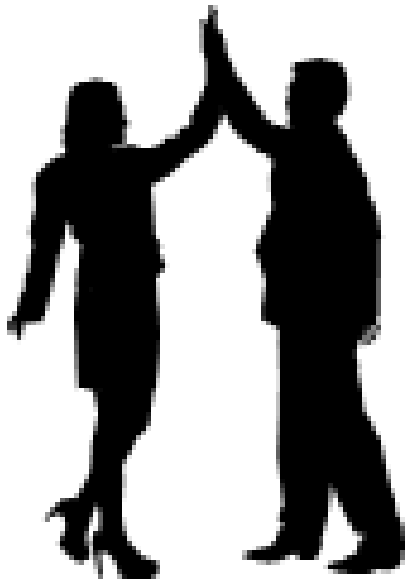
SOX & Other Key Topics

July 2019

pwc

Day 1 Agenda

- Introductions
- SOX Background
- Determining SOX Risks and Controls
- Types of Controls
- Management Review Controls
- Test of Design vs. Test of Operating Effectiveness
- Completeness and Accuracy of Source Data
- Sufficiency of Evidence
- Roll-forward procedures



SOX Background

Role of Our Regulators

The responsibility of the ***Public Company Accounting Oversight Board ("PCAOB")*** includes:

- registering public accounting firms;
- establishing auditing, quality control, ethics, independence, and other standards relating to public company audits;
- conducting inspections, investigations, and disciplinary proceedings of registered accounting firms; and
- enforcing compliance with Sarbanes-Oxley.

The responsibility of the ***Securities & Exchange Commission ("SEC")*** includes:

- Oversight authority over the PCAOB, including the approval of the Board's rules, standards and budget; and
- Establishing laws and rules that govern the securities industry.

Sarbanes-Oxley Act of 2002 - Main Components

The CEO and CFO are responsible for the adequacy of internal controls.

Section 302 Requirements state that the signing officers:

Are responsible for establishing and maintaining internal controls.

Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.

Section 906 Requirements state that the signing officers:

Must certify periodic reports containing financial statements filed by an issuer with the SEC.

Similar to Section 302, however, Section 906 imposes criminal penalties.

Management is responsible for maintaining a system of internal control over financial reporting ("ICFR"). ICFR is a process under the supervision of the issuer's CEO and CFO that provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

Required Management Documentation for a 404 Attestation

Key Controls	• Those controls that, individually or in combination are judged to be both effective in addressing the assessed assertion level risk of misstatement and efficient to test in order to achieve the expected controls reliance. • A control's impact on ICFR may be entity-wide or specific to an account balance, class of transactions or application.
Risk and Control Objectives	• Management should identify "what could go wrong" within a financial reporting element in order to identify the sources and potential likelihood of risk of material misstatement of the financial statements. • Control objectives provide specific criteria against which to evaluate the effectiveness of controls, to assist in evaluating whether controls can prevent or detect misstatements.
Evaluation of Design Effectiveness	• Documentation of the design of controls serves as evidence that controls within ICFR, including changes to those controls, have been identified, are capable of being communicated to those responsible for their performance, and are capable of being monitored by the Company. • The form and extent of the documentation can vary depending on the size, nature and complexity of the Company and the documentation can be presented in a number of ways (for example, flowcharts).
Tests of Operating Effectiveness	• Considers whether the control is operating as designed and whether the person performing the control possesses the necessary authority and competence to perform the control effectively. • Evaluation procedures should be tailored to management's assessment of risk characteristics • Evidence may be obtained from direct testing of controls and on-going monitoring activities.

Required Management Documentation for a 404 Attestation (cont'd)

Control Deficiency Evaluation

- Should include both quantitative and qualitative factors
- Consider whether there is a reasonable possibility that the Company's ICFR will fail to prevent or detect a misstatement of a financial statement amount or disclosure and the magnitude of the potential misstatement resulting from the deficiency or deficiencies.
- The severity of a deficiency in ICFR does not depend on whether a misstatement actually has occurred but rather on whether there is a reasonable possibility that the Company's ICFR will fail to prevent or detect a misstatement on a timely basis.
- Management should evaluate the effect of compensating controls when determining whether a control deficiency or combination of deficiencies is a material weakness.
- To have a mitigating effect, the compensating control should operate at a level of precision that would prevent or detect a misstatement that could be material.

Material Weakness

A deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

Significant Deficiency

A deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting.

Determining SOX Risks and Controls

Understanding Control Risk

Risk of material misstatement is the risk that the financial statements are materially misstated due to fraud or error. This consists of inherent risk and control risk. Such risks may exist at either the financial statement level or at the assertion level

- Inherent risk (at the assertion level) refers to the susceptibility of an assertion to a misstatement, due to error or fraud, that could be material, individually or in combination with other misstatements, before consideration of any related controls

Understanding the intended purpose of a control activity (i.e., which risk it is intended to address and what exactly the control operator is expected to accomplish) is fundamental to understanding, and evaluation, of ANY control and its relevance.

Management may perform certain activities within their process to address business and operational risks which do not have a financial reporting impact. Key controls are those that impact one or more relevant financial statement assertions for one or more significant accounts or disclosures.

Assertions Defined

- ***Transaction-level assertions:***
  - *Accuracy*. The assertion is that the full amounts of all transactions were recorded, without error.
  - *Classification*. The assertion is that all transactions have been recorded within the correct accounts in the general ledger.
  - *Completeness*. The assertion is that all business events to which the company was subjected were recorded.
  - *Cutoff*. The assertion is that all transactions were recorded within the correct reporting period.
  - *Occurrence*. The assertion is that recorded business transactions actually took place.

Assertions Defined

- ***Account balance assertions:***
  - *Completeness*. The assertion is that all reported asset, liability, and equity balances have been fully reported.
  - *Existence*. The assertion is that all account balances exist for assets, liabilities, and equity.
  - *Rights and obligations*. The assertion is that the entity has the rights to the assets it owns and is obligated under its reported liabilities.
  - *Valuation*. The assertion is that all asset, liability, and equity balances have been recorded at their proper valuations.

Assertions Defined

- ***Presentation and disclosure assertions***
  - *Accuracy*. The assertion is that all information disclosed is in the correct amounts, and which reflect their proper values.
  - *Completeness*. The assertion is that all transactions that should be disclosed have been disclosed.
  - *Occurrence*. The assertion is that disclosed transactions have indeed occurred.
  - *Rights and obligations*. The assertion is that disclosed rights and obligations actually relate to the reporting entity.
  - *Understandability*. The assertion is that the information included in the financial statements has been appropriately presented and is clearly understandable.

Identifying & Assessing Control Risk

- Assessing Control Risk includes:
  - Identify the specific points in the process where misstatements due to fraud or error could arise that, individually or in combination with other misstatements, would be material.
  - Identify risks of misstatement for all relevant assertions
  - Address whether segregation of duties is important to the process and related controls
  - Identify where management's process and related controls depend on the use of IT (and therefore ITGCs)
  - Identify the risk of misstatement in journal entries related to the business process, whether due to error or fraud

- Identifying risks includes identifying those activities which have a financial statement impact
  - Not all risks have a financial statement impact
  - Example - Inefficiencies in a pricing tool used to underwrite policies may represent an operational risk to a Company; however, controls around setting pricing of a policy does not have a direct financial statement impact and therefore does not necessarily represent a key SOX risk

Control Risk Examples

- Purchases & Payables :
  - Purchases are not appropriately authorized
  - Payments are not recorded in the correct period
  - Purchases and payables transactions and balances are not appropriately classified, presented or disclosed
- Mortgage Loans
  - Investment is made in loans that are not credit worthy
  - Delinquent or impaired loans are not identified in a timely manner

Specificity and granularity are key when documenting control risks. For example:

Before:

Loss reserves are not valued correctly.

Best Practice:

Actuarial model used to estimate loss reserves is not appropriate.

Expected loss ratio used to estimate loss reserves are not reasonable.

Loss development factors used to estimate loss reserves are not reasonable.

Identifying Key Controls

Identifying key controls begins with a thorough understanding of the end to end business process.

To further understand the risks within a process and to identify controls to test, it is important to perform the following:

- Understand the flow of transactions related to the relevant assertions, including how these transactions are initiated, authorized, processed, and recorded;
- Identify the points within a process at which a misstatement—including a misstatement due to fraud—could arise that, individually or in combination with other misstatements, would be material;
- Identify the controls that management has implemented to address these potential misstatements; and
- Identify the controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could result in a material misstatement of the financial statements.

The decision as to whether a control is key depends on which controls, individually or in combination, sufficiently address the assessed risk of misstatement to a given relevant assertion.

Assessing the Risk of a Key Control

Factors that affect the risk within a specific control may include:

- The nature and materiality of misstatements that the control is intended to prevent/detect
- The inherent risk associated with the related accounts/assertions
- Changes in the volume or nature of transactions
- Nature of the control and frequency that it operates
- Degree to which the control relies on the effectiveness of other controls
- Whether the control relies on performance by an individual or is automated

The level of evidence required to assess the operating effectiveness of a control is typically linked to the risk associated with that control.

Assessing the Risk of a Key Control

Some common execution pitfalls related to assessing the "risk associated with a control" include using a 'relative to each other' rating method (i.e., assessing the risks associated with various controls in a particular transaction cycle or within the information technology environment as relatively higher or lower amongst that smaller group of controls).

The ramification of incorrectly risk rating a control (including an ITGC) is the potential mismatch with the amount of work performed and resulting evidence obtained. It can also be challenging to support an otherwise rational conclusion a deficiency is only a control deficiency (versus a significant deficiency or material weakness) when the deficient lower risk control has been rated higher risk.

Not all controls that address relevant assertions over significant accounts are high risk. Each control is assessed on its own merits.

Control Types

Types of Controls

Entity level controls (ELCs)

- Entity level controls include:
  - Controls related to the control environment, management override
  - Controls to monitor other controls
  - Controls over the period-end financial reporting process
- ELCs are important to the overall understanding and evaluation of ICFR, and many ELCs are control activities.

Transaction level controls

- Transaction level controls are a type of control activity operating within business processes relevant to financial reporting and surrounding the underlying information systems by which transactions are initiated, authorized, recorded, processed, corrected as necessary, transferred to the general ledger, and reported in the financial statements. These control activities are designed to operate at a level of precision that would prevent, or detect and correct on a timely basis, misstatements to FSLIs at the assertion level.

Entity Level Controls

ELCs vary in nature and precision and could have a direct or an indirect effect on the likelihood that a misstatement will be prevented, or detected and corrected on a timely basis. ELCs may exist at multiple levels within an entity (or component of the entity), including the group, region, sector, segment, division, shared services center, location and/or other business unit levels.

The following diagram depicts a continuum relating to the level of precision at which an ELC operates and its impact on a relevant assertion for a significant account, class of transaction, or disclosure:

COSO 2013 – Components and 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. 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & 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

Review Controls

Identifying Review Controls

Controls whereby the control operator reviews certain information and takes other necessary actions based on the results of the review

Some serve to monitor the effectiveness of other controls, some are designed to detect misstatements that could occur if there are failures in other controls (e.g., business performance reviews).

While others serve as the 'final check' to prevent the misapplication of GAAP or other potential misstatements (e.g., the review of an estimate developed by others).

Identifying Review Controls

- Review controls might include:
  - Review of manual or spreadsheet calculations
  - Review of estimates or other accounting analyses
  - Reviews of the effectiveness of other controls
- Methodology and approach for evaluating controls is the same for all types of controls.
- Develop an understand of what the control operator (i.e., the "reviewer") does

Developing an Understanding of Operator

We need to develop an understand of what the control operator (i.e., the "reviewer") does and how the reviewer executes the control in order to assess the level of precision and effectiveness of design:

- First and foremost, we understand the intended purpose of the control – without this understanding we cannot effectively evaluate the design of the control.
- Level of aggregation
- Consistency of performance
- Criteria for investigation
- Predictability of expectations

Test of Design vs. Test of Operating Effectiveness

Test of Design vs. Test of Operating Effectiveness

Test of Design

- Includes understanding the likely sources of potential misstatement and identifying controls to test
- Understand transaction flow initiated, processed and recorded
- Verify that points at which a material misstatement could arise have been identified
- Walkthroughs usually consist of a combination of inquiry of appropriate personnel, observation of the company's operations, and inspection of relevant documentation.

Test of Operating Effectiveness

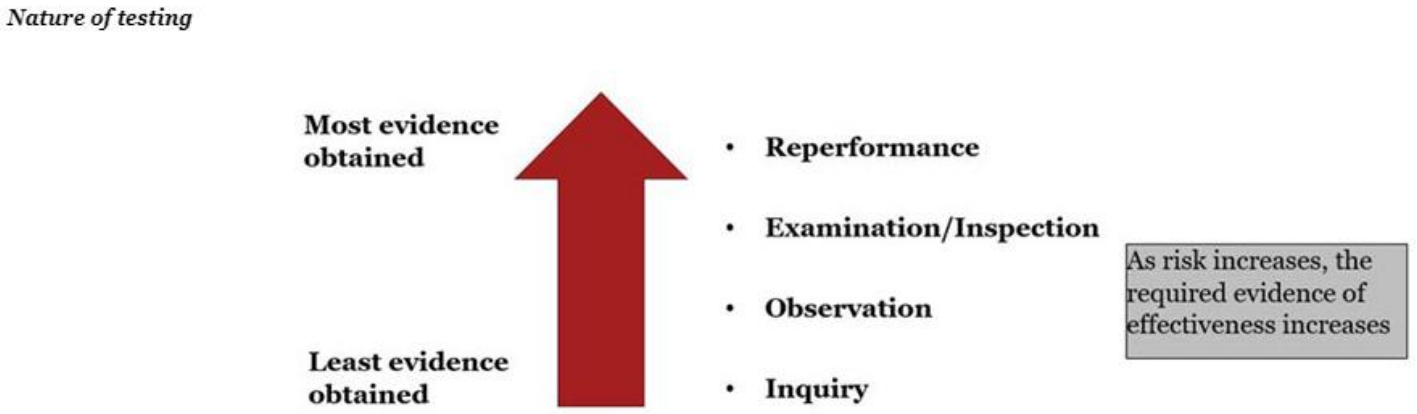
- Includes testing key controls to assess whether they are operating as designed to prevent or detect a material misstatement

Nature of Testing

There are four techniques used in testing selected manual controls, each providing a different level of evidence:

- Inquiry
- Observation
- Examination/Inspection
- Reperformance

Persuasiveness of the evidence is impacted by the type of procedure used.



Nature of Testing

Inquiry

- Provides some relevant information, especially when we apply professional skepticism in discussions
  - Can obtain further support by corroborating inquiry with others in the entity
- Inquiry alone will not provide sufficient evidence to support a conclusion about the implementation or operating effectiveness of a control

Observation

- Provides an appropriate way to obtain evidence if there is no documentation of the operation of a control (i.e. segregation of duties)
- Observation can also be useful in review controls where management conducts meetings to review certain information and take necessary action as part of the review.

Nature of Testing

Inspection/Examination

- Provides evidence used to determine whether manual controls are being performed
  - Evidence of the performance can include written explanations, check marks, or other indications of follow-up documented
  - Absence of evidence may indicate that the control is not operating as prescribed.
- Note, it is important to recognize that a signature does not necessarily mean that the person carefully reviewed before signing.
  - In this case, reperformance of the control may provide more persuasive evidence.

Reperformance

- Provides more persuasive evidence than the other techniques
  - Used when a combination of inquiry, observation, and inspection do not provide sufficient audit evidence.
- Reperformance provides the most persuasive evidence but may not be needed for all controls selected for testing.
  - Some controls do not lend themselves to reperformance (i.e. complex estimates, future cash flows, etc.)

Control Examples

Direct ELC:

Business performance reviews (BPRs), including group and operating units' analyses of actual financial performance versus budget or prior period(s)

Example of testing / support:

Inspect BPR Review, including support for any fluctuations over the determined threshold that were analyzed by Management; Inspect evidence of review by Senior Management

Indirect ELC:

A company requires all employees to sign a code of conduct once a year

Example of testing / support:

Inspect report to evidence certification for year; Inspect report to verify that Code of Conduct certification was accomplished for the set percentage established by management.

Control Examples

Transaction Level Control:

Reconciliation of third-party investment reports to accounting records

Example of testing / support:

Inquire of control operator; Inspection of reconciliation and follow-ups for any variances that exceed any established threshold, supplemented with some level of reperformance of the reconciliation.

Management Review Control:

Reserve committee review of actuarial estimates

Example of testing / support:

Inquire of control operator; Inspection of relevant materials presented, including any follow-ups that come out of the review and other relevant documents (e.g., meeting minutes, actions established from review); Inspect resolution of any actions arising from the review and support to evidence that those actions were taken; Supplement inspection with observation of the meeting.

Completeness and Accuracy of Source Data

Completeness / Accuracy of Source Data

When using information produced by the company, the auditor should evaluate whether the information is sufficient and appropriate by performing procedures to:

- Test the accuracy and completeness of the information, or test the controls over the accuracy and completeness of that information
- Evaluate whether the information is sufficiently precise and detailed for the purpose of the audit

Completeness - All transactions and accounted that should be presented in the financial statements are so included

Accuracy - The assertion is that all information disclosed is in the correct amounts, and which reflect their proper values.

Ensuring completeness entails gaining comfort that a full population of the relevant transactions are captured and presented in the support.

Ensuring each report is accurate involves validating that the integrity of data compiled by the report is maintained throughout the report creation process.

Sufficiency of Evidence

Sufficiency of Evidence

- The auditor should test the operating effectiveness of a control selected for testing by determining whether the control is operating as designed and whether the person performing the control possesses the necessary authority and competence to perform the control effectively.
- The evidence provided by the auditor's tests of the effectiveness of controls depends upon the mix of the nature, timing, and extent of the auditor's procedures. Further, for an individual control, different combinations of the nature, timing, and extent of testing might provide sufficient evidence in relation to the degree of reliance in an audit of financial statements.
- For each control selected for testing, the evidence necessary to persuade the auditor that the control is effective depends upon the risk associated with the control. The risk associated with a control consists of the risk that the control might not be effective and, if not effective, the risk that a material weakness would result. As the risk associated with the control being tested increases, the evidence that the auditor should obtain also increases.
- n order to test the operating effectiveness of a control, we need persuasive evidence that it operates effectively as designed (i.e., we need evidence that the control operator performed the control exactly how it is designed to meet the intended control objective). A sign-off or other indicator of operation does not provide persuasive evidence.
- We generally obtain more persuasive evidence if the control we plan to test:
  - relates to a significant risk or
  - Is particularly important to the sub-process or FSLI or is the primary or only test to assess the effectiveness of the control for a particular assertion

Sufficiency of Evidence

When determining the persuasiveness of the evidence needed to support the conclusion that a control operates effectively, we may consider the following factors (note the following list is not intended to be all-inclusive nor is every factor expected to be addressed):

Factor	Impact on persuasiveness of evidence needed
The inherent risk associated with the related account(s) and assertion(s)	The higher the inherent risk, the more persuasive the evidence needed
The level of reliance placed on the control	The higher the level of reliance, the more persuasive the evidence needed
The nature and materiality of misstatements that the control is intended to prevent or detect	The more material a potential misstatement associated with the operation of the control, the more persuasive the audit evidence needed
Whether the account to which the control relates has a history of errors	The more significant the history of errors, the more persuasive the audit evidence needed
Whether there have been changes in the volume or nature of transactions that might affect control design or operating effectiveness	The more significant the change in the volume or nature of transactions, the more persuasive the audit evidence needed
The nature of the control and the frequency with which it operates	The more routinely and frequently a control operates, the less persuasive the evidence needed
The degree to which the control relies on the effectiveness of other controls (e.g., the control environment or information technology general controls)	The more effective the other controls, the less persuasive the audit evidence that may be needed
The complexity of the control and the significance of the judgments that need to be made in connection with its operation	The less complex the control and the less significant the amount of judgment made in connection with its operation, the less persuasive the evidence needed

Roll-forward Procedures

Roll-forward Procedures

The purpose of Roll-forward procedures is to obtain coverage through 12/31

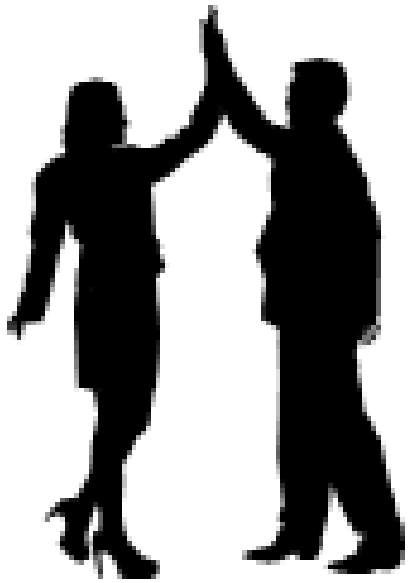
When performing roll-forward procedures, the procedures performed should be directly correlated with the risk associated with the control.

Example roll-forward procedures based on relevant risk:

Risk	Procedures
Low	Inquiry
Medium	Inquiry & Inspection
High	Inquiry / Observation / Inspection / Reperformance

Day 2 Overview

- Overview of Key IT Areas
- Key Reports / Assessing Reliability of System Generated Information
- IT Baseline vs Benchmark testing
- Use of Service Organizations' SOC 1 Reports
- Control Deficiency Evaluation
- SAB 99
- Elements of an Action Plan
- Remediation Testing
- Wrap Up



Overview of Key IT Areas

Overview of Key IT Areas

The decision as to whether a control is key depends on which controls, individually or in combination, sufficiently address the assessed risk of misstatement to a given relevant assertion.

- **In scope systems support the business process controls either directly (OneClaim aggregate limits automated control, or CDW Key Reports) or indirectly (GitHub Release Management Tool used in the ITGC change management process)**

- **Key Reports are reports / system-generated information used in the performance of a key control, whereas populations might not be used in the performance of a key control but we are required to gain comfort over their completeness and accuracy, similar to a key report.**

- **For each key business process, the completeness and accuracy of interfaces from one system to another, key reports used in the performance of a key control, and configurations within a system might be used to reduce the risk of material misstatement.**

Key reports/Assessing Reliability of System Generated Information

Reliability of System Generated Information

When evaluating effectiveness of a control (whether the key report is used in the performance of a key control, or whether a population is used for substantive testing) , we assess the reliability of information used by management in the execution. Factors we consider include:

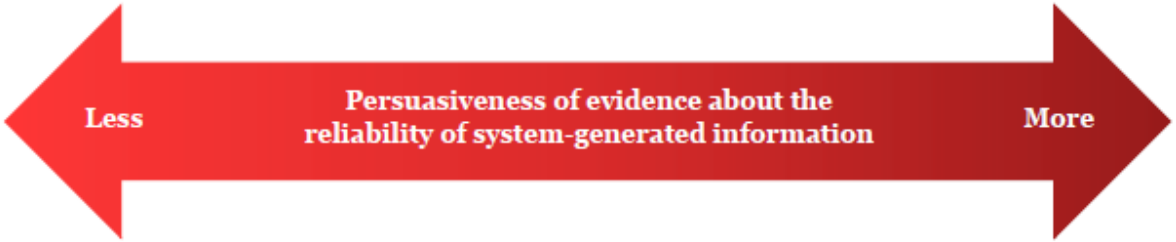
- The level of assurance we are seeking from the control
- The risk of material misstatement associated with the control's failure
- The degree to which the effectiveness of the control depends on the completeness and accuracy of the information
- The nature, source, and complexity of the information, including the degree to which the reliability of the information depends on other controls (i.e. manual or automated applications controls and/or ITGCs)
- Prior experience relevant to the assessment (i.e. prior year deficiencies, changes in the control environment, or other assessed risks)

Key reports/Assessing Reliability of System Generated Information

PwC Audit 4512.01

System-generated reports or data ("key reports") are information generated by IT systems, used in and important to the effective execution of relevant controls or used in our substantive procedures. When key reports are used in and important to the effective execution of a relevant control or used in our substantive procedures, PCAOB standards require that we assess the reliability of such information.

Factors to consider when assessing the reliability of system-generated information



Less persuasive evidence	Factors	*More persuasive evidence*
▪ *Non-complex system*	Complexity of system	▪ *Complex system*
▪ *Standard report*	Report type	▪ *Ad-hoc query*
▪ *Seeking lower level of assurance from testing*	How the report is used in the audit	▪ *Seeking higher level of assurance from testing*

Key reports/Assessing Reliability of System Generated Information

Report types

Report type	Definition
▪ **Standard report ("canned")**	▪ A report designed by the software developer and has not been modified or customized by the entity. Standard reports are reports that come preconfigured and/or predefined in well-established software packages used by clients. For example large ERPs, such as SAP and JD Edwards provide standard A/R aging reports irrespective of the type of entity. It is important to work with Process Assurance professionals to understand if a report is a standard report.
▪ **Customized report**	▪ A modified standard report or a report developed to meet the specific needs of the end-user. Custom reports allow an entity to determine the information included in the report and how it is formatted. For example, management may modify a standard A/R aging report to show aging by customer instead of invoice which would then become a custom report. Reports generated from a client-developed ("in-house") system are considered custom reports, generated by a complex system.
▪ **Query**	▪ A report generated ad hoc or on a recurring basis that allows users to define a set of criteria to generate specific results. Queries are common when information is needed for a user defined item, transaction, or group of items or transactions. For example, a query could be used to generate a list of all journal entries for a defined business unit. Query languages (e.g., SQL, SAS, etc.) may be used by IT or sophisticated end-users to design these reports. Recurring queries subject to ITGCs may have similar characteristics to a custom report. Such characteristics may include that the query cannot be modified other than by authorized individuals once it is developed, tested, and placed into production. Ad hoc queries are typically performed for a specific use and likely are not subject to ITGCs. System-generated information used in substantive testing (e.g., populations used for making selections for substantive tests of details, or data for use in a disaggregated analytical procedure) may often be the result of ad hoc queries.

Key reports/Assessing Reliability of System Generated Information

Accuracy & completeness of key reports

Report type	Management's control(s) (important to support our ICFR opinion)	Engagement team's procedures
Standard report ("canned")	▪ Testing over the system implementation and/or change management. ▪ Changes subject to the entity's ongoing change management controls and effective ITGCs. ▪ If input parameters are used, verification of the input parameters used to generate the report each time the report is used.	▪ Validating a report is a standard report, including verification there were no changes to the report since system implementation. ▪ Testing ITGCs to support the report continues to function as intended. ▪ If input parameters are used, verify the input parameters each time the report is used to support our testing.
Customized report or query (subject to ITGCs)	▪ Initial user acceptance testing. ▪ Changes subject to the entity's ongoing change management controls and effective ITGCs. ▪ If input parameters are used, verification of the input parameters used to generate the report each time the report is used.	▪ Testing the accuracy and completeness of the report. ▪ Testing ITGCs to support the continued reliability of the report. ▪ If input parameters are used, verify the input parameters each time the report is used to support our testing.
Customized report or query (not subject to ITGCs)	▪ Specific procedures to address the accuracy and completeness of the customized report/query each time it is extracted from the system and used in the execution of a control including, but not limited to verification of the parameters used to run the customized report/query.	▪ Testing the accuracy and completeness of the report each time it is used to support our testing including but not limited to verification of the input parameters used to run the report (controls or substantive).

Note: This table is not intended to address whether the source data in the system is accurate, complete and valid.

In an ICFR audit, our substantive procedures, if applicable, over the accuracy and completeness of system-generated information do not substitute for testing management's control(s) over the reliability of the information

IT Baseline vs. Benchmark Testing

IT Baseline vs. Benchmark Testing

Baseline Approach

- Obtain evidence directly from the system to validate that the system performs the control as designed.
- Evaluate changes to the core functionality of the automated control or key report during the period.
- ITGCs are in place and are effective.

Benchmark Approach

- An alternate test approach where reliance can be placed on prior period testing, when **all** of the following are true:
  - Automated control or key report functions as intended (it was tested in the past)
  - Generally, “past” = within the past 3 years
  - ITGCs are in place and are effective
  - No changes have been made to the core functionality of the automated control or key report since it was last tested

Use of Service Organizations' SOC 1 Reports

Identification of a Relevant Service Organization

Understanding of the business process and related transaction flows	***Understanding the User Entities use of the Service Organization***
What is the information being processed and key reports generated? *Who performs the processing and is it outsourced?* *How is the information processing controlled?* *Who performs the controls?* *What are the likely sources of potential misstatement?* *Are the outsourced activities, processes, and functions critical to financial statement reporting?*	*Does the user entity have a contractual arrangement to receive a SOC 1 report?* *Are the relevant services covered by the SOC 1 report?* *What are the user entity's controls (including CUEC's) over their relationship with the Service Organization?*

Identification of a Relevant Service Organization (signed contract exists)

Note 1:

A SOC 1 report may carve out certain services that are performed by Sub- service Organizations. The user entity has the ability to request these SOC 1's from the Sub- service Organizations under the signed contract with the original Service Organization.

- CSOCS – are Complementary Subservice Organization Controls

Note 2:

Considerations regarding the use of Sub-service Organizations and the corresponding approach should be evaluated and documented.

The contract states that the user entity has the ability to request that the Service Organization provide them a SOC 1 report, covering the outsourced services, which are ***relevant*** and are ***financially significant***. Once obtained, the user entity may then share the SOC 1 report with their Independent Auditor.

Identification of a Relevant Service Organization (signed contract does not exist)

If you believe that your user entity uses a SOC 1 report without a contractual arrangement with the Service Organization, this should be evaluated. Refer to AICPA SOC 1 Guide "Downstream User Entities."

Identification of a Relevant Service Organization – Client Management Responsibilities

User entities should:

- Understand whether they are recipients of a SOC 1 report (and not that the parent company or an affiliate is the issuer and/or a recipient).
- Have a mechanism for monitoring and conduct oversight of activities at the Service Organization as part of their system of internal controls.
- *Evaluate and map Complementary user entity controls (CEUC's) and CSOCS.*

Supervision of a service provider

Various ways to monitor the effectiveness of the processes outsourced to a service provider:

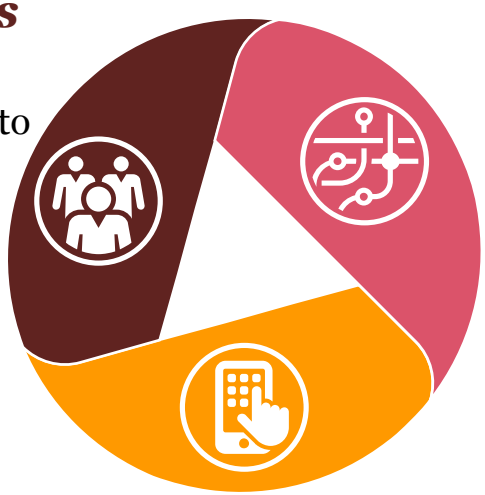
1. **Direct monitoring of service provider**
    - *Review meetings with service provider management*
    - *Not independent*
1. **Service Level Agreements / Service Level Reports**
    - *Performance based (≠ control effectiveness)*
    - *Not independent*
1. **Obtaining, assessing and following up on SOC reports**
    - *Globally accepted frameworks*
    - *Controls based*
    - *Independent*

SOC Reports

What is the subject matter of the engagement?

SOC 1® Reports

Controls at a service organization relevant to user entities' internal control over financial reporting



SOC 3® Reports

Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy

SOC 2® Reports

Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy

Key Questions to Consider

What is the purpose of the report?

SOC 1 Reports	SOC 2 Reports	SOC 3 Reports
To provide the user auditor of the entity's financial statements with a report and a Service Auditor's opinion about controls at a service organization that may be relevant to a user entity's internal control over financial reporting.	To provide management of the service organization, user entities, and other specified parties with a report and a Service Auditor's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy.	To provide interested parties with a CPA's opinion about controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.
Enables the user auditor to perform a risk assessment and, in the case of at type 2 report, use the report as evidence the controls operated effectively.	The report does not cover controls relevant to user entities internal control over financial reporting.	SOC 3 reports serve a similar purpose as the SOC 2 report however are less in detail and can be made available to the public.
	Report may be used for the following purposes: •Oversight of the service organization (e.g. vendor management program). •Internal corporate governance, risk management and compliance processes. •Regulatory oversight. •The overlap with other internal controls reporting (e.g. SOC 1) and overlap with existing assurance functions (e.g. internal audit, risk, compliance, etc.) to understand the cost and opportunities for leverage.	

Assessment of a SOC 1 Report – Report Structure

User Entity Responsibilities

Description of Covered & Excluded/Carved-Out Services

- Evaluate the qualifications of the SOC 1 report auditor - professional reputation, competency, and independence.
- Review sections to understand the context for the controls tested in Section 4 in order to plan the reliance strategy.

Evidence of Controls

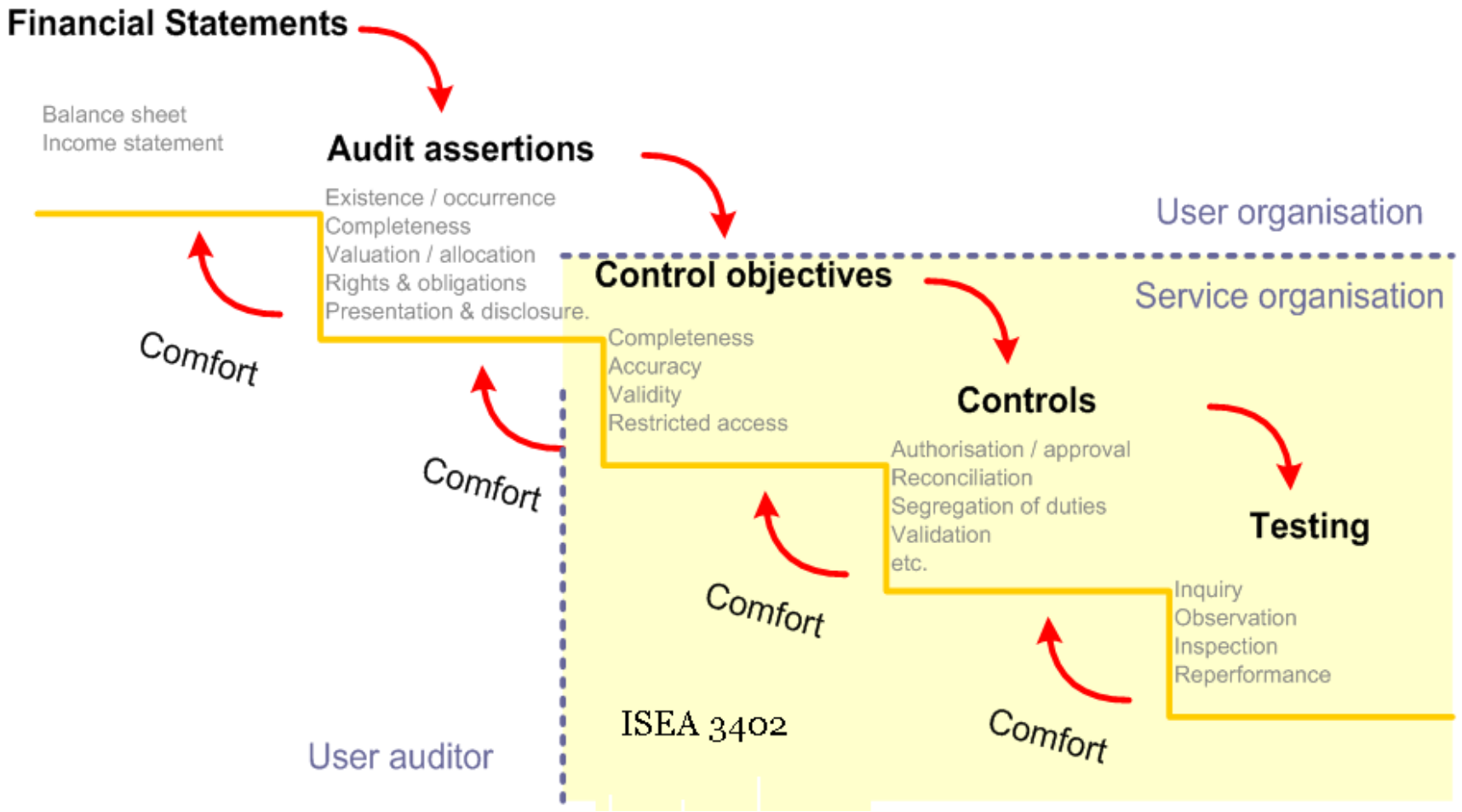
- Evaluate exclusion of relevant Sub-service Organizations.
- Timing and Scope Alignment to user ICFR
- Assess whether the N/T/E of test procedures is sufficient (including that key reports are named and tested and that all relevant assertions and attributes are tested).
- Assess control exceptions/opinion/ assertion.
- Assess the relevance of CUEC's.
- Assess CSOCS

Additional Information

These sections are optional and are **unaudited**

- Service Organization discloses additional information to its customers (e.g., business continuity).
- Independent Service Auditor provides clarification/ context to the procedures they performed in Section 4.
- Because unaudited – no reliance can be placed on these sections. Informational only.

SOC 1 - Relating Financial Statements to controls

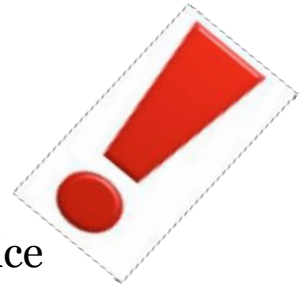


Assessment of a SOC 1 Report

If SOC 1 report test procedures are not deemed sufficient:

- Ask probing questions and re-assess understanding of the user entity control environment/monitoring.
- Determine if other audit evidence to test the information produced by the Service Organization (e.g., tie the Service Organization's system information to an independent source).
- Request additional procedures by the Service Auditor. ie (AUP)
- Discuss with the Service Organization/Service Auditor to modify the scope and/or the N/T/E of the SOC 1 report.
- Perform supplemental testing.

Recap



- SOC 1 report scope may not align to the relevant dependencies on the Service Organization:
  - All key reports or other information used in company processes may not be covered by the scope of a SOC 1 report.
  - Additional audit/ SOX procedures may be required.
- Document your planned approach to capture:
  - An understanding of the transactions flow between the Service Organization and the company, including the *relevant services* performed and the *key information/reports* produced by the Service Organization and if it is in scope of SOC report.
- Document your response, if the evidence of testing is not sufficient or there are exceptions qualifications noted in the SOC 1 report.

Common Pitfalls

Auditors did not:

- Evaluate whether the scope of the SOC 1 report included design and operating effectiveness testing of controls over the information used by the auditor as audit evidence.
- Obtain evidence regarding the effectiveness of necessary controls at Sub- service Organizations.
- Test the operating effectiveness of necessary complementary user entity controls ("CUEC's") at the Client as specified in the SOC 1 report.
- Obtain and evaluate the SOC 1 report or perform their own procedures related to the accuracy and completeness of statements or other information produced by the Service Organization that the auditors used in their audits.
- Evaluate the period covered by a SOC 1 report and time elapsed since the performance of the SOC 1 report testing.

Evaluating Control Deficiencies

Identifying Control Deficiencies

Deficiencies in internal control over financial reporting can be identified through various sources during an audit. These situations include situations when management informs us about misstatements or break-downs in controls and when we obtain an understanding of the entity's internal control, evaluate the design and implementation of controls relevant to the audit, perform walkthroughs or other procedures, or test the operating effectiveness of key controls.

Deficiencies may relate to the design or operation of entity level controls, review controls, transaction level controls, and ITGCs. Deficiencies may also relate to omitted, incomplete, or inaccurate financial statement disclosure exceptions.

Considering Root Cause

- An error is not a root cause, it is a consequence
- A root cause can be:
  - A failure of a control to operate as designed (operating deficiency)
  - A failure to have a control, or a well-designed control (design deficiency)
- The root cause will identify what transactions, accounts and/or disclosures and related assertions are exposed to the deficiency so that we can evaluate the likelihood and potential magnitude of the deficiency

Considering Root Cause

When identifying the root cause, we need to ask ourselves:

- What went wrong?
- How did this happen?
- Is there a control designed to prevent or detect a material misstatement?
- To identify the deficiency, we need to understand why the error occurred, not just what occurred. "What" occurred is the result of the deficiency. Answering "why" it occurred can lead to understanding what the deficiency is.
- Repeatedly ask the question "why" to peel away the layers until you reach the root cause

Magnitude considerations (i.e., "could factor")

Is the magnitude of the potential misstatement, which is at least reasonably possible (considering quantitative and qualitative factors), material to either interim or annual financial statements? (AS 2201.66-.67)

- Magnitude is about what "could" go wrong.
- Magnitude is assessed absent compensating controls, if any.
- Factors that affect the potential magnitude include, but are not limited to the following:
  - The financial statement amounts or total of transactions exposed to the deficiency; and
  - The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods

Magnitude considerations (i.e., "could factor")

- The maximum amount that an account balance or total of transactions can be overstated is generally the recorded amount, while understatements could be larger
- Consideration should be given to any known audit adjustments recorded by management or any amounts posted to the SUM (i.e., actual misstatement) as well as to potential misstatements.
- ***The "could factor" is usually not limited to the amount of the error.***

Magnitude considerations (i.e., "could factor")

- In situations where actual errors have occurred and the client has "scrubbed" the accounts to make sure there is not further misstatement, the "gut" reaction may be that the potential magnitude is limited to the actual error. However, this is often not the case.
- A thorough evaluation of what transactions were exposed to the deficiency not just those transactions that had an error, needs to occur to conclude on the potential magnitude.
  - The "scrub" performed is management's substantive response to conclude whether there are additional errors that need to be corrected in the financial statements.
  - The "scrub" performed after the error is identified is not a control.

Magnitude considerations (i.e., "could factor")

- Qualitative factors should be considered and documented in the evaluation of the magnitude of the internal control deficiency. The potential magnitude is directly related to the root cause and an understanding of what could possibly go wrong given the situation.
- We need evidence to support the potential magnitude and how this links to the root cause.
- Examples of qualitative factors include:
  - The existence of multiple deficiencies related to a specific account or disclosure
  - The potential magnitude of deficiencies in control activities related to the same significant account or disclosure
  - The potential impact of the same deficiency in multiple aggregation categories

Quantifying IT Issues

IT issues are quantified in various ways, and a number of factors are considered in determining the magnitude of an IT issue including:

- the severity of the deficiency and the "could factor"
- the financial statement amounts or total of transactions exposed to the deficiency; and
- the volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods.

Note: The evaluation of whether a control deficiency presents a reasonable possibility of misstatement can be made without quantifying the probability of occurrence as a specific percentage or range.

Net Exposure Analysis

Do compensating controls exist and operate effectively at a level of precision sufficient to prevent or detect a misstatement that could be material to either interim or annual financial statements?

- Compensating controls should be designed and performed with the appropriate level of rigor and precision to address the same likely source of potential misstatement as the deficiency control(s) and prevent/detect a material misstatement.
- The testing of the operating effectiveness of this control should provide evidence as to the level of rigor and precision in which this control operates.
- Document a description of any compensating controls we intend to rely on to reduce the severity of the deficiency. Consider whether the compensating control identified the misstatement in question or whether or not it should have.
    - ***It is critical that when we are evaluating the compensating controls, we need to obtain evidence that the controls are not only designed effectively to compensate, but also are operating effectively.***
    - If the error is greater than the precision of the compensating control then most likely the compensating control is not precise enough to detect misstatements resulting from the control deficiency.

Determining the Severity of a Deficiency

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.
- A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

A ***significant deficiency*** is a deficiency, or a combination of deficiencies, in internal control over financial reporting, that is less severe than a material weakness yet important enough to merit attention by those responsible for oversight of the company's financial reporting.

A ***material weakness*** is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

There is a reasonable possibility of an event when the likelihood of the event is either "reasonably possible" or "probable."

Determining the Severity of a Deficiency

Risk factors affect whether there is a reasonable possibility that a deficiency, or a combination of deficiencies, will result in a misstatement of an account balance or disclosure. The factors include, but are not limited to, the following:

- The nature of the financial statement accounts, disclosures, and assertions involved;
- The susceptibility of the related asset or liability to loss or fraud;
- The subjectivity, complexity, or extent of judgment required to determine the amount involved;
- The interaction or relationship of the control with other controls, including whether they are interdependent or redundant;
- The interaction of the deficiencies; and
- The possible future consequences of the deficiency.

Multiple control deficiencies that affect the same financial statement account balance or disclosure increase the likelihood of misstatement and may, in combination, constitute a material weakness, even though such deficiencies may individually be less severe. Therefore, the auditor should determine whether individual control deficiencies that affect the same significant account or disclosure, relevant assertion, or component of internal control collectively result in a material weakness.

Determining the Severity of a Deficiency

The severity of a deficiency depends on

- Whether there is a reasonable possibility that the company's controls will fail to prevent or detect a misstatement of an account balance or disclosure; and
- The magnitude of the potential misstatement resulting from the deficiency or deficiencies.

The severity of a deficiency does not depend on whether a misstatement actually has occurred but rather on whether there is a reasonable possibility that the company's controls will fail to prevent or detect a misstatement.

Just because a control deficiency doesn't result in a material error today doesn't mean that it could not be a material weakness.

SAB 99

SAB 99 Defined

Management is responsible for performing an analysis to evaluate the materiality of misstatements identified by management or the auditor pursuant to the requirements of SEC Staff Accounting Bulletin No. 99 ("SAB 99"), Materiality, SAB 108, Considering the Effects of Prior Year Misstatements when Quantifying Misstatements in Current Year Financial Statements, and ASC 250, Accounting changes and error corrections. Management documents their analysis and conclusion in a client SAB 99 memo.

Misstatements are evaluated for their impact on the assessment of internal control.

SEC Staff Accounting Bulletin: No. 99 - Materiality:

- This staff accounting bulletin expresses the views of the staff that exclusive reliance on certain quantitative benchmarks to assess materiality in preparing financial statements and performing audits of those financial statements is inappropriate; misstatements are not immaterial simply because they fall beneath a numerical threshold.

Remediation Testing

Remediation Testing

When a control is not designed or operating effectively to prevent or detect a material misstatement in the financial statements, management may remediate a deficiency in a selected control either by changing its design or implementing new control(s), or both, during the audit period.

When controls are remediated during the year, we rely on those controls only for the period in which the controls have been remediated and are operating effectively in determining the nature, timing, and extent of our substantive audit procedures.

Our approach for testing a remediated control is consistent with testing any control and is based on specific facts and circumstances.

Questions?