner Responsibilities				ITGCs
General	Management Review	IPE	User Access	
Effectively design, operate and monitor controls; understand control risks.	Articulate the review process.	Ensure IPE is complete and accurate.	Ensure the right people have the right level of access to the right system(s).	MDC's IT systems are fundamental to the operation of many of the County's business processes
Participate in walkthroughs, provide evidence, inform internal and external team of planned control changes.	Maintain written evidence of management review.	Review manual spreadsheet controls every instance the control takes place to ensure they are operating as intended; retain evidence of reviews.	Define and maintain list of critical roles (i.e., user access roles) impacting financial data.	
Develop a corrective action plan to remediate the root cause of identified deficiencies.	Obtain comfort that there are no material matters undetected.	Understand the source of data and the business controls that would detect an error in the report data.	Ensure all user access marked for removal/change during the quarterly review is properly removed/changed.	

The following two slides address control owner responsibilities related to active monitoring of control effectiveness as well as during control testing.

Control Owner Responsibilities: Active Monitoring

Control owners are responsible for the effective design, operation and real-time monitoring of controls. They can accomplish this by:

- Understanding the relevant risks associated with the control and serve as the subject-matter expert
- Understanding how the control fits and impacts the overall financial reporting process
- Developing and maintaining desk procedures that describe the control
- Articulating, documenting and maintaining evidence of **management review** procedures
- Understanding the source of data and how that data is controlled
- Developing and maintaining key manual spreadsheets with proper controls in place
- Self-reporting and correcting issues that are identified
- Understanding the impact of changes (e.g., people, processes and technology) on the control and ensuring continued effective design and operation

Control Owner Responsibilities: During Testing

During control testing, control owners are expected to

- Participate in control walkthroughs with the internal audit team and external auditors
- Provide evidence and other requested documentation for the sample selections
- Inform the internal audit team when any significant changes to the control are planned (e.g. people, processes and technology)
  - This may have an impact on the timing of internal control testing
- Participate in discussions surrounding identified deficiencies and irregularities
- Collaborate with the internal audit team in the deficiency review and remediation process
  - Ensure the root cause of the deficiency is identified and the remediation process addresses the root cause and not the symptom

As stated, control owners are responsible for the effective design, operation and real-time monitoring of controls. In the next section, we will provide further detail on control owner responsibility as it relates to evaluating control design.

Control Owner Responsibilities: Evaluating Control Design

Evaluating Design of Controls

Once the management has obtained an understanding of significant classes of transactions and processes and identified the controls over the significant accounts and disclosures, several determinations should be made:

- Is the design of controls effective?

- Which controls should be tested for operating effectiveness?

It is generally not necessary to test the design and operating effectiveness of **all** controls identified that relate to significant accounts and disclosures. In general, controls to be tested are those that are important to achieving control objectives that have been implemented by management to mitigate identified risks of misstatement in the financial statements.

Many organizations identify the controls that should be tested as *key controls*. *Key controls* are generally those that are considered as the primary controls for the achievement of a control objective. Other organizations may rate controls as to their importance (such as high, medium, low; A, B, C; or 1,2, 3) and test only those at or above a particular rating scale.

The following slide will address control owner considerations as they assess control design.

Test of Design

Ultimately, an effective system of internal control takes into account its inherent limitations. Hence, the management should include policies and procedures to minimize the risks associated with the systems of internal control.

When considering design effectiveness, the management should consider broad questions such as:

- Are identified controls appropriate considering the transaction process? If operating, would they achieve the control objective(s) for that area?
- Do controls address all relevant financial statement assertions?
- Do the individuals responsible for performing the control have the appropriate knowledge and experience?
- Is there appropriate segregation of duties?

The following slide will address procedures control owners may use to assess design effectiveness.

Procedures for Assessing Design Effectiveness

- Generally, walkthroughs will contain a combination of inquiry, observation, and inspection procedures and are, therefore, normally sufficient to evaluate design effectiveness.
- In describing the identification of risks, SEC indicates that some knowledge of processes will generally be necessary by stating:

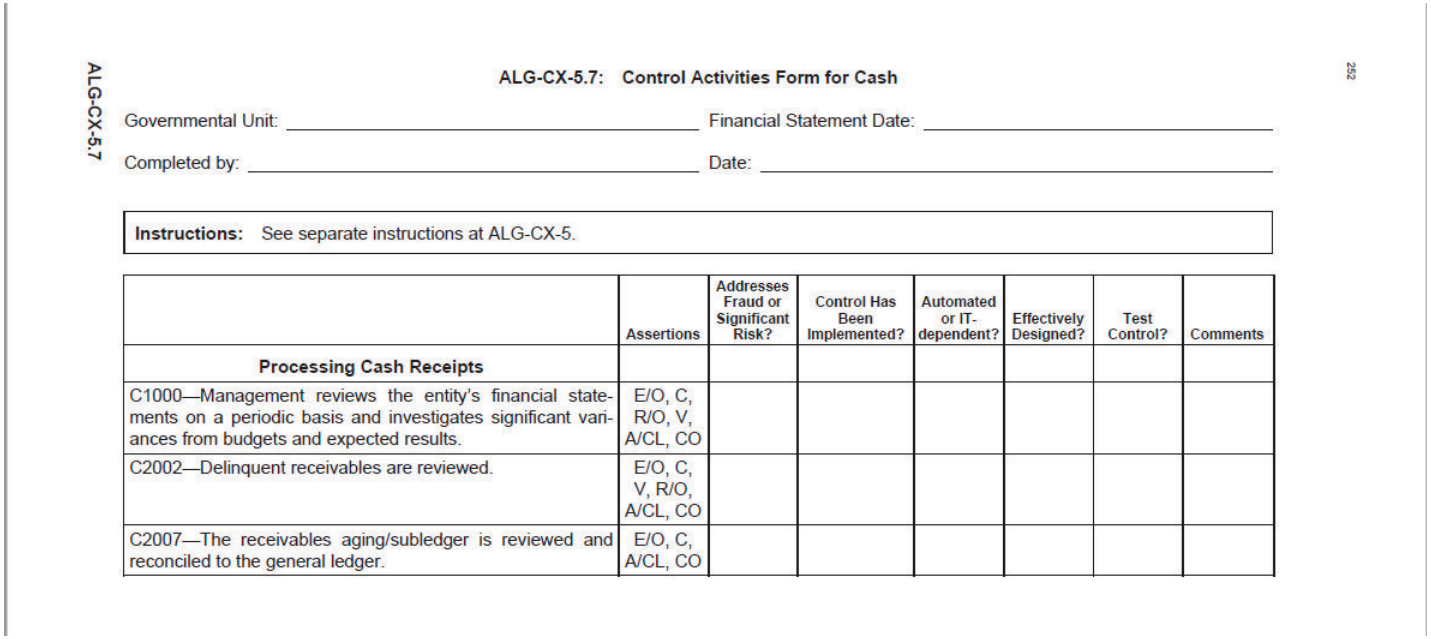
"To identify financial reporting risks in a larger business or a complex process, management's methods and procedures may involve a variety of company personnel, including those with specialized knowledge. These individuals, collectively, may be necessary to have a sufficient understanding of GAAP, the underlying business transactions and the process activities, including the role of computer technology, that are required to initiate, authorize, record and process transactions."

- Management should utilize COSO Entity-Level Control and Control Activities checklists.

The following slide includes a checklist that County control owners are expected to use to monitor and design internal controls.

County Control Activities Checklist

Control Owners should use county checklists to monitor and design controls.



ALG-CX-5.7

ALG-CX-5.7: Control Activities Form for Cash

252

Governmental Unit: _____ Financial Statement Date: _____

Completed by: _____ Date: _____

Instructions: See separate instructions at ALG-CX-5.

	Assertions	Addresses Fraud or Significant Risk?	Control Has Been Implemented?	Automated or IT-dependent?	Effectively Designed?	Test Control?	Comments
Processing Cash Receipts							
C1000—Management reviews the entity's financial statements on a periodic basis and investigates significant variances from budgets and expected results.	E/O, C, R/O, V, A/CL, CO						
C2002—Delinquent receivables are reviewed.	E/O, C, V, R/O, A/CL, CO						
C2007—The receivables aging/subledger is reviewed and reconciled to the general ledger.	E/O, C, A/CL, CO						

As stated, control owners are responsible for the effective design, operation and real-time monitoring of controls. In the next section, we will provide further detail on control owner responsibility as it relates to testing and monitoring.

Control Owner Responsibilities: Testing and Monitoring using Sample Selection Methodology

Testing the Operating Effectiveness of Controls

A major component of evaluating internal control over financial reporting is the testing of identified key controls to determine their operating effectiveness. In most cases, management cannot assess controls as being effective without testing the operation of controls. In an evaluation of an entire internal control system over financial reporting, testing should include controls over ***all five components and related principles*** of COSO Framework.

Typically, testing of controls should occur at the significant locations and those locations with specific risks identified.

Testing is typically confined to the key controls previously identified and tested for design effectiveness. However, if a control is found to have a deficiency in design, its operating effectiveness need **not** be tested because a control that has a design flaw cannot be an effective control, no matter how well it functions.

Note: AS 2201, and SEC Interpretive Release, indicates that the amount of evidence needed by the management depends upon the risk associated with the control. As the control risk increases, the evidence required by the management should increase to reduce the risk to an acceptable low level.

The following slide includes specific steps a control owner may take to monitor and test effectiveness of their controls.

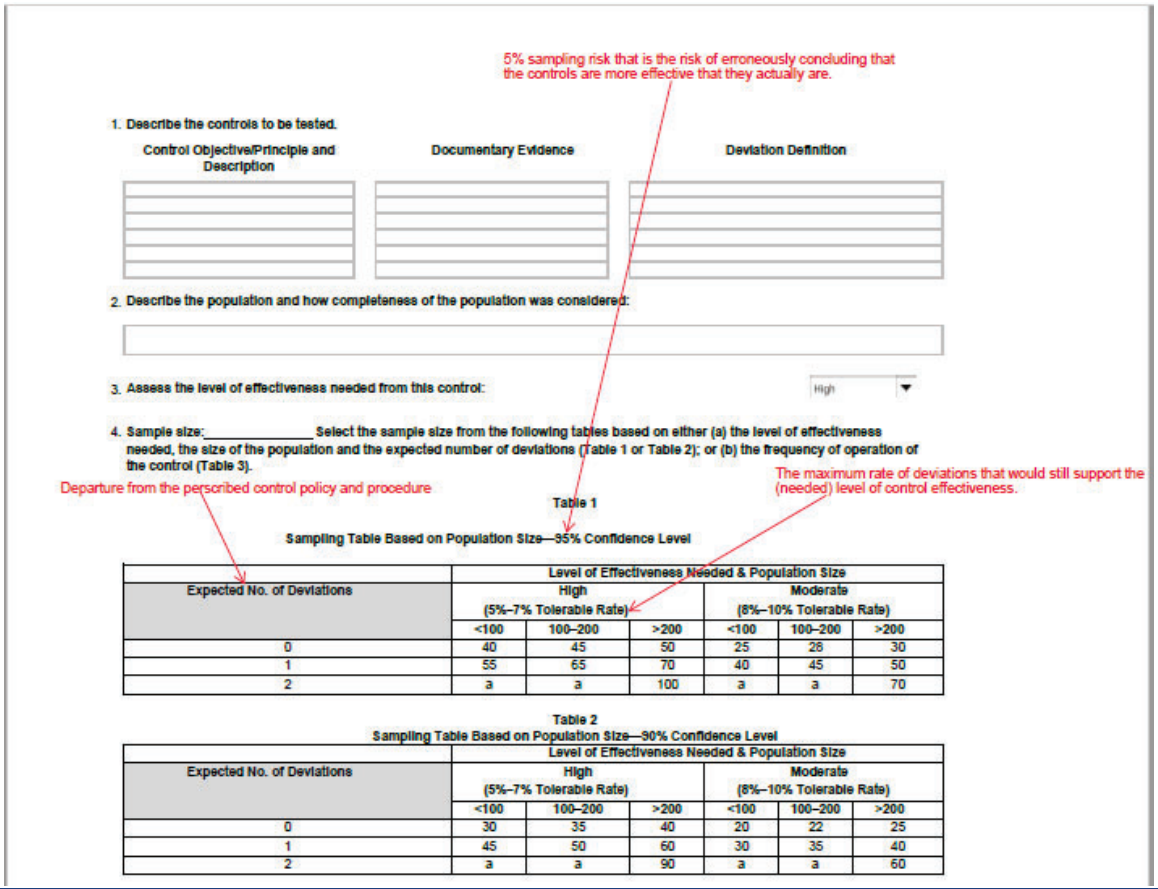
Test of Effectiveness

Control owners should test and monitor their controls for effectiveness. The process for monitoring controls for effectiveness is as follows:

1. Describe the controls to be tested
2. Describe the population and how completeness of the population was considered
3. Assess the level of effectiveness needed from this control
4. Sample Size
5. Sample Selection Method
6. Results
7. Conclusion

The following slide outlines this process in more detail using visual examples of a workpaper used to monitor a control.

Test of Effectiveness



5% sampling risk that is the risk of erroneously concluding that the controls are more effective that they actually are.

1. Describe the controls to be tested.

Control Objective/Principle and Description	Documentary Evidence	Deviation Definition

2. Describe the population and how completeness of the population was considered:

3. Assess the level of effectiveness needed from this control: High

4. Sample size:_____ Select the sample size from the following tables based on either (a) the level of effectiveness needed, the size of the population and the expected number of deviations (Table 1 or Table 2); or (b) the frequency of operation of the control (Table 3).

Departure from the perscribed control policy and procedure

The maximum rate of deviations that would still support the (needed) level of control effectiveness.

Table 1

Sampling Table Based on Population Size—95% Confidence Level

Expected No. of Deviations	Level of Effectiveness Needed & Population Size					
	High (5%–7% Tolerable Rate)			Moderate (8%–10% Tolerable Rate)		
	<100	100–200	>200	<100	100–200	>200
0	40	45	50	25	26	30
1	55	65	70	40	45	50
2	a	a	100	a	a	70

Table 2

Sampling Table Based on Population Size—90% Confidence Level

Expected No. of Deviations	Level of Effectiveness Needed & Population Size					
	High (5%–7% Tolerable Rate)			Moderate (8%–10% Tolerable Rate)		
	<100	100–200	>200	<100	100–200	>200
0	30	35	40	20	22	25
1	45	50	60	30	35	40
2	a	a	90	a	a	60

Test of Effectiveness

Note:

- Sampling would not be efficient in this situation because the sample size would comprise a large portion of the population.

Table 3

Sampling Table for Infrequently Operating Controls

Control Frequency and Population Size	Sample Size
Quarterly (4)	2
Monthly (12)	2–4
Semimonthly (24)	3–8
Weekly (52)	5–9

5. **Document your sample selection method:** ○ Haphazard ○ Random ◉ Systematic

   Does the sample seem representative of the population? ◉ Yes ○ No

   Note: If the sample does not seem representative, then reselect the sample. Document the selected sample items.

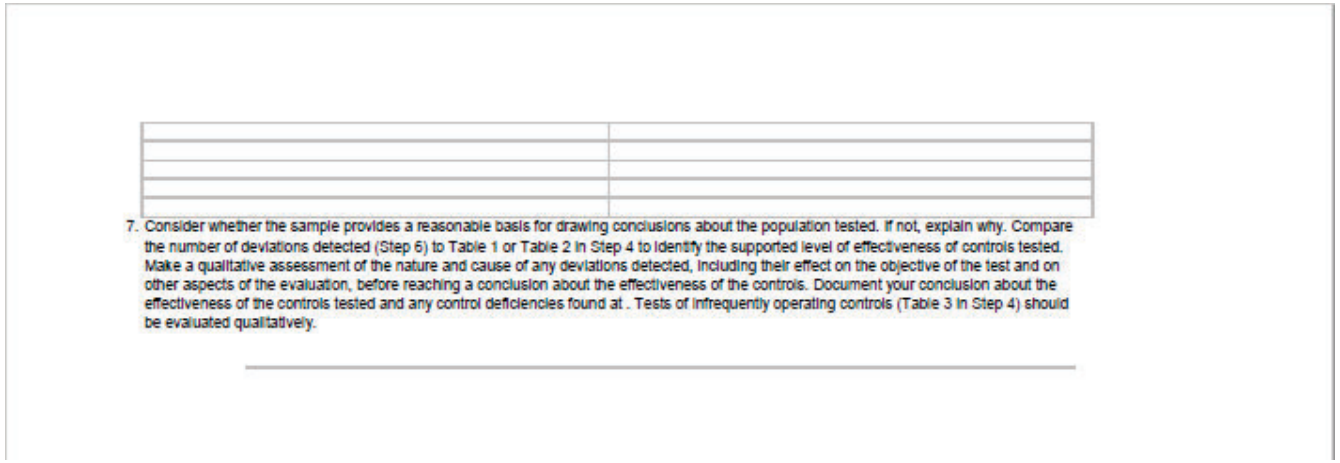
6. **Document the results of this test below.**

   Number of deviations detected:

   Describe deviations in the space below and inquire about their cause.

Deviation	Cause

Test of Effectiveness



7. Consider whether the sample provides a reasonable basis for drawing conclusions about the population tested. If not, explain why. Compare the number of deviations detected (Step 6) to Table 1 or Table 2 in Step 4 to identify the supported level of effectiveness of controls tested. Make a qualitative assessment of the nature and cause of any deviations detected, including their effect on the objective of the test and on other aspects of the evaluation, before reaching a conclusion about the effectiveness of the controls. Document your conclusion about the effectiveness of the controls tested and any control deficiencies found at . Tests of infrequently operating controls (Table 3 in Step 4) should be evaluated qualitatively.

In the next several slides, we will cover how to perform random sampling to perform internal control test of effectiveness.

Random Sample Selections - Random Number Tables

- Regardless of the method of sampling used, statistical or nonstatistical, a simple random selection provides each item in the population an equal chance to be selected.

Below is an example of a Random Number Table used to perform random sample selections.

- The number of digits selected from the random digit table should be the same as the number of digits of the population size.
- For example, if population is 500 invoices, select 3 digits at the time moving left to right or top to bottom. Using the table below , the first 3 selected invoices will be: 111th invoice, 643 (should be ignored because is larger than the population size of 500), 631 also ignore, 875 also ignore, 061 valid invoice, 376 valid invoice.

The next several slides help visualize random number tables used to perform random sampling.

Random Number Tables

TABLE 1 - RANDOM DIGITS

11164	36318	75061	37674	26320	75100	10431	20418	19228	91792
21215	91791	76831	58678	87054	31687	93205	43685	19732	08468
10438	44482	66558	37649	08882	90870	12462	41810	01806	02977
36792	26236	33266	66583	60881	97395	20461	36742	02852	50564
73944	04773	12032	51414	82384	38370	00249	80709	72605	67497
49563	12872	14063	93104	78483	72717	68714	18048	25005	04151
64208	48237	41701	73117	33242	42314	83049	21933	92813	04763
51486	72875	38605	29341	80749	80151	33835	52602	79147	08868
99756	26360	64516	17971	48478	09610	04638	17141	09227	10606
71325	55217	13015	72907	00431	45117	33827	92873	02953	85474
65285	97198	12138	53010	94601	15838	16805	61004	43516	17020
17264	57327	38224	29301	31381	38109	34976	65692	98566	29550
95639	99754	31199	92558	68368	04985	51092	37780	40261	14479
61555	76404	86210	11808	12841	45147	97438	60022	12645	62000
78137	98768	04689	87130	79225	08153	84967	64539	79493	74917
62490	99215	84987	28759	19177	14733	24550	28067	68894	38490
24216	63444	21283	07044	92729	37284	13211	37485	10415	36457
16975	95428	33226	55903	31605	43817	22250	03918	46999	98501
59138	39542	71168	57609	91510	77904	74244	50940	31553	62562
29478	59652	50414	31966	87912	87154	12944	49862	96566	48825
96155	95009	27429	72918	08457	78134	48407	26061	58754	05326
29621	66583	62966	12468	20245	14015	04014	35713	03980	03024
12639	75291	71020	17265	41598	64074	64629	63293	53307	48766
14544	37134	54714	02401	63228	26831	19386	15457	17999	18306
83403	88827	09834	11333	68431	31706	26652	04711	34593	22561

Another method of sampling is called systematic sampling. The next slide provides detail on this methodology.

Systematic Sampling

- This method can be used with nonstatistical or statistical sampling to give every item in the population an equal chance of being selected if a random start (item) is used. However, it may not produce an equal opportunity for all combinations of sampling units to be selected unless numerous random starts are made. The sampling interval is determined by dividing the population by the number of items to be sampled.
- Example: Assume that we have a population of 5,000 invoices, with 95% confidence level needed, and applying a sample size of 50 invoices. First step, we randomly select one invoice from the population, then systematically (i.e., we select one invoice every 100 invoices to represent the whole population) select until you have reached the sample size of 50 invoices. (Statically Systematic Sampling satisfies the standards)

On the next slide we will talk about the final method of sampling, which is haphazard selection.

Haphazard Selection

- In this sense, haphazard does not mean "careless;" it means "without conscious bias."
- Under this method, sampling items are selected in no specific pattern without bias for or against any items in the population.
- This could be done by selecting a sample of items from the paid invoices for the year if there were no bias for or against large ones.
- The management may use this method for nonstatistical samples, provided care is taken to be sure no conscious bias is added to the selection process.

Once test of effectiveness has taken place, control owners may form a conclusion on control effectiveness. The next slide addresses how to form a conclusion.

Forming a Conclusion on Control Effectiveness

If a material weakness is identified, the conclusion must be that internal controls over financial reporting are **not** effective. If a report is issued by management to third parties, under the requirements of COSO Frameworks, a material weakness would disqualify a conclusion that internal control was effective.

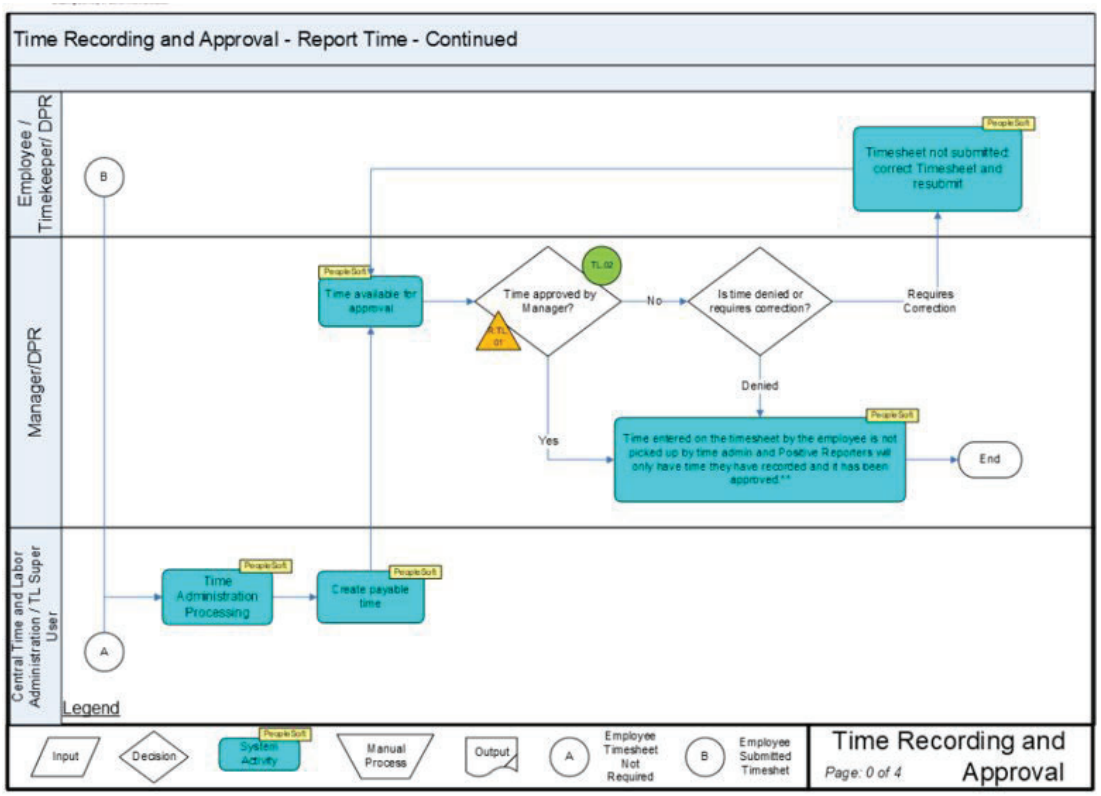
The following slides tie together the concepts we've learned thus far including evaluating the design of controls, monitoring and testing effectiveness of controls. We will share an example using a control in the County's Risk and Control Matrix to illustrate where to identify controls in the County's flowcharts as well as how this control was designed and how it will be tested for effectiveness.

Example Internal Control

Example: Time Recording and Approval

- The flowchart to the right depicts the time recording and approval process.
- Within the time recording and approval process, there is risk that time entered by employees is not accurate and therefore, employees are paid for incorrect hours. (yellow triangle)
- To mitigate this risk, a control was identified over manager approval of time entered by employees. (green circle)

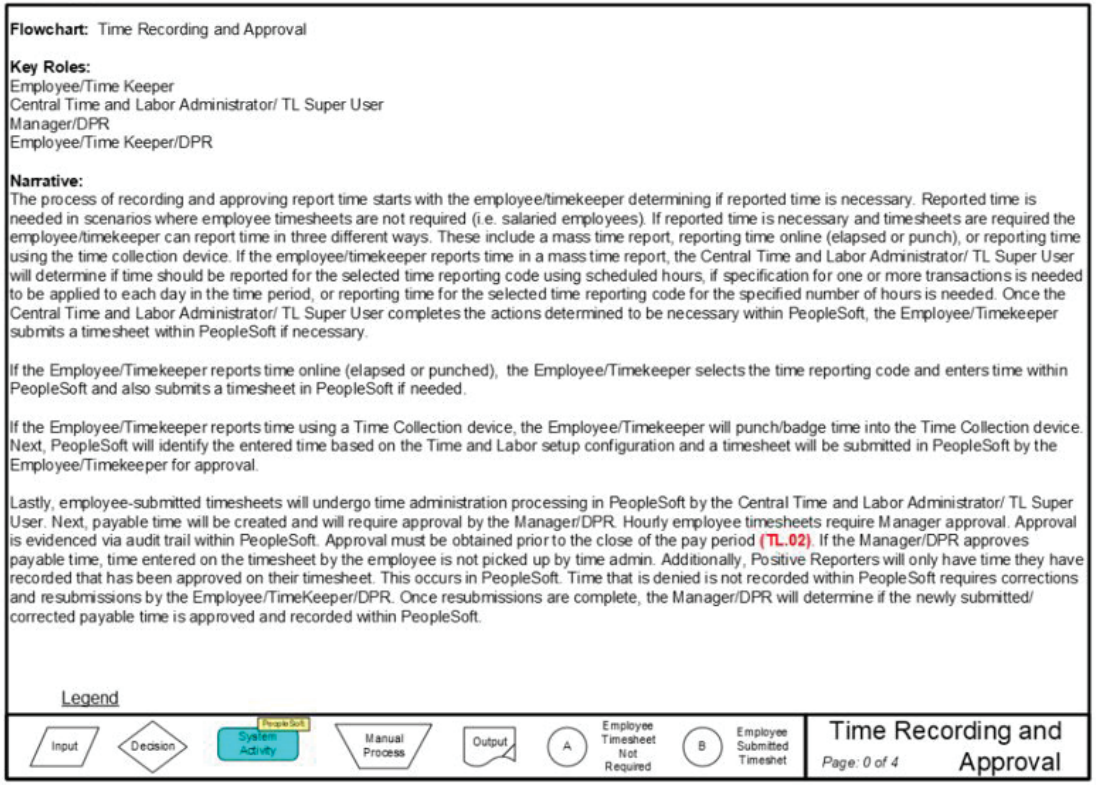
The next slide provides detail around the narrative for this process.



Example: Time Recording and Approval

- Once risks and controls are identified, placed on the corresponding process flow diagrams, and defined in the Risk and Control Matrix, a control narrative can be created.
- A control narrative is a detailed written explanation of the process and any related controls that are in place to mitigate the risks identified in the process. The narrative shown here was written for the Time Recording and Approval process.

The next slide provides detail around the design of this control.



Flowchart: Time Recording and Approval

Key Roles:
Employee/Time Keeper
Central Time and Labor Administrator/ TL Super User
Manager/DPR
Employee/Time Keeper/DPR

Narrative:
The process of recording and approving report time starts with the employee/timekeeper determining if reported time is necessary. Reported time is needed in scenarios where employee timesheets are not required (i.e. salaried employees). If reported time is necessary and timesheets are required the employee/timekeeper can report time in three different ways. These include a mass time report, reporting time online (elapsed or punch), or reporting time using the time collection device. If the employee/timekeeper reports time in a mass time report, the Central Time and Labor Administrator/ TL Super User will determine if time should be reported for the selected time reporting code using scheduled hours, if specification for one or more transactions is needed to be applied to each day in the time period, or reporting time for the selected time reporting code for the specified number of hours is needed. Once the Central Time and Labor Administrator/ TL Super User completes the actions determined to be necessary within PeopleSoft, the Employee/Timekeeper submits a timesheet within PeopleSoft if necessary.

If the Employee/Timekeeper reports time online (elapsed or punched), the Employee/Timekeeper selects the time reporting code and enters time within PeopleSoft and also submits a timesheet in PeopleSoft if needed.

If the Employee/Timekeeper reports time using a Time Collection device, the Employee/Timekeeper will punch/badge time into the Time Collection device. Next, PeopleSoft will identify the entered time based on the Time and Labor setup configuration and a timesheet will be submitted in PeopleSoft by the Employee/Timekeeper for approval.

Lastly, employee-submitted timesheets will undergo time administration processing in PeopleSoft by the Central Time and Labor Administrator/ TL Super User. Next, payable time will be created and will require approval by the Manager/DPR. Hourly employee timesheets require Manager approval. Approval is evidenced via audit trail within PeopleSoft. Approval must be obtained prior to the close of the pay period (TL.02). If the Manager/DPR approves payable time, time entered on the timesheet by the employee is not picked up by time admin. Additionally, Positive Reporters will only have time they have recorded that has been approved on their timesheet. This occurs in PeopleSoft. Time that is denied is not recorded within PeopleSoft requires corrections and resubmissions by the Employee/TimeKeeper/DPR. Once resubmissions are complete, the Manager/DPR will determine if the newly submitted/ corrected payable time is approved and recorded within PeopleSoft.

Legend

Input | Decision | PeopleSoft System Activity | Manual Process | Output | A | Employee Timesheet Not Required | B | Employee Submitted Timesheet

Time Recording and Approval

Page: 0 of 4

Test of Design

- Control Description: Hourly employee timesheets are approved by an appropriate manager/supervisor for each pay period.
- During the Test of Design, control owners would walk through the process to verify that the control is still designed effectively. They would provide an example to show how the process works. Formal documentation over the conversation and sample would be completed.
- For Example: The control owner would show that the timesheets had been approved by the appropriate manager/supervisor prior to the employee being paid. This would be evidenced via a signature and review date physically on the timesheets, or through an approval process within the system.
- Control owners would utilize the county checklists to assess the design of the control, and to track progress.

The next slide provides detail around the effectiveness of this control.

Test of Effectiveness

- Control Description: Hourly employee timesheets are approved by an appropriate manager/supervisor for each pay period.
- Population: All hourly payroll cycles for the year
- Level of Effectiveness needed from this control: High
- Sample Size: table 3, weekly control, 5-9 samples required
- Sample Selection Method: Random, randomly select weeks for the year
- Testing: Tested 9 weeks of payroll, and noted the proper approval was evidenced for all of these weeks
- Results: Control is operating effectively

Next, we will address how to evaluate internal control deficiencies.

Control Owner Responsibilities: Evaluating Deficiencies

Control Owner - Deficiency Review Process

During the control deficiency review, control owners should

- Assist in determining the root cause of the deficiency
- Assess the outcome of the failure (e.g. magnitude /impact, number of failures noted in sample set)
- Develop a corrective action plan to remediate the root cause of the deficiency:
  - Include a detailed description of the action plan
  - Identify key personnel responsible for the action plan implementation
  - Establish a target date for implementation
- Participate in the executive review of all control deficiencies

Effectiveness of the design and operation of the controls ultimately impacts the County's financial statements. We will address how to evaluate a deficiency on the following slide.

Evaluating Deficiencies

The COSO Framework defines an *internal control deficiency* as a "shortcoming in a component or components and relevant principle(s).

When an entity determines that an internal control deficiency exists, the COSO Framework indicates that management uses judgment in assessing the severity of the deficiency to determine whether (a) each of the components and relevant principles are present and functioning, (b) the control components are operating together, and ultimately, (c) the entity's system of internal control is effective.

The COSO Framework defines a major deficiency exists when management concludes that ***a component and one or more relevant principles are not present or functioning*** or that components are not operating together. When a major deficiency exists, the COSO Framework is clear: management cannot conclude that the entity's internal control system is effective.

Not all exceptions are necessarily control deficiencies. However, to conclude that an identified exception is not a control deficiency, it is necessary to obtain additional evidence beyond that initially planned and beyond inquiry that supports the conclusion.

Frequently, this may necessitate additional testing. For example, if a sampling test identifies one control exception and tests of additional items identify another exception, the conclusion would be that the control was **not** effective.

Not all control deficiencies will be considered significant deficiencies or material weaknesses under the definitions of **AU-C 265** , COSO, or AS 2201. The severity of identified control deficiencies should be evaluated, considering both quantitative and qualitative factors, individually and in combination with other control deficiencies.

Note: COSO Framework recommends the guidance in **AU-C 265** and **AU-C 940** to evaluate the relative severity of a control deficiency.

The next slide provides examples of combination of multiple deficiencies that combine to a material weakness.

Examples of Combination of Multiple Deficiencies That Combine to a Material Weakness

The management has identified the following control deficiencies and concluded that, individually, each of the deficiencies are a significant deficiency:

- Several *accounts receivable* transactions were not properly recorded in the subsidiary ledger (the transactions were not material, either individually or in the aggregate).
- Account balances affected by the improperly recorded *accounts receivable* transactions were not reconciled on a timely basis.
- The company has inadequate segregation of duties over IT access controls related to the *accounts receivable* and billing function.

Because each of the significant deficiencies affects the same account (accounts receivable), the deficiencies, when considered together, represent a reasonable possibility that a material misstatement could occur and not be prevented or detected or corrected. Thus, the management likely would conclude that, in combination, the significant deficiencies represent a material weakness.

In another example, assume that management identified several control deficiencies that relate to a specific component principle of internal control instead of to a specific account balance or disclosure. Three control deficiencies relate to the entity's lack of adequate reviews and approvals. While each of these control deficiencies relate to different account balances, they all relate to the monitoring component of internal control. Thus, even though the management determined that individually each deficiency was only a control deficiency, the requirement in **AU-C 265.09** to combine control deficiencies by internal control component might cause the management to consider them a significant deficiency or even a material weakness.

In conclusion, our next couple slides will outline a summary of key concepts covered in this training.

Summary

Summary of Key Concepts

1. COSO Integrated Framework: Identifying potential risks and methods to mitigate risks is a critical control owner responsibility.
2. Internal Controls Over Financial Reporting at Miami-Dade County are internal controls that specifically focus on the activities which prevent and/or detect errors in financial reporting.
3. Control Owner Responsibilities include the following:
    a. Identifying Potential Fraud and Accounting Risks
    b. Identifying Significant Accounts
    c. Evaluating Control Design
    d. Testing and Monitoring using Sample Selection Methodology
    e. Evaluating Deficiencies

Questions?

For questions related to internal controls and for resources to facilitate evaluation, design and monitoring of controls please contact the Finance Department.

Leany Perez, CPA
Director of Accounting and Reporting
Leany.Perez@miamidade.gov

Arben Hankollari
Financial Controls & Policy Administrator
Arben.Hankollari@miamidade.gov

FAQ document will be circulated to all training participants following this training.