

Understanding SAS 94

The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit

*Joint Meeting ISACA and IIA
NY Metropolitan Chapters
April 19, 2002*

**Bruce H. Nearon, CPA
J.H. Cohn LLP**

**Joel Lanz
Joel Lanz, CPA, P.C.**

Presentation Overview

- What's SAS 94?
- How Much Effort?
- Which IT Risks Need to be Considered?
- What Are The Relevant Planning Issues?
- Why?
- Strategies
- Questions

What's SAS 94?

- Au Section 319 (SAS 94)
 - The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit
- What is the effective date of SAS 94?
 - Audits of financial statements for periods beginning on or after June 1, 2001
- Need to implement to comply with second standard of fieldwork

What's SAS 94? (cont.)

- Helps auditors cope with the issues surrounding the explosive growth of IT
- Amends SAS 55 and 78 on providing guidance on considering the effect on internal control
- Acknowledges that IT impacts internal control
- IT can be so significant that quality of audit evidence depends on IT controls
- IT has a major influence on the process use to prepare financial statements

How Much Effort?

- Size of the organization
 - Assets? Sales?
- Number of transactions
 - 1000's, 10,000's, 100,000's, millions
- Complexity and sophistication of the IT environment
- Reliance of audit strategy on internal controls

How Much Effort? (cont.)

- Taking the easy way out
 - Assessing Control Risk at the Max
- **WARNING!** Practitioner needs to be satisfied that performing only substantive tests will be effective
- But - if initiation, recording, and processing of financial data exists only in computers then the **effectiveness** of substantive tests is significantly reduced.

Which IT Risks Need to be Considered?

Au 319.19

- Unauthorized access to menus, programs, and data
 - destruction or improper changes
 - unauthorized, nonexistent or inaccurate transactions.
 - errors and fraud.
- Failure to make necessary changes to systems or programs i.e. obsolete programs and patch levels

Which IT Risks Need to be Considered? (cont.)

Au 319.20

- A lack of control at a single user entry point might compromise the security of the entire database.
 - Improper changes
 - Destruction of data
- When IT personnel and users are given, or can gain access privileges beyond necessary to perform their assigned duties, a breakdown in segregation of duties can occur

Which IT Risks Need to be Considered? (cont.)

Au 319.21

- Errors may occur in designing, maintaining, or monitoring IT controls
- IT personnel may not completely understand how the system processes transactions

AU 319.22

- Edit routines in programs designed to identify and report transactions that exceed certain limits may be overridden or disabled

What Are The Relevant Planning Issues? (cont).

Au 319.30

- What IT risks can result in misstatements?
- The more complex and sophisticated the entity's operations and systems the more likely the need to increase the auditor's understanding of internal control

Au 319.31

- Do you need an IT Audit specialist?

What Are The Relevant Planning Issues? (cont).

Au 319.49

The auditor should understand

- Critical procedures to record, process, and report transactions from occurrence to inclusion in the financial statements.
- Related records - electronic or manual - used to initiate/record transactions
- Capturing of events and conditions significant to the financial statements by IT

What Are The Relevant Planning Issues? (cont).

Au 319.51

- Understand how nonstandard, nonrecurring, or unusual transactions are authorized, documented, and posted to the system
- Such entries may exist only in electronic form and may be more difficult to identify through physical inspection of printed documents

Why?

- Much of the information used in auditing may be produced by IT
- This information may be unintentionally or intentionally incomplete and erroneous
- System monitoring logs may not be retained, may have gaps in them, or be subject to alteration.
- Management and auditors may rely on this information and develop a false sense of confidence.

Strategies

- Assessing control risk at the maximum so that only substantive tests are performed
 - Confirm bank balances
 - Confirm a/r
 - Observe inventory
- Substantive tests are typically performed based on information produced by the entity's IT system (Catch-22)
 - What evidence do you have that information from the IT system is accurate, valid, and complete?

Strategies (cont.)

Au 319.68

- Is there a significant amount of information supporting the financial statements electronically:
 - Initiated and recorded?
 - Processed and reported ?
- What evidence do you have that controls over IT are effective?
 - Your audit evidence derived solely from substantive tests may not be competent and sufficient

Strategies (cont.)

Au 319.71

Assessing control risk below the maximum

- Identify the types of misstatements that can occur
- Consider factors that affect the risk of material misstatement
- Identify controls that are likely to prevent or detect material misstatement in specific assertions

Strategies (cont.)

- Warning for those that assess risk at the maximum (e.g., don't consider IT risks and controls)
 - Audit samples, records, and reports that originate from a control environment that allows undocumented, unauthorized, and unmonitored changes may not be competent and sufficient.

Strategies (cont.)

- The “Integrated Audit” Team
 - Coordination
 - Leveraging skills
 - Ask the next question
 - IT audit is more than security review
 - Use of specialists
 - Master the fundamentals

Questions

**Bruce H. Nearon, CPA
J.H. Cohn LLP
75 Eisenhower Parkway
Roseland, NJ 07068
(973) 403-6955**

**bnearon@jhcohn.com
www.jhcohn.com**

**Joel Lanz, CPA, CISA, CISSP
Joel Lanz, CPA, P.C.
P.O. Box 597
Jericho, NY 11753-0597
(516) 637-7288
jlanz@itriskmgt.com
www.itriskmgt.com**